Journal of Information Systems Engineering and Management
2025, 10(42s)

e-ISSN: 2468-4376

https://www.jisem-journal.com/

Research Article

Impact of Cyber Attack over Business

Dr. Sriprasadh K[1*]

[1*]Assistant Professor ,Department of computer science and applications, Faculty of Science and Humanities, SRM Institute of Science and Technology., Vadapalani, Ph: 9994215812; srisaiprasadhhh@gmail.com ,

ARTICLE INFO

Received: 20 Dec 2024
Revised: 12 Feb 2025
Accepted: 20 Feb 2025

ABSTRACT

Business is the activity performed based on trust, without trust the business can't be run in easy manner. Crimes are in the form of threats, the attackers' attempts to steal the individual credentials and make use of that and steal the money or the credentials. The attack on business is in the form of data breaches, malware infections, phishing scams and denial of service attacks and identity theft. This attack and threats will cause the business in increasing production cost, operational disruptions due to vulnerable attack, chances of changing business practices , reputational damages and the loss of trust of the customers ,loss of revenue and threat to intellectual property This trust has the threat through cybercrimes. This will impact in the business , there will be loss of business, loss of credits and in some cases there will be the loss of customer also is unavoidable . In this paper the cyber threats are discussed and security aspects for the threats is been discussed. In this paper various security aspects are considered and discussed. This work provides ideas to defend the cyber attack and overcome the loss caused by the attack.

Keywords : Cybercrime ,Cyber, Cyber attack preventation

Introduction

Nowadays business transactions are made through system ,hand to hand money transactions are reduced to 50% and below nowadays.Most of them are not carrying nowadays . Most of them prefer digital mode of transaction rather than cash oriented transaction. Cash is the blood of the business. Without cash flow there is no business. Business is for cash , if cash is not the moto then it is service .

As the cash is been transferred through online there are some pit holes that to derail the business , it is meant as cyber attack , cyber attack mostly classified into way two ways in name of Active attack and Passive Attack Active Attack : In today's digital world, cybersecurity is an ever-growing concern. Active attacks are Therefore, it is crucial for individuals and organizations alike to implement strong cybersecurity measures, such as antivirus software and two-factor authentication protocols, to protect themselves from these threats.

Different Ways of Active Flak

Denial of service Attack (DoS) :This flak will flood the service request to the server by that entire business server service will come to halt ,by that real users will denied to access the service

Distributed denial of service Flak (DDoS) : The work meant as A Distributed Denial of Service *(DDoS)* flack is a form of cyber flack aimed at rendering an online service unavailable to its intended users. The attack is carried out by overwhelming the targeted server, website, or network with a massive influx of accumulation from aggregate origin. This is typically achieved by leveraging a network of compromised computers, known as a botnet, to flood the target with requests until it can no longer function as intended.DDoS attacks can be distinguished based on the attack vectors and methods employed.

Journal of Information Systems Engineering and Management
2025, 10(42s)

e-ISSN: 2468-4376

https://www.jisem-journal.com/

Research Article

Denial of service Attack impact in Business *Distributed denial of service (DDoS)* attacks continue to pose a persistent threat, primarily due to their high success rate. The ramifications of an effective DDoS attack can be catastrophic, both financially and operationally. Furthermore, businesses of all sizes remain vulnerable to these threats, which can result in severe reputational damage. Beyond the obvious financial losses, a successful DDoS attack can cause a loss of productivity, customer dissatisfaction, and permanently dissatisfied customers. Additionally, DDoS attacks can serve as a gateway for malicious actors to access sensitive information, thereby jeopardizing an organization's data and resources. Taking proactive measures to protect against these attacks is, therefore, of utmost importance. This includes investing in advanced DDoS protection solutions and implementing a comprehensive cybersecurity strategy that is tailored to the business's specific needs. Such measures can effectively mitigate the risks posed by DDoS attacks and safeguard business operations and reputation.

Phishing Attack

One of the active attack is phishing attack in this attack,the sources of phishing can be identified when attackers would use email to trick users into providing their login credentials. Since then, phishing has taken many.Vishing involves the use of voice to deceive individuals.Given the serious consequences of phishing attacks, it is crucial for organizations to prioritize the protection of their systems and data instead falling victim to these attacks and safeguard their operations and reputation.

Phishing is a social engineering tactic that has gained notoriety for its ability to deceive individuals into divulging sensitive information or downloading malware. The term “phishing” is derived from the analogy of a fisherman throwing a line and bait with the hope that an unwary fish will bite. The term gained popularity among hackers in the 1990s, particularly among those who targeted AOL users and their login credentials. The spelling of “phishing” with a “ph” rather than an “f” is attributed to the hacker tradition of coining techniques using unconventional spellings, as seen in the term “phreaking” or phone phreaking, an earlier form of hacking. Despite the advent of sophisticated cybersecurity technology, phishing continues to be the most widespread form of social engineering and has caused significant damages to organizations. Notable phishing attacks have resulted in losses of millions of dollars. For instance, Facebook and Google lost $100 million between 2013 and 2015 in a phishing campaign that exploited their Taiwanese vendor Quanta, while the Crelan Bank in Belgium and Austrian aerospace parts manufacturer FACC suffered CEO Fraud attacks that resulted in losses of $75.8 million and $65 million, respectively. Phishing flack carry on to be a epochal menace to organizations, with the Verizon Data Breach Incident Report for 2020 revealing that phishing was responsible for 22% of the reported incidents. As such, organizations must remain vigilant and implement measures to protect against these attacks. This includes training employees on how to identify and respond to phishing attempts, implementing security best practices, and regularly testing the organization's security posture.

Phishing attacks have two primary objectives: to solicit sensitive information or to infect systems with malware. In the former case, attackers may send fraudulent messages that impersonate trusted entities, tricking unsuspecting For instance, attackers may masquerade as a bank and send phishing emails to a large number of individuals, hoping to lure one of them into entering their login details on a fake website designed to look like the actual login page of the bank.

Prevention of Phishing

In addition to education, there are several tips that individuals can follow to protect themselves from phishing attacks. These include verifying the spelling of URLs and email addresses, being cautious of spoofed website pages designed to mimic popular websites, communicating with the sender to verify suspicious messages, and limiting the amount of personal information shared online. Organizations can also play a significant role in protecting their employees from phishing attacks. This can involve conducting penetration

Journal of Information Systems Engineering and Management
2025, 10(42s)

e-ISSN: 2468-4376

https://www.jisem-journal.com/

Research Article

tests or vulnerability assessments to identify and fix system weaknesses that can be exploited in a phishing attack. Other measures include monitoring web traffic on all devices, screening communications for suspect links and reputation. Individuals can also protect themselves by adopting a proactive approach to security and remaining vigilant when receiving messages that may be suspicious.[3]

Impact of Cyber attack over Business

1. Increasing Cost

The financial implications of cybercrime on businesses cannot be overemphasized. Firms must incur various expenditures, including In the aftermath of the breach, Equifax was subjected to extensive litigation, culminating in the company agreeing to pay up to $425 million to assist affected individuals. The U.S. Federal Trade Commission reports that this settlement was the largest in U.S. history, and it included up to $300 million for free credit monitoring services for affected individuals and up to $125 million for out-of-pocket expenses and other losses.

2. Disruption of Operation

The potential for operational disruption underscores the importance of cyber resilience planning. Businesses must have robust strategies in place to ensure that they can continue with their normal activities in the event of a cyberattack. These strategies should include contingency plans such as backup systems and communication protocols to enable business continuity in the face of disruption. Companies that prioritize cyber resilience can mitigate the risk of operational disruption and the associated financial and reputational costs that arise from cybercrime.

The 2010 cyberattacks against Mastercard and Visa by a group of individuals with links to WikiLeaks demonstrate how cybercrime can be employed as a tool for activism or political agendas. The attacks resulted in temporary website crashes, causing significant reputational and financial damage to the targeted organizations. Hacktivists frequently target prominent corporations or government agencies to call out perceived injustices or express dissent. Such attacks can pose a threat to national security and result in significant financial and reputational losses for the targeted organizations.

3. Alteration of Business

The dynamic nature of cybercrime underscores the importance of cyber resilience planning. Companies must prioritize cybersecurity measures to safeguard their systems and confidential information. By investing in cybersecurity technology and expertise, they can mitigate the risks of cyberattacks, and reduce the potential for operational disruption or reputational harm. In addition, companies should make concerted efforts to educate their customers on the steps they are taking to protect their sensitive information. This can enhance customer confidence and trust, leading to increased customer loyalty and patronage.

4. Damage of Reputation

The impact of cyberattacks on a company's brand equity can be challenging to quantify but can be substantial. Following a cyberattack, customers and suppliers may be less inclined to entrust their trust. The 2013 data breach involving the credit card information of over 40 million customers was a significant setback for retail giant Target (TGT), resulting in damaged reputation and a settlement cost of $18.5 million. In addition to the loss of institutional trust, research suggests that publicly traded companies may experience a short-term drop in market value following a cyberattack. . The potential for loss of brand equity and market value underscores the importance of cyber resilience planning. Companies must prioritize cybersecurity measures to safeguard their systems and confidential information. By investing in cybersecurity technology and expertise, companies can mitigate the risk of cyberattacks and reduce the potential for operational disruption or reputational harm. In addition, companies must take proactive steps to communicate their efforts to secure sensitive information to their stakeholders, including customers and shareholders. This can help to preserve brand equity and instill confidence in a company's ability to protect sensitive information.

Journal of Information Systems Engineering and Management
2025, 10(42s)

e-ISSN: 2468-4376

https://www.jisem-journal.com/

Research Article

5. Loss of Income

It become cautious and shift their business elsewhere to protect themselves against cybercrime. The year after 2013 cyberattack on Sony Pictures illustrates the potential impact of cybercrime on revenue.Stole of sensitive information, is a major attack on the business .The evaluations from its staff. Although the perpetrator of the attack was widely attributed to North Korea, the country denied the allegations. As a result, . The potential for substantial financial losses underscores the importance of cyber resilience planning. Companies must prioritize cybersecurity measures to safeguard their systems and confidential information. By investing in cybersecurity technology and expertise, companies can mitigate the risk of cyberattacks and reduce the potential for operational disruption or reputational harm. Furthermore, companies must take proactive measures to communicate their efforts to secure sensitive information to their stakeholders, including customers and shareholders. This can help to preserve brand equity and instill confidence in a company's ability to protect sensitive information and mitigate the risk of financial losses due to cybercrime.

6. Theft of Intellectual Property

The idea theft of an organization, including its creation stylisme, applications, and all kind of tactics, frequently represents important assets. Accordant to ideological possession consultancy firm However, the storage of such intellectual property in the cloud also exposes it to the risk of cyberattacks. Alarmingly,.[4]

Protection the Business for m Cyber Attack

In order to safeguard against cyber threats, businesses must implement proactive measures to secure their networks and databases. Such measures include setting up firewalls, encrypting information and minimizing the risk of cyber criminals gaining access to confidential information. It is also critical to ensure that Wi-Fi networks are hidden and password-protected, and that only selective information is stored in databases. Companies must schedule automatic data backups, either on a daily or weekly basis, depending on the levels of activity within the organization. Timely data backups increase the chances of data recovery in the event of a cyber attack, a situation that is all too common. In addition, it is essential to train employees in cybersecurity best practices. Employers must educate their . This should include setting policies and guidelines for acceptable and unacceptable practices, and limiting administrative access to minimize the risk of malicious software downloads and viruses. To further protect against cyber attacks, companies should establish security policies and practices. This includes outlining how situations will be handled and the consequences of policy violations. Physical access to company devices should be controlled, and devices should be disposed of properly to prevent unauthorized access to company information. Employees should be trained to distinguish between fake antivirus warnings and real notifications.

Conclusion

Companies must communicate to service receivers about why their personal information is collected and how it will be used. It is important to assure customers that sensitive information will not be requested over unprotected methods of communication, such as text messages or email. Customers should be encouraged to report any suspicious communications.[5]

References :

[1] https://cybermagazine.com/cyber-security/how-are-ddos-attacks-impacting-businesses-and-services
[2] https://www.arkoselabs.com/blog/stop-ddos-attacks-from-hurting-your-business/
[3] https://www.stickmancyber.com/cybersecurity-blog/what-is-phishing
[4] https://www.investopedia.com/financial-edge/0112/3-ways-cyber-crime-impacts-business.aspx
[5] https://www.mass.gov/info-details/protect-your-company-from-cyber-attacks