CYBER SECURITY- CHALLENGES AND ITS EMERGNING TRENDS

[1] MEENAKSHI R, [2] SHWETHA T P
LECTURER
Department of Computer science and Engineering,
Government Plytechnic College Bellary,Ballari,India

ABSTRACT : Cyber Security plays an important role in the field of information technology .Securing the information have become one of the biggest challenges in the present day. When ever we think about the cyber security the first thing that comes to our mind is 'cyber crimes' which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cyber crimes. Besides various measures cyber security is still a very big concern to many. This paper mainly focuses on challenges faced by cyber security on the latest technologies .It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security.

Keywords: cyber security, cyber crime, cyber ethics, social media, cloud computing, android apps.

1.INTRODUCTION

Today man is able to send and receive any form of data may be an e-mail or an audio or video just by the click of a button but did he ever think how securely his data id being transmitted or sent to the other person safely without any leakage of information?? The answer lies in cyber security. Today Internet is the fastest growing infrastructure in every day life. In today's technical environment many latest technologies are changing the face of the man kind. But due to these emerging technologies we are unable to safeguard our private information in a very effective way and hence these days cyber crimes are increasing day by day. Today more than 60 percent of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions. Hence cyber security has become a latest issue. The scope of cyber security is not just limited to securing the information in IT industry but also to various other fields like cyber space etc.

Even the latest technologies like cloud computing, mobile computing, E-commerce, net banking etc also needs high level of security. Since these technologies hold some important information regarding a person their security has become a must thing. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic wellbeing. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as governmental policy. The fight against cyber crime needs a comprehensive and a safer approach. Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cyber crime effectively. Today many nations and governments are imposing strict laws on cyber securities in order to prevent the loss of some important information. Every individual must also be trained on this cyber security and save themselves from these increasing cyber crimes

1.1 Definition

It could be defined as the procedure to ease the security fears in order to protect repute damage, commercial loss or financial loss of all group. The term Cybersecurity obviously required that it's a gentle of security that we proposal to the organisation that frequent users can contact using the internet or over a network. There are numerous tackles and techniques that are castoff to deploy it. The greatest significant fact around safeguarding informations is that it's not a one interval procedure but a non-stop process. The organisation proprietor has to keep stuffs modernised in mandate to keep the hazard low.

1.2Types of Cyber Security Phishing

1.2.1 Phishing is the rehearsal of distribution fake communications that look like emails from dependable sources. The goal is to bargain thoughtful data comparable to credit card details and login data. It's the greatest kind of cyber attack. You can help defend manually over learning or an expertise solution that sieves malicious electronic mail.

1.2.2 Ransomware

It is a type of malicious software. It is considered to extract currency by blocking contact to records or the PC system until the deal is paid. Paying the ransom does not assurance that the records will be recuperated or the system returned.

1.2.3 Malware

It is a type of software intended to gain illegal right to use or to cause impairment to a system.

1.2.4 Social engineering

It is a tactic that opponents use to pretend you into illuminating delicate information. They can importune a monetarist payment or improvement access to your reserved informations. Social engineering can be collective with some of the pressures registered above to style you additional probable to connect on links, transfer malware, or belief a malicious cause.

Privacy and security of the data will always be top security measures that any organization takes care. We are presently living in a world where all the information is maintained in a digital or a cyber form. Social networking sites provide a space where users feel safe as they interact with friends and family. In the case of home users, cyber- criminals would continue to target social media sites to steal personal data. Not only social networking but also during banktransactions a person must take all the required security measures.

Incidents	Jan-June 2012	Jan-June 2013	% Increase/ (decrease)
Fraud	2439	2490	2
Intrusion	2203	1726	(22)
Spam	291	614	111
Malicious code	353	442	25
Cyber Harassment	173	233	35
Content related	10	42	320
Intrusion Attempts	55	24	(56)
Denial of services	12	10	(17)
Vulnerability reports	45	11	(76)
Total	5581	5592	

The above Comparison of Cyber Security Incidents reported to Cyber999 in Malaysia from January–June 2012 and 2013 clearly exhibits the cyber security threats. As crime is increasing even the security measures are also increasing. According to the survey of U.S. technology and healthcare executives nationwide, Silicon Valley Bank found that companies believe cyber attacks are a serious threat to both their data and their business continuity.

- 98% of companies are maintaining or increasing their cyber security resources and of those, half are increasing resources devoted to online attacks this year
- The majority of companies are preparing for when, not if, cyber attacks occur
- Only one-third are completely confident in the security of their information and even less confident about the security measures of their business partners.

2.CYBER SECURITY TECHNIQUES

Access control and password security

The concept of user name and password has been fundamental way of protecting our information. This may be one of the first measures regarding cyber security.

2.1Authentication of data

The documents that we receive must always be authenticated be before downloading that is it should be checked if it has originated from a trusted and a reliable source and that they are not altered. Authenticating of these documents is usually done by the anti virus software present in the devices. Thus a good anti virus software is also essential to protect the devices from viruses.

2.2 Malware scanners

This is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.

2.3 Firewalls

A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. All messages entering or leaving the internet pass through the firewall present, which examines each message and blocks those that do not meet the specified security criteria. Hence firewalls play an important role in detecting the malware.

2.4 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. 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.

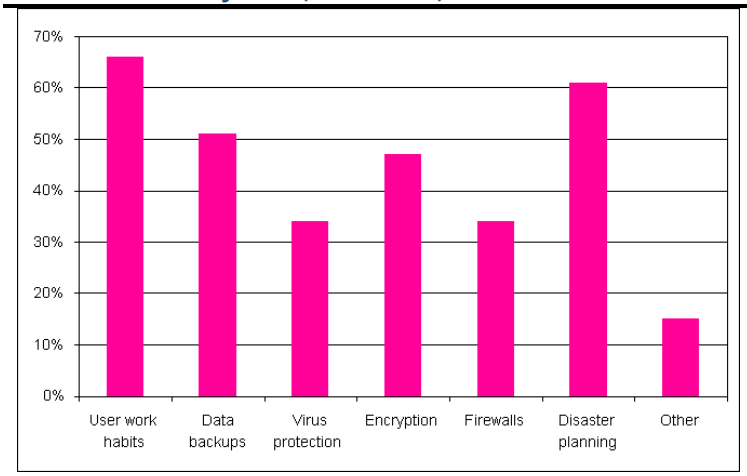

Table I: Techniques on cyber security

3.GOALS

The majority of the business operations run on the internet exposing their data and resources to various cyber threats. Since the data and system resources are the pillars upon which the organization operates, it drives lacking maxim that a risk to these individuals is definitely a threat to the group itself. A threat can be anywhere between a minor bug in a code to a complex cloud hijacking liability. Risk assessment and estimation of the cost of reconstruction help the organization to stay prepared and to look ahead for potential losses. Thus knowing and formulating the objectives of cybersecurity exact to every organization is crucial in protecting the valuable data. Cybersecurity is a practice formulated for the safeguard of complex data on the internet and on devices safeguarding them from attack, destruction, or unauthorized access. The goal of cybersecurity is to ensure a risk-free and secure environment for keeping the data, network and devices guarded against cyber terrorisations.

Goals of Cyber Security?

The definitive objective of cybersecurity is to defend the data from actuality stolen or co-operated. To attain this we aspect at 3 important goals of cybersecurity.

1. Defensive the Privacy of Information
2. Conserving the Integrity of Information
3. Controlling the Obtainability of information only to approved users

These objectives practise the confidentiality, integrity, availability (CIA) triad, the base of entirely safety agendas. This CIA triad model is a safety model that is intended to guide strategies for data security inside the places of a society or corporation. This model is similarly mentioned to in place of the AIC (Availability, Integrity, and Confidentiality) triad to side-step the mistake with the Central Intelligence Agency. The rudiments of the triad are reflected the three greatest vital mechanisms of safety. The CIA standards are one that greatest of the societies and businesses practice once they have connected a new request, makes a record or when assuring access to approximately information. On behalf of data to be totally safe, all of these safe keeping areas must originate into result. These are safe keeping strategies that all effort together, and hence it can be incorrect to supervise one policy.

CIA triad is the greatest collective standard to measure, choice and appliance the proper safety panels to condense risk.

3.1 Confidentiality

Making guaranteed that your complex statistics is reachable to accredited users and safeguarding no informations is revealed to unintended ones. In case, your key is private and will not be shared who power adventure it which ultimately hampers Confidentiality.

Methods to safeguard Confidentiality:

- Data encryption
- Two or Multifactor verification

• Confirming Biometrics

3.2 Integrity

Make sure all your data is precise; dependable and it must not be changed in the show from one fact to another.

Integrity ensure methods:

• No illegal shall have entrance to delete the records, which breaks privacy also. So, there shall be
• Operator Contact Controls.
• Appropriate backups need to be obtainable to return proximately.
• Version supervisory must be nearby to check the log who has changed.

3.3 Availability

Every time the operator has demanded a resource for a portion of statistics there shall not be any bout notices like as Denial of Service (DoS). Entirely the evidence has to be obtainable. For example, a website is in the hands of attacker's resultant in the DoS so there hampers the obtainability.

4. TRENDS CHANGING CYBER SECURITY

Here mentioned below are some of the trends that are having a huge impact on cyber security.

4.1 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 they've compromised. But data-stealing attacks, many of which get the attention of 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 these cyber criminals to steal the data. Hence one must always use a safer browser especially during important transactions in order not to fall as a prey for these crimes.

4.2 Cloud computing and its services These days all small, medium and large companies are slowly adopting cloud services. In other words 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 are being brought up about their security. Cloud may provide immense opportunities but it should always be noted that as the cloud evolves so as its security concerns increase.

4.3 APT's and targeted attacks APT (Advanced Persistent Threat) is a whole new level of cyber crime 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.

4.4 Mobile Networks Today we are able to connect to anyone in any part of the world. But for these mobile networks security is a very big concern. These days 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 cyber crimes a lot of care must be taken in case of their security issues.

4.5 IPv6: New internet protocol IPv6 is the new Internet protocol which is replacing 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 very 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 regarding cyber crime.

4.6 Encryption of the code Encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it.. In an encryption scheme, the message or information is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be 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 being transferred via networks (e.g. the Internet, ecommerce), 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.

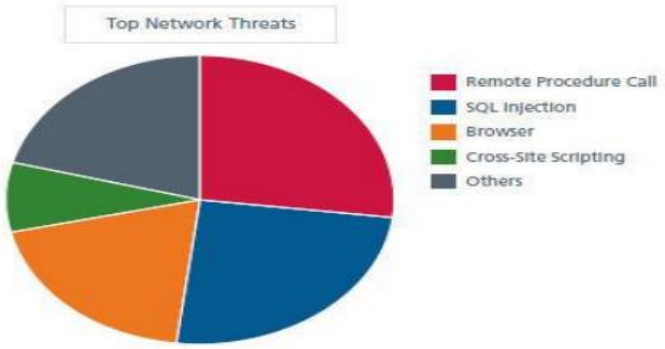

Fig -1

Fig -1 The above pie chart shows about the major threats for networks and cyber security.

5. CYBER ETHICS

Cyber ethics are 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. Email 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 others accounts using their passwords.
- Never try to send any kind of malware to other's systems and make them corrupt.
- Never share your personal information to anyone as there is a good chance of others misusing it and finally you would end up in a trouble.
- When you're online never pretend to the other person, and never try to create fake accounts on someone else as it would land you as well as the other person into trouble.

6. CONCLUSION

Computer security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. Cyber crime 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 platforms 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.

REFERENCES

1. Ali, A. 2001.Macroeconomic variables as common pervasive risk factors and the empirical content of the Arbitrage Pricing Theory. Journal of Empirical finance, 5(3): 221–240.

2. Basu, S. 1997. The Investment Performance of Common Stocks in Relation to their Price to Earnings Ratio: A Test of the Efficient Markets Hypothesis. Journal of Finance, 33(3): 663-682.

3. Bhatti, U. and Hanif. M. 2010. Validity of Capital Assets Pricing Model.Evidence from KSE-Pakistan.European Journal of Economics, Finance and Administrative Science, 3 (20).

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

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

6. 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