RESEARCH ARTICLE

CYBER SECURITY

Aimma Butt

INTRODUCTION

Today man is capable to send and receive any form of data may be by an e-mail audio or video just by the click of a button but how data is transferred to another person without leakage of information?? The answer is in cyber security. Today Internet is flourishing its infrastructure in everyday life. But due to these evolving technologies we are unable to safeguard our private information in a very effective way and therefore cybercrimes are increasing day by day.

Cybersecurity is a very broad term also known as Information Technology (IT) security, it is actually the set of technologies, processes which are made to protect networks, internet, social sites, private data, accounts from hacking attacks, or damage by a hacker or other unauthorized access. This concept is further based on 3 fundamental concepts called as "The CIA Trait". CIA stands for Confidentially, Integrity and Availability. It is the practice to ensure the integrity, confidentially and availability of information or data. Cyber security thus includes controlling physical access to the hardware and protect against destruction that may come via network access and due to malpractice by operators.

In this time period, more than 60 percent of the people preferred their financial transactions to be done online, so this field required a high quality of security for best transactions. Hence cyber security has become a most recent issue.

The opportunity of cyber security is not just restricted to securing the information in IT industry but also to several other fields.

Even the latest tools like cloud computing, mobile computing, E-commerce, net banking etc. also claim a high level of safety. Since these technologies hold some important information concerning a person their security has become a requirement. Enhancing cyber security and protecting critical information infrastructures are essential to each state's security and economic safety. Making the Internet safer or protecting Internet users has become primary to the development of new services and governmental policy. The fight against cybercrime needs a complete and a safer methodology. Currently other nations and administrators are imposing strict laws on cyber securities in order to prevent the loss of data and information. Every individual must also be educated on this cyber security so that they can save themselves from these increasing cybercrimes.

LITERATURE SURVEY

Today's world totally depends upon the technologies, networks and internet. As a result digital data has increased. All the companies store their personal data on computer systems even government store their secret data and public data on computers and even share it on other networks. Banks store accounts data on computers. So, with all this it is compulsory to protect employee's data or other important information from third party. To ensure their privacy, cyber security is very important. Even at low level the social media profiles must be secured to protect user's data and records. Accordingly cyber security plays an important role in the field of information technology.

Areas of Concern

Computer Security is concerned with four main areas:

1. Confidentiality that only authorized users can access the data resources and information.
2. Integrity that only authorized users should be able to modify the data when needed.
3. Availability means data should be available to users when needed.
4. Authentication is that you really communicating with whom you think you are communicating with.

PRINCIPLES OF CYBER SECURITY

Cyber security is used for the business security and to secure them to escape the incidents in cyber space. It has 10 rules which were guided by the real production of NCSC (National Cyber Security Center) therefore one who wants to use this security has to follow these 10 steps.

1. Risk Management Regime:

The risk management regime is a rule which concluded many policies and practices which was guide and applied for the workers and assure them that everyone knows to this step. And also they are able to decide for the risky activities. This management is also helped to the government features to make them high and also established a board of members and the seniors who are able to selected area.

2. Secure configuration:

Selected policies and that would organize security permit a safe line and a process that progressed for ensuring configuration management one can also be able to remove useless functions from the system which was harmful for the security. All software and systems should be fixed which was used to guide the security. The wrong use of the system would be falling to any risk for the companies and the system.

3. Network Security:

Network security was used for the connection to unsaved network for example HTTP. On the internet we faced a risk to overcome the system to be attacked influenced by the opposition. Therefore we must be applied policies and suitable buildings and technically responded and also be established which would help for the base line for network. It would be sure that bounded and unbounded network steps should be securing your network. By applying these policies any organization can minimize the chance to become a victim of cyber-attack. Moreover SIM problems should be more applied SOC institutions should be selected for the technology to make them affected to your network.

4. Managing user privileges:

Anyone who use these steps should be provided them suitable access privileges that would be permission them to become sincere to their work. If the users are guided to more development then they deserved it also a big issue that it can be misuse and become a big risk for the information security therefore it would be granted that highly privilege should be carefully control and managed.

5. User Education and Awareness:

The user organization and awareness people played an important role to make organized and safe secure. If the users do not know the policies risk management would be set and selected by the organization. These policies will also be filled in their purpose those users must be guided to the awareness of the security and trained them regularly, also be assured that the users are also aware of this policy and the misdeeds which guided to the security breaches. More over cyber security organized by professionally and highly trained in any time of need that would be happened.

6. Incident Management:

A SIEM solution will always be ready to provide security connected to the incident. This organization should be established effected incident management policies to be sported a business and make sure the security throughout the organization and all points as well all points in active

7. Malware Prevention:

Malware Prevention is required that the selected policies that directly connected to the business process and also be in front of effected by malware like email, web, private devices, USB. This policy also be established which would be bounded USB to the computer likely other policies maybe stricted to the internet request. This is a dependent on the condition and their needs. Separate expertise solutions should be selected to save malware like email threats and the safety for emails. The last point should be effected and secure to the antivirus problem that secure them and remediate malware from the final points

8. Monitoring:

A monitoring category should be producer for the help of organization which would totally selected for the security posture. It also is used to provide another source of security when the security is through for the safety of system. The last point solution would be able to protect the malware but it was in less to block are remove that malware. In this case the monitoring problems would be produced a security tragic.

9. Removable Media Controls:

Every organization would be divided to its removed media policies and should be bounded by the using of media how much it would be possible if there are any case where the user is unsafe the policy should be selected the types of media which be used and the and the information steps can be spread out.

10. Home and Mobile Networks:

When the users are at home are mobile they are no more connected to the company's LAN or WAN this control a network problem where the organization not be able to over control the internet therefore such policies should be organized which support mobile and working home. The company should also be select to range the profile of users on mobile and also control their data that is collected in mobile and home computer.

TYPES OF CYBER SECURITY

The types of cyber security are nothing, but the techniques and processes used to prevent the stolen or assaulted data. It needs knowledge of possible threats to data, such as malware. People use digital devices daily connecting with online services. These online services made lives of end-users easier

1. Critical infrastructure security:

Critical infrastructure security is the protection of cyber-physical system on which modern society depends upon. It is the protection of systems, networks and asset whose continuous operation is very necessary to ensure the protection of nation, and country's economy.

Common examples of critical infrastructure are electricity grid, water purification, traffic lights, shopping centers and hospitals.

Putting Infrastructure of electricity grids online makes it unprotected from cyber-attacks. Organizations with responsibility for critical infrastructures should understand the weakness and secure their business against them.

Organizations that are not responsible for critical infrastructure, but still depend upon it for their business, should develop a plan by evaluating how damage on critical infrastructure they depend on might affect them.

2. Application security:

Application security uses software and hardware methods to detect any external threats that can happen in the development stages of an application.

Due to networks, applications are much more reachable to other people. So, it is necessary to adopt security measures during the development stages of an application.

Types of application security are antivirus programs, firewalls, encryption programs. These all are to protect an application from any unauthorized access. Companies can protect their sensitive data through special application security processes.

3. Network security:

Network security is the set of policies and practices used to prevent, observe and detect unauthorized access, misuse and changings in computer networks. Through network security person require authorization of access to data which is controlled by administrator .It stop third person to enter and spread on your network. Some common examples of network security implementation are new passwords, application security, antivirus software, antispyware software, and encryption, firewalls and Monitored internet access.

4. Cloud computing security:

The advantages of rapid deployment, flexibility, extensibility, and low cost have made the cloud security universal among all organizations and institution Cloud security is a software-based security tool that protects and observe your cloud resources . Cloud recourses are different applications (such as Google docs, Google drive, Xdrive) on which your data is stored instead on your mobile, laptop or other device. Through Cloud resources we can see our stored data on any device by login.

There is a myth that data on cloud resources are less secure than other things. However, the fact is data is secured through its accessibility and integrity not through its location.

According to Logic Cloud Security Report on-premises environment users suffer more attack incidents that those of service provider environments.

The report further finds that on premise environment users experience an average of 61.4 attacks while on the other hand Service provider environment customers experienced an average of 27.8 attacks.

5. Internet of Things Security:

Internet of Things (IoT) security refers to a wide collection of critical and non-critical cyber physical systems, interconnecting computing devices, digital and mechanical machines and the ability to transfer data and information without human to human or human to computer interaction. According to Bain & Company's prediction the combined markets of IoT will grow to about $520 billion in 2021. Moreover, more than double of $235 billion spent in 2017 on IoT. The data center, consumer devices, networks, legacy embedded systems and connectors are the core technology of the IoT market.

Moreover, enterprisers are optimistic about Iot business growth and they would buy more IoT devices on average if security concerns were addressed. This all calls trader to invest more in learning security challenges and to take measures to ensure security.

Cyber Security Challenges

In today's world, Cyber Security Challenges are from small institution to larger institution including national security, government and private hospitals, banks, universities etc. to protect them from cyberattacks. With increase in a digital world, cybercrimes have also increased, thus cyber security challenges.

1. Baiting:

Baiting is one of the threats faced by cyber security. It is like a real life Trojan horse in which hacker use physical media to check the greed of the victim by offering them fake free music, films etc. by login in their site they surrender their personal information, data to the hacker. To defend ourselves from such hackers educating ourselves is one of the important strategies .We should not become prey of their master plan.

2. Malware:

A cybercriminal might leave a USB stick, filled with malware. In addition, the criminal might label the USB in an attractive way like "Confidential" or "Bonuses." A victim who takes the bait will pick up the USB and plug it into his computer to see what's on it. The malware may be virus will automatically inject itself into the computer infecting other files too.

3. Phishing:

Now-a-days it is frequently used especially in small businesses. Hackers use emails to steal victim personal data. Through emails victim directed to phony websites and trickled into giving their personal information like login details, address, credit card details etc. To protect ourselves from such hackers we should not pay attention to emails from unknown names with attachments.

4. Pretexting:

Pretexting is a fraud in which person tends to be someone else may be telemarketer, police officer , bank manager asking you to tell about your credit card details, bank account details , passwords etc. We should not pay attention to such fraud people.

5. Quid Pro-Quo Scam:

Quid Pro-Quo Scam generally offers victims fake free services or prize in return of valuable information. The hacker may tell victims they can fix their IT problems resulting in stealing of valuable data.

6. Vishing:

It is the voice version of phishing. V means voice but the scam effort is same. The criminal uses the phone to fake a victim into handing over valued information.

7. Hacking:

It can also be done through computers using assessing their data similarly through emails, attachments without their permission. Sometimes hackers just stole their data without disrupting or changing it may result in risk of national security.

8. Email Bombing:

It is the form of denial of service attack that floods an inbox and mail server with messages. If enough messages are sent, the systems may be overloaded and they will stop working.

CYBER SECURITY TOOLS

1. GNU Privacy Guard:

The GNU Privacy Guard is a software tool used for files and email encryption. A strong encryption quantity will provide vast security at the data level. This is a feasible open-source substitute to Pretty Good Privacy (PGP). It complies with Open PGP standards. This is a command-line tool part of major Linux helps such as Ubuntu, CentOS, and Fedora. So this amazing tool is used to protect data by using Pretty Good Privacy to generate public and private sources in the backup server and import the port source to all data servers from where the backup has to be occupied and code it.

2. True crypt:

It is there for disk level encryption. True crypt is perfect or a real solution for disk level encryption. This is a handy open-source security tool which is used for on the disk encryption. Furthermore it is a precise choice because it encrypts automatically before data is saved on the disk and decrypts it completely after it is loaded from the disk without user intervention.

3. Open Web Application Security Project:

OWASP is an open-source web application security project which provides great performance and code review steps among other strategies that developers, architects, and designers can use to secure software.

4. ClamAV:

The host level security deals for protection of single devices such as servers, laptops and PCs. ClamAV is the flawless antivirus system that helps to scan data originating from different sources. This is an open-source antivirus designed for gathering malware, viruses and harmful Trojans which try to steal information.

5. Open Source Security:

Open Source Security is an open-source tool that offers SIM and SEM solutions along with log monitoring. This is Home Based Intrusion Detection System. It helps customers to fulfill standards. It also integrates Security Event Management. It has features such as file integrity checking, detecting rootlets, monitoring logs and providing network security.

6. Snort:

Snort is an open-source network Intrusion Detection and Prevention System which performs detection and analysis of network movement moving across in a more comprehensive way than an average firewall. Intrusion Detection and Prevention System tools are well-known for analyzing traffic and comparing the packet to a database of attacked profiles. IDs tool alerts IT workers regarding these attacks, but IPS tool block harmful traffic. The mixture of these two systems is an essential part of comprehensive security architecture.

6. OpenVAS:

It is a framework of services and tools which provides comprehensive and intensive vulnerability scanning and management systems. It is the open source version of Nessus software. Vulnerability management can be added to configuration management plus antivirus software for abolishing malware.

7. OSSIM:

Open Source Security Information Management (OSSIM) is all in one security solution. It offers a the solution of Security Information and Event Management that has integrated open-source software's Snort, OpenVAS, Mrtg, NTOP, and Nmap. This is an economical solution for monitoring the security of grid.

RECOMMENDATIONS

The top 5 recommendations for secure the individuals data, information or network are following;

1. Patch Management:

Patching devices is difficult. The software of computer or network patch fixes security flaws in the system. It is the important part to secure your computer to ensure the regularly updates of the device and software. Patching should regularly be done on mobile phones, laptops, network devices like routers and firewalls, service infrastructure and clod services.

2. General User Practices:

To become a cyber smart, it requires general user practices such as turning of devices when you are not using it. Also then report the suspicious activities to IT and practice good physical security to devices etc.

3. Protection Software's:

Antivirus, Malware and threat protection software's are very important to keep the virus away from the devices or networks. The software's should always be active and up-to-date on regular basis. Organize the antivirus in such a way that it automatically scans the downloaded files, other media and emails attached.

4. Password Management:

Password management plays a key role in security the data or networks. This can stop the hacker to gain access to the data and assets. The password should be the unique one so that everyone cannot guess it easily and a single password should not be used for multiple accounts.

5. Multi-Factor Authentication:

Multi-Factor Authentication (MFA) is also a way to secure or safe the account or data that if a user hacks your account or knows your password then the account requires authentication to login to other than the device user use.

RESULTS AND DISCUSSION

Cybersecurity is a complex issue which is not only limited to computer science and information technology but it's study require the knowledge and expertise in multiple disciplines such as psychology, economics, political science, engineering, sociology, decision sciences, international relations, and law. In preparation, although technical measures are an important portion and it is easy for policy analysts and others to get lost in the technical details.

Most of all, it tries to leave the reader with two dominant ideas. The problem of cyber security will never be solved once and for all. Solutions to this problem is limited in scope and long life though they may be, are at least as much nontechnical as real world in nature. It is accordingly clarified that network or data is still unsecured unless they are secured through guaranteed security.

The issue of cyber threats has gained importance universally both in literature, practice and government policies. Cyber threats further exceeds to political, social and private boundaries. As the world become more and more digitized and the economy more dependent, cyber space tends to be the medium through which our progress would develop. Countries are increasing their inspection of cyber laws and policies as threats increase. Pakistan is also growing its cyber extent within the country and its worldwide connectivity. The same cyber threats that the world is facing in internet are also faced by Pakistan. These threats are increasing day by day and targeting to more complex systems now. The military and other state institutions are also not safe from such cybercrime attacks. Pakistan has worked on the laws and progress regarding cyber space. But, those laws and regulations have not effectively solved the issue. Further there is a need for more laws, regulation, policymaking, collective efforts and responsibility when it comes to safeguarding Pakistan's cyber space.

CONCLUSION

Computer security is a vast and complex topic that is attaining more and more importance because the world is now highly interlocked, with networks being used to carry out serious transactions. Cybercrime continues to diverge down different paths with each New Year that passes and so does the security of the information. The latest up-to-date and troublemaking technologies are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so. There is no proper solution for cybercrimes but we should try our level best to minimize them in order to have a safe and protected future in cyber space.

Cybersecurity is an everlasting conflict. A ceaseless significant solution to this problem will not be found in the imaginable future.

REFERENCES

1. https://mind-core.com/blogs/cybersecurity/5-types-of-cyber-security/
2. https://www.educba.com/types-of-cyber-security/
3. https://www.freecodecamp.org/news/10-tools-you-should-know-as-a-cybersecurity-engineer/
4. https://www.softwareworld.co/top-computer-security-software/
5. https://www.ncbi.nlm.nih.gov/books/NBK223216/
6. https://www.think-asia.org/bitstream/handle/11540/9714/Cyber-security-where-does-pakistan-stand%28W-167%29.pdf?sequence=1
7. file:///C:/Users/DELL/Downloads/An-Introduction-to-Cyber-Security.p
8. file:///C:/Users/DELL/Downloads/Introduction%20to%20the%20Concept%20of%20IT%20Security%20(1).pdf
9. https://techwisegroup.com/weekly-tech-tips/top-5-cybersecurity-recommendations/