Nizami et al.LGU (IJECI) 2017

LGU (IJECI)
ISSN: 2522-3429

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol.1 issue1 Oct-Dec 2017

The Reality of Cyber Security

Syeda Marrium Nizami[1] and Gulfraz Naqvi[2]
Lahore Garrison University
mariyum002@yahoo.com[1,], gulfraz.naqvi@gmail.com[2]

Abstract

The purpose of this article is to provide information about cyber security. It gives an analysis that would be useful in taking measure to prevent attacks. The judgment of this analysis is made by expertise and knowledge of databases, hardware, encryption, networks, and firewalls. Moreover it will give users an idea about how to keep computer system running smoothly, which ensures that they are considering such actions which could prevent them from their data being theft or financial information being stolen. Further the article gives an insight view about the techniques, which could restrain intruder from accessing, and revealing user's personal information.

Keywords: cybercrime, cyber-terrorism, cyberspace, cyber attacks, Cyber war, cyber terrorism

1. Introduction

IInformation is power. [1] Nowadays cyber security is the submissive compulsory and the upper most priority of government. The request of cyber security for sparing foundation has expanded to a considerable measure, to a degree where government has made its need to manage cyber dangers by upgrading cyber security. Increased the assurance of consumers, ensure the likelihood of requesting system on which our subsidence can depend, and enhance national security all these things depends on Cyber security. [2] However, to preserve privacy, freedom, alteration, and the motivating nature of the Internet cyber security achievements must be attentively mended set. Each part of the country's critical framework must be considered independently to design an active and fair cyber security strategy.

General, cyber terrorism has been defined as the use of computers and the internet to engage in terrorist activity [3]. The new daring challenges for the legal world are pose growing with the Inventions, discoveries and technologies that broaden scientific horizons. New difficulties in legal matters are posed by the Information Technology that are brought by computers, the Internet, and cyberspace. While managing the Information innovation, it has demonstrated the lack of law. With regards to Information innovation still there is appropriate need of enactment to manage cybercrime issues.

On the off chance that harsh arrangements are played out the highlights have made the web an accomplishment that, it scatter and a nature in which it is controlled by the client, and its support for modernization and free-form might be in risk. On the off chance that low approach of supporting the highlights of web is viewed as it's an accomplishment in itself, which is extremely various and controlled by the clients. Despite the fact that this strategy if offering control to the client backs the belief system of innovation, yet it can be a wellspring of danger to the general public.

Cold War, corruption, violation, civil crime and terrorist activities are classical approaches that arises in our surrounding and those act cause physical damage to an individual. The fundamental difference between those approaches of crimes and cybercrime, or cyber warfare or cyber terrorism is of the “cyber” adjunct. Here cyber war refers to the battle in cyberspace and includes cyber attacks against a nation state and defect critical infrastructure of casting communication network. Psychological warfare is executed when the utilization of the internet is shown by the digital fear mongering. Digital psychological warfare is executed when fear based oppressors have determined the internet. It is generally known to mean wrongful strikes and dangers of assault against PCs, systems and the data put away in that when done to threaten or pressure an administration or its kin to encourage political or social targets. The motivation behind cyber Terrorism is to assault basic foundation, including sites, organizes, and to take data from these Critical Infrastructures to pressurize the legislature and its kin to accomplish political, social or money related goals. The goal of most of the cybercriminals is to achieve monetary awards against the computer-related corruption.

2. Threats from Cyber crime

Respectively, from the point of view of Information security, a threat can be explained as the possibility that can cause something unpleasant or violent, an unwanted incident that can harm an asset, system or organization. Basically there are three basic origins of the threat:

- Intentional threat
- Accidental threat
- Environmental threat

The use of malicious software or illegal software are the examples of intentional threats. The errors that are caused because of the failure of the hardware, or because of the error in design made by the human or because of service failure are the examples of Accidental threats. On the other hand lightning, thunderstorms or earthquakes are the examples of environmental threats. We can get rid of all these threats or can at least minimise these threats to great level, by taking some efficient steps and actions to confine the harmful affect within each organisation. Threats in whatever way, if not correctly managed, can produce an undesired influence on socio-economy and security of human lives.

3. Cheap method

Conventional, space and cyber- warfare are the categories of the dimension of warfare. Cyber warfare is cheap. Conventional warfare and space warfare are expensive. To many groups and individuals it is easily accessible. There are many individuals who have these capabilities and abilities to undermine the critical infrastructure of the state. Whereas cyber warfare allows asymmetric warfare. The intensity of the destruction caused by the cyber warfare could be similar to the conventional war, as if someone get access to personal computer of a victim through internet, it is inexpensive in contrast to the cost of making, maintaining and using advanced military capabilities that's why it is very pleasant for many of the attackers to use this strategy to harm other nations.

Nowadays less technical knowledge is required and the more of hacking tools and techniques are utilised by the hackers in order to achieve the hacking goals, these tools and techniques are becoming more powerful than ever before. Furthermore, on Internet all of these tools are accessable, which is easier to use, at a very low cost or are free of charge in some occurrences.

Having finite potential and insufficient prospects with great possibility of being caught, there are known threats. Having several potentials and broad fortuity and provide low possibility of being caught, there are also emerging threats. These are some of the difficulties we face in today's world.

4. Case History

Till the day regularity bodies either from academic end or from internal legal body have failed to reach to the consensus to define "terrorism" [4].

Different organisations have defined terrorism in a different way, either its relevant to the government body or any other legal system. Since it's not yet properly defined in every part of the world and international community is slow to reach any conclusion which is agreed universally, this act is emotionally and politically charged in different circumstances.

Various legal systems and government agencies use different definitions of 'terrorism'. Moreover, the international community has been slow to formulate a universally agreed upon, legally binding definition of this crime. These difficulties arise from the fact that the term 'terrorism' is politically and emotionally charged. [5] There are several case histories of cyber threats recorded:

4.1 The Japanese government experienced a Cyber-attack Use of Styles

According to a report on 4 Aug 2004, the Japanese government's computer systems were under attack. Almost synchronously, eight of the Japanese government agencies' computer networks were disordered, in telecommunication terms that are furthermore known as barrage jamming. The damaged networks were not available for a few hours and sock networks experienced rejection-of-service attacks.

4.2 For hours, hackers congest the US customs' computers

In August 2005, the case was reported where thousands of people were concerned by the viruses that have made the US Customs and Border Protection system victim for certain hours.

The attack took place on the computers, which were placed on Huston, Miami, New York, Los Angeles, and few other airports, the viruses left a heavy burnt.

4.3 Hacker's attack on Estonia's Critical Infrastructure.

Among many dark days of the cyber world the history will remember those three weeks when Estonian critical infrastructure systems were under attack by the hackers, who have hijacked critical infrastructure system of Estonia in May 2007, and have completely disturbed the government, banking, media and police websites, the attacks disabled Internet communications as online transactions were disturbed heavy economic trouble were obtained.

4.4 Russia and Georgia Cyber-warfare

In August Russia's aggression of Georgia had moved into cyberspace as the Russians educated to annoy and achieve candid routing calculated for Georgia.

It is said that the network traffic to Georgia was hijacked by the Russians and changed the path to their attendant. Many Internet servers were under the command and control of Russia there were many Internet servers of Georgia.

Network to a dead lock. This was a simple example of framework attack. To resolve this issue the concerned agencies took three months to eradicate this.

4.5 Cyber-attack on Malaysian Critical Infrastructure

Malaysia's Internet framework was invaded by the Code Red worm, in 2001. They have injected a worm, which had spread in their system very rapidly and brought national communication down.

The approximate minimum losses was RM22mil, which does not includes the losses to the business fraternity and other sectors.

Then later in 2003 the worm by Blaster and Naachi was another mishaps to the Malaysian Critical Infrastructure. The cause of the Incident is the Nacchi worm, which has propagated by the blaster worm in scanning machines through network for vulnerability assessment. This vulnerability found was inly found in the Windows NT, 2000 and XP software were exploited by these worms. The approximate loss was RM31mil, which does not include loss of productivity and the cost of lost opportunity was estimated cost to eradicate this worm .

4.6 Modern hostilities

Whenever there is conflicts between

countries nowadays, cyberspace is the new war frontier. The disfigurement of websites is a popular method of a cyber attack. A website is "vandalized" when a wicked activity like Web defacement is applied. Often the site's original content are replaced with a political or social messages the hacker. Hacker may delete all the content available on the site considering the security accountability of the site. A good example to illustrate this scenario is conflict between US-China in May 2001, which resulted after a Chinese fighter was misplaced at sea from an incident after colliding with a US naval reconnaissance plane.

5. Conclusion

In conclusion, the threats that have taken birth because of the internet or generally because the computer are presenting a difficulty of today and the coming tomorrow. A comprehensive manner of actions are required to address them. A country standing alone cannot deal with the cyber threats. To deal with threats and sensitivity in the cyber world there is a need to have strategic connection. To intensify the security of cyberspace Coordination and collaboration from all parties is very consequential.

6. References

1 See Cybersecurity, Civil Liberties and Innovation: Hearing Before H. Comm. on Energy and Com., 111th Cong. (2009) (statement of Gregory T. Nojeim), available at http://www.cdt.org/security/20090501_cybersecurity.pdf; Cybersecurity: Preventing Terrorist Attacks and Protecting Cyberspace: Hearing Before S. Comm. on the Judiciary, Subcomm. on Terrorism and Homeland Security, 111th Cong. (2009), available at http://www.cdt.org/files/pdfs/20091117_senate_cybersec_testimony.pdf.

2 Crime in India: 2011-Compendium (2012), National Crime Records Bureau, Ministry of Home Affairs, Government of India, New Delhi, India.

3 Clay Wilson, Cong. Research Serv., RL32114, "Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress 5 (2005)", (Wilson argues that defining any particular act as Cyberterrorism is problematic because of the inherent difficulties in determining the attackers identify, motive and intent, but recognizes the potential for Cyberterrorism). Available on http://www.dtic.mil/get-tr-doc/pdf?AD=ADA44479, Retrieved on 12 March, 2009.

4 Myra Williamson, *Terrorism, War and International Law: The Legality of the Use of Force against Afghanistan in 2001*. p. 38, Ashgate Publishing. United Kingdom, 2009.; Alex P. Schmid, *The Definition of Terrorism.* p. 39, *The Routledge Handbook of Terrorism Research.* Routledge, 2011.

[5] Bruce Hoffman, *Inside Terrorism*, p. 32, 2nd ed., Columbia University Press, 2006, p. 32, See review in The New York Times, Inside Terrorism, Available on http://www.nytimes.com/books/first/h/hoffman-terrorism.html. Retrieved on 11 February 2012. Cited in “Cyber-Terrorism: Finding a Common Starting Point” by Jeffrey Thomas Biller, to The Faculty of The George Washington University Law School.