ISSUES AND CHALLENGES IN CYBER SECURITY.

Ashu Rai[1]

ABSTRACT

The functionality of modern computer systems is often regarded as the function of the five basic attributes of secure computer systems and information: availability, accuracy, accuracy, confidentiality, and integrity. The concepts generally apply to government, business, education, and the general life of private individuals. Consideration often includes extended Internet programs - hence the name Cybersecurity. Acquiring and maintaining secure cyberpace is a complex process, and some of the concerns include personal identity, privacy, creative ownership, sensitive infrastructure, and organizational stability. Threats to secure operating infrastructure are critical and very deep: cyber terrorism, cyber war, cyber intelligence, and cyber crime, to which the tech community responds with security and procedures, often brought about by the private sector. This paper provides a complete overview of cyber security in the main purpose of developing the science of cyber security.

RESEARCH PAPER

Today one can send and receive any kind of data can be email or audio or video just by clicking a button but you have done it consider how secure his data id is or safely sent to another person without any information leak ?? The answer lies in cyber security. Today the Internet is very fast growing infrastructure in everyday life. In the modern environment of many of the latest technologies technology transforms a man's face he is kind. But thanks to this emerging technology. we cannot protect our privacy details in a very effective way and that is why these days cyber crime is increasing day by day. Today more than 60 percent of the total business transactions are done online, so this is it field required high security for open and moving transactions. So it is cyber security has become a recent issue. Width of cyber security is not just about protecting details in the IT industry but also in various other sectors such as cyber space etc. Even the latest technology is like a cloud computer, laptop, E-commerce, net Banking etc also requires a high level of security. As this technology holds the key details relating to a

[1] 2nd Year Student, UPES (Dehradun)

person's safety it's something to do. Improves cyber security and protection of sensitive information infrastructure is important for each nation security and economic well-being. To make The Internet is secure (and protects Internet users) they become part of the development of new services and government policy. The the fight against cybercrime requires a wide and safe way. In that technical measures alone cannot prevent any crime, it is important that they are legal agencies are allowed to investigate again to successfully prosecute cyber crime. Today many nations and governments are pushing hard cyber security rules to prevent loss of other important details. Always each person should also be trained in this cyber safety and save themselves from these increasing cyber crime.

2. THE CRIME OF TIME

Cyber crime is a term for any illegal activity that uses a computer as its main means of commission and theft. The U.S. Department of Justice extends the definition of cyber crime to install any illegal computer use preservation of evidence. Growing list for cyber crime includes pre-existing crime made available by computers, such as a network computer login and distribution viruses, and computer-based variants of existing cases, such as who you are theft, tracking, exploitation and terrorism which they have become a major problem for people too nations. It is usually in the language of the common man cyber crime can be defined as a crime committed using a computer and the internet to make an instrument a personal ownership or sale of illegal goods or title victims or disrupted the operation of malicious programs. As day by day technology plays out a major role in human life is cyber crime and it will increase with technology development.

3. CYBER PROTECTION

Data privacy and security will remain the same top security measures for any organization he cares. We now live on earth where all information is stored in digital or cyber form. Social networking sites provided a space where users feel as safe as they are work with friends and family. In the case of home users, cyber criminals will continue this identify social networking sites to steal personal information. Not just social networking but also banking transaction a person must take all that is required. There will be new attacks on Android performance Devices

are rooted in the system, but will not be turned on large scale. True pills share the same an operating system like smart phones means the same malware as soon as those platforms. Malware number Macs models will continue to grow, however very little happens in PCs. Windows 8 will allow users to upgrade applications of any device (PCs, tablets and smart phones) running Windows 8, so it will be possible to develop malicious ones applications like those for Android, which is why these are some of the predicted methods on cyber safety.

4. TIME CHANGING ANSWERS

SAFETY

Listed below are some of the practices which have a significant impact on cyber security.

4.1 Web servers:

Threat of web applications attack to extract data or distribute malicious code it goes on. Cyber criminals spread theirs malicious code on legitimate web servers they have retreated. As for data theft attacks, many of which are gaining media attention, are and a major threat. Now, we need more Emphasis on protecting web and web servers applications. The best web servers a platform for these cyber criminals to steal data. So one should always use what is safe browser especially during important tasks so that you do not fall as a victim of this crime.

4.2 Cloud computing and its services

These are all days small, medium and large companies are less accepting of cloud services. In other words the world is moving slowly towards the clouds. This latest trend introduces a major cyber security challenge, as traffic can do go around the traditional check points. In addition, as a number of applications available in the cloud is growing, policy controls for web applications and cloud services will do the same You need to appear to prevent loss of important details. Although cloud services are available developing their models is still a lot of problems they were raised in their safety. Cloud it can provide great opportunities but it does it should always be noted that as the cloud changes therefore its security concerns are increasing.

4.3 APT attacks and targets

APT (Continued Advanced Threat) is complete a new level of cyber crime material. Age the power of network security as a web filtering or IPS played an important role in identifying that targeted attack (especially in the background initial relaxation). As the invaders grow older resilience and the use of unconventional strategies, network security must be combined security

forces to detect attacks. So one has to improve our security strategies for the purpose of preventing further threats the future.

4.4 Mobile Neremove

malicious software programs, such as viruses and worms. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. An anti virus software is a must and basic necessity for every system works. Today we can connect to anyone anywhere part of the world. But in these mobile networks safety is paramount. These days firewalls and other safety measures are in place explosion as people use devices such as tablets, phones, PCs etc. and requires additional security other than those currently in used applications. You must keep in mind the safety issues of these mobile networks. Mobile networks in progress most prone to these cyber criminals is a lot of attention should be taken in case of safety issues.

4.5 IPv6: New Internet Protocol

IPv6 is a new Internet protocol instead of IPv4 (older version), with you have become the backbone of our global network too the Internet as a whole. IPv6 protection is not just IPv4 power input question. While IPv6 replaces the hotel in doing more IP addresses are available, there are many more fundamental changes to the law that need to be considered in security policy. That is why it is so it is always best to switch to IPv6 immediately it is possible to reduce the risk in relation to cyber crime.

Encryption code

Encryption is the process of encoding messages (or details) in such a way that eavesdroppers or hijackers cannot read it. In an encryption scheme, message or information encrypted using an encryption algorithm, convert it into readable cipher text. This usually done using a encryption key, which specifies what the message should be encoded. Encryption at the very first level protects data privacy and its integrity. But much more the use of encryption brings many challenges to cyber security. Encryption is used for security data on the go, for example existing data transmitted over networks (eg Internet, ecommerce), mobile phones, wireless microphones, wireless intercoms, etc. coding a person who does not know if it exists leakage of information. So the above is one of the styles changing the face of cyber security in the world.

5. ROLE OF COMMUNICATION NEWS

CYBER SECURITY

As we become more connected world, companies should find something new ways to protect your information. Public the media plays a major role in cyber security and will contribute significantly to personal cyber threats. The acceptance of social media among employees is a thing rising as well as the threat of attack. Since social media or social networking sites exist it is almost used for most of them every day he has become a major platform for cyber criminals by hacking personal information and stealing important data. In a world where we are quick to sacrifice our own personal details, companies must verify they are quick to point out threats, to respond in real time, and to avoid violations of any kind. As people are easily attracted to these social media hackers use it as a trap get the details and data they need. People must therefore take appropriate action especially in dealing with social media in a way to prevent the loss of their information. People's ability to share information with millions of listeners in the heart of a particular challenge posed by social media businesses. In addition to giving anyone the ability to spread commercial risk details, social media also provide the same the ability to spread false information, which could just as it hurts. Rapid spread of false information through social media is in the middle emerging risks known to Global Risks 2013 report. Although social media can be used for cyber crime these companies can not stop using social media as it plays an important role in company information. Instead, it should have solutions that will alert them to the threat to fix it before doing real damage. However, companies need to understand this as well see the importance of analyzing details especially in social discussions and provide appropriate security solutions to order to stay away from risks. One has to manage media outlets through specific policies and rights technology.

6. CYBER SECURITY METHODS

6.1 Access and password control Username and password concept has it has been our basic defense mechanism details. This could be the first measures related to cyber security.

6.2 Data verification

The documents we receive must always be so verified before download which should be checked if it appears on trustworthy and reliable source and that they are not changed. Verification of

these documents it is usually done by existing anti virus software on devices. So good software for viruses is not and it is important to protect devices from viruses.

Malware Scanners

This software usually scans all files and documents available in the system for malicious code or harmful viruses. Bacteria, worms, and Trojan horses are examples of malicious software that is often collected together it is also called malware.

6.4 Firefighters

A firewall is a software program or a piece of hardware that helps get rid of hackers, viruses, and worms trying to access your computer more the Internet. All incoming and outgoing messages the internet goes through the fire model, checks each message and blocks them which does not meet the prescribed security procedures. Fire extinguishers therefore play an important role in detection of malware.

Anti-virus software

Antivirus software is a computer program called detects, blocks, and takes action to reduce or remove malicious software programs, such as germs and worms. that it can test new viruses quickly are available. This is an anti virus software must also have a basic need for the whole system.

Table II: Cyber security strategies

CYBER BEHAVIOR

Cyber behavior is nothing but a code online. When we do these cyber principles there is a good chance we will use the internet in a proper and safe manner. A few below of which: MAKE use of the Internet to communicate and share with other people. Email and instant messaging makes it easy stay in touch with friends and family members, contact work colleagues, and share ideas again details and people throughout the city or in the middle of the earth. Don't be a bully on the Internet. Don't call people names, lie about them, send their shameful images, or do anything else to try to hurt them. The Internet is considered to be the largest in the world a library with information on any topic in any subject area, so use this details in a proper and legal manner it is always important. Not Do not use other accounts using their passwords. Never try to send any kind of malware in other programs and do it it's broken. Never share your personal information

to anyone as there is a good chance that others misuse it and eventually you it will end in trouble. You're If you're online don't pretend in other programs and do it yourself it's broken. Never share your personal information to anyone as there is a good chance that others misuse it and eventually you it will end in trouble. You're If you're online don't pretend someone else, and never try to create fake accounts to another person as they are it would be as good as any other someone in trouble. Always have copyright details and download games or videos only if allowed. The above are just a few cyber measurements a person should make follow while using the internet. We are always human he thought of appropriate rules from the very first stages the same here we use in the cyber space.

8. CONCLUSION

Computer security is a major issue that it becomes even more important because the earth high communication, through networks is used to make sensitive transactions. Cyber crime continues to vary widely ways to go with each passing New Year as well as information security. The latest and disruptive technologies, as well as youth cyber tools and threats from every day, challenges in not only organizations. how they protect their infrastructure, but how they need new platforms and ingenuity to do so. There is no valid cyber solution crime but we must try our best to reduce them to have a safe again a secure future in the cyber space.

REFERENCES:

1. A Sophos Article 04.12v1.dNA, eight trends changing network security by James Lyne.

2. Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole

3. Computer Security Practices in Non Profit Organisations – A NetAction Report by Audrie Krause.

4. A Look back on Cyber Security 2012 by Luis corrons – Panda Labs.

5. International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 Page nos.68 – 71 ISSN 2229-5518, "Study of Cloud Computing in HealthCare Industry " by G.Nikhita Reddy, G.J.Ugander Reddy

6. IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013.

7. CIO Asia, September 3rd , H1 2013: Cyber security in malasia by Avanthi Kumar.