IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Cyber security: Issues and Emerging Trends

Mrs. Nagarathnamma S.M.

Assistant Professor, Department of Computer Science, G.F.G.C. K.R. Puram, Bangalore-560036.

Abstract:

An effective cybersecurity method employs multiple layers of defence spread across the networks, computers, programmes, or information that are intended to be non-toxic. To generate a real defence against or after cyber-attacks, a society's processes, people, and tools must all complement one another. The main objectives of the study are To know the importance of cyber security. To discuss about challenges and trends of cyber security. 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.

Keywords: Cyber Security, Web server, Malware, Ransomware etc.

Introduction

An effective cybersecurity method employs multiple layers of defence spread across the networks, computers, programmes, or information that are intended to be non-toxic. To generate a real defence against or after cyber-attacks, a society's processes, people, and tools must all complement one another. A unified threat management system can automate additions to select Cisco Security products and accelerate key security process functions such as discovery, examination, and remediation.

Cyber security refers to the techniques used to protect the user's cyber environment. This environment includes the user, devices, networks, applications, all software, and so on. Computer security is much more difficult now than it was previously. A computer system used to have a few dozen programmes.

Consumers must appreciate and obey with basic informations security ethics like selecting strong passwords, actuality wary of accessories in email, and back-up up data. Learn extra around basic cybersecurity values. Governments must have an outline for how they contract with together attempted and popular cyber attacks. Some well-respected outline can escort

you. It clarifies how you can recognise bouts, protect organisations, notice and reply to threats, and improve from successful occurrencesTechnology is vital to giving individuals and
organizations the system security tools wanted to protect themselves as of cyber attacks. Three chief objects essential be threatened: endpoint strategies like PCs, handheld devices, and routers; systems; and the cloud. Shared technology cast-off to defend these objects contain next-generation firewalls, DNS pass through a filter, malware defence, antivirus tools, and
email safety results.

Cyber might be distinct as somewhat connected to the collection of workstations or the network. At the same time, security means the mechanism of protecting anything. Consequently the terms Cyber and safety took organized define the way of defensive user informations on or after the spiteful attacks that might clue to the security break. It is the time that has been cast-off for a period back afterward the internet happening developing like
whatever. By asset of Cybersecurity, any society or any user can protected their critical data from hackers. However it is apprehensive with hacking at around point, it in fact used ethical hacking to contrivance Cybersecurity in any structure.

Objectives:

- To know the importance of cyber security.
- To discuss about challenges and trends of cyber security.

Importance of Cyber Security

Cyber crime is a term for any illegal activity that uses a computer as its primary means of commission and theft. The U.S. Department of Justice expands the definition of cyber crime to include any illegal activity that uses a computer for the storage of evidence. The growing list of cyber crimes includes crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism which have become as major problem to people and nations. Usually in common man's language cyber crime may be defined as crime committed using a computer and the internet to steel a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs. As day by day technology is playing in major role in a person's life the cyber crimes also will increase along with the technological advances.

Challenges and Emerging Trends

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.

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.

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.

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.

How does Cyber Security make working so easy?

No hesitation that the tool of Cybersecurity makes our work very easy by ensuring the obtainability of the capitals limited in any network. A commercial or society could look a huge damage if they are not honest about the safety of their online occurrence. In today's linked world, everyone aids from progressive cyber defence agendas. At a separate level, a cybersecurity outbreak can result in entirety from individuality theft, to blackmail attempts, to the damage of vital data similar family photographs. Everybody relies on dangerous structure like influence plants, infirmaries, and monetary service businesses. Securing these and other societies is essential to trust our civilization operative. One and all also remunerations from the work of cyberthreat investigators,

similar the team of 250 risk investigators at Talos, whoever explore new and developing fears and cyber bout policies. They disclose new susceptibilities, teach the community on the position of cybersecurity, and toughen open source gears. Their work marks the Internet harmless for one and all. Types of Cyber Security Phishing 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.

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.

Malware

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

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.

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

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. 1) Confidentiality Making uaranteed 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

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. 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. Here are few steps to maintain these goals 1. Categorising the possessions based on their position and precedence. The most important ones are kept back safe at all periods.

2. Holding down possible threats. 3. Determining the method of security guards for each threat 4. Monitoring any breaching activities and managing data at rest and data in motion.

5. Iterative maintenance and responding to any issues involved. 6. Updating policies to handle risk, based on the previous assessments.

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 cyber crimes but we should try our level best to minimize them in order to have a safe and secure future in cyber space.

References

Abadi and Needham, Prudent engineering practice for cryptographic protocols. IEEE Trans. Software Engineering 22, 1 (Jan 1996), 2-15, dlib.computer.org/ts/books/ts1996/pdf/ e0006.pdf or gatekeeper.dec.com/pub/DEC/SRC/researchreports/abstracts/src-rr-25.html.

CERT Coordination Center, CERT advisory CA-2000-04 Love Letter Worm, www.cert.org/advisories/CA-2000-04.html.

Denning, A lattice model of secure information flow. Comm. ACM 19, 5 (May 1976), 236-243.

Ellison et al., SPKI Certificate Theory, Oct. 1999, Internet RFC 2693, www.faqs.org/rfcs/rfc2693.html

Wobber et al., Authentication in the Taos operating system. ACM Trans. Computer Systems 12, 1 (Feb. 1994), pp 3-32, www.acm.org/pubs/citations/journals/tocs/1994-12-1/p3-wobber

ZDNet, Major online credit card theft exposed. ZDNet News, 17 Mar. 2000, www.zdnet.com/zdnn/stories/news/0, 4586,2469820,00.html