International Journal of Recent Engineering Research and Development (IJRERD)
ISSN: 2455-8761
www.ijrerd.com || Volume 09 – Issue 03 || May - Jun 2024 || PP. 23-27

Cybersecurity is One of the Most Challenges and Crucial Aspects of the Modern Technological Domain- A Review

Srinjoy Mitra
BTech, CSE Second Year, Section-B, KIIT University, Bhubaneswar

Abstract: In the world of information technology, cybersecurity is crucial. One of the major problems in today's society, where technology and network connections rule, is information security, if crucial data, files, systems, and other virtual assets are not effectively protected, there is no such thing as security. The number of cybercrimes dramatically rises daily. Because of the tremendous amounts of data that organizations in the medical, financial, economic, and military sectors collect, use, and store on PCs and other devices, cybersecurity is crucial. Numerous steps are being taken by the government and businesses to stop these cybercrimes. Despite the emergence of new cybersecurity technologies, ethical hackers continue to provide issues for cybersecurity. Hackers are also evolving their methods for evading cybersecurity measures. breaking the techniques of cybersecurity.This paper focuses on the most recent technologies of cybersecurity, ethics and trends changing the face of cybersecurity.

Keywords: cybersecurity, cybercrimes, technology, information technology, cyber ethics, cloud computing.

1. Introduction:

To protects system, program and network from digital attack, cybersecurity is very essential. Sensitive information, extorting money are usually aim by cyber hackers and they access via ransomware. An effective cybersecurity method has numerous layers of defence. The cyber-hacker cracks the cybersecurity mechanism in dynamic environments. Cybersecurity measures are implemented effectively in changing environment, as hackers are more innovative. So, unified management system of threat through Cisco Security products can accelerate key security operation, detection, investigation and remediation.

Through computer network, computer viruses/worms, DoS, knowledge disruptions, can be attacked by cyber hackers. Cyber-attacks are still rising, and more waiting to harm to their targeted systems and networks. Detecting intrusions in cybersecurity has become challenging due to their intelligence performance. So, it has a negative impact on data integrity, privacy availability and security. Today, Internet is the part and parcel in every day's life. For these, we have to safeguard our private information in a very effective way and as cybercrime areincreasing day by day. Now- a- day cybersecurity has become a latest issue, as more than 80 percent of total transaction are done through online mode.

High levels of security require through latest technologies like cloud computing, mobile computing, E-commerce, net banking etc. So, infrastructure developments are essential for protecting critical information, nation's security and economic upliftment through cybersecurity.

Consumers have to obey the basic information security like creating strong passwords, wary accessories in email, and back-up data.

Governments must have a guideline for what to do after cyber- attack. It clarifies to recognise bouts, protect organisation, notice and threats reply.

2. Technology:

Technology plays a vital role to giving individual and organizations, the system security tools, to protect themselves against cyber-attacks. Three essential threatened objects like PCs, handheld devices, and routers, systems and cloud. Shared technology defends these objects contain next generation firewalls, DNS pass through a filter, anti-virus tools, malware defence and email safety results.

Security means, the mechanism of protecting anything. Cyber and safety together play a defensive role after the spiteful attack to break the security. So, user can protect their data from hackers. There are numerous tackles and techniques that are castoff to deploy it and it is a nonstop process.

The tools of cybersecurity make our work easy. Cybersecurity outbreak can result in individuality theft, to blackmail attempts, to the damage of vital data like family photograph.

2.1 Cybercrime:

Cybercrime is a term for any illegal activity that uses by a computer for the storage of evidence.Cybercrimesinclude network intrusions in computer and the spreading of computer viruses as well as identity theft, stalking, bullying and terrorism that creates a major problem to people and nations.

2.2 Cybersecurity:

Cybersecurity resilience emerges top priorityby an organization for their privacy and maintained thesecurity of the data. Recently,alldocuments andinformationwerestored and maintainedinadigital form. Family and friends always interact in social networking sites as they feel comfortable.Taking this opportunity, cyber criminals always target social media site to steal personal data, of home users. Not only social networking but also a person would careful during banktransactions and take all the requiredsecuritymeasures.

Incidents	Jan- June2012	Jan-June 2013	% Increase / (decrease)
Fraud	2439	2490	2
Intrusion	2203	1726	(22)
Spam	291	614	111
Maliciouscode	353	442	25
Cyber Harassment	173	233	35
Content related	10	42	320
Intrusion Attempts	55	24	(56)
Denial of services	12	10	(17)
Vulner ability reports	45	11	(76)
Total	5581	5592	

Table-1

The above incidents of cybersecurity threats reported to Cyber 999 in Malaysia from January–June 2012 and 2013. As crime is increasing even the security measures are also increasing. Silicon Valley Bank found that cyber-attacks are a serious threat to their data and business continuity (survey report by U.S. technology and health care executives).

Cybersecurity resources are maintaining or increasing 98 percent by different companies for their online attack. But, only one third companies are completely confident about their security, more or less of their business partners.

There will be new attacks on Android operating system-based devices in a low scale. The fact, tablets share the same operating system as smart phone has and it will be soon targeted by the same malware platforms. The number of malware specimens for Macs would continue to grow, though much less than in the case of PCs.Windows 8 will allow users to develop applications for virtually any device (PCs, tablets and smart phones) running Windows 8, so, it will be possible to develop malicious applications like those for Android, hence these are some predicted trends found in cybersecurity.

3. Trends Changing Cybersecurity:

Here are some trends which have a huge impact on cybersecurity.

3.1 Web servers:

The threat of attacks on web applications to extract data or to distribute malicious code persists. Cyber criminals distribute their malicious code via legitimate web servers. But data-stealing attacks, which paid attention to media, are also a big threat. Now, we need a greater emphasis on protecting web servers and web applications. Web servers are especially the best platform for cyber criminals to steal the data. Hence one must always use a safer browser especially during important transactions, and not to fall as a prey for this crime.

3.2 Cloud computing and its services

These day all small, medium and large companies are slowly adopting cloud services i.e., the world is slowly moving towards the clouds. This latest trend presents a big challenge for cyber security, as traffic can go around traditional points of inspection. Additionally, as the number of applications available in the cloud grows, policy controls for web applications and cloud services will also need to evolve in order to prevent the loss of valuable information. Though cloud services are developing their own models, still a lot of issues were being brought up about their security. Cloud may provide immense opportunities but it should always be noticed that as the cloud evolves, so as its security concerns increase.

3.3 APT’s and target attacks

APT (Advanced Persistent Threat) is a whole new level of cybercrime ware. For years, network security capabilities such as web filtering or IPS have played a key part in identifying such targeted attacks (mostly after the initial compromise). As attackers grow bolder and employ more vague techniques, network security must integrate with other security services in order to detect attacks. Hence one must improve our security techniques in order to prevent more threats coming in the future.

3.4 Mobile Networks

Today we are able to connect to anyone in any part of the world. But for this mobile network's security is a very big concern. These day firewalls and other security measures are becoming porous as people are using devices such as tablets, phones, PC's etc. all of which again require extra securities apart from those present in the applications used. We must always think about the security issues of these mobile networks. Further mobile networks are highly prone to these cybercrimes and a lot of care must take in case of their security issues.

3.5 IPv6: New internet protocol

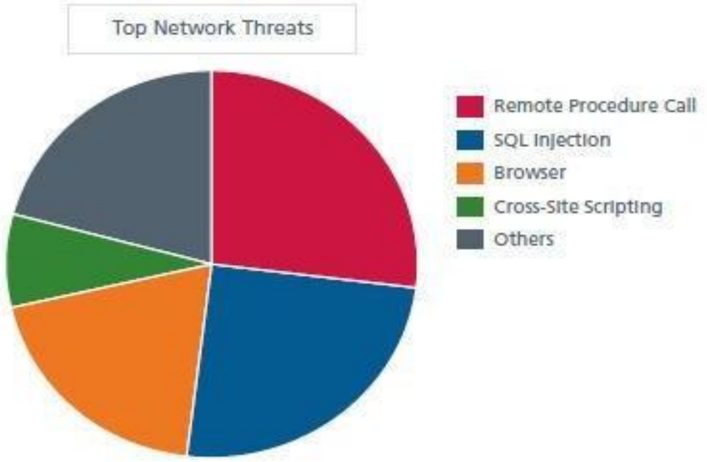
IPv6 is the new Internet protocol that replaces IPv4 (the older version), which has been a backbone of our networks in general and the Internet at large. Protecting IPv6 is not just a question of porting IPv4 capabilities. While IPv6 is a wholesale replacement in making more IP addresses available. There are some fundamental changes to the protocol which need to be considered in security policy. Hence, it is always better to switch to IPv6 as soon as possible in order to reduce the risks with regards to cybercrime.

3.6 Encryption of the code

Encryption is the process of encoding messages (or information) in such a way that eaves droppers or hackers cannot read it. In an encryption scheme, the message or information is encrypted by using an encryption algorithm, turning it into an unreadable cipher text. It is usually done with the use of an encryption key, which specifies how the message encoded. Encryption at a very beginning level protects data privacy and its integrity. But more use of encryption brings more challenges in cyber security. Encryption is also used to protect data in transit, for example data transferred via networks (e.g., the Internet, e- commerce), mobile telephones, wireless microphones, wireless intercoms etc. Hence by encrypting the code one can know if there is any leakage of information.

Hence the above are some of the trends changing the face of cyber security in the world. The top network threats are mentioned in below Fig -1.

Fig-1



The above pie chart shows about the major threats for networks and cyber security.

4. Role of social media in Cybersecurity:

As we become more social in an increasingly connected world companies must find new ways to protect personal information. Social media plays a huge role in cyber security.

Social media adoption among personnel is skyrocketing and so is the threat of attack. Since, social media or social networking sites are almost used by most of them every day and it has become a huge platform for the cyber criminals for hacking private information and stealing valuable data.

In a world, where we're quick to give up our personal information, companies have to ensure they're just as quick in identifying threats, responding in real time, and avoiding a breach of any kind. Since, people are easily attracted by these social media, the hackers use them as a bait to get the information and the data they require. Hence, people must take appropriate measures especially in dealing with social media in order to prevent the loss of their information. The ability of individual to share information with an audience of millions is at the heart of the particular challenges that social media presents to businesses. In addition to giving anyone the power to disseminate commercially sensitive information, social media also gives the same power to spread false information, which can be just being as damaging. The rapid spread of false information through social media is among the emerging risks identified in Global Risks 2013 report.

Though social media can be used for cybercrimes these companies cannot afford to stop using social media as it plays an important role in publicity of a company. Instead, they must have solutions that will notify them of the threat in order to fix it before any real damages is done. However, companies should understand this and recognize the importance of analyzing the information especially in social conversations and provide appropriate security solutions in order to stay away from risks. One must handle social media by using certain policies and right technologies.

5. Cybersecurity Techniques:

5.1 Access control and password security

The first measures with regards to cybersecurity are to use username and password to protect our information.

5.2 Authentication of data

Verification of documents must always to be authenticated i.e., it has originated from a trusted and reliable source before downloading. Documents authentication are usually done by antivirus software present in the devices which is also essential to protect the devices from viruses.

5.3 Malware scanners

This software usually scans all the documents and files present in the system for malicious code or harmful viruses. Examples of malicious software are Viruses, worms, and Trojan horses are that are often group together.

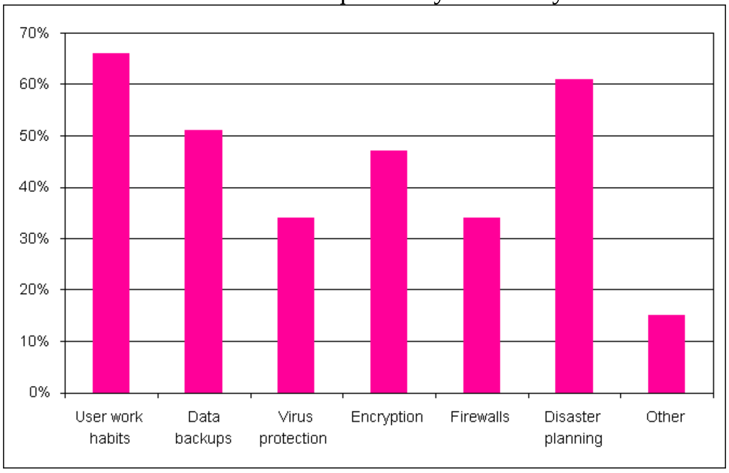
5.4 Firewalls

A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach computer over the Internet. Messages are blocked if it do not meet the specified security criteria in the firewall. Hence, firewalls play an important role in detecting the malware.

5.5 Anti-virus software

Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. It includes 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 discover. So, in every system anti-virus software is must.

Table II: Techniques on cybersecurity



6. Cyber Ethics:

Cyber ethics were nothing but the code of the internet. When we practice these cyber ethics there are good chances of us using the internet in a proper and safer way. The below are a few of them:

- DO use the Internet to communicate and interact with other people. E-mail and instant messaging make it easy to stay in touch with friends and family members, communicate with work colleagues, and share ideas and information with people across town or halfway around the world
- Don't be a bully on the Internet. Do not call people names, lie about them, send embarrassing pictures of them, or do anything else to try to hurt them.
- Internet is considered as world's largest library with information on any topic in any subject area, so, using this information in a correct and legal way is always essential.
- Do not operate other's accounts using their passwords.
- Never try to send any kind of malware to other's systems and make them corrupt.
- Never share person's personal information to anyone, as there is a good chance of others misusing it and finally it creates some trouble.
- During online mode never pretend to the other person, and never try to create fake accounts on someone else as it would land both the person into trouble.
- Always adhere to copyrighted information and download games or videos only, if they are permissible to others.

The above are a few cyber ethics, one must follow while using the internet. We are always obey proper rules from out very early stages, the same here we apply in cyber space.

7. Conclusion:

Computer security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being use to carry out critical transactions. Cybercrime continues to diverge down different paths with each New Year that passes and so does the security of the information. The latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging organizations with not only how they secure their infrastructure, but how they require new platform and intelligence to do so. There is no perfect solution for cybercrimes, but we should try our level best to minimize them in order to have a safe and secure future in cyber space.

8. References:

[1]. Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole

[2]. Computer Security Practices in Non-Profit Organisations – A Net Action Report by Audrie Krause.

[3]. A Look back on Cyber Security 2012 by Luis corrons – Panda Labs.

[4]. 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

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

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

[7]. Research Paper on Cybersecurity- Emerging advancement and challenges in Science, Technology and Management-April 2021 by Ashwani Sheth, Sachin Bhosale and Farish Kurupkar