IJCSN - International Journal of Computer Science and Network, Volume 8, Issue 4, August 2019
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

The Impact of Cyber Attacks on E-Businesses

[1] Odero Eunice; [2] Bundi Dorothy; [3] Omari Omosa

Abstract - Globally, the cyberattack headlines keep getting grimmer and grimmer: Hackers Steal Bank's Valuable Data. Big Box Store Says Millions of Credit Card Records May Have Been Snatched. US Indicts Chinese Army Officers for Hacking Industry Trade Secrets and most recent of all Wannacry Ransomware infiltrates windows platform. Cyberattacks of the past year have been rattling the IT world, making executives and IT managers wonder how vulnerable their own networks might be. And the incidents are increasing. A recent global survey PwC conducted with CIO Magazine and CSO Magazine shows that the number of attacks reported by midsize companies has jumped 64% since a year ago. Today's hackers are farsighted and more tenacious now when it comes to midsize and smaller companies. To avoid these losses, companies need to take a hard look at their defenses up front. Yet a big reason companies often fail to invest in cybersecurity is that they see it as discretionary spending, not a business imperative. With profitability being top of mind, businesses tend to be more inclined to invest in growth activities than defensive measures. This paper employs an exploratory research design on existing literature with a focus to generate a workable hypothesis to be tested in future empirical studies. The objective of the study is to create awareness of cyber-attacks and to explore the impacts of cyber-attacks on e-businesses. This will be followed by identification of cyberattack techniques that can be used against e-business. This will be followed by recommendation of preventive mechanisms that should counter cyberattack attempts since most e-businesses are focused more on reactive rather than proactive measures. The results of this paper will be used to advice e-business stakeholders on how to improve cyber security and how to prevent a cyberattack.

Keywords - Hackers, Code Red, E-Business, Cyberattacks, Ransomware

1. Introduction

The 'e' revolution has swept through business creating e-business and e-commerce. Increased customer access to services has driven businesses to move operations to e-business. With this move to a new method of doing business, businesses have adapted operating procedures to capitalize on this new distribution channel. (Harris, 2016) In addition to business to consumer (B2C) channels, business to business (B2B) channels have changed as well. Internal business operations have also become enhanced through the communication channels provided by e-business. (Anderson, 2014).

E-Businesses come in many sizes, shapes and markets. Whereas Amazon can be viewed as a reinvention of normal business, e-Bay, Yahoo, and Google can be seen as entirely new creations. Each of these firms has had its business troubles, yet has ridden out the tough times and joined the ranks of profitable firms in the business landscape. Regardless of the industry, the basic business model is one of firms interfacing with suppliers and customers. The number of relationships is bounded in type, but not in quantity. (Anderson, 2014) For a firm to double its ability to service its customer base the driver is mostly just one of capital – just add servers.

Compared to the time requirements for adding trained personnel and physical facilities, the advantages with respect to speed become obvious. The next generation of e-business involved not just automating normal business processes, but enhancing them with new offerings. A prime example would be the integrated financial offerings offered to ordinary people. (Bicknell, 2015) Bank accounts and investment accounts are electronically linked so that a user can execute trade orders or transfer funds anytime, day or night. Advanced information tools such as charting and analysis functions provide information. (Burns & Fiftheen 2013) Marketing determines business opportunities and business units execute on the plans. These required changes present challenges and opportunities to agencies as they move services to new media. A simple example of records security and retention provides illustration to this concept. (Harris, 2016).

Cyber security can simply be defined as security measures being applied to computers to provide a desired level of protection. (Anderson, 2014)The issue of protection can be defined using the acronym CIA for Confidentiality, Integrity, and Availability. (Bicknell, 2015) Confidentiality refers to the property that data should only be viewable by authorized parties. Integrity refers to the principle that only authorized users are allowed to change data, and that these changes will be reflected uniformly across all aspects of the data. (Burns & Fiftheen 2013)

Availability refers to the principle that data and computer resources will always be available to authorized users. Using the word simple to describe computer security is misleading however, much as it can be said to be simple to play golf. Just it the ball in the hole in as few strokes as possible. (Burns & Fiftheen 2013).

The current lack of Government support for security on the Internet is forcing businesses to rely on their own personal security measures to protect themselves from cybercrimes, however this is not sufficient in ensuring that cyberspace is a safe haven. (Bicknell, 2015)

2. Research Methods

This paper employs an exploratory research design on existing literature with a focus to generate a workable hypothesis to be tested in future empirical studies. The objective of the study is to create awareness of cyberattacks and to explore the impacts of cyberattacks on e-businesses. This will be followed by identification of cyberattack techniques that can be used against e-business. This will be followed by recommendation of preventive mechanisms that should counter cyberattack attempts since most e-businesses are focused more on reactive rather than proactive measures. The results of this paper will be used to advice e-business stakeholders on how to improve cyber security and how to prevent a cyber-attack.

The security threats in E-Business environment are as follows:

- ✓ **Virus:** A virus is a malevolent program which is anticipated to affect the system with severe loss. The virus may get fix itself to the separate file or a group of files leading to severe loss by acquiring more space, modifying files, folders, slow response of the system. (Anderson, 2014)
- ✓ **Adware:** Adware is considered to be a malevolent which are embedded into the advertisement if the customer unknowingly clicks on it leads to fraudulent activity by seizing customer credentials. (Bicknell, 2015)
- ✓ **Spyware:** Spyware that performs like an application but its main motive is to gather the credentials of the individuals after gathering the credentials it will send this to the malicious attacker which are connected in the network. (Burns & Fiftheen 2013)
- ✓ **Ransomware:** Ransomware is a type of malicious software that threatens to publish the victim's data or block access to it until a ransom is paid. On June 2017, one of the worst ransomware attacks in history was carried out by attackers. The Wannacry ransomware led to unimaginable losses for the big companies and was also a major blow to many e-businesses (Gengler, 2017)

The cyber-attack that are possible at customer side are as follows

- ✓ **Phishing**: Phishing is an attempt to seize customer's identifications such as PIN number, account details. The malicious attacker may add the forged E-commerce login page to the legitimate website if the website is vulnerable to attack. Normally, the forged e-commerce websites are widely spread by emails. If the customer has an awareness of this type of cyber-attack he/she will be protective from this attack otherwise it leads to an identity theft by grabbing the user credentials. Seized credentials may leads to threatening the customer by fulfilling the attacker needs. (Bicknell, 2015)
- ✓ **Pharming**: Pharming is similar to phishing attack. The main motive of this attack is to steal customer information by redirecting them to the spurious website. When the domain name of the website is typed in the web browser it first converted into the Numerical address that is IP address which are done using DNS Server. If the IP address is redirected to spurious website it will lead to Pharming attack. This can be done by compromising the DNS Server also it is not a usual attack like phishing. (Anderson, 2014)
- ✓ **Log Forgery**: The un-sanitized input from the user to access the log files may leads to log forgery or inserting malevolent things to the log. By altering the log file information may leads to a severe impact. (Bicknell, 2015)
- ✓ **Password attacks**: To crack the customer login id and password there are many password cracking tools by cracking the password the attacker may steal the customer's online credentials. Also it leads to cancelation of ordered products by the customer or ordering the new product. (Burns & Fiftheen 2013)
- ✓ **Cross side scripting Attack**: The other name for cross side scripting attack is XSS Attack. It is the most common type of attack that occur on the website. In this attack, the legitimate E-commerce site is inserted with malevolent code which is done by the attacker. The attacker may vandalize the E-commerce site by exploiting this attack. (Franlin, 2011)
- ✓ **Brute force attack**: It is a type of password guessing attack by using the trial and error method. If the attacker knows about the target customer this type of attack can be performed easily by guessing the password. (Gengler, 2017)
- ✓ **Man in the middle attack**: It is a common type of attack on the internet. The attacker may silently listen the communication that has been taken place between the customer and the server. (Burns & Fiftheen 2013)

- **Session hijacking**: It is also a common type of attack on the internet. In this attack, the one particular session can hijacked for example payment session can be hijacked after gaining the proper authentication. (Franlin, 2011)
- **Snooping**: In order to perform this attack, the attacker executes the malicious program such as key logger to capture the keystrokes that are pressed by the user. (Pastore, 2010) While performing the payment transaction it is better to use virtual keyboard that is present in the website instead of using the keyboard that are connected with the system. (Burns & Fiftheen 2013)
- **Spoofing**: The malicious attacker mimicked himself as the legitimate to access the network or to control the entire network. (Anderson, 2014)

Cyber Attacks in E Commerce at Server Side

- **SQL injection**: The attacker may gain aces to the server if it is vulnerable to query statements. (Harris, 2016) By gaining the access the attacker may perform malicious activities such as viewing, altering or damaging the data that are present on the server. (Burns & Fiftheen 2013)
- **LDAP**: By compromising the vulnerability present on the website the LDAP statement is executed by the attacker. The modified LDAP statement may leads to severe effect such as defacement of the website, illegitimate access to the data. (Bicknell, 2015)
- **Weak Authentication**: It is a type of attack by exploring the vulnerability present on the server by using this the attacker may gain entire access to the server where the entire details are stored. (Franlin, 2011)

Security tools to be used in E-business To Counter Cyber-attacks

- **Firewalls**: The network security system come in handy in monitoring and controlling the traffic (both incoming and outgoing) based on security rules that are predetermined. (Burns & Fiftheen 2013)
- **Intrusion detection system:** This may be either a device or a software program that monitors either a network or a system for malicious activities and incase of any malicious activity there is a notification. (Anderson, 2014)
- **Digital certificate:** This is an attachment to an electronic message that is used to verify if the sender of a certain message is who they claim to be. (Gengler, 2017)
- **One Time Password**: This is a type of password which is valid for only one login session or transaction. (Gengler, 2017)
- **Two factor Authentication:** This is an extra layer of security where authentication of users is verified by reaching them on their mobile devices. (Anderson, 2014)
- **Security tokens:** These are physical devices used to gain access to an electronically restricted resource.
- **Biometrics:** This refers to measurement and statistical analysis of people's physical and behavioral characteristics for authentication and authorization purposes. (Burns & Fiftheen 2013)
- **Salting and hashing for securing passwords:** This is the process of securing password hashes from a rainbow table attack. (Gengler, 2017)
- **Digital signature:** This is an electronic signature that encrypts documents with digital codes that are very difficult to duplicate. (Harris, 2016)
- **Vulnerability Scanning Tools:** These are tools that help in determining how vulnerable the systems are. (Gengler, 2017)

Recommendations to the E-Business Stakeholders and the Government

- Government should implement clear mechanisms that support security on the Internet: The Government must be supported for attempting to offer advice to companies for a small or minimal charge as E-Businesses are more dependent on this type of information due to the restriction on resources available to invest into researching into areas such as these themselves. This must also have a bearing on the advice offered, as SMEs do not share the same characteristics as larger companies.
- The I.T personnel must create awareness of cybercrime and help all E-Business stakeholders to understand what cybercrime is.
- The E-Business stakeholders should create awareness on what really defines an E-Business from the aspect of security.
- The government I.T sector should create awareness of what resources are available to the E-Businesses to improve security.
- E-Businesses thought process should be more based on proactive measures than reactive measures: Many E-Businesses do not perceive themselves to be in any great danger and so do not take it as seriously as they should. Their thought process is based on reactive measures rather than proactive measures.

3. Conclusion

There is a lack of knowledge throughout as to what cybercrime and its threats are. The Government's efforts to encourage e-businesses and discourage cybercrime are virtually unknown and the majority feels that it would have little impact on their company. Many E-Businesses do not perceive themselves to be in any great danger and so do not take it as seriously as they should. Their thought

process is based on reactive measures rather than proactive measures.

The Government should support security on the Internet is so as to protect E-Businesses from cybercrimes thus ensuring that cyberspace is a safe haven.

From the above foregoing, the following two hypotheses are derived: the involvement of the government in supporting security on the internet will improve e-business security and focusing more on proactive rather than reactive measures by the e-business stakeholders will lead to a more secure e-business environment.

References

[1] Anderson, J. 2014, An Analysis of Fragmentation Attacks, Sans Institute, [on-line 11/02/2014], http://rr.sans.org/threats/frag_attacks.php (Anderson, 2014).

[2] Bicknell, C. 2015, Credit Card Fraud Bedevils Web, [on-line 04/03/2015] http://www.wired.com/news/print/0,1294,18904,00.html (Bicknell, 2015).

[3] Business Leaders Warn of cybercrime Threat to Internet Development, 2010, [on-line 24/11/2010].

[4] Burns, R.2013, Introduction to Research Methods, 4th ed, Sage Publications, London [Fifthen, K. 2013, Internet Denial of Service Attacks and the Federal Response, [on-line 13/02/2002] www.cdt.org/security/000229judiciary.shtml (Burns & Fiftheen 2013).

[5] Franklin, I. 2011, A Can of Worms, Science Direct, vol.2016, issue 12, pp12-13.(Franlin, 2011).

[6] Gengler, B. 2017, PayPal's anti-fraud team, ScienceDirect, vol.2002, issue3, (Gengler, 2017).

[7] Harris, G. 2016, Compsec 2016: Watching the Threat from Without, ScienceDirect, Queen Elizabeth II Centre, London pp.19 (Harris, 2016).

[8] Miller, A. 2015, More than half of IT managers are ignorant of rising cybercrime threat, [on-line 3/3/2002] http://www.accoutancyage.com/News/104814 (Milner 2015).

[9] Olusada, C. 2013, DNS Vulnerabilities – Nine Days in the Spotlight, Sans Institute, [on-line 13/02/2002] http://rr.sans.org/DNS/spotlight.php (Olusada, 2013).

[10] Pastore, M. 2010, Retailing: Online Fraud: How Bad is It? [on-line04/03/2002] http://cyberatlas.internet.com/markets/retail/article/0,,6061_46481,00.html(Pastore, 2010)