Cyber security in E-commerce

CH. Sireesha, V.Sowjanya, Dr K.Venkataramana

Abstract:

Now a day, World Wide Web has become a popular medium to search information, business, trading and so on. Various organizations and companies are also employing the web in order to introduce their products or services around the world. Therefore E-commerce or electronic commerce is formed. E-commerce is any type of business or commercial transaction that involves the transfer of information across the internet. In this situation a huge amount of information is generated and stored in the web services. This information overhead leads to difficulty in finding relevant and useful knowledge, therefore web mining is used as a tool to discover and extract the knowledge from the web. Besides, the security issues are the most precious problems in every electronic commercial process. This massive increase in the uptake of e-commerce has led to a new generation of associated security threats. In this paper we use techniques for security purposes, in detecting, preventing and predicting cyber-attacks on virtual space.

Indexterms:E-commerce,Cybercrime,threats,security,attacks.

1. INTRODUCTION

The early struggle with the internet was finding a way to safely buy and sell goods or transfer funds using computer and telecommunication networks. The goal was to enable e-commerce by providing a safe, convenient and immediate payment system on the internet. But internet is notorious for giving its users a feeling of anonymity. The inadequate security results in major damage. Now a day's a number of critical transactions are carried out by computer systems over networks. There is an internet security threat - cyber crime which enables ecommerce transaction face significant financial and information losses.

Recent years have exponentially witnessed the growth of e-commerce. The growth of e-commerce as a business technology is the result of such Internet driven initiative, It has created a universal platform for buying and selling goods and services and driving important business process inside the organization.

Ch.Sireesha is pursuing Mca in KMMIPS University of SVU in Thirupati.

Email:sirichitteni7076@gmail.com

V.Sowjanya is pursuing Mca in KMMIPS University of SVU in Thirupati.

Email:sowjivemula123@gmail.com

Ecommerce offers huge business opportunities from small scale industries to large scale industries. Many organizations now want to host their business on the web to reach the new market as they could not reach effectively with its sales force or advertising campaigns. Since ecommerce is not bounded with time, huge shop rentals, distance etc. With respect to the benefits of modernization of the traditional concepts of shopping, business transactions which use to consume whole lot of time, money etc

E-commerce is suffering with a security threat called cyber crime. The concept of crime has been very dynamic in the past century due to rapid changes in the information technology. Cybercrime has become a rapidly growing underground business built by savvy criminals, who buy and sell valuable stolen financial information from millions of unsuspecting internet users every year in an on online black market. Cyber criminals are so skilled at hacking into thousands of computers every day; the crime is potentially a billion-dollar business. Cyber attacks mostly come from malware, or malicious software, that handles

control of your computer, and anything on it or entered into it, over to the cyber criminals without you even knowing it. The future is likely to be more alarming in the sense that crimes will be committed without the knowledge and cooperation of the victim. Preventing cyber crime in the future will require strong e security rather than plain human prudence. The role, function and efficacy of Law in curbing cyber crimes have been questioned in the recent years due to various technological invasion of individual's privacy. Most of these technologies are legal and hence it is of utmost priority to analyse the necessary changes that have to be made in our legal system in order to avoid technological invasion of privacy. Internet and Electronic Commerce might have become part and parcel of very individual's life in the world but it is also one of the most dangerous aspect of ones life as there is very rare scope for privacy protection and possibility of cyber crimes.

2.E-COMMERCE:

E-commerce (electronic commerce or EC) is the buying and selling of goods and services, or the transmitting of funds or data, over an electronic network, primarily the internet. These business transactions occur either as business-to-business, business-to-consumer, consumer-to-consumer or consumer-to-business. The terms e-commerce and e-business are often used interchangeably. The term e-tail is also sometimes used in reference to transactional processes for online shopping.

2.1 History of e-commerce:

The beginnings of e-commerce can be traced to the 1960s, when businesses started using Electronic Data Interchange (EDI) to share business documents with other companies. In 1979, the American National Standards Institute developed ASC X12 as a universal standard for businesses to share documents through electronic networks. After the number of individual users sharing electronic documents with each other grew in the 1980s, in the 1990s the rise of eBay and Amazon revolutionized the e-commerce industry. Consumers can now purchase endless amounts of items online, both from typical brick and mortar stores with e-commerce capabilities and one another.

2.2 E-commerce applications:

E-commerce is conducted using a variety of applications, such as email, online catalogs and shopping carts, EDI, File Transfer Protocol, and web services. This includes business-to-business activities and outreach such as using email for unsolicited ads (usually viewed as spam) to consumers and other business prospects, as well as to send out e-newsletters to subscribers. More companies now try to entice consumers directly online, using tools such as digital coupons, social media marketing and targeted advertisement.

3. CYBER ATTACKS AND SECURITY FOR E-COMMERCE:

Like the wolf's eyes that always preys on the hen's pen, a hacker's eyes always scurries to steal your online store's data. Hackers are ripping off credit card information, personal identity credentials and even sensitive organizational data (including those of governments) from online databases. The Internet is not a safe place to hoard your data anymore. For E-Commerce businesses, the risk is even grave. The entire business model is pillared on trust. In the words of Jack Ma, the founder of Alibaba , "For E-Commerce, the most important thing is trust." We can't agree anymore. The moment customers start losing trust on your website, they will start logging into your store. With that conversions will go down a spiral pulling your store's profitability along with it. That said, the security worries of E-Commerce business owners are mounting. They are left clueless about:

- How to keep sensitive information safe?
- What counteractive measures should one adopt?
- What common mistakes must one steer clear of?

We'll explain all this and much more in this article.

4. CHOICE OF ECOMMERCE PLATFORM

It not boasts the level of security and functionality that recent versions offer. The first step to guarding your online store begins with choosing a reliable E-Commerce platform. An E-Commerce platform is what a foundation is to a building. The stronger the foundation, sturdier the building will be. There are a number of secure and reliable E-Commerce platforms in the market like Magneto, Shoplift, BigCommerce, WooCommerce, Prestashop, etc. to pick from. Be informed that each platform has its own native features and extensions which can make a sea change to the way you transact your online business. While making a final choice, check for scalable security provisions. Preferably, third party security extensions should also be easily integrable with the platform. Also, make it a point not to pick a platform that runs on expired or near-expiry versions. For instance, Magento has several versions starting from 1.x to 2.x. The older versions may.

4.1 CHOICE OF HOSTING PROVIDER:

Choose a hosting provider who is vested in online security as much as you are interested about your store's security. It is practical to opt someone who offers all or most of the following:

- AES encryption
- Scheduled/Regular backup program
- Network monitoring
- Round the clock technical assistance
- Immediate disaster recovery
- Swift service

At the least, ensure you go with a hosting provider who can keep your store up and running without downtimes interferences. A safe bet will be to opt for quality and reliability over cost-affordability.

4.2 HAVE LESS ,LOSE LESS DON'T STORE SENSITIVE INFORMATION

If you have 20 dollars, you have the possibility of being stolen of 20 dollars. If you have nothing on you, there is no chance you are going to be robbed .The same with sensitive information. Critical records of customer accounts, usernames, credit card information, etc. need to be kept far from the reach of hackers.

The best way is to store them in offline servers which can be accessed when need arises. As for the what to store online, keep only those records relating to immediate charge backs, returns or exchanges that need to be processed.

4.3 GIVE GREEN SIGNAL TO HTTPS ENCRYPTION:

Google hinted in its 2014 I/O Conference that it is going to introduce HTTPS encryption as a major ranking signal for search engine ranking. Apart from the boost that Google will give to your page, you can also make your customers trust your store with an EV SSL certificate. An EV SSL certificate can make your website look trustworthy in the eyes of customers. It works by adding a green HTTPS prefix to the URL and a green padlock symbol on the address bar. The primary benefit of SSI certificate (some refer to it as TLS) is that it encrypts transmission of data between points, i.e. the web server and the browser. Studies like these from digits have also proven that websites with HTTPS encryption enjoy higher conversions than without HTTPS encryption.

4.4 STAY COMPLIANT, STAY SAFE WITH PCI COMPLIANCE:

The PCI (Payment Card Industry) requires every website processing credit card or online financial transacting websites to perform certain security tasks. Annual vulnerability risk assessment is one such requirement for PCI compliance. There are various levels to PCI compliance. Depending on the number of transactions your business transacts in a year, the level of PCI compliance will vary. If your online store has 20,000 transactions or less, then it is required to conduct an annual risk assessment using a self-assessment questionnaire.

Bonus Tip: leave too much of time gap between successive assessment. Do it periodically based on schedules.

4.5UPDATE SOFTWARE, PLUGINS, TEMPLATES, ETC:

All E-Commerce websites have at least few plugin's extensions or templates running in the backend. They are easy to configure, deliver results that are quite difficult to achieve through coding.

Well, they have their own downsides too. To begin with, these plugin's may not be so good at withstanding hacking attempts. They might have potential loopholes which can be exploited to gain backdoor entries into your store and its databases. An ideal way to ensure that the extensions, plugin's and everything else you use in your website is always updated for security. Most extension publishers release periodical security updates that can thwart the latest hacking trends and practices.

4.6 STRENGTHEN PERIMETER DEFENSES:

Do you know? Most of the hackers get into your websites by exploiting weak or broken links in your website. Things like fire wall, VPN, etc. go a long in preventing that. Compare such security measures to a home's perimeter defense. When the perimeter defense is equipped with a card wire, there is no possibility of infiltration. Similarly, your entry points when guarded with a firewall, ensures that only authorized users are allowed entry. Alternatively, you can also set up a user password system where the user must use a minimum strength password. Without setting up such a minimum strength password, the user must not be allowed to log into the store.

5. ADDRESS & CARD VERIFICATION SYSTEM:

An Address Verification System or a Card Verification Value is a great way to weed out the possibilities of fraudulent charges. It is a win-win situation for you as well as your customers. The CVV is the three or four digit number that is imprinted on the back of user's credit or debit card. The user and none else has access to it. Combined with One Time Password, it is a formidable security measure that can prevent online credit card information leaks. Asking for direct input of CVV on checkout has become a default process for most online stores. It ensures that only those payments which the customer sanctioning is getting through.

5.1EMPLOYEE TRAINING AND AWARENESS:

When it comes to organizational information security, employees seem to be lethargic in practicing password hygiene and safety. We all have that peer in our office, who keeps the username and password in broad daylight to be seen by all. Nothing could be more dangerous than

this. This login credentials in wrong hands can spell doom to the entire organization.

It is never too late to make your employees aware of the pitfalls in sharing passwords, login credentials, use of USB devices, unsecured networks, etc. Even if they are shared, they must be immediately replaced with a new password to sustain security.

Some headers to make your employees practice password safety:

- Suggest them to use strong passwords containing a combination of alphabets, symbols and alphanumeric characters
- Set a password expiry period. Every password must be changed every month or quarter
- Deactivate user accounts and their credentials as soon as they leave the organization
- Instruct employees to abstain from writing down passwords anywhere

5.2 IN A NUTSHELL:

Let's face the hard truth. Protecting your E-Commerce store and your customers from harm's way is not easy. Each day the cyber crime rate is increasing by arithmetic proportions. So swift that nations are setting up separate agencies to monitor and curtail fraud and scams targeting E-Commerce. While they are doing their part to ensure online safety, you as a business owner must also ensure that the E-Commerce store is geared up in all possible manner to prevent cyber attacks.

6. CYBER SECURITY CURRENT THREATS:

THE 2 ECOMMERCE MOST DANGEROUS CYBERSECURITY THREATS FOR 2016:

From identity theft and fraud to corporate hacking attacks, cyber security has never been more important for E-Commerce sites, large or smaller ones. Hacking experts warn there are plenty more security risks ahead in 2016 as cyber criminals become more sophisticated. Discover in this article the two most dangerous cyber security threats for 2016.

1 D) E-Commerce site should care about DOS Attack:

What: An attacker overwhelms a server with bogus traffic, causing the website or applications hosted there to slow down or become unavailable. In a recent survey, 60% of respondents saying they are worried about DDOS attacks and 39% admitting it is likely their organization has already been targeted.

Beware: By watching a youtube video, anyone can learn to send DDOS attacks. If website uptime is critical, get DDOS protection. In April 2015, police arrest six UK teenagers on suspicion of using a DDOS attack tool targeting a national newspaper, a school and online gaming companies and retailers.

Solution: On this last point, OZON offers an operational response to all companies that want to be protected against DDOS attacks and much more .OZON is a cloud platform that integrate several innovative security technologies working in synergy. OZON detects vulnerabilities and

malwares, identifies fraudulent transactions and protects against cyber-attacks like DDOS, SQL injection or Cross-Site Scripting (XSS) attacks. All these functions are performed in real time.

2) Poor Patch Management will affect your online business:

What: Many organizations don't force security updates on browsers, applications and databases, leaving easy access for hackers. A few years ago, patch management was barely a blip on the radar screens of most security and IT personnel. 'Install and forget' was a fairly common practice; once deployed, many systems were infrequently or never updated. Obviously, for a number of reasons, this approach is no longer an option. The rise of widespread worms and malicious code targeting known vulnerabilities on unpatched systems, and the resultant downtime and expense they bring, is probably the biggest reason so many organizations are focusing on patch management.

Beware: Recent research indicates. that 80% of data breaches happen by way of known vulnerabilities Hackers will exploit these security holes via spyware, ransom ware, root kits and spam bots. Update, patch, or prepare to be hacked.

Solution: OZON solution enables the detection of vulnerabilities & malwares used in sophisticated cyber-attacks and fraud attempts. The vulnerabilities identified in this assessment give an overview of your application attack surface. Vulnerabilities are grouped above in 4 risk categories. OZON's platform protects you from all these attacks.

7. CONCLUSION:

Cyber crimes have started to create a fear in the minds of many people linked to the networks mostly worried to ecommerce technology as its success lies in the internet. The various mechanisms used for securing internet based transactions or communication can be grouped into ´ Authorization, Authentication and Integrity ´ Privacy ´ Availability by controlling access In order to safe guard the present success of e-commerce The IT Act 2000 has to be reviewed in order to save India from Cyber criminals and privacy invaders. Cyber criminals should not take the advantages of browser ignorance, legislative delay, enforcement lapse, judicial inefficiency.

8. REFERENCES:

1.http://cse.stanford.edu/class/cs201/projects/computer-crime/theft.html.

2. http://en.wikipedia.org/wiki/E-mail_bomb.

3.http://legal.practitioner.com/computer-crime/computercrime_3_2_7.htmL.

4. Lech J. Janczewski, Andrew Colarik, Managerial Guide For Handling Cyber-terrorism and Information Warfare, IGI publishing, Hershey, PA, 2005.

5. Carr, I., 'Anonymity, the internet and criminal law issues', in C. Nicoll, J.E.J.Prins, .J.M C Asser Press, pp.197-206(2003).

6 .Sankar Sen 'Human Right & law Enforcemaent'. 1st ed., Concept publishing New Delhi (2002).

7. Dr. Subhash Chandra Gupta, 'Information technology Act, and its Drawbacks', National Conference on Cyber laws & legal Education, Dec. 22-24th 2001, NALSAR, University of Law, Print House, Hyderabad(2000).

8. Dr. Farooq Ahmed, 'Cyber Law in India (laws on Internet)', Pioneer Books, Delhi U.S. App(1992).

9. C.S. V. Murthy," E-Commerce", Himalaya

Publishing House.1st Edition (2002).