INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

CYBER ATTACKS AND IT'S COUNTERMEASURES

AUTHORED BY - MITALI VASISHTHA & SHIVANGI SINHA

Abstract

Nowadays, the majority of international relations, commerce, economics, culture, social contact, and government at all levels—involving individuals, non-governmental organizations, governments, and governmental institutions—take place online. Cyberattacks and the risk associated with wireless communication technology have become major issues for several government agencies and commercial businesses worldwide in recent times. The modern world relies heavily on electronic technology, and safeguarding this information against cyberattacks is a difficult problem. The intention of cyberattacks is to financially damage businesses. Cyberattacks may also serve political or military objectives in other circumstances. Computer viruses, knowledge gaps, data distribution services (DDS), and other attack vectors are a few examples of these harms. To this goal, different companies employ different strategies to stop the harm that comes from cyberattacks. Cybersecurity keeps up with the most recent IT data in real time. Researchers from all across the world have so far put out a number of strategies to stop cyberattacks or lessen the harm they inflict. While some of the approaches are at the study stage, others are in the operational stage. This study aims to analyse the difficulties, shortcomings, and strengths of the suggested approaches as well as to evaluate and thoroughly review the standard advancements in the field of cyber security. Various new descendent attack kinds are thoroughly examined. The history and first-generation cyber-security techniques are covered together with standard security frameworks.

Introduction

Several digital gadgets and the internet that powers them have made life much more comfortable in today's world. Like anything wonderful, there is a dark side to modern technology. This is also true with digital. Although the internet has improved our lives, safeguarding your data has become much more difficult as a result of it. Cyberattacks are a result of this.

ISSN: 2582-6433

Cyber-attacks are when someone gains illegal access to a system or network. Hackers or attackers are those who carry out cyberattacks.

Hackers can do harm in a number of ways. Data loss or manipulation may arise from the execution of an attack that results in data breaches. Businesses suffer reputational harm, financial losses, and deterioration of consumer confidence. We employ cybersecurity in order to stop cyberattacks. Keeping computers, networks, and their parts safe from unwanted online access is known as cybersecurity.

Cybersecurity has suffered because of the COVID-19 problem as well. Interpol and the World Health Organization report that the COVID-19 epidemic has resulted in a substantial rise in cyberattacks.

Types Of Cyber Attacks: -[1]

1.Malware attack

One of the most typical kinds of cyberattacks is this one. Malicious software viruses, such as worms, spyware, ransomware, adware, and trojans, are referred to as "malware". The trojan infection poses as trustworthy software. Whereas spyware is software that secretly collects all of your private information, ransomware prevents access to the network's essential components. Adware is software that shows banner ads and other forms of advertising on a user's screen. A vulnerability allows malware to infiltrate a network. When a person uses an infected pen drive or clicks on a risky link, an email attachment is downloaded.

Now let's examine ways to stop a malware attack:
Employ antiviral protection. It has the ability to defend your computer against malware. Among the well-known antivirus programs are Avast, Norton, and McAfee.

Utilize firewalls. Traffic that may reach your device is filtered by firewalls. The built-in firewalls that come pre-installed on Windows and Mac OS X are called Windows Firewall and Mac Firewall, respectively.

[1] Tietsort, J.R. (2023a) 17 most common types of cyber attacks & examples (2024), RSS. Available at: https://www.aura.com/learn/types-of-cyber-attacks (Accessed: 17 January 2024).

ISSN: 2582-6433

Remain vigilant and refrain from clicking on shady links.
Regularly update your browsers and operating system.

2. Phishing Attack

Phishing attacks are among the most well-known and often occurring categories of cyberattacks. This is a kind of social engineering assault in which the perpetrator poses as a reliable contact and sends fictitious emails to the target.

Unaware of this, the victim opens the email and opens the attachment or clicks on the malicious link. Attackers are able to obtain account passwords and private data in this way. Via a phishing attempt, they may potentially install malware.

The actions listed below can help avoid phishing attacks:
Examine every of the emails you get. Significant flaws, such as misspellings and formatting variations from reliable sources, are included in the majority of phishing emails.
Use a toolbar that blocks phishing scams.
Frequently change your passwords.

3. password attack

It is a type of attack where a hacker uses programs and password-cracking tools such as Aircrack, Cain, Abel, John the Ripper, Hashcat, etc. to break your password. Keylogger, dictionary, and brute force assaults are a few of the several kinds of password attacks.

A few strategies to stop password assaults are given below:
Make secure, distinctive character-filled alphanumeric passwords.
Never use the same password on more than one website or account.
You may reduce your vulnerability to a password assault by updating your passwords.
Don't leave any password clues visible.

4. Man in the middle

Eavesdropping attacks are often referred to as Man-in-the-Middle (MITM) attacks. This attack involves the interception of a communication between two parties by an attacker, who then takes control of the session between the client and the host. Hackers pilfer and alter data in this way.

ISSN: 2582-6433

It's evident from the image below that the hacker is acting as a middleman in place of the client-server connection.The following procedures can be used to stop MITM attacks:

Keep in consideration the website's security while you browse it. Employ encryption on all of your gadgets.

Avoid utilizing WIFI networks that are open to the public.

5. SQL Injection Attack

When an attacker modifies a conventional SQL query, a database-driven website is subjected to a Structured Query Language (SQL) injection attack. The method of carrying it out involves inserting malicious code into a search box on a vulnerable website, forcing the server to divulge important data.

Consequently, the hacker gains access to the databases' tables for viewing, editing, and deleting. This can also provide attackers administrative privileges.

A SQL injection attack can be avoided by:

Detect unwanted network access by using a system for intrusion detection, which is intended for this purpose.

Validate the data that was provided by the user. It takes the user input under control using a validation procedure.

6. Denial-of-Service Attack

One serious danger to businesses is the Denial-of-Service Attack. To use up all of the resources and bandwidth available to them, attackers flood servers, networks, and systems with traffic.

It is at this point that the servers are unable to handle the influx of requests and the website they host either crashes or experiences a slowdown. The rightful service requests go unanswered as a result.

When attackers employ several hacked systems to initiate this assault, it is also known as a DDoS (Distributed Denial-of-Service) attack.

Now let's examine defence strategies against DDoS attacks:

ISSN: 2582-6433

To find malicious traffic, do a traffic analysis.

Recognize the warning indicators, such as sporadic website shutdowns and sluggish networks. The company has to act quickly in these situations to take the appropriate action.

Create a checklist, ensure that your staff and data centre are prepared for a DDoS assault, and develop an incident response strategy.

Contract out the defence against DDoS attacks to cloud service providers.

7. Insider Threat

Insiders pose a threat to others, as the word implies, but they do it from within. Under these circumstances, it can be someone who works for the company and is well-versed in its operations. The potential for enormous harm from insider threats is present.

Since small firm employees have access to several accounts containing data, insider threats are common there. This type of attack can be caused by a variety of factors, such as recklessness, avarice, or malice. Insider threats can be problematic since they are unpredictable.

To stop the assault by an insider threat:
There should be a strong security awareness culture within organizations.

Businesses need to restrict employee access to IT resources based on their job functions.

Employees must be trained by organizations to recognize insider risks. This will make it easier for staff members to recognize when an attacker has altered or trying to abuse data belonging to the company.

8. Crypto Jacking

The word "crypto jacking" has a tight connection to cryptocurrencies. The act of hackers breaking into another person's computer to mine bitcoin is known as crypto jacking.

By tricking the target into clicking on a malicious link or infecting a website, access is obtained.

ISSN: 2582-6433

They do this by using JavaScript code in web advertisements. The only indication victims may notice is a pause in the execution of the crypto mining code, which operates in the background and is invisible to them.

The following actions can be taken to stop crypto jacking:
Since crypto jacking may infect even the most vulnerable computers, update all of your security programs and software.

Employees should get training on crypto jacking awareness since this will enable them to recognize potential risks.

Ads are a major source of crypto jacking programs, so install an ad blocker. possess add-ons like as Miner Block, which detects and prevents cryptocurrency mining programs.

9. Zero-Day Exploit

When a network vulnerability is announced, a Zero-Day Exploit occurs; often, there is no fix for the issue. Hence the seller discloses a flaw so that consumers are aware; unfortunately, the information also reaches the perpetrators.

The vendor or developer may need some time to address the vulnerability before a solution is provided. The revealed vulnerability is the attackers' focus in the meantime. They take care to take advantage of the vulnerability even prior to the implementation of a patch or other fix.

One way to stop zero-day exploits is to:
Organizations must to have clear and concise procedures for managing patches. Automate the processes by utilizing management solutions. Deployment delays are therefore avoided.

To assist you in handling a cyberattack, create an incident response strategy. Maintain a zero-day attack-focused approach. Damage can either be minimized or prevented entirely by doing this.

10. Watering Hole Attack

Here, a certain group inside an organization, area, etc. is the victim. Websites that are often visited by those who are being targeted are the focus of this type of assault. Websites are found by

ISSN: 2582-6433

guesswork or by keeping a close eye on the group.

Following this, the attackers use malware to infect these websites and the PCs of the victims. In an instance like this, the spyware goes for the user's private data. Here, the hacker may also be able to access the compromised machine remotely.

Now let's examine how to stop the watering hole attack:
To lessen the chance that an attacker may take advantage of vulnerabilities, update your software. Always remember to check for safety updates.

To identify watering hole attacks, make use of your network security tools. When it comes to identifying such questionable activity, intrusion prevention systems (IPS) perform admirably.

It is recommended that you keep your internet activity hidden to avoid a watering hole assault. Use a VPN for this as well as the private browsing option in your browser. With the help of a VPN, you may securely connect over the Internet to another network. It serves as a barrier for the web browsing you do. One excellent VPN is NordVPN.

11. Spoofing

To get access to private data and carry out destructive actions, an attacker assumes the identity of someone or something else. They can, for instance, mimic a network address or an email address.

12. Identity-Based Attacks

These involve using someone else's PIN to gain unauthorized entry to their systems or stealing or manipulating their personal information.

13. Injection Code Exploits

carried out by introducing malware into a software program in order to alter data. For instance, to steal data, the attacker inserts spyware into a SQL database.

14. Attacks on the Supply Chain

Take advantage of weaknesses in hardware or software supply chains to obtain private data.

ISSN: 2582-6433

15. DNS Tunnelling

An attacker can interact with a remote server and get around security measures by using the Internet's Domain Name System (DNS).

16. DNS Manipulation

cyberattack in which the perpetrator modifies a website's DNS records in order to regulate traffic.

17. Cyberattacks with IoT

Take advantage of holes in devices connected to the Internet, such as security cameras and smart thermostats, to steal information.

18. Crypto-attacks

Demand money in return for encrypting the victim's data.

19. Distributed Denial of Service (DDos) Attacks

These attacks aim to take advantage of network weaknesses by flooding a website with traffic, rendering it unavailable to authorized users.

20. Direct Message

Distribute phony emails to propagate phishing schemes.

21. Hacked login credentials

Are used by Commercial Account Takeover (CATO) hackers to get access to other people's bank accounts.

2. Cash Out using Robotic Teller Machine (ATM)

In order to take massive cash withdrawals from ATMs, hackers gain access to the financial institution's computer networks.

23. Attacks using Whale Phishing

Employ advanced social engineering strategies to target prominent people, such as CEOs or celebrities, in order to get private data.

ISSN: 2582-6433

Target certain people or groups inside an organization using spear-phishing attacks (24). To obtain private information, attackers employ social engineering strategies.

25. Deciphering URLs

An attack in the URL decoding process is achieved by a web browser interpreting a Uniform Resource Locator, or URL, and requesting the associated web page.

26. The Hijacking of Session

Using the user's session ID, the hacker gains access to the web application and uses it to take over the user's session and authenticate it.

27. Utilizing brute force techniques

Through a series of guesses until the right one is discovered; an attacker gains unauthorized entry to a system. When used to weak passwords, it may be rather successful.

28. Web-Based Assaults

It aims to incorporate SQL injection, file inclusion, and cross-site scripting (XSS) into websites.

29. Trojan Horses

malware that seems like a trustworthy application but is really made of harmful code. It can carry out harmful tasks, such as taking over the machine and stealing data, once installed.

30. Uninvited Visits

By accessing its hacked website, the user's computer becomes infected with malware, which is then installed on it without the user's awareness by taking advantage of flaws in other applications.

31. Scripting attacks on the cross-site (XSS)

Unauthorized code is inserted into a trustworthy website by an attacker in order to obtain user credentials and credit card information, among other sensitive data.

ISSN: 2582-6433

32. Violations of Eavesdropping

To gain access to private data, an attacker eavesdrops on a conversation between two people.

33. Birthday Assault

A hash function collision is accessed using a cryptographic attack that takes use of the birthday paradox. To obtain the identical output hash value, the attacker is able to correctly produce two inputs. This can be leveraged to get around access restriction measures.

34. Attacks Based on Volume

To prevent authorized users from accessing a system, the attacker overwhelms it with large amounts of data. As an example, DDoS assaults cause a website to fail by flooding it with traffic from several infected machines.

35. Protocol Attacks

These attacks take advantage of holes within network protocols to access a system without authorization or interfere with its normal operations. The Internet Control Communication Protocols Flood attack and the Transmission Control Protocol, or TCP, SYN Flood attack are two examples.

36. Attacks at the Application Layer

Attempts to take advantage of holes in web servers or apps by targeting the programming layer of a system.

37. Dictionary Assaults

An attacker uses a list of frequently used terms in an effort to figure out a user's password. Because so many people use simple or weak passwords, this attack is successful.

38. A virus

Malicious software has the ability to replicate and propagate to more systems. Viruses have the power to destroy files, steal data, seriously harm systems, and more.

ISSN: 2582-6433

39. Worms

In contrast to viruses, replicate themselves and spread to other computers without the need for human contact.

40. Rear access doors

Because to this vulnerability, attackers can access a system or network without authorization and avoid regular authentication procedures.

41. Automatic

Automating network or internet chores is what these software tools do. Distributed Denial of Service, or DDoS, assaults are one malevolent usage for them.

42. Business Email Compromise (BEC)

This type of email compromise targets companies and organizations. In order to deceive the victim into sending money or private information to them, the attackers assume the identity of a reliable source.

43. XSS (Cross-Site Scripting) Incursions

It intends to carry out unlawful assaults or steal confidential data by inserting harmful code into a website that is susceptible to vulnerability.

44. Attacks Using AI

Get beyond conventional security measures with the help of machine learning and artificial intelligence.

45. Root-kitting

Grant special access to the victim machine for attackers. In addition to being difficult to find and eliminate, rootkits may be used to conceal additional infections, such as malware or keyloggers.

ISSN: 2582-6433

How Can Cyber Attacks Be Prevented?[2]

Even though we looked at a number of strategies to stop the various kinds of assaults we covered, let's review and take a look at some individual strategies you may use to completely prevent a cyberattack.

1. Use strong, difficult-to-crack alphanumeric passwords and change them on a frequent basis. Avoid using excessively complex passwords that you could find difficult to remember. Never use the same password more than once.
2. Update your apps and operating system on a regular basis. This is the main defence against any cyberattack. Vulnerabilities that hackers frequently take advantage of will be eliminated. Make use of reputable and authentic antivirus software.
3. Make use of firewalls and additional network security solutions, such as application security, access control, intrusion prevention systems, and so on.
4. Refrain from opening emails from senders you are not familiar with. Look closely for any gaps or serious mistakes in the emails you receive.
5. 5.Utilize a virtual private network. Encrypting the traffic between your device and the VPN server is ensured by doing this.
6. Take frequent data backups. It is recommended by many security experts to have three copies of your data on two distinct types of media and an additional copy off-site (cloud storage). That means you may delete all of the data on your machine and use a recent backup to restore it, even in the midst of a cyberattack.
7. Principles of cybersecurity should be known to staff members. They have to understand the different kinds of cyberattacks and how to defend against them.
8. Employ multi-factor or two-factor authentication. Users must authenticate themselves using two distinct factors when using two-factor authentication. Multi-factor authentication is the phrase used when you are prompted for more than two authentication methods in addition to your password and login. This turns out to be a crucial step in keeping your account safe.
9. Protect your wireless networks and stay away from public WIFI if you can't get a VPN.
10. Protect your smartphone, as they are a target for cyberattacks as well. Make sure your

[2] 4 things you can do to keep yourself cyber safe: CISA (2024) Cybersecurity and Infrastructure Security Agency CISA. Available at: https://www.cisa.gov/news-events/news/4-things-you-can-do-keep-yourself-cyber-safe (Accessed: 17 January 2024).

ISSN: 2582-6433

smartphone is updated and only install apps from reputable and trustworthy sources.

Conclusion

You now have a thorough understanding of cyberattacks thanks to this essay on their many forms. You've read about the definition of a cyberattack, the 10 most common kinds, and how to defend yourself from one. Knowing about cyberattacks and network security measures is important given the rise in cybercrimes in the modern world. We should take measures to keep our information protected, there are also various preventive ways in which we can assure full security to our systems.