Available Online at http://www.journalajst.com

ASIAN JOURNAL OF SCIENCE AND TECHNOLOGY

ISSN: 0976-3376

Asian Journal of Science and Technology
Vol. 08, Issue, 05, pp.4712-4714, May, 2017

RESEARCH ARTICLE

NOVEL DESIGN OF TREND IN CYBER SECURITY AS AN INTEGRATED APPROACH

[1]Sandeep Kulkarni and [2,*]Dr. Yadav, K. P.

[1]R/S Himalayan University, Arunachal Pradesh, India
[2]IIMT College of Engineering, Greater Noida, India

ARTICLE INFO

Article History:
Received 02nd February, 2017
Received in revised form
21st March, 2017
Accepted 17th April, 2017
Published online 17th May, 2017

Key words:

Botnet, Malware,
Virus,
Cryptography,
Network Security.

ABSTRACT

In the present day world, World has witnessed an huge increase in Cyber crimes whether they pertain to Trojan attacks, salami attacks, e-mail bombing, DOS attacks, information theft, botnets, phishing, exploiting vulnerabilities or the most common offence of hacking the data or system to commit crime. Cyber crime refers to the act of performing a criminal act using computer or cyberspace (the Internet network), as the communication vehicle. Though there is no technical definition by any statutory body for Cyber crime, it is broadly defined by the Computer Crime Research Centre as - "Crimes committed on the internet using the computer either as a tool or a targeted victim." All types of cyber crimes involve both the computer and the person behind it as victims; it just depends on which of the two is the main target. Cyber crime could include anything as simple as downloading illegal music files to stealing millions of dollars from online bank accounts. Cyber crime could also include non-monetary offenses, such as creating and distributing small or large programs written by programmers called viruses on other computers or posting confidential business information on the Internet.

INTRODUCTION

Here we shall see various types of cyber crimes:

Online Banking: As a customer you may be seen as a potential target for fraudulent activities. Such as:

Credit/Debit card fraud: The creation and/or alteration of a credit/debit card occurs when the information contained on the magnetic strip is reproduced. Protect your credit/debit card: Memorise your personal identification number (PIN).

Cheque fraud: Using false invoices to get legitimate cheques**.** Depositing a cheque into a third party account without authority.

Protect yourself from cheque fraud: Reconcile your accounts promptly and regularly. Email scams and fake websites: The purpose of these websites is to obtain your log on details to access your bank accounts. Others communicate security messages and advise you to install software from the email that checks and removes viruses. By downloading the software you are in fact tricked into downloading a virus. Botnet is a number of Internet-connected computers autonomously communicating with other similar machines in which components located on networked computers communicate and coordinate their actions by command and control (C&C) or by passing messages to one another. Botnets have been used many times to send spam email or participate in distributed denial-of-service attacks. Malicious software, commonly known as malware, is any software that brings harm to a computer system. Malware can be in the form of worms, viruses, trojans, spyware, adware and rootkits, etc., which steal protected data, delete documents or add software not approved by a user.

Denial-of-service attack

In computing, a denial-of-service attack (DoS attack) is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. Some Malwares like Spida Network Worm, Blaster Worm, Sasser, Trojan horse, Root kit, Spyware, Spam, Drug trafficking, Cyber terrorism, SMS Spoofing, Cyber squatting, Cyber vandals, Computer transmitting virus, Computer Tresspass, Online gambling.

****Corresponding author: Dr. Yadav, K. P.,***
IIMT College of Engineering, Greater Noida, India

Prevention: Well, the most important step would be to educate people on how to protect themselves (privacy) from being intrusively invaded by cyber criminals. Secondly the employees need to be trained on how to protect their work. the 5P mantra for online security: Precaution, Prevention, Protection, Preservation and Perseverance. It is better to use a security programs by the body corporate to control information on sites.

Data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud. Cyber-Crime-Securities-Markets-and-Systemic-Risk

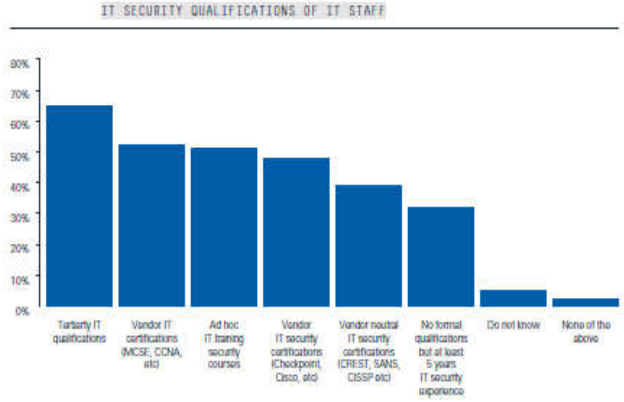
Network Security: Improved ECC algorithm based on network information security, the algorithm based on the original ECC algorithm and its optimization dot product operation optimization and square residual determination, optimization and transformation of the private key update to improve the original operational efficiency and safety performance of the ECC algorithm.

Cloud computing: can provide security services to end users, using the PIF algorithm to describe the process of the detection and analysis of suspicious files, optimized distributed CFO algorithm is used in the cloud computing distributed environment, and through the integration of neural network to realize the classification of suspicious files.

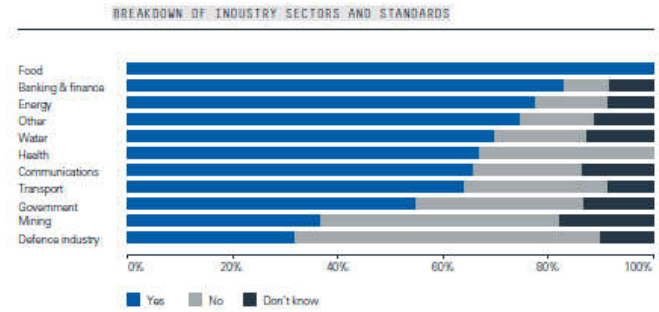
Cryptography: is a concept to protect network and data transmission over wireless network. Applications of cryptography include ATM cards, computer passwords, and electronic commerce. The development of the World Wide Web resulted in broad use of cryptography for e-commerce and business applications. Cryptography is closely related to the disciplines of cryptology and cryptanalysis.

Survey based on business and what security measures they have taken(2012)

Responses indicated that 65% of participating organisations had IT security staff with tertiary level IT qualifications. More than 50% of participating organisations had IT security staff with some type of vendor based IT certifications. Almost 35% of participating organisations had IT security staff with no formal training, although most of these staff had more than five years working in the IT security industry.

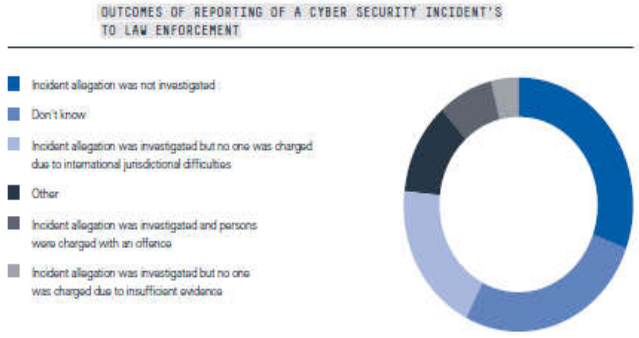


Security Standard: Overall, 64% of respondents reported their organisation did apply IT security standards or guidelines. Of the remaining respondents, 25% reported their organisation did not apply IT security standards or guidelines, and 11% did not know. These findings are a concern and warrant future investigation.



Motives for the Attacks

Interestingly, more than half the respondents viewed the attacks to be targeted at their organisation – with motives being illicit financial gain (15%), hactivism (9%), using the system for further attacks (9%), using the system for personal use (6%), being from a foreign government (5%), personal grievance (5%), and being a competitor (4%).



Cyber attacking techniques

Cracking
Key logging
Electronic funds attacks
Denial of service attacks
Botnets attacks
Hoax email
Malware
Xxs and csrf attacks

Pharming
Phishing,smishing and vishing
Website defacement
Spoofing
Salami attacks
Misinformation spread
Firewalls and anti-virus
Anti-DNos and ANti-bot detection systems
Intrusion prevention systems(IPS)(often combined as intrusion detection and prevention systems).
Clean pipe solutions
End-point security

Terminal safety controls

Proactive defence-in-depth
Penetration testing,ethical hacking and simulations.regular training exercises on social engg techniques
Vulnerability assessment
Internal and external audits
Data encryption
Counter attacks
Air-gapping or partial air-gapping

Conclusion

In conclusion, computer crime does have a drastic effect on the world in which we live. It affects every person no matter where they are from. It is ironic that those who in secret break into computers across the world for enjoyment have been labeled as deviance. Many hackers view the Internet as public space for everyone and do not see their actions as criminal. Hackers are as old as the Internet and many have been instrumental in making the Internet what it is now. In my view point hacking and computer crime will be with us for as long as we have the Internet. It is our role to keep the balance between what is a crime and what is done for pure enjoyment. Luckily, the government is making an effort to control the Internet. Yet, true control over the Internet is impossible, because the reasons the Internet was created. This is why families and the institution of education of is needed, parents need to let their children know what is okay to do on the computer and what is not and to educate them on the repercussions of their actions should they choose to become part of the subculture of hackers. In finishing this paper, the true nature of what computer crime will include in the future is unknown. What was criminal yesterday may not be a crime the next day because advances in computers may not allow it. Passwords might be replaced for more secure forms of security like biometric security.

Most of the recorded computer crimes cases in most organization involve more than individual and virtually all computer crime cases known so far are committed by employer of the organization. Criminals have also adapted the advancements of computer technology to further their own illegal activities. Without question, law enforcement must be better prepared to deal with many aspects of computer-related crimes and the techno-criminals who commit them.

REFERENCES

An Improved Weighted Clustering for Ad-hoc Network Security New by Basant Kumar Verma and Binod Kumar, 2015
An Introduction to Cyber Crime and Cyber Law.Author(s) : Dr R K Chaubey
Aparna Viswanathan Cyber Law
Cyber Crime – A Threat to Persons, Property,Government and Societies by Er. Harpreet Singh Dalla, Ms. Geeta ,2013
Cyber Crime and Corporate Liability.Author(s) : Rohas Nagpal
Cyber Crime and Cyber Security: A White Paper for Franchisors, Licensors, and Others by Bruce S. Schaeffer, Henfree Chan,Henry Chan and Susan Ogulnick
Cyber Crime and Research paper 2013
Cyber Crime and Security Survey Report 2012
Cyber Crime Criminal Threats From Cyberspace.Author(s) : Susan W Brenner
Cyber Crime Research,Presentation by the Australian Institute of Criminology by Dr Russell G Smith Principal Criminologist
Cyber-crime, securities markets and systemic risk by Rohini Tendulkar , 2013
Cybercrime: A threat to Network Security by Ammar Yassir and Smitha Nayak , 2012
Network Security with Cryptography by Prof. Mukund R. Joshi, Renuka Avinash Karkade , 2015
Network Security: Hybrid IDPS by Youssef Senhaji and Hicham Medromi , 2015
Research on Computer Network Virus Defense Technology in Cloud Technology E18] Computer Network Security and Attacks on Wireless Sensor Network,Hacking issues by Sonal R.Jathe ,Dipti S. Charjan, Pallavi A.Patil,2016
Research on Improved ECC Algorithm in Network and Information Security
Software Vulnerabilities, Banking Threats, Botnets and Malware Self-Protection Technologies by Wajeb Gharibi1, Abdulrahman Mirza, 2011.

****