International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com
Volume 8, Issue 2, March - April 2019 ISSN 2278-6856

A Review Paper on Cyber Security and Cyber Crime

[1]Parul Doyla and [2]Kajol Mittal

[1]Scholar of Computer Science & Engineering,
ABES Institute of Technology, Ghaziabad,

[2]Assistant Professor, Department of Computer Science & Engineering
ABES Institute of Technology, Ghaziabad

Abstract:
Cyber security is the biggest treat as well as opportunity in the contemporary world. The exponential rise in the volume, veracity and variety of cyber-crime cases are matched with a significant increase in cyber security professionals. Cyber Security is a discipline which involves security of all its related resources. I have given a brief evaluation of cyber security and cyber crimes by reviewing some articles and research papers about cyber security and cyber-crime.Cyber-crime, or Computer oriented crime, is a crime that involves a computer and a network. The computer may be used in the commission of a crime, or it may be the target. Crimes that done against any person or an individual to gain the profit or to harm the reputation of the person or cause physical or mental harm to the person directly or indirectly, using modern technology i.e. Internet and mobile phones etc. And cyber security is the term used to protect a system from the theft and damage of their hardware,software and information as well as disruption and misdirection of a service.

Keyword:hacking, hacker, threats,vulnerability, exploits, server, crime against person, crime against property, crime against government, internet-basedthefts, sections etc.

INTRODUCTION

We know that the cyber-crime hacking, phishing, cracking and various forms of cyber frauds are increasing day by day that makes us necessary to deploy forces to protect our information system. This make people looking for security measures to protect their system from the unwanted threats.

TERMINOLOGIES

There are some common terminologies that we use when we talk about cyber security that are:

1. **Hacking**
   Hacking can be defined as unauthorized access to anyone's information system. It could be access to their computers, laptops, phones etc. we have number of examples of hacking in our daily lives. The most common is gaining access to someone's social account and modify it. And one common example is CCTV systems getting hacked to rob a bank.

2. **Hackers**
   We can say that hackers are "clever programmers". Hackers enjoy their work and never think work as an overload, sometimes the activities thatdone by hackers are for only enjoyment. There are number of tools that can be used by hackers for gaining access in a system. Computer virus, worms, back door programs and Trojans are some common tools.
   There are three types of hackers:

   2.1. **Black hat hackers:** Black hat does not mean that they wear a black hat. They called as crackers. They are expert programmers who break the security or gain access to the system without prior information. The work done by black hat hacker is always consider as a crime.

   2.2. **Grey hat hackers:** They gain access to the system without any prior permission but without malicious intent. They are mixture or we can say amalgam of black and white hat hackers.

   2.3. **White hat hackers:** White hat hackers are the security specialists who break into system with prior information. They have company permission for doing work on the system.

   2.4. **Script kiddie:** they are the hackers who learn about some tools from other sources and trying to work as a hacker.

3. **Vulnerability**
   In cyber security, this term means that a problem that exist in the system which the developer unaware of.

4. **Exploit**
   The process of practically exploring the vulnerabilities to a system is known as exploiting. Exploit is source code.
   There are three types of exploit
   a. **Remote exploit**
   b. **Local exploit**
   c. **Zero-day exploit**

5. **Zero-day attack/vulnerability**
   It is a undetected flaw in a software, hardware or application. As soon as the occurrence of such vulnerability is released to the public, the hackers deploy a source code attacking that vulnerability and since the authors of the application are

unaware of the fix this become a severe threat to the users of cyberspace.

6. **Insider threats**
Hackers who are either employees of an organization or outsiders posing as employees of an organization, threatening the information system of the organization.

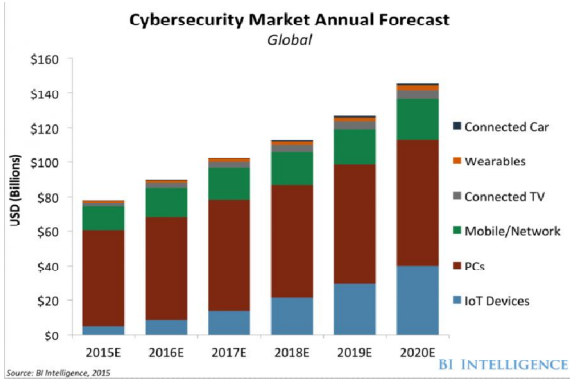

Figure 1 Cybersecurity Market Annual Forecast

DOMAINS OF CYBERSECURITY

1. **Risk Assessment:**
Cyber security risk assessment is very necessary for the protecting an organization's system. There are various threats that could the assets like hardware, laptops, customer information etc.

2. **Vulnerability Assessment:**
The companies perform vulnerability assessment for the safety of their system. With the help of large number of tools companies scan their network and find the problems and then solve it.

3. **Penetration testing**
It basically the practice of exploiting a bug and discovering the depth of the problem to find out exactly what type of information could be revealed if the website was exploited.

4. **Application Security**
Security simply means granting authorized access to the protected data and refusing access to unauthorized access. There are two software testing methods i.e. white box testing and black box testing

5. **Infrastructure security**
It is known as one of the developed disciplines of cyber security. It is the security provided to safeguard infrastructure,principally critical infrastructure etc.

6. **Social Engineering**
It is a practice in which a person is manipulated by the hacker to give confidential information for breaking any security.
This can be done by mails, SMS and videos etc.
The common attacks of social engineering are
   a. **Email from a friend**
   b. **Phishing attempt**
   c. **Baiting attempt**

JOB OPPORTUNITIES

If a person is technically strong, familiar to the tools that are used in cyber security, knowledge of operating systems and person is up to date with new technologies then he has many jobs not only in private but government also give them good package etc.

1. **Security testing**
2. **Cyber forensics**
3. **Threat intelligence**
4. **Bug bounty**
5. **Security researcher**

THREATS TO CYBER WORLD

They can be classified as IT based threats and non-IT based threats.

NON-IT THREATS

Some of them are due to different resources belonging to information technology and some arises from environment.

1. Physical Damage
Threats that inflict physical damage to the information system are classified as physical threats. Fire breakouts, short circuits, theft, water flooding or clogging are some of the physical threats to an information system.

2. Natural disasters
There are threats to the information systems that human being does not have no control over. The disastermakes information or data loss to an information system. The natural calamities are Earthquakes, Floods and cyclones.

IT THREATS

IT threats to information system is one which targets IT system through different attack vectors.

1. **At Server**
This attack is most common attack to the IT system and it also said as a most successful attack to the IT system.

   a. **Application Server**
   There are number of ways to target a application server
   i. ARP spoofing
   ii. Botnet
   iii. Cache poisoning

iv. Computer Worm
v. Key logger
vi. Malware
vii. Rootkit
viii. Unpatched servers

b. File Server

File server can be targeted in various ways, the actual attack principle may change but methods remain same.

The common attacks are mentioned below:

I. Bounce attack at FTP
II. Packet sniffing
III. Spoof Attack
IV. Port Stealing

c. Database server

Database server is affected by the threats like SQL injection where an attacker through a query.

There are various methods used in

1. Excessive Privilege Abuse
2. Platform Vulnerabilities
3. SQL Injection
4. Database Rootkits

2. ON User

Users are the weakest link in an organization as they unwillingly disclose the information.

SOCIAL ENGINEERING

It is an IT based threat in which attacker gain information regarding a user's credentials etc. through manipulation.

Types of social engineering

i. Technology based Social Engineering
ii. Human based Social Engineering

INSIDER THREATS

User and Employees can be a threat to a company or a service.

PHASES OF HACKING

1. **Footprinting**
2. **Scanning**
3. **Gaining Access**
4. **Maintaining Access**
5. **Clearing Tracks**

CYBER LAWS

Cyber laws are associated with establishing the rules and regulations governing the use of cyber space in a country. Cyber laws, like any other law, are specific to a nation. Cyber laws define the legal framework of using the internet, computers, routers and other IT enabled devices.

CYBER CRIMES

Crime against person

Crime against property

Crime against government

1. **Crime against people**

a. Cyber Stalking
b. Harassment via email
c. Dissemination of Obscene material
d. Hacking
e. Defamation
f. Cyber bullying
g. Cracking
h. Email spoofing
i. SMS spoofing
j. Carding

2. Crime against Property

a. Intellectual Property crimes
b. Cyber Squatting
c. cyber vandalism
d. Hacking Systems
e. Internet-based Time Thefts

3. Crime against government

a. Cyber Terrorism
b. Pirated Software
c. Acquiring Unauthorized Information

4. Crimes Targeting the society

a. Cyber Trafficking
b. Child pornography
c. Online Gambling
d. Financial Crimes
e. Forgery

STATISTICS OF CYBER CRIME

The global cyber-crime cost will reach $2 trillion by the year 2019, much more increased from the 2015 approximation of $500 billion.

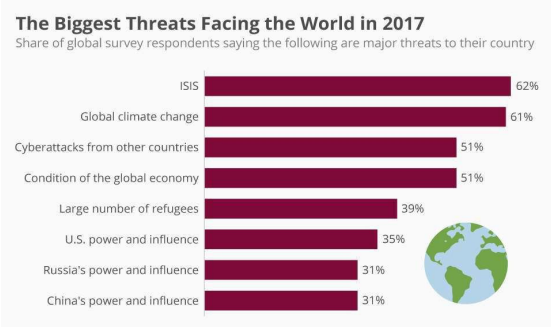

Figure 2 THREATS FACING THE WORLD

INDIAN CYBER LAWS

The act essentially dealt with-

i. Legal recognition of Electronic Documents
ii. Legal recognition of Digital Signatures
iii. Offenses and Contraventions
iv. Justice Dispensation System for Cyber Crimes

INFORMATION TECHNOLOGY ACT

1. Penalties, Compensation and Adjudication sections

Section 43A- Compensation for failure to protect data

Section 44-Penalty for failure to furnish information or return, etc

Section45- Residuary Penalty

Section 47- factors to be taken into account by the adjudicating officer

2. Offenses sections

Section 65
Section 66
Section 66A
Section 66B
Section 66C
Section 66D
Section 66E
Section 66F Cyber Terrorism
Section 67 – punishment for publishing or transmitting obscene material in electronic form
Section 67B – punishment for publishing or transmitting of material depicting children in a sexually explicit, etc. in electronic form
Section 69 – Powers to issue directions for interception or monitoring or decryption of any information through any computer resource
Section 69A- Power to issue direction for blocking for public access of any information through any computer resources
Section 69B- Power to authorise to monitor and collect traffic data or information through any computer resources for cyber security
Section 71- Penalty for misrepresentation
Section 72- Breach of confidentiality and privacy
Section 72A- the penalty for publishing electronic Signature Certificate false in certain particulars
Section 74- publication for the fraudulent purpose
Section 75- act to apply for offence or contraventions committed outside India
Section 77A- Compounding of Offences
Section 77B- Offences with three years imprisonment to be cognizable
Section 78- Power to investigate offences

CONCLUSION

We can say that people should be aware about the cyber laws in a society that is dependent more and more on this technology. The criminal activities based on electronic devices are the main concerned in cyber security. As we all know that time increasing our demand of cyber security. now a days everything isdepend to the technologies which indirectly means that on the system so that the security of the system is most important for securing it government make many laws.We need cyber security in every hour of our day.

REFERENCES

[1.] Lim B (2014) Aviation security – emerging threats from cyber security in aviation – challenges and mitigations. J AviatManag
[2.] Lykou G, Anagnostopoulou A, Gritzalis D (2018) Implementing cyber-security measures in airports to improve cyber-resilience, WIIoTS in the 2nd global IoT summit.
[3.] CANSO (2014) Cyber security and risk assessment. Civil Air Navigation Services Organization
[4.] Kumar S, Xu B (2017) Vulnerability assessment for security in aviation cyber-physical systems. IEEE 4th international conference on cyber security and cloud computing
[5.] Lim B (2014) Aviation security – emerging threats from cyber security in aviation – challenges and mitigations, J AviatManag
[6.] Stander A, Ophoff J (2016) Cyber security in civil aviation
[7.] Jeyakodi D (2015) Cyber security in civil aviation
[8.] International Civil Aviation Organization (ICAO) (2017) Aviation security manual, 10th edition