Ace Cloud Hosting

9 SECURITY THREATS

YOU SHOULD BE AWARE OF

Index

Introduction

The new-age technological developments have impacted businesses in different ways. Although these developments have eased various business operations by introducing automation, mobility, and flexibility into the systems, these changes come with a higher risk of security threats.

According to a study by the University of Maryland, every 39 seconds, hackers attack the computer system that is connected with an internet connection. It accounts for up 2,244 times a day.[1]

The security attacks on a company can lead to significant data loss, which can disrupt business operations. Hence, it is essential to step-up your security measures to ensure integrity, confidentiality, and availability of the information.

The very first step you must follow is to increase awareness concerning the threats that can harm your business data. These attacks can be classified under three sources:

Environmental

Technological

Human-factor

1.Environmental

Environmental threats to data are non-malicious attacks that can be caused by natural phenomena such as floods, fire, earthquakes, hurricanes, and other natural disasters. It causes disruptions at the physical level and involves only external factors.

Precautions:

You can secure your data by ensuring its redundancy within the system. It can be achieved either by backing up the information on local servers or by opting for third-party cloud backup solutions. Opting for cloud hosting means that your data is stored at off-site server farms, i.e., away from the office location.

Also, you can check with your cloud provider if they offer business continuity and disaster recovery options wherein data is backed up at multiple locations. It allows you to continue operations even if one of the locations is not operable at any time.

2. Technological

Threats due to hardware malfunctions can increase the vulnerability of data. The main reasons for the same are the use of outdated software and hardware. Also, hosting the business information on the local device can compromise with the integrity of the data, which can be caused due to reasons like a power failure.

Precautions:

It is essential to update your IT infrastructure regularly. Old technology hardware can hinder business processes as they are not reliable.

Moreover, it is crucial to implement 24/7 hardware monitoring to ensure there are no anomalies on the IT infrastructure.

3. Human-Factor

The threats caused by human agents can be malicious as well as non-malicious. While some of the threats are a result of errors caused by ignorant employees, most of the attacks are malicious that are deliberately perpetrated by hackers in order to cause unavailability, corruption, and misuse of information. These attacks can be categorized as cyberattacks.

HERE ARE SOME OF THE MOST COMMON CYBERATTACKS YOU MUST KEEP A NOTE OF:

A. Malware Attack

Malware attack is a type of attack carried out through malicious applications that are installed on the end-user's system. It can potentially cause damage to any computer device, network, or server. Some of the prevalent malware attacks include:

- Worms - It is a self-replicating malware that consumes the bandwidth of the network by overloading the system.
- Virus - It is a kind of malware that is spread from one system to another through emails, program codes, files, and more.
- Ransomware - In this malware attack, a malicious user restricts the access of a user's system until and unless he/she agrees to pay a ransom. According to the predictions by Cybersecurity Ventures, the ransomware attacks are expected to attack every 11 seconds in 2021.[2]
- Trojan Horse - This malware attack gives the malicious user remote access to the victim's computer.
- Spyware - It is a malware attack that involves spying of user's activity by the unauthorized user.
- Rootkit - In this malware attack, third-party users can remotely access the data on a system without the knowledge of the user.

Precautions:

Installing antivirus and anti-malware software can help keep these malware attacks at bay. It is also essential to setup multiple firewalls along with a multi-level authentication system to avoid any unwanted intrusion.

You can also prevent such attacks by adopting simple techniques, such as using stronger passwords, staying wary of suspicious emails, downloading files from a verified source, not opening untrusted URLs, etc.

B. Phishing Attack

A phishing attack is a practice of sending fake emails that trick users into taking a particular action, such as clicking a link or downloading a file. These files contain malware that gets injected into the system when the user downloads or opens them.

As per the stats provided by CSO, 80% of the security threats are identified as phishing attacks.[3]

These emails are often difficult to distinguish from the original ones and appear as if they are sent from trusted sites.

Precautions:

It is essential to be vigilant while clicking any link in an email. Most of the links might seem like they are from a well-known source. However, they can have subtle changes in spellings or a slightly different format. For example, scammers can send out an email from "faceb00k.com" instead of "facebook.com". Hence, there is a need to notice these slight changes carefully in order to protect your business information.

Also, check for any redirected links that can send you to a similar looking website page and gather your personal data.

C. Drive-by Attack

The drive-by attack uses insecure websites to plant a code that injects malware into the systems of the website visitors. Unlike other malicious attacks, the drive-by attack can be activated simply by visiting a website.

Precautions:

In order to avoid the drive-by attack, the system should be regularly updated, firewalls should be implemented, and an antivirus system should be deployed. Also, avoid opening any suspicious websites and try to stick to reliable sites for surfing the web.

D. Password Attack

One of the most common methods of security breaches is password attacks. Setting up weak passwords can endanger your company's data. Cybercriminals mainly use two types of approaches to figure out the password:

Brute Force attack- It is applied by trying out words or numbers related to a person's name, date of birth, job, etc.

Dictionary attack- It constitutes trying out commonly used words or numbers for passwords. For example- 123456789.

Precautions:

It is essential to implement various methods of setting up strong passwords that are not easily hacked. These practices include:

- Create strong passwords that are a combination of alphabets, numbers, and special characters.
- Choose a longer password with more character strength.
- Don't use a single password for all of your business accounts.
- Don't give your password/ OTP to random strangers.

E. Distributed Denial of Service (DDoS)

Denial of Service attack overloads the system/network by sending in unnecessary traffic. It further restricts the bandwidth of the system, limiting the ability to do high-priority tasks.

An advanced version of the DoS attack is DDoS (Distributed Denial of Service) attack wherein the victim's system is attacked by a large number of host systems that are controlled by a single system belonging to the malicious user. It makes tracking down the unauthorized user much more difficult compared to the one in the DoS attack.

Precautions:

It is important to setup a reliable firewall to mitigate the DDoS attack. Another helpful step you can take is to adopt cloud technology.

Cloud technology uses larger bandwidth than on-premise servers, and hence can hold on more traffic and is less likely to fail in case of an attack. It also helps to diminish the impact on the destination server, as the cloud gateway is the first point of contact during the DoS attack, which further filters out the unwanted traffic.

F. Cryptojacking Attack

Cryptojacking is an attack on someone else's system, mainly targeted to mine cryptocurrency. An unauthorized user uses two techniques to achieve it.

One is by sending fake emails and prompting users to click on a link, which further leads the crypto-mining code to run in the background of the victim's system. The other way is by targeting different websites and popping ads that will execute the infected script in the system.

Precautions:

In order to prevent this attack, you must be careful about opening any spam mail in your inbox.

Moreover, it is crucial to install ad-blocking extensions on the web browser as they are an effective measure to detect any crypto-mining code.

G. Man In The Middle Attack

In a man-in-the-middle attack, an illegitimate user poses as a user in a session or one of the sites that the clients are trying to access. The malicious user sits in the middle to spy on the information or disclose any confidential data which can exploit the privacy of a company.

In this attack, an unauthorized person somehow manages to gain control of the user's system and replaces the system's IP address with its IP address, hence, tricking the server into believing that it is still communicating with a legitimate user.

Precautions:

It is crucial to implement end-to-end encryption in the system to ensure the integrity and confidentiality of data.

The man-in-the-middle attacks are less likely to happen over an HTTPS website. Therefore, always try to download files from such websites as they are much more reliable. Also, you must not access any public Wi-Fi as it can compromise with the security of data.

Wrapping Up

Security attacks are on the rise, and in order to take effective measures, it is crucial to understand the potential threats on the system and its vulnerabilities. Data security is one of the most significant factors that give a company a competitive edge over others.

It further helps to counter corruption and illegal usage of personal information that may include your social security number, bank details, medical records, passport data, and more. Moreover, having a secure environment facilitates a better focus on core business tasks and hence, enhances customer experience.

About Ace Cloud Hosting

Ace Cloud Hosting is a leading hosting provider in the field of accounting, construction, legal, real estate, and several others.

We have also won awards like K2 2019 Quality Award for Customer Satisfaction, FinancesOnline Great User Experience Award 2018, and Accountex USA 2016 User Favorite Award in the application hosting category.

We offer cloud hosting on superfast SSD-based servers with 99.999% uptime, 100-days rolling data backup, and always-on support. We also ensure the security of data through various security measures that include end-to-end encryption, antivirus and anti-malware system, multiple firewalls, multi-level authentication, and more.

At Ace Cloud Hosting, we take the security of our user's data very seriously. Learn more about the measures we implement to help protect your data from cyberattacks. - www.acecloudhosting.com/ace-security/

References

1) https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds

2) https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

3) https://www.researchgate.net/publication/266686928_Classification_of_Security_Threats_in_Information_Systems

4) https://www.acecloudhosting.com/blog/security-threats-accounting-firms/

5) https://www.acecloudhosting.com/blog/cybersecurity-trends-2020/

6) https://www.acecloudhosting.com/blog/stay-safe-against-ransomware/

Ace
Cloud
Hosting

www.acecloudhosting.com