INTERNATIONAL JOURNAL OF HUMAN COMPUTING STUDIES

https://journals.researchparks.org/index.php/IJHCS e-ISSN: 2615-8159 | p-ISSN: 2615-1898

Volume: 04 Issue: 9 | Sep 2022

Cyber Attacks and Preventive Measures on Network Applications

Umoh, Mfreke E. (PhD)

Department of Computer Science

Udoh, Godwin Joseph

Department of Computer Engineering

mumoh216@gmail.com

----------***----------

Abstract: Computer network security is of great importance for many users. With the increase in network development applications, the problem of network security is becoming more and more serious. Due to the diversity of computer network connections, terminal distribution in homogeneity, network openness, and sharing of network resources, the computer network is vulnerable to different forms of attacks such as viruses, hackers, malware attacks, and other misconduct. To ensure the safety and smoothness of information, the network security and preventive measures are eyebrow nimble. This paper analyzes the following with regards to the subject matter. History of cybercrime, motives behind cybercrime, cyber-attacks. cyber-attacks prevention and the cost of not being cyber secured.

Keywords: Cyber-attack, Network security, Cybercrime, Cyber prevention, network Applications.

Introduction

Cyber-attack can be defined as an unlawful act where a bad actor or group of bad actors gain unauthorized access to a computer, computing system or computer network with the intent to cause damage. Cyber-attack aims to disable, disrupt, destroy or take full control of a computer system in other to alter, delete, manipulate or steal that data held within these systems. With the new era of the digital world, the Internet has now made life so easy and stress-free for everyone. Be it storing data, having a conference meeting, or accessing information. The Internet has made the world a global community, bringing everything and everyone closer with just a click of a button. The continuous growth and daily involvement in cyberspace have made us prone to cyber-attacks.

Following the frequent invention of new tech, the majority of the businesses are now done online including bank transactions, church service, and electronic transfer of election results. Companies now employ expertise from around the world to work for them remotely. Relying so much on the Internet has given rise to cybercrime and cyber-attack is increasing at an exponential rate. With the introduction of new innovative tech and cyber mechanisms, increase in the availability of bandwidth, connected devices, and affordable attack tools, hackers are becoming more sophisticated and are now targeting consumers as well as public and private organizations. They are continuously attacking cyberspace and stealing sensitive information and holding companies and individuals to ransom. It has become imperative for everybody including companies, be it small or multinational to secure their network in other to prevent hackers from intruding into their computers and stealing their client information. Hackers can attack your network and hack into your application by identifying any vulnerable application in your security using SQL injection, brute force attack, etc. To prevent cybercrime, you need to all the mechanisms and methodology use for performing cyber-attack.

Copyright (c) 2022 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

INTERNATIONAL JOURNAL OF HUMAN COMPUTING STUDIES

https://journals.researchparks.org/index.php/IJHCS e-ISSN: 2615-8159 | p-ISSN: 2615-1898

Volume: 04 Issue: 9 | Sep 2022

CYBER-ATTACK:

A cyber-attack is a malicious and deliberate attempt to gain unauthorized access into a cyberspace for the purpose disrupting, stealing sensitive information or taking full control of the computer system for its own good. Lifars. (2020) Retrieved from https://www.lifars.com/2020/03/motivations-behind-cyber-attacks/

To fight effectively against cyber-attacks, it is important to understand the purpose and motivation behind all the attacks. Even though the methods and purpose of cyberattacks are varied, the major motivations can be anything from information theft to money theft. Some of the key reasons behind carrying out a cyber-attack are as follows.

To make a political and social point: Hackers can attack for the purpose of expressing their criticism of everything from governments, politicians, society, big brand companies, and current affairs. They tend to attack their targets, such as crashing their website, when they disagree with them. Compared to other types of attackers, they are less technical and tend to attach their targets with pre-made tools.

1) ***Radical hacktivism***: This group of people is usually formed by boring teens who seek a surge in adrenaline or try to vent their anger or frustration with institutions (such as school) or with people they believe to be wrong. in addition, some people are just seeking attention and respect from peers. Radical hackerism is largely ignored by companies because their purpose does not involve financial affairs.
2) ***Intellectual challenge****:* Similar to radical hacktivism, this group of people commit cyber-attacks for seeking attention and respect from peers through challenging network security. This type of hackers plays to the stereotype of the society awkward loner who lives in a virtual world and turns to hack for both intellectual challenge and the adrenaline rush of breaking into a network.
3) ***Business competition:*** DDoS attacks are increasingly being used as a competitive business tools. Some of these attacks are designed to prevent competitors from participating in major events, while others target the complete shutdown of online businesses for months. In either case, the idea is to cause disruption business operation and cause their competitors customers/clients to move over to their own side and patronized them while causing financial and reputation damage.
4) ***Cyber-warfare/Espionage:*** Cyber-warfare is the use of politically motivated cyber attacks on adversary networks or systems to conduct sabotage and espionage. Nation-states leverage offensive cyber-warfare with hostile intent hoping to disrupt or destroy systems of their adversaries. They can either utilize home grown hackers or hackers for hire to launch these attacks. Nation-state actors have an advantage over other types of cyber-attackers due to their larger budgets and availability of resources. They can dedicate time and personnel to cyber based efforts to produce highly skilled hackers with the best cyber weapons. The scale of effort, choice of victims and the technical sophistication of the cyber weapons are used to identify attacks sponsored by nation-states.

Cyber-warfare is a favourable option to nation-states as it allows them to attack other nations, sabotage systems and steal information with relatively no possibility of escalation to conventional warfare. No other resource can give a nation-state as much access to sensitive information with so little physical effort and low probability of attribution.

5) ***Religion:*** Cyber-terrorism can be defined as unlawful attacks and threats against systems, networks and electronic information to create fear, chaos with the goal of intimidating or coercing a government or people in furtherance of ideological objectives. Cyber-terrorists are motivated by radicalized religious beliefs and use their interpretation of religion as justification for their actions and can escalate to compel persons not normally associated with violent behavior to elevated levels of deviant behavior. These

Copyright (c) 2022 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

https://journals.researchparks.org/index.php/IJHCS e-ISSN: 2615-8159 | p-ISSN: 2615-1898
Volume: 04 Issue: 9 | Sep 2022

terrorists are well funded and have developed a wide range of skills that can prove formidable to cyber-security systems. This is the result of opportunistic collaboration with nation-states and criminal ventures.

6) ***Revenge/Anger:*** Cyber-attacks can be used as an outlet for seeking revenge or expressing anger. The attackers may be spurned lovers or spouses/ex-spouses, disgruntled or fired employees, dissatisfied customers, feuding neighbours, students angry about a bad grade, to name a few. Even a loss during online gaming can cause someone to launch a cyber-attack. The ease of access to hacking toolkits is one of the major contributors to this phenomenon. Anyone can become a hacker overnight and have the ability to launch a cyber-attack on anyone they believe did them wrong with little effort or fear of being caught.

Anger motivated attacks can be person-to-person, rather than person-to-company such as in cyber-stalking and cyber-bullying. Cyber-stalking is a targeted cyber-attack on one person for reasons of anger, revenge or control. Cyber-bulling occurs when a person is bullied, harassed, humiliated, threatened, embarrassed, or targeted in some way by another person using modern communication systems such as cellular phones (SMS/MMS) and Internet.

7) ***Financial gain***: Criminals have discovered that technology has created many opportunities for illegally gaining wealth. Both individual criminals and organized crime groups utilize the Internet and computers in their criminal activity. There are essentially three ways criminals use the Internet in their criminal efforts. First, cyber-attacks are used to penetrate computers and networks to steal personal data and extort businesses with threats of attacks or exposure of sensitive data. Secondly, social engineering is utilized to trick computer and network users to divulging sensitive information. Thirdly, the Internet is used to facilitate illegal enterprises and enterprises that facilitate illegal activity. No matter the way the Internet is used the goal remains the same, to make money.

Financially motivated attackers are indiscriminate in their attacks; they generally throw a broad net of online scams and phishing expeditions in the hope of getting as many victims as possible. They use these scams and social engineering to steal identities, get banking information and to siphon money out of bank accounts.

8) ***Notoriety/Challenge:*** Persons motivated by hopes of notoriety of just seeking a challenge tend to be teenagers and sometimes even younger individuals36. They engage in network intrusions, theft of intellectual property and deface websites. They do not launch attacks with malice, although the victim who incurs the cost of their fun may have a different opinion. These hackers have often only wanted to prove that they can perform these cyber-attacks, to themselves and/or their peers. Smith, T.E. (2013).

The origin of cybercrime

Cybercrime is one of the largest and globally most active forms of crime. After all, the internet is available and visible to everyone, and that of course involves risks. Committing a crime via a computer or other device that is connected to the Internet is dangerous because the identity of the perpetrator is difficult to find out.

Cybercrime occurs in various forms and always continues to develop. Security software and hardware companies are therefore constantly looking for ways to better protect people. Always being on alert and using security software or a VPN service are essential to protect yourself against cyber criminals. In addition, these security measures should make surfing the internet not only safer but also more enjoyable!

The history of cybercrime

At the beginning of the 1970s, criminals regularly committed crimes via telephone lines. The perpetrators were called Phreakers and discovered that the telephone system in America functioned based on certain tones. They were going to imitate these tones to make free calls.

Copyright (c) 2022 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

https://journals.researchparks.org/index.php/IJHCS e-ISSN: 2615-8159 | p-ISSN: 2615-1898
Volume: 04 Issue: 9 | Sep 2022

John Draper was a well-known Phreaker who worked on it daily; he toured America in his van and made use of public telephone systems to make free calls. Steve Jobs and Steve Wozniak were inspired by this man and even joined him. Of course, they all ended up on the right path: Steve Jobs and Wozniak founded Apple, the well-known computer company.

Hacking in the '80s

There was no real cybercrime until the 1980s. One person hacked another person's computer to find, copy or manipulate personal data and information. The first person to be found guilty of cybercrime was Ian Murphy, also known as Captain Zap, and that happened in the year 1981. He had hacked the American telephone company to manipulate its internal clock so that users could still make free calls at peak times. Watering, J.V(n.d) (https://goosevpn.com/blog/origin-cybercrime)

Hackers, however, proceeded in different ways over time. Although telephone companies were the very first target, banks, web shops, and even private individuals quickly followed suit. Nowadays, online banking is very popular, and that also carries a big risk. For example, hackers can copy log-in codes and names, or retrieve passwords from credit cards and bank accounts. The result is that one can just empty accounts or make purchases online with someone else's account!

Different types of cyber-attack

Cyber attacks occur when an individual, group, or organized gang attempts to maliciously breach the security system of another person or organization.

While this might prompt you to envision hackers breaking into an online banking system to steal billions, the most common example of a cyber attack is a data breach.Data breaches take place when hackers bypass a company or organization's security and steal sensitive information. They use this information for extortion, to commit frauds, or to sell it on the Dark Web. In 2021, the number of data breaches rose by a staggering 68%. But data breaches are only one of the consequences caused by cyber attacks.

Credit Card Frauds and Skimming

Often hackers make random telephone calls to person by pretending themselves as a bank officer or credit card authorized representative. They will tell you that your bank account or credit card will be blocked and you have to follow certain steps for making them work and mindfully they get your account and card details; sometimes hacker can also be able to take the one time Password (OTP) from you and successfully complete the fraudulent transaction over internet. Having the access to your financial information (Card number, Expiration date, CVV number), hacker can seamlessly perform any online transaction from your bank account.

The skimming is basically a physical process, where the hacker steal all the information of your Debit/Credit card by swiping or scanning your card on a particular device called Card Skimmer. The card number, Creation Date, Expiration Date, CVV number details are stored in the respective card with the help of the magnetic stripe or chip present on the card. Crooks often plant such skimming machines in public places such as shopping mall, ATM machine, sometimes they pretend themselves to be a bank or survey agent and get your card swap/scan through the skimming machine. By swiping the card they will have all the card details with them, which they can use for performing any kind of financial transactions on your behalf. In some cases skimmers can make duplicates of your card without your consent.

Copyright (c) 2022 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

https://journals.researchparks.org/index.php/IJHCS e-ISSN: 2615-8159 | p-ISSN: 2615-1898
Volume: 04 Issue: 9 | Sep 2022

Prevention Tips

1) Always be alert about your bank account balance and credit card limit.
2) Never respond to Fake callers.
3) Frequently change your Internet banking Passwords, Credit/ Debit card PIN.
4) Use Two factor Authentication in all your banking applications.
5) Use Official Mobile application of respective bank.
6) Never Swipe your card in un-trusted places.

Matrimony Fraud

Popular matrimony websites now-a-days are also becoming a hackers den, with all these theft identity hackers opening accounts in matrimonial websites (both as male and female) and communicating with other matrimony users and trapping them in several cyber frauds. These frauds are alternatively known as honey trap cyber frauds. Initially these hackers communicate with potential vulnerable users over concerned websites chat room, later they communicate over telephone call and WhatsApp. Sometimes these hackers also harass victims mentally and sexually. These are cyber frauds but not financial frauds.

There are several examples of matrimonial frauds known as Black Dollar fraud. In this context, hacker pretends to be from abroad and request the victim to accept some gift (Black Dollar) presented over pre-paid courier, i.e. the victim has to pay certain amount to the courier boy and then he will be given the box containing black dollar. The dollar (Fake dollar) was coated in a black-like material and that has to clean using some chemical. After cleaning the black dollar, we can see the dollar and that dollar is fake dollar.

Prevention Tips

1) Never get intimated with anyone in Matrimonial sites, without proper background investigation.
2) Don't involve in anything which gifts you freebies.
3) Make proper privacy setting in all social media accounts.

Juice Jacking

Juice jacking is a kind of cyber-attack which involves in performing data transfer, malware installation activities in victims mobile phone over USB cable. This happens while changing your mobile phones at public charging stations like hotels, bus stops, airports, railway stations, etc. The USB charging points in these public places can be easily replaced with some modified versions, which can copy the all the data, make a clone of your mobile, also inject malwares into your phone clandestinely.

A clone version of Phone's data can be easily access through any computer/Mac device. Any personal files, photographs, videos, etc. in the phone will be in the hacker's hand. Hacker can use those files in any means. In some cases hackers can crawl your phone and copy only selective information such as Bank account data, passwords, PINs, etc. Later they can use these details and perform any kind of financial frauds.

The malwares which are generally injected to your phone by using juice jacking method are Trojans, adware, ransomwares, crypto-miners, spywares, etc. which can do massive damage to your mobile devices. Ransomwares can freeze (Encrypt) all the data inside the device and hacker asks for ransom in order to giving the decryption key.

Copyright (c) 2022 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

INTERNATIONAL JOURNAL OF HUMAN COMPUTING STUDIES

https://journals.researchparks.org/index.php/IJHCS e-ISSN: 2615-8159 | p-ISSN: 2615-1898

Volume: 04 Issue: 9 | Sep 2022

Jacking

Juice jacking works over USB cables because USB design standard is done in such a way that it can convey both data and electricity. Generally an USB connecter contains five pins inside it, only one is needed for charging the receiving end. The other two are used for data transfer by default.

In the mobile devices the data transfer mode is disabled by default, unless you have made any changes to it. Only the power connection end is visible, which in the case of juice jacking is typically not the owner. That implies, when a user gets connected over USB port for charging, they could also be opening up a pathway for performing data transfer between the devices.

Prevention Tips

1) Avoid Mobile charging in public places.
2) In emergency if you are charging mobile in public places, then at least switch it off while charging.
3) Don't connect to internet by using public Wi-Fi.

Man-In-The-Middle Attacks

A man-in-the-middle (MitM) attack is a form of cyberattack where important data is intercepted by an attacker using a technique to interject themselves into the communication process. The attacker can be a passive listener in your conversation, silently stealing your secrets, or an active participant, altering the contents of your messages, or impersonating the person/system you think you're talking to.

MitM attack process

Most MitM attacks follow a straightforward order of operations, regardless of the specific techniques used in the attack.

In this example, there are three entities, Alice, Bob, and Chuck (the attacker).

1. Chuck covertly listens to a channel where Alice and Bob are communicating
2. Alice sends a message to Bob
3. Chuck intercepts and reads Alice's message without Alice or Bob knowing
4. Chuck intercept Alice messages, alters it and forward the altered messages to Bob, causing unwanted/damaging responses.

MitM techniques are usually employed early in the cyber kill chain – during reconnaissance, intrusion, and exploitation. Attackers often use MitM to harvest credentials and gather intelligence about their targets. Buckbee, M. (2020). https://www.varonis.com/blog/man-in-the-middle-attack.

Multi-factor authentication (MFA) can be an effective safeguard against stolen credentials. Even if your username and password are scooped up by a man-in-the-middle, they'd need your second factor to make use of them. Unfortunately, it's possible to bypass MFA in some cases.

Here is an example of how MiTM attack against Microsoft Office 365 where MFA can be bypassed by the attacker:

1. User clicks a phishing link that takes them to a fake Microsoft login page where they enter their username and password.
2. The fake webpage forwards the username and password to the attacker's server.

Copyright (c) 2022 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

https://journals.researchparks.org/index.php/IJHCS e-ISSN: 2615-8159 | p-ISSN: 2615-1898
Volume: 04 Issue: 9 | Sep 2022

3. The attacker forwards the login request to Microsoft, so they don't raise suspicion.
4. Microsoft sends the two-factor authentication code to the user via SMS.
5. User enters the code into the fake webpage.
6. The fake page forwards 2FA code to the attacker's server.
7. The attacker uses Evilginx to steal the session cookie.
8. The attacker forwards the user's 2FA code to Microsoft, and now the attacker can log in to Office 365 as the compromised user by using the session cookie, and has access to sensitive data inside the enterprise.

MitM Attack Techniques and Types

Here are a few of the common techniques that attackers use to become a man-in-the-middle.

1. ARP Cache Poisoning

Address Resolution Protocol (ARP) is a low-level process that translates the machine address (MAC) to the IP address on the local network.

Attackers inject false information into this system to trick your computer to think the attacker's computer is the network gateway. When you connect to the network, the attacker is receiving all of your network traffic (instead of your real network gateway) and passes the traffic along to its real destination. From your perspective, everything is normal. The attacker is able to see all of your packets.

Chuck (our attacker) joins your network and runs a network sniffer

Chuck inspects your network packets to attempt to predict the sequence numbers of your packets between you and the gateway

Chuck sends a packet to your computer with the faked source address of the gateway and the correct ARP sequence to fool your computer into thinking the attacker's computer is the gateway

At the same time, Chuck floods the gateway with a Denial of Service (DoS) attack so you receive the fake ARP packet before the gateway is able to respond

Chuck fooled your computer into thinking the attacker's laptop is the real gateway, and the MitM attack is successful

2. DNS Cache Poisoning

DNS cache poisoning is when the attacker gives you a fake DNS entry that leads to a different website. It might look like Google, but it's not Google, and the attacker captures whatever data – username and password, for example – you enter into the faked website.

Chuck figures out that you use a certain DNS resolver.

Chuck knows this resolver is vulnerable to exploits, like an older version of BIND.

Chuck uses this exploit to tell the DNS resolver that www.example.com lives at an IP address that they own.

You go to www.example.com from your computer, and the DNS resolver tells you that the IP address of that site is the attacker's machine!

Chuck completes the connection to the real website so you don't realize there is anyone listening, but he is able to see all the packets that you (or anyone else that uses this DNS resolver to connect to www.example.com) are sending.

Copyright (c) 2022 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

https://journals.researchparks.org/index.php/IJHCS e-ISSN: 2615-8159 | p-ISSN: 2615-1898
Volume: 04 Issue: 9 | Sep 2022

3. HTTPS Spoofing

HTTPS is one of the ways users know that their data is “safe.” The S stands for secure. At least that is what an attacker wants you to think. Attackers set up HTTPS websites that look like legitimate sites with valid authentication certificates, but the URL will be just a bit different. For example, they will register a website with a Unicode character that looks like an ‘a’ but isn’t. Continuing with the “example.com” example, the URL might look like https://www.example.com, but the ‘a’ in “example” is a Cyrillic “a”, which is a valid Unicode character that appears just like an Arabic “a” with a different Unicode value.

Chuck gets you to visit his website www.example.com with the Cyrillic “a” using some kind of attack, phishing for example.

You download the CA certificate for the fake website.

Chuck signs the certificate with his CA private key and sends it to you.

You store the certificate in your trusted key store.

Chuck relays the traffic to the real www.example.com, and he is now a real MitM listening to your traffic

4. Wi-Fi Eavesdropping

Attackers listen to traffic on public or unsecured Wi-Fi networks, or they create Wi-Fi networks with common names to trick people into connecting so they can steal credentials or credit card numbers or whatever other information users send on that network.

5. Session Hijacking

Session hijacking is a MitM attack where the attacker wait for you to login to a web page (banking account, email account, for example) and then steals your session cookie to log into that same account from their browser.

Once the attacker has your active session cookie on their computer, they can do whatever you could do on that website. The hacker can transfer all of your savings to an offshore account, buy a bunch of goods with your saved credit card, or use the stolen session to infiltrate your company network and establish a stronger foothold on the corporate network.

How to Detect a Man-in-the-Middle Attack

MitM attacks can be difficult to catch, but their presence does create ripples in the otherwise regular network activity that cybersecurity professionals and end-users can notice.

It's important to take precautionary measures to prevent MITM attacks before they occur, rather than attempting to detect them while they are actively occurring. Being aware of your browsing practices and recognizing potentially harmful areas can be essential to maintaining a secure network. Below, we have included five of the best practices to prevent MITM attacks from compromising your communications.

Signs to Look Out For

Unexpected and/or repeated disconnections: Attackers forcefully disconnect users so they can intercept the username and password when the user tries to reconnect. By monitoring for unexpected or repeated disconnections, you can pinpoint this potentially risky behavior proactively.

Copyright (c) 2022 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

https://journals.researchparks.org/index.php/IJHCS e-ISSN: 2615-8159 | p-ISSN: 2615-1898
Volume: 04 Issue: 9 | Sep 2022

Strange addresses in your browser address bar: If anything in the address looks odd, even by a little, double-check it. It could be a DNS hijack. For example, you see https:\\www.go0gle.com instead of https:\\www.google.com

You log into a public and/or unsecured Wi-Fi: Be very careful of what networks you connect to, and avoid public Wi-Fi if possible. Attackers create fake networks with known IDs like "local free wireless" or some other common name to trick people into connecting. If you connect to the attacker's Wi-Fi, they can easily see everything you send on the network

How to Prevent a Man-in-the-Middle Attack

Here are several best practices to protect you and your networks from MitM attacks. None of them are 100% fool-proof.

General Best Practices

Overall, good cybersecurity hygiene will help protect you from MitM attacks.

1) Only connect to secured Wi-Fi routers or use your wireless carrier's encrypted connection. Connect to routers that use WPA2 security. It's not totally foolproof, but it's much better than nothing.
2) Add a VPN to encrypt traffic between end-points and the VPN server (either on the enterprise network or on the internet). If traffic is encrypted, it's harder for a MiTM to steal or modify it.
3) Use end-to-end encryption for your emails, chat, and video communication (Zoom, Teams, etc.)
4) Keep the system patched and malware updated
5) Use a password manager to protect your passwords and prevent reuse of passwords
6) Only connect to HTTPS connections, use a browser plugin to enforce this rule
7) Use multi-factor authentication wherever available

Employ DNS over HTTPS, which is a new technology that protects you from DNS hijacking by encrypting your DNS requests

Follow the zero-trust principles to build internal barriers around access to data, which prevent infiltrators from moving freely throughout the network if they were to get inside

Monitor activity on the network to detect evidence (malicious network connections or abnormal user behavior, for example) of a compromise or MitM techniques in use.

Phishing

Phishing is a popular cybercrime, which is the act of creating fraudulent websites, sending fraudulent emails, text messages that appear to be from a legitimate source. Using phishing the hackers try to obtain various sensitive information from victim such as Online banking user name and passwords, Email ID and passwords and other login details by disguising oneself as a trusted entity over electronic communication.

Steps of Phishing attack.

As per the above figure, the hackers first make a plan for phishing and make a replication of any legitimate website such as Leading Social media website or Popular Online banking website and host the replication website in any webserver and assign a similar domain name to it e.g., Facebook.com is Facelook.com, onlinesbi.com as sbionline.net, gmail.com as Hmail.com. While making similar web design (replication) of

Copyright (c) 2022 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

https://journals.researchparks.org/index.php/IJHCS e-ISSN: 2615-8159 | p-ISSN: 2615-1898
Volume: 04 Issue: 9 | Sep 2022

any legitimate website hackers generally use very similar logo and exact same to same color combination of the legitimate site so that the victim will not able to identify whether it's the real website or phishing website easily. There must be some login and register page in the phishing page, which is also so similar to the original one.

Then scammers run several email campaigns to populate the phishing websites around the vulnerable users. When any user finds the phishing site either from email campaign or any other medium and enters the Username and Password, the username and passwords will be stored at the database that is being deployed by the hacker to store the victim's details. In this way the hacker will get the direct access of many users' bank account and social media account, etc.

Prevention Tips

1) In order to prevent phishing attack, first you need to identify the phishing page or phishing email. You need to check carefully the sender of the email, the subject, the attachment, etc.
2) Spam emails can be filtered using spam filter options, which is available with almost all leading email service providers.
3) Use latest updated antivirus in your mobile, laptop and other devices, which you use for browsing internet and be sure for enabling the Internet Security options.
4) It's not advisable to open the email attachments from suspicious sender.
5) Don't click any link inside an email, which received from unknown/suspicious sender. First verify the by hovering mouse on it, that where the link is taking to you, then click on the link.
6) Immediate report to concerned legitimate brand, if you find any phishing website or email related to their brand/business.
7) While visiting any website, lookout for the SSL certificate of the website.
8) Never use same password/usernames for multiple accounts.

Vishing/Smishing

Vishing is also a cyber-crime, which is very similar to the phishing concept. In the case of Vishing, the hacker/spammers generally put a call to potentially vulnerable victims and pretend that they are calling from any legitimate organization. Here fraudster collects sensitive user information over phone.

Smishing refers to the same type of crime like phishing and vishing but the only difference here is spammers use SMS instead of Email or telephone for acquiring sensitive user data.

IP Spoofing

Spoofing means to pretend as someone else. IP spoofing is a technique used for gaining anonymous access to the victim's computer with an IP address of any trusted host. While implementing IP spoofing technique, attacker obtains the IP address of the client and injects their own spoofed packet along with the client IP over the TCP session. So the server will be fooled and it will treat this like communicating with the original host, i.e. the victim.

There are several tools such as: mitmproxy, Wireshark, sslstrip that these hackers use on Kali linux for IP Spoofing.

Copyright (c) 2022 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

https://journals.researchparks.org/index.php/IJHCS e-ISSN: 2615-8159 | p-ISSN: 2615-1898
Volume: 04 Issue: 9 | Sep 2022

Prevention

1) Promote the use of Transport Layer Security (TLS), HTTP secure (HTTPS), and Secure Shell (SSH).
2) Use better packet filtering mechanism or tool. Regular network audit should be also an option for IP spoofing Prevention.

Cross-Site Scripting (XSS) Attack

Cross-site scripting attack is abbreviated as XSS attack. This is basically a client side code injection attack. In XSS attack the motive of the hacker is to execute malicious scripts. The hacker will perform the trick in such a way that the malicious code execution will be done by the victim/users only. The hacker tries to inject the malicious script from the web browser by accessing the web forms of the website. The malicious script may be Java Script (JS), or shell script or any xml file. Once the hacker successfully uploads the script into the web server, then the real attack will take place when the user tries to access the malicious file/script or code.

By performing XSS attack hacker can gain access to the victims file on the web server, victim's computer through the browser. Hackers are able to change all the files and database on the particular server, the malicious script can further mutate and getting auto injected to all the files and directories of the webserver. In some cases the hacker can gain the overall access to the victim's computer through the malicious script injection.

Generally hackers target all the forums, comment and contact form section of the websites and from there they try to inject the codes. The webservers which are using un-sanitized user inputs are most vulnerable to XSS attack.

Here are the steps for the XSS attack.

1. From the very beginning, the hacker injects the malicious code into the database or the file system of the webserver.
2. The Webpage is being requested by the victim.
3. The server serves the required page as requested by of the victim to the browser (victims), the victim also receives the malicious code along with the webpage.
4. The malicious code gets executed on the victim's browser, in this instance by executing the script, the victim's cookie will be sent to the attacker's server.
5. Now the attacker can extract the victim's cookie as and when the http request reached the server.
6. Attacker can use the stolen cookie for many anonymous activities.

Preventive measures.

How to Prevent Cross-site Scripting (XSS)

Preventing Cross-site Scripting (XSS) is not easy. Specific prevention techniques depend on the subtype of XSS vulnerability, on user input usage context, and on the programming framework. However, there are certain general strategic principles that you should follow to keep your web application safe.

1: ***Train and maintain awareness:***

To keep your web application safe, everyone involved in building the web application must be aware of the risks associated with XSS vulnerabilities. You should provide suitable security training to all your developers, QA staff, DevOps, and SysAdmins. You can start by referring them to this page.

Copyright (c) 2022 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

https://journals.researchparks.org/index.php/IJHCS e-ISSN: 2615-8159 | p-ISSN: 2615-1898
Volume: 04 Issue: 9 | Sep 2022

2: ***Don't trust any user input:***

Treat all user input as untrusted. Any user input that is used as part of HTML output introduces a risk of an XSS. Treat input from authenticated and/or internal users the same way that you treat public input.

3: ***Use escaping/encoding:***

Use an appropriate escaping/encoding technique depending on where user input is to be used: HTML escape, JavaScript escape, CSS escape, URL escape, etc. Use existing libraries for escaping, don't write your own unless absolutely necessary.

4: ***Sanitize HTML:***

If the user input needs to contain HTML, you can't escape/encode it because it would break valid tags. In such cases, use a trusted and verified library to parse and clean HTML. Choose the library depending on your development language, for example, HtmlSanitizer for .NET or SanitizeHelper for Ruby on Rails.

5: ***Set the HttpOnly flag:***

To mitigate the consequences of a possible XSS vulnerability, set the HttpOnly flag for cookies. If you do, such cookies will not be accessible via client-side JavaScript.

6: ***Use a Content Security Policy:***

To mitigate the consequences of a possible XSS vulnerability, also use a Content Security Policy (CSP). CSP is an HTTP response header that lets you declare the dynamic resources that are allowed to load depending on the request source.

7: ***Scan regularly (with Acunetix):***

XSS vulnerabilities may be introduced by your developers or through external libraries/modules/software. You should regularly scan your web applications using a web vulnerability scanner such as Acunetix. If you use Jenkins, you should install the Acunetix plugin to automatically scan every build.

SQL injection

SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. This information may include any number of items, including sensitive company data, user lists or private customer details. Imperva. (2021).https://www.imperva.com/learn/application-security/sql-injection-sqli/

The impact SQL injection can have on a business is far-reaching. A successful attack may result in the unauthorized viewing of user lists, the deletion of entire tables and, in certain cases, the attacker gaining administrative rights to a database, all of which are highly detrimental to a business. When calculating the potential cost of an SQLi, it's important to consider the loss of customer trust should personal information such as phone numbers, addresses, and credit card details be stolen. While this vector can be used to attack any SQL database, websites are the most frequent targets.

Steps to Prevent SQL Injection Attacks

Preventing SQL Injection vulnerabilities is not easy. Specific prevention techniques depend on the subtype of SQLi vulnerability, on the SQL database engine, and on the programming language. However, there are certain general strategic principles that you should follow to keep your web application safe.

Copyright (c) 2022 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

https://journals.researchparks.org/index.php/IJHCS e-ISSN: 2615-8159 | p-ISSN: 2615-1898
Volume: 04 Issue: 9 | Sep 2022

1) ***Validate User Inputs:*** A common first step to preventing SQL injection attacks is validating user inputs. First, identify the essential SQL statements and establish a whitelist for all valid SQL statements, leaving invalidated statements out of the query. This process is known as input validation or query redesign. Additionally, you should configure inputs for user data by context. For example, input fields for email addresses can be filtered to allow only the characters in an email address, such as a required "@" character. Similarly, phone numbers and social security numbers should only be filtered to allow the specific number of digits for each.

2) ***Sanitize Data By Limiting Special Characters:*** Another component of safeguarding against SQL injection attacks is mitigating inadequate data sanitization. Because SQLi attackers can use unique character sequences to take advantage of a database, sanitizing data not to allow string concatenation is critical. One way of doing this is configuring user inputs to a function such as MySQL's mysql_real_escape_string(). Doing this can ensure that any dangerous characters such as a single quote ' is not passed to a SQL query as instructions. A primary method of avoiding these unauthenticated queries is the use of prepared statements.

3) ***Enforce Prepared Statements And Parameterization:*** Sadly, input validation and data sanitization aren't fix-alls. It's critical organizations also use prepared statements with parameterized queries, also known as variable binding, for writing all database queries. By defining all SQL code involved with queries, or parameterization, you can distinguish between user input and code. While dynamic SQL as a coding technique can offer more flexible application development, it can also mean SQLi vulnerabilities as accepted code instructions. By sticking with standard SQL, the database will treat malicious SQL statements inputted like data and not as a potential command.

4) ***Use Stored Procedures In The Database:*** Similar to parameterization, using stored procedures also requires variable binding. Unlike the prepared statements approach to mitigating SQLi, stored procedures reside in the database and are called from the web application. Stored procedures are also not immune to vulnerabilities if dynamic SQL generation is used. Organizations like OWASP say only one of the parameterized approaches is necessary, but neither method is enough for optimal security. Crafting parameterized queries should be done in conjunction with our other recommendations.

5) ***Actively Manage Patches And Updates:*** Vulnerabilities in applications and databases that are exploitable using SQL injection are regularly discovered and publicly identified. Like so many cybersecurity threats, it's vital organizations stay in tune with the most recent news and apply patches and updates as soon as practical. For SQLi purposes, this means keeping all web application software components, including database server software, frameworks, libraries, plug-ins, and web server software, up to date.

Denial of Service Attacks

A denial-of-service (DoS) attack is a tactic for overloading a machine or network to make it unavailable. Attackers achieve this by sending more traffic than the target can handle, causing it to fail—making it unable to provide service to its normal users. Examples of targets might include email, online banking, websites, or any other service relying on a targeted network or computer.

There are different types of DoS attacks such as resource exhaustion and flood attacks. Resource exhaustion attacks cause the targeted infrastructure to use all of its available memory or storage resources, slowing the service's performance or stopping it all together. Flood attacks send an overwhelming number of packets that exceed server capacity. ExtraHop. (n.d). https://www.extrahop.com/resources/attacks/dos/

Copyright (c) 2022 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

INTERNATIONAL JOURNAL OF HUMAN COMPUTING STUDIES

https://journals.researchparks.org/index.php/IJHCS e-ISSN: 2615-8159 | p-ISSN: 2615-1898

Volume: 04 Issue: 9 | Sep 2022

A distributed denial-of-service (DDoS) is a type of DoS attack where the traffic used to overwhelm the target is coming from many distributed sources. This method means the attack can't be stopped just by blocking the source of traffic.

Botnets are often employed for DDoS attacks.

Types of DDoS Attacks

SMURF ATTACK:

A smurf attack is a DDoS attack that sends packets spoofing the victim's source IP. When devices on the network attempt to respond, the amount of traffic slows the targeted device to the point of being unusable.

SYN FLOOD:

A SYN flood attack opens many connections with the target target server and then never closes them. The attacker, acting as a client, sends a SYN message. When the server responds with a SYN-ACK, the malicious client never sends an ACK message. In this way the server is forced to keep numerous connections open, taxing it's resources until it fails.

LAYER 7 DDOS ATTACK:

A Layer 7 DDoS attack (or application attack) targets a specific service instead of an entire network. These are becoming increasingly more common than broad network attacks.

Protection Against Denial of Service Attacks

While DoS attacks are less challenging to stop or prevent, DDoS attacks can still present a serious threat.

Prevent spoofing: Check that traffic has a source address consistent with the set of addresses for its stated site of origin and use filters to stop dial-up connections from spoofing.

Limit broadcasting: Often attacks will send requests to every device on the network, amplifying the attack. Limiting or turning off broadcast forwarding where possible can disrupt attacks. Users can also disable echo and chargen services where possible.

Streamline incident response: Honing your incident response can help your security team respond quickly when DoS attacks are detected.

Protect endpoints: Ensure that all endpoints are patched to eliminate known vulnerabilities. Endpoints capable of running EDR agents should have them installed.

Dial in firewalls: Ensure your firewalls are limiting ingress and egress traffic across the perimeter wherever possible.

Monitor the network: The more you know about what normal inbound traffic looks like, the quicker you'll spot the start of a DDoS attack. Real-time visibility with network detection and response (NDR) is an efficient and reliable way to maintain a profile of what your network should look like (using machine learning) so you can detect suspicious surges immediately.

Malware

Malware is malicious software used by cybercriminals to disrupt, damage, or exploit an endpoint or network. Malware can be used to steal or destroy data, encrypt information, spam users, spy on users, extort money, take over a system, or change how a system works. Malware can access computers or networks using various

Copyright (c) 2022 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

https://journals.researchparks.org/index.php/IJHCS e-ISSN: 2615-8159 | p-ISSN: 2615-1898
Volume: 04 Issue: 9 | Sep 2022

methods, including infected email attachments, advertisements, applications, and websites. Byos. (n.d). Retrieved from https://www.byou.io/blog/how-to-prevent-malware-attacks

Types of Malware

The list below covers the significant categories of malware that all cybersecurity professionals should know.

***Viruses*:** The classic form of malware, viruses function much like their biological namesake. They can infect an endpoint, proliferate throughout the system, and change how it works. They can also multiply and spread from system to system in a network.

***Worms*:** Worms behave much like viruses, infecting, multiplying, and spreading through network endpoints. Unlike viruses, they do not need to be attached to a program or activated by a user to metastasize — an attribute that makes them particularly destructive.

***Ransomware*:** This increasingly popular malware uses encryption to block legitimate users from being able to access their systems, devices, or information. The attacker will only return control to the rightful users only if their demands are met. To add pressure, cybercriminals often threaten to destroy or release the data.

***Spyware*:** This is malicious software that can steal data and monitor user activity, like specific keystrokes. Spyware can also tap into computer cameras and microphones. The data gathered using spyware could be valuable or could help break into the system — for example, when log-in information is stolen.

***Adware*:** While not as dangerous as the other types of malware on this list, adware can cause a high degree of frustration. Once adware infects a computer, the user's online activity data is compromised and used to force the user to view advertisements.

***Trojans*:** Like the battle strategy of legend, trojans disguise themselves as something a user wants, like a software update, to gain access to a system. This can open the gates to additional cyber attacks like ransomware or spyware.

Rogueware: Much like trojans, rogueware lures users into comprising their systems through a ruse. In this case, the counterfeit is a malware alert. Once the user clicks on this notice, the device is infected.

Malware Prevention

There are no ways to prevent malware attacks but there are reliable ways to detect and block attacks, thus protecting your systems from being infected by malicious software.

1. *Install anti-virus and anti-spyware software.*

Anti-virus and anti-spyware programs scan computer files to identify and remove malware. Be sure to:

1) Keep your security tools updated.
2) Immediately remove detected malware.
3) Audit your files for missing data, errors, and unauthorized additions.

2. *Use secure authentication methods.*

The following best practices help keep accounts safe:

1) Require strong passwords with at least eight characters, including an uppercase letter, a lowercase letter, a number and a symbol in each password.
2) Enable multi-factor authentication, such as a PIN or security questions in addition to a password.

Copyright (c) 2022 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

https://journals.researchparks.org/index.php/IJHCS e-ISSN: 2615-8159 | p-ISSN: 2615-1898
Volume: 04 Issue: 9 | Sep 2022

3) Use biometric tools like fingerprints, voiceprints, facial recognition and iris scans.
4) Never save passwords on a computer or network. Use a secure password manager if needed.

3. ***Use administrator accounts only when absolutely necessary.***

Malware often has the same privileges as the active user. Non-administrator accounts are usually blocked from accessing the most sensitive parts of a computer or network system. Therefore:

1) Avoid using administrative privileges to browse the web or check email.
2) Log in as an administrator only to perform administrative tasks, such as to make configuration changes.
3) Install software using administrator credentials only after you have validated that the software is legitimate and secure.

4. ***Keep software updated.***

No software package is completely safe against malware. However, software vendors regularly provide patches and updates to close whatever new vulnerabilities show up. As a best practice, validate and install all new software patches:

1) Regularly update your operating systems, software tools, browsers and plug-ins.
2) Implement routine maintenance to ensure all software is current and check for signs of malware in log reports.

5. ***Control access to systems.***

There are multiple ways to regulate your networks to protect against data breaches:

1) Install or implement a firewall, intrusion detection system (IDS) and intrusion prevention system (IPS).
2) Never use unfamiliar remote drives or media that was used on a publicly accessible device.
3) Close unused ports and disable unused protocols.
4) Remove inactive user accounts.
5) Carefully read all licensing agreements before installing software.

6. ***Adhere to the least-privilege model.***

Adopt and enforce the principle of least-privilege: Grant users in your organization the minimum access to system capabilities, services and data they need to complete their work.

7. ***Limit application privileges.***

A hacker only needs an open door to infiltrate your business. Limit the number of possible entryways by restricting application privileges on your devices. Allow only the application features and functions that are absolutely necessary to get work done.

8. ***Implement email security and spam protection.***

Email is an essential business communication tool, but it's also a common malware channel. To reduce the risk of infection:

1) Scan all incoming email messages, including attachments, for malware.
2) Set spam filters to reduce unwanted emails.

Copyright (c) 2022 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

https://journals.researchparks.org/index.php/IJHCS e-ISSN: 2615-8159 | p-ISSN: 2615-1898
Volume: 04 Issue: 9 | Sep 2022

3) Limit user access to only company-approved links, messages and email addresses.

9. *Monitor for suspicious activity.*

Monitor all user accounts for suspicious activity. This includes:

1) Logging all incoming and outgoing traffic
2) Baselining normal user activity and proactively looking for aberrations
3) Investigating unusual actions promptly

10. *Educate your users.*

At the end of the day, people are the best line of defense. By continually educating users, you can help reduce the risk that they will be tricked by phishing or other tactics and accidentally introduce malware into your network. In particular:

1) Build awareness of common malware attacks.
2) Keep users up to date on basic cybersecurity trends and best practices.
3) Teach users how to recognize credible sites and what to do if they stumble onto a suspicious one.
4) Encourage users to report unusual system behavior.
5) Advise users to only join secure networks and to use VPNs when working outside the office.

Password attack

Passwords are an easy and efficient way to secure data and IT systems from unauthorized access when used appropriately. Many people, however, continue to use passwords in ways that put them at risk, and IT policies don't always improve overall user behavior.

Types of Password Attacks

Hackers typically rely on different techniques to obtain and authenticate with a legitimate user's password. These include:

Dictionary Attacks:

In a Dictionary attack, cyber-criminals use password guessing techniques to bypass the security walls of a password-protected device. In this, hackers use numerous combinations of usernames and passwords to guess the correct credentials. A series of dictionary words are used in a systematic order to crack the password combinations. Adrian. (2020).
https://www.internetsecurity.tips
t/#:~:text=In%20a%20Dictionary%20attack%2C%20cyber,to%20guess%20the%20correct%20credentials.

Because a dictionary attack can be done quickly, many organizations require users to create passwords that have a special character, number, capital letter, and be eight characters or greater.

Brute Force

This type of password attack employs trial-and-error methods to guess a user's authentication information. The bad actor uses automated scripts to work through as many permutations as possible to guess the user's password correctly. While it is a relatively old method that requires a lot of patience and time, a Brute force attack is still standard in account breach attempts since they are automated and straightforward. Cashtest Security. (2022). https://crashtest-security.com/password-attack/

Copyright (c) 2022 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

INTERNATIONAL JOURNAL OF HUMAN COMPUTING STUDIES

https://journals.researchparks.org/index.php/IJHCS e-ISSN: 2615-8159 | p-ISSN: 2615-1898

Volume: 04 Issue: 9 | Sep 2022

Keylogging

While orchestrating a Keylogging attack, a hacker installs monitoring tools in the user's computer to record the keys struck by the user covertly. A keylogger records all information that users type into input forms and then sends it to the malicious third party. While keyloggers often have essential uses in enterprise settings (UX improvement, employee monitoring, etc.), attackers often use them to extract information such as login credentials for unauthorized access maliciously.

Preventive measures against password attack:

1. ***Strong passwords***: It is one of the easiest yet the most effective preventive measures that one could ever use. By increasing your password complexity you can easily fight Dictionary attacks. A complex, unique, and long password with alphanumeric characters are not found in dictionaries and are hard to guess.

1) The minimum length of your password should be 8 characters.
2) It should contain both small and uppercase alphabets.
3) Your password must include a numeric digit.
4) The usage of special characters is a must for strong passwords.

2. ***Regularly change your passwords:*** Changing your passwords regularly will also guard you against Dictionary attacks. Many enterprise-level organizations require you to reset your account passwords in regular intervals, the same should be followed by home users. Changing account passwords every 30 days can help you strengthen the security walls of your device.

3. ***Disable Root Login:*** A good way of protecting your root connection is by disabling the root login of your device.

4. ***Device lockout on failed login attempts***: This method involved disabling your account after several failed login attempts. This creates a pause between each attempt and will avoid the hackers from guessing your password too quickly.

5. ***Use Two-Factor Authentication (2FA):*** 2FA adds another layer of security to your login form. Once you login with appropriate credentials, you will need to enter a code which can only be accessed by you, such as an email or a unique code generated by an authentication tool. This additional layer prevents anyone that has successfully obtained your credentials/password from accessing your account without a secondary piece of authentication.

The Negative Effects Caused By Cyber-Attack

Hackers have a number of reasons for breaking through network security. Some do it just for the challenge, others for information, some for fame and some for honing their skills. Whatever the reason, hacking causes damage to the computing devices of individuals and businesses, sometimes resulting in millions of dollars lost. McCoy M. (2019). https://itstillworks.com/negative-effects-hacking-12040354.html

Business disruption:

This is arguably the largest risk in relation to a cyber-attack. Such attacks can prove to be extremely disruptive where complex business activities are concerned. Denial of services and access to customer information, email systems, phone systems, the internet, information databases, booking software, tracking software and EDI services can quickly cause great operational difficulties. A denial of services attack could also negatively

Copyright (c) 2022 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

https://journals.researchparks.org/index.php/IJHCS e-ISSN: 2615-8159 | p-ISSN: 2615-1898
Volume: 04 Issue: 9 | Sep 2022

impact your sub-contractors or tenants where they are afforded access to your systems. This highlights the importance of having a robust business continuity plan in place.

***Financial losses**:*

The motivation of many targeted cyber-attacks is to extort money. Using denial of service ransomware, an attacker is able to leverage a ransom payment in return for granting access back to IT services. Internet enabled mandate fraud can also result in large financial losses to a business. Every year, reports of hacked businesses reveal staggering financial losses as a result. In 2011, Sony lost $170 million due to a hack of their PlayStation system. Also in 2011, CitiGroup lost $2.7 million and AT&T lost $2 million as a result of cyber-attack. Brenntag Ransomware Attack, April

In April, hackers successfully deployed a high-profile ransomware attack against German chemical distribution company Brenntag. Brenntag is a large corporation and a world leader in their field, with thousands of employees across the world at over 670 locations.

The perpetrators in this scenario were hacker group DarkSide, who netted an eye-watering $4.4 million ransom paid for in Bitcoin by Brenntag in a bid to prevent stolen data from being released and for the key to decrepit their files to be handed over.

The attack, which focused on the North American side of the business, managed to encrypt the company network and steal 150GB of data, including highly sensitive personal information pertaining to the company's employees.

The ransom had originally been much higher but was reduced to $4.4 million after negotiations. Part of these negotiations included DarkSide telling Brenntag how they managed to pull off the attack. When it came down to it, the "gateway" to this attack turned out to be stolen credentials, or so DarkSide claims.

The cost of patching the holes in security, repaying customer losses, addressing lawsuits and weathering shutdowns of their systems contributed to those huge numbers. Even for an individual who loses his credit card information to a hacker, however, the cost of repairing damage and tracking down the culprit can be significant.

Damaged Reputation:

Companies that get hacked have a bigger problem than just paying for the initial damage costs and lawsuits. Reputation damage can be devastating to a company's fortunes. If a bank has been compromised multiple times, customers are less likely to give them their personal information. The same goes for retailers who lose information to hackers. These companies lose business over time because of damaged or weakened reputations. Individuals with stolen identities as a result of hacking have a similar reputation problem when it comes to their credit ratings

Cost:

There will inevitably be an upfront financial cost in managing a cyber-attack. Whether replacing or updating computers and systems or having to pay for experts to assist in overcoming the challenges faced, the upfront costs can be unexpected and high.

Loss of Information:

Hacking often results in a loss of data due to files being deleted or changed. Customer information and order information can be stolen and deleted, or a leak of top-secret information could cause real-world security issues. Servers at the Pentagon, FBI, Interpol and NASA have all been compromised at various points in the

Copyright (c) 2022 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

https://journals.researchparks.org/index.php/IJHCS e-ISSN: 2615-8159 | p-ISSN: 2615-1898
Volume: 04 Issue: 9 | Sep 2022

past ten years. Sometimes, these hackers even post information from these governmental organizations online, which could in theory cause unrest between countries.

Security attack:

Security attack often happen in different forms or can be classified into passive and active attack. The first form of attack is that in which the hacker attempts to learn or make use of information from the system but does not affect the system's resources. The goal of the attack is to obtain information that is being transmitted. The second attack is when the hacker intercepts the information transmitted on the system, modifies it, and retransmit it to achieve his/her evil aim.

Passive attack: A passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive attack are in the native of eavesdropping on or monitoring of transmission. The goal of the attacker is to obtain information that is being transmitted. Types of passive attacks are as follow.

The release of message content: In release of message content, a telephonic conversation, an E-mail message or a transferred file may contain confidential data. A passive attack monitors the content of the transmitted data. Passive attack are very difficult to detect because they do not involve in any alteration of the data. When the message are exchange, neither the sender nor the receiver is aware that there is a third party capturing their message. This can be prevented by encryption of data.

Traffic analysis: In a traffic analysis attack, a hacker tries to access the same network as you to listen (and capture) all your network traffic. From there, the hacker can analyze that traffic to learn something about you or your company. Suppose that we had a way of masking (encryption) of information, so that the attacker even if captured the message could not extract any information from the message. The hacker could determine the location and identity of communicating host and could observe the frequency and length of the messagee being exchanged. This information might be useful in guessing the nature of the communication that was taking place. Expert Insights. (2022). https://expertinsights.com/insights/10-high-profile-attacks-2021/

Active attack: In an active attack, the attacker attempts to alter system resources or manipulate the operations of the system. Active attack involves modification of the data stream or creation of false statement. Types of active attacks are as follow.

1) Masquerade: A masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification. If an authorization process is not fully protected, it can become extremely vulnerable to a masquerade attack. Masquerade attacks can be perpetrated using stolen passwords and logons, by locating gaps in programs, or by finding a way around the authentication process.

2) Modification of messages: it means that some portion of the message is altered or that message is delayed or reordered to produce an unauthorized effect. For example, a message meaning “Allow JOHN to read confidential file X” is modified as “Allow Smith to read confidential file X”.

Repudiation: A repudiation attack happens when an application or system does not adopt controls to properly track and log users’ actions, thus permitting malicious manipulation or forging the identification of new actions. This attack can be used to change the authoring information of actions executed by a malicious user in order to log wrong data to log files. Its usage can be extended to general data manipulation in the name of others, in a similar manner as spoofing mail messages. If this attack takes place, the data stored on log files can be considered invalid or misleading. An example of a repudiation attack might be someone accessing your e-mail server and sending inflammatory information to others. This information can prove embarrassing to

Copyright (c) 2022 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

https://journals.researchparks.org/index.php/IJHCS e-ISSN: 2615-8159 | p-ISSN: 2615-1898
Volume: 04 Issue: 9 | Sep 2022

you or your company if this happens. Repudiation attacks are fairly easy to accomplish because most e-mail systems do not check outbound mail for validity. Repudiation attacks usually begin as access attacks. A common type of repudiation attack would involve a customer who claims that they never received a service for which they were billed. In this situation, the burden of proof is on the company to prove that the information used to generate the invoice is accurate. If the data has been modified by an external attacker, accuracy verification of the information may be difficult. Owasp. (n.d). https://owasp.org/www-community/attacks/Repudiation_Attack#:~:text=A%20repudiation%20attack%20happens%20when,the%20identification%20of%20new%20actions.

Denial of Service Attacks (DoS): *Denial of service* (*DoS*) attacks, prevent access to resources by users authorized to use those resources. An attacker may attempt to bring down an e-commerce website to prevent or deny usage by legitimate customers. DoS attacks are very common on the Internet. They have hit large companies such as Amazon, Microsoft, and AT&T. These attacks are often widely publicized in the media. Most simple DoS attacks occur from a single system, and a specific server or organization is the target. Several different types of attacks can occur in this category. These attacks can deny access to information, applications, systems, or communications. In a DoS attack on an application, the attack may, bring down the website while the communications and systems continue to operate. In a denial of access to a system, the operating system is crashed. A simple reboot may restore the server to normal operation. A DoS attack against a network is designed to fill the communications channel and prevent authorized user access. A common DoS attack involves opening as many TCP sessions as possible. This type of attack is called a TCP SYN flood DoS attack. An attack that is similar in the objective is called a *Distributed Denial of Service Attack*. This type of attack amplifies the concepts of a DoS by using multiple computer systems to conduct the attack. Flylib. (n.d). https://flylib.com/books/en/4.213.1.25/1/

Replay: A replay attack occurs when a cybercriminal eavesdrops on a secure network communication, intercept it, and then fraudulently delay or resend it to the receiver to misdirect the receiver into doing what the hacker wants. The added danger of replay attacks is that a hacker doesn't even need advanced skills to decrypt a message after capturing it from the network. The attack could be successful simply by resending the whole thing. Biswal, C.S. & Dr. Pani, A.K. (2020).

Conclusion

Due to the increase in network applications, the problem of network security is becoming more and more serious. Due to the diversity of computer network connections, terminal distribution in homogeneity, network openness, and sharing of network resources, the computer network is vulnerable to viruses, hackers, malware attacks, and other misconduct. To ensure the safety and smoothness of information, the network security and preventive measures are eyebrow nimble.

Recommendations

1) The Government should develop national cybersecurity laws to prevent, investigate, and take actions against cybercrimes that their citizens, businesses, and critical infrastructure face.
2) Enforcement of National Cybersecurity Agency (NCA)
3) Provision of a national critical infrastructure protection program
4) Provision of a national robust mobilization incident response and recovery plan
5) Defined laws pertaining to all cybercrimes
6) Provision of vibrant cybersecurity ecosystem

Copyright (c) 2022 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/

https://journals.researchparks.org/index.php/IJHCS e-ISSN: 2615-8159 | p-ISSN: 2615-1898
Volume: 04 Issue: 9 | Sep 2022

References

1. Adrian. (2020). *What is a dictionary attack and how to prevent it*?. https://www.internetsecurity.tips/what-is-a-dictionary-attack-and-how-to-prevent it/#:~:text=In%20a%20Dictionary%20attack%2C%20cyber,to%20guess%20the%20correct%20credentials.
2. Biswal, C.S. & Dr. Pani, A.K. (2020). *Cyber-crime prevention methodology*, utkal university, p8-10,
3. Buckbee, M. (2020). *What Is a Man-in-the-Middle Attack: Detection and Prevention Tips* https://www.varonis.com/blog/man-in-the-middle-attack.
4. Byos. (n.d). *How to prevent malware attacks*. Retrieved from https://www.byos.io/blog/how-to-prevent-malware-attacks
5. CASHTEST SECURITY. (2022). What is password attack. https://crashtest-security.com/password-attack/
6. Expert Insights. (2022). *The top 10 biggest cyberattacks of 2021*. https://expertinsights.com/insights/10-high-profile-attacks-2021/
7. ExtraHop. (n.d). *Denial of service attack: definition, examples, and prevention*. https://www.extrahop.com/resources/attacks/dos/
8. Flylib. (n.d). *Attack strategies*. https://flylib.com/books/en/4.213.1.25/1/
9. Imperva. (2021). *What Is SQL Injection: SQL (Structured query language) Injection*. https://www.imperva.com/learn/application-security/sql-injection-sqli/
10. Lifars. (2020). *Motivations behind cyber-attacks. LIFARS, a Security Scorecard company*. Retrieved September 18, 2022, from https://www.lifars.com/2020/03/motivations-behind-cyber-attacks/
11. McCoy M. (2019). *Negative effects of hacking*. https://itstillworks.com/negative-effects-hacking-12040354.html
12. Owasp. (n.d). *Repudiation attack*. https://owasp.org/www-community/attacks/Repudiation_Attack#:~:text=A%20repudiation%20attack%20happens%20when,the%20identification%20of%20new%20actions.
13. Smith, T.E. (2013). *A conceptual review and exploratory evaluation of the motivations for cybercrime*, p13, 19.
14. Watering, J.V (n.d). *The Origin of Cybercrime*. https://goosevpn.com/blog/origin-cybercrime.

Copyright (c) 2022 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY).To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/