Benjamin DiYanni

E-Commerce: Attacks and Preventative Strategies

Abstract:

The majority of not only our nation, but most of the world, is performing and conducting business over the internet. For the most part, this is a very efficient and cost effective way to trade and conduct business, not just locally, but internationally as well. However, this valuable piece of communication comes under constant attack from hackers and people who would wish to harm and steal from individuals and organizations that conduct their business in this way. What are the risks to businesses, organizations, and individuals that rely on this amazing and rapidly changing resource to perform and interact with each other? And how can these entities protect their identities and resources, both financial and physical, from these attacks? The purpose of this paper will be to analyze the different types of attacks that we each face on a daily basis, and some of the most current type's defenses that are being implemented so we can ensure that we are protected when using the internet to conduct our personal, social, and professional business.

Introduction

"The sustained growth of eCommerce continues to attract criminals who continuously develop new schemes to defraud merchants and their customers."(source 10)

To first understand why people would want to attack e-Commerce we must first explain what e-Commerce is and why it is such a popular target amongst hackers. E-Commerce "*...refers to the exchange of goods and services over the Internet."(Source 1)* However this definition is just a simple explanation, to really understand e-Commerce we need to go a little more in depth. E-Commerce is something that most every human with access to the internet has participated in. Anytime you get on the internet to buy a book, order some clothes, or even banking and paying

bills online, you are partaking in e-Commerce. However, e-Commerce is not just something that individuals like you and I can part take in, but huge multinational corporations and organizations participate as well. In fact the traditional view of a store has become obsolete. It used to be that a store was a physical building that you would go to and purchase products or services. Today, you do not need to have a physical location from where you conduct business. You can simply have a website where customers log on and make purchases that are shipped directly to them. Even if the customer does not wish to purchase a product online they will still be able to research the product and the price, this too is also a part of e-Commerce. Like I have stated before, organizations use e-Commerce everyday as well, *"e-Commerce also applies to business to business transactions, for example, between manufacturers and suppliers or distributors." (Source 1)*

So E-commerce is *"… buying and selling of goods and/or services, or indulging in any other commercial transaction over the Internet." (source 4)* and as you can see e-Commerce has become a huge part of the developed world. Everybody takes part in it at some point or another. With such a valuable and essential commodity, you may be asking yourself who and why would want to attack something like this? Believe it or not there are irrational and immoral people that know their way around how the networks, servers and software that e-Commerce runs on and these people use it to steal from innocent individuals, corporations and organizations. *"Several software tools are readily and freely available the Internet that enables the hacker to expose a system's vulnerabilities. Denial-of-Service (DDoS) attacks are well known and have affected the lives of millions, and malicious code attacks (viruses, worms, and Trojan horses)."*(source 2) E-Commerce is such a big target for hackers mainly for the amount of information that is contained and stored from individuals and organizations using it. For example when you buy something online that is going to be shipped to you; you have to put in a lot of information to complete the whole process. You must give them your home address (or where the package is being shipped), you must give them your name and age, and most importantly you must give up credit card or bank information. Some databases even store a customers or members social security number, this could be one of the pieces of information that can be the most detrimental if it is compromised to a hacker. These pieces of information are what the attacker is going for. If they are able to obtain some or all of this information then they will be able to essentially steal the identity of the individual. When they own the identity of the victim they will be able to make

purchases, take out loans and credit cards, or perform malicious activities all in the name of the victim. This is what is known an identity theft and it is something that nobody wants to find out has happened to them. It can take years to reverse the damage of identity theft, it can ruin a person. Just as they can attack individuals, attackers can cause damage to organizations and businesses too. They can attack businesses by flooding their servers, essentially causing their websites to crash so that it is in-operable to customers who are trying to make purchases. Businesses are a huge target for hackers because it is very easy for them to find out how strong there security is, and also because these stores can hold huge databases of every customer that comes through and pays with a credit card, and some stores even hold more information such as telephone numbers, addresses, and age as well.

Now that e-Commerce has been explained in more detail and since you have a better understanding of the information that is contained within e-Commerce and why some people choose to try and steal this valuable information, the rest of this paper will focus on the types of attacks that are implemented and the types of defenses that are used to defend from attackers and their attacks.

Findings

Types of Attacks

There are several types of attacks that a hacker can choose to deploy. Some attacks aim at gaining specific information on individuals or companies to do harm to. Other types can just shut down the network so it is in operable which could cause a business to lose on revenues. Some of these attacks are easily repairable and others can cause a significant amount of damage to individuals and to companies.

Malicious Code Attacks

"...malicious, or rogue programming code is introduced into the server in order to gain access to the system resources. Very often, the intent of Malicious Code Attacks is to cause large scale damage to the E-Commerce server." (source 11) *"Malware is very much a part of the digital online landscape no matter it is welcome or not."(source 12)*

Viruses

One of the most common types of malicious code attacks is called a virus. Chances are you have heard of a virus and you know that it will bring nothing good. A virus is a form of malicious code that will attach itself to a legitimate program. Once that legitimate program is run then the virus can unload its own code, causing damage to the machine. This makes it hard to detect if you are about to download a virus because it is hidden inside of a legitimate program. "*This damage can range from the deletion of some files to the total reformatting of the hard drive." (*source 11*)* Before the explosion of the internet viruses were transferred from computer to computer through floppy disk drives. However today, viruses can duplicate and multiply very rapidly because of the internet; they can attach themselves to emails, be downloaded by users from untrustworthy websites, or physically put on to a person's machine. A virus can spread very rapidly when there a lot of computers all connected together on the same network, such as an office or work place setting.

Worms

Another type of malicious code attack that can cause mass amounts of damage very quickly is called a worm. Unlike the virus that needs a host file to attach itself to, a worm can be independent and live on its own without a host file; this is what is called a stand-alone program. Also, unlike viruses a worm does not need any human intervention to infect itself onto the computer. It can simply just unload it's malicious code when it finds a vulnerable machine. *"...worms can shut down parts of the Internet or E-Commerce servers, because they can use up valuable resources of the Internet, as well as the memory and processing power of servers and other computers."* (source 11)Worms are very dangerous because they can copy themselves onto computers and servers all over the world in a short amount of time.

Trojan Horses

A Trojan horse is another piece of malicious code that will cause damage. A Trojan horse works by disguising it's self by deleting a legitimate file and consuming that files name, making it hard to detect that you even have a Trojan horse. One type of Trojan horse is the Remote Access Trojans which will give the attacker remote access over the victims computer. Once the attacker gains remote access they are able to control the machine, sometimes without the actual owner of the machine even realizing that there machine has been compromised until it's too late.

Logic Bombs

A logic bomb is essentially the same thing as a Trojan horse, however it is set to go off at a certain time or when a certain series of events has occurred. This means that the attacker can set the logic bomb up and have it go off at two totally different times.

"Malware is sometimes confused with defective software, which is a legitimate resource unintentionally corrupted by harmful bugs prior to release and undetected by quality control."(source 7)

Denial-of-Service Threats

When an attacker sends out a Denial-of-Service attack against a company or organization they are not targeting to steal information or company resources. A Denial-of-Service attack will send and overload the company server with requests. It will send a vast amount of requests, and coupled with the legitimate threats, the server gets overloaded and needs to shut down. The goal of the attacker is to bring down the server so that it is unusable. They would want this to cause confusion to the company and to halt sales making the company lose out on revenues and sales.

Distributed Denial-of-Service

"In Distributed Denial of Service (DDoS) attacks, hackers write a program that will covertly send itself to dozens, hundreds, or even thousands of other computers. These computers are known as 'agents' or 'zombies', because they will act on behalf of the hackers to launch an attack against target systems. The network of such computers is called a BotNet." (source 6)Distributed Denial-of-Service attacks are very popular amongst hackers and attackers because they are able to disguise themselves behind multiple layers of the *"zombie"* computers that they are using to send the attack. It is also a popular form of attack because when they control that many *"zombie"* computers it gives the attacker the ability to easily flood the intended server.

SYN Flooding

Whenever you type in a web address and you click "go" or "enter" to get to that website destination, your computer and the server on the other side of the website you are attempting to communicate with each other. This communication is what connects the two machines together so you can access the website. The process of communication goes like this:

1. SYN message is sent to the server from you

2. The server sends a SYN ACK (synchronization acknowledgment)to you
3. Then you send back an ACK message from the server

It is at step number 3, when the server is waiting your ACK message to come back to it that it is at its most vulnerable. *"At this point, since the E-Commerce server is awaiting to receive the ACK message from the client computer, this is considered to be a half-open connection. It is at this point in which the E-Commerce server becomes vulnerable to attacks. Phony messages (which appear to be legitimate) could be sent to the E-Commerce server, thus overloading its memory and processing power, and causing it to crash.***"** (source 11)

Threats Against Customers

A lot of or most of the attacks that pertain to e-Commerce are usually attacks against big corporations that have their customers data and information stored on their huge databases, which is why they are such a popular target. However, not all attacks go after big corporations, some attacks are also aimed at individuals like you and I.

Phishing Attempts

A phishing attempt is an attack that will try and target the customer directly. The most common phishing attacks are that of illegitimate emails that are disguised and sent to the customers with clever wording that makes the email look professional and legitimate. However, these emails are not legitimate, they usually contain a link taking the customer to a different site that will ask for a certain username/password (usually for a bank that the customer is enrolled with)and the customer thinking that the website is a legitimate one, gives up this information not knowing that it can be used to do harm against them.

Now that you know about the attacks that are out there, we will look at the opposite end of the e-Commerce spectrum and identify the techniques and strategies of protecting the consumers, business, and individual against these attacks.

Preventative Strategies

"When it comes to protecting company's stored data on the computer, protective strategies takes place."(source 8)

It is a sad but true statement when I say that the "good guys" of IT security are constantly playing catch up with the hackers and attackers. The hackers and attackers are constantly coming up with new techniques to try and gain illegal access to information, and as a result IT security

professionals need to be on their toes looking for new attacks and ways to prevent them. IT security professionals cannot guess what type of attack will be discovered next, they have to wait for these attacks to surface so they can attempt to deploy new tactics of fighting off the attacks. This next section is going to discuss the commonly used preventative strategies that are being deployed by IT security officials today to thwart against hackers attempts at causing mayhem and destruction on the e-Commerce servers. These are tools that are designed to protect valuable information that is traveling across servers and networks.

Firewalls

A firewall is a very important tool to use to protect personal information and company data as well. *"A personal firewall helps protect your computer by limiting the types of traffic initiated by and directed to your computer."(source 5)* The firewall acts as security checkpoint that all communication with your server has to cross through. It is a very effective spot to impose security rules. A firewall is like a bodyguard that information and data from outside the network needs to pass through and get inspected by before the data and information can be passed onto the E-Commerce server that it is protecting. Firewalls can come both as software packages and as physical hardware devices. A more formal definition for a firewall is *"...a network configuration, usually both hardware and software, that forms a fortress between networked computers within an organization and those outside the organization."* (source 3)So the firewall acts like a bodyguard, by examining data packets that are trying to come through onto the E-commerce server. It will allow proper and legitimate data packets to get through but will deny access to data packets that do not meet the firewall specifications.

Along with inspecting all of the data packets that try to enter the E-commerce server a firewall can also serve the function of a proxy server." *A proxy server is an intermediary computer that is between the user's computer and the Internet."*(source 13) This means that when you are on the internet the firewall is standing between your E-Commerce server and the internet blocking bad and unwanted communication attempts from hackers but accepting the legitimate ones that you are trying to initiate. You can manually set the level of security you want the firewall to use. Maximum security will block all access to the server from the outside. Minimal security will allow too much access. You need to determine how much security you will need when you set up your firewall and you can add or remove certain security features overtime as you realize that you may or may not need them. *"The Firewall can also provide valuable*

*information to the Systems Administrator, such as the types and amount of data packet traffic, number of attempted network break ins, etc." (*source 3*).* It is important to know that firewalls are very good at protecting your server from outside attacks, it does not protect against an internal threat, such as a disgruntled employee. Frequently monitoring the firewall is probably a good idea to make sure there are no internal attacks on the network.

Routers

Earlier in the last section it was mentioned that a firewall can come in software packages or as a physical hardware device. A router is an example of a firewall in hardware form. Routers are devices that computers and servers on the network can connect to, to have access to the network. Routers are used to accomplish two main goals: *"(1)It is a Firewall, so it protects the network and the ECommerce*
Servers, and (2)Routers insure that data packets do not go where there are not intended to, and make sure that they arrive where there are intended to."(source 3)The Router will decide which path in the network to send the data packets so they end up at the desired location in the fastest time. Routers also have an additional level of security over software firewalls because they have a Network Address Translation (NAT) feature in which it will disguise your servers IP address to the outside world and show the routers IP address instead.

Network Intrusion Devices

A Network Intrusion Device (IDS) is a device that takes the role in not only defending your network but it will constantly be looking for threats both inside and outside the network. If a threat is picked up by the Network Intrusion Device then it will alert the security professionals monitoring the device so they can decide what security measures to implement on the intrusion.

Network Intrusion Devices can come in two different ways with different security features being unique to each one. The first one, called "NIDS" for Network Based Intrusion Detection Device, is usually used to look through the incoming data packets to inspect them before they make contact with the network. One drawback with the NIDS Network Intrusion Device is that as your E-commerce networks are gaining in growth and the number of packets increases the NIDS must have enough room to support the growth. So if you start a small

business that does not get a lot of communication on your server, you might want to make sure that if your business takes off that you can handle the changes in network traffic that will be coming with new business. The second type of Network Intrusion Device is called “HIDS” for Host Based Intrusion Detection Device. This HIDS is connected to only a single server or computer, as compared to a NIDS which is connected to a network of computers and servers. HIDS will more than likely be used for smaller personal protection while NIDS should be used for more organized E-commerce transactions.

Authentication

When your customer logs onto your E-commerce server, they are logging on assuming that they are going to a secure valid site. From the owner’s point of view, they will want to ensure that the right authorized user is logging on and not some hacker trying to gain access through the user. Authentication is what we use to describe this. Authentication is *“. . . .verification who the user is and whether the user is allowed access to the network.”* (source 3)To process through Authentication we use something called Secure Sockets Layer, “SSL”. Secure Socket Layer uses digital certificates that are sent between the two servers, or the computer and server, that are trying to make contact with each other. The Secure Sockets Layer is frequently used to control the security of messages being sent over the internet. SSL has been improved to something called Transport Layer Security which was founded on the same principles of SSL. *“TLS and SSL are not interoperable. However, a message sent with TLS can be handled by a client that handles SSL but not TLS.” (*source 14*)* SSL and TLS should be used on an E-Commerce website when a customer must input a username and password, and also if they have to give credit card information. *“Even though today obtaining a SSL, secure socket layer, certificate is very easy and costless some online shopping websites still does not use SSL during the checkout process.”(source 9)*

Encryption

So authentication checks to make sure that you are communicating with the actual person or machine that you are supposed to be communicating with, and not a hacker. However, what if the data that is being sent back and forth between the two parties is intercepted? If this happens we use a method called Encryption to shuffle and confuse the data so the hacker cannot make sense of the data. *“. . .a method of scrambling or encoding data to prevent unauthorized users*

*from reading or tampering with the data."(*source 3*)*There are many differenet types of encryption and many different ways to implement it but for an E-commerce server you should make use of the Secure Shell or SSH method. *"..It is a method that provides for an encrypted login connection to a server, for example, your Ecommerce Server. In this case, your customer's Username and Password, which would normally be sent as plain text over an insecure Internet connection, would be scrambled into an undecipherable format."(*source 3) This is saying when your customer types in their username and password to log on to the server, the SSH will make the username and password encrypted and scrambled so if a hacker does get a hold it they will not be able to figure out what the customer's username and password is. This prevents illegitimate users from accessing the E-commerce server.

Virtual Private Networks (VPNs)

Secure Sockets Layer (SSL) and Secure Shell (SSH) both encrypt your customer's Username/Password, Credit Card Number, Social Security Number, Home Address, etc. so that if a hacker gets a hold of this information then they will not be able to figure out or use the information. Another way to accomplish this task is to incorporate the use of a VPN or Virtual Private Network. Virtual Private Networks are not just limited to encryption, but they make use of a feature called "tunneling" which adds another layer of protection. Tunneling is a very easy idea to grasp. To put it simply, the data packet that contains all of the information (username/password, email, social security number, etc.) from either the server or the customer and puts that data packet inside of another data packet to further hide and make the sensitive information even harder for a hacker to get into.

The three main network protocols that are used for VPN's are *Point To Point Tunneling Protocol(PPTP), Internet Protocol Security(IPsec),* and *Layer 2 Tunneling Protocol(L2TP).* Point To Point Tunneling is used to access the Internet through a dial up modem. It also is a more secure form of Point To Point Protocol. Internet Protocol Security has different types and levels of security, such as ensuring the confidentiality and authenticity of the data packets. *"This protocol makes use of advanced encryption techniques, such as Digital Signatures and Digital Certificates."(*source 3) Layer 2 Tunneling Protocol, *"The primary advantage of L2TP is that it can support other protocols." (*source 3) This means that you can use L2TP with other VPN's that might be using a different protocol from the one that you are currently using. This can be a

big advantage as not every protocol would make sense to use for every company, different companies will use different protocols depending on what their VPN must be able to accomplish. *"It does not provide any encryption or confidentiality by itself; it relies on an encryption protocol that it passes within the tunnel to provide privacy."(*source 15)

Discussion

Whether you realize it or not you play a part in making E-commerce stay alive. Whether you are the consumer trying to purchase products and services, or the business proprietor providing the products and services, your actions of conducting business over the internet can come with a very heavy risk of substantial loss to your personal or company assets. No matter the level of activity that you use or participate in using E-commerce servers you must protect yourself. Even if you make a single purchase or oppositely if you own a business and are constantly making use of this commodity you are still at risk to suffer losses.

1. What are the risks?

For the consumer, like you and me, potentially any information that you are dealing with is at risk to be discovered by hackers. One example is if you are on a website trying to make a purchase, then you are dealing with a lot of information that is at risk to be compromised. You probably need to input a Username and Password to access the site. To pay for your purchase you need to input a Credit/Debit card. To know where to ship the purchase you input your home or work address. The hacker could potentially take all of this information and use it to steal a victim's identity taking out loans in their name or make other purchases by using their credit card numbers.

For a business or organization, a hacker could compromise an E-commerce server a few different ways. The result of an attack could crash a business server not allowing any communication even with valid legitimate users. This will halt all progress of conducting business which is never good for a business. A hacker does not need to disable a server; they could hack into the server and steal sensitive information or data. They could steal company

information that could ruin a company if it is exposed. Also, if the company holds user data in a database then that too could be compromised by an attack from a hacker.

2. ***What are some common types of attacks?***

Types of Attacks

- **Malicious Code Attacks**
  - Viruses
  - Worms
  - Trojan Horses
  - Logic Bombs
- **Denial-of-Service Threats**
  - Distributed Denial-of-Service (DDoS)
  - SYN Flooding
- **Threats Against Customers**
  - Phishing Attempts

3. ***What can you use to protect your data and information?***

Preventative Strategies

- **Firewalls**
  - Proxy Server
- **Routers**
  - Network Address Translation
- **Network Intrusion Devices**
  - Network Based Intrusion Detection Device (NIDS)
  - Host Based Intrusion Detection Device (HIDS)
- **Authentication**
  - Secure Sockets Layer (SSL)
- **Encryption**
  - Secure Shell (SSH)
- **Tunneling**
  - Virtual Private Networks (VPN)

4. **How can I ensure completely security?**

Unfortunately, there is no such thing as being completely 100% secure. Hackers and attackers are constantly coming up with new ways of hacking and stealing data and information. The only way you can be prepared for an attack is to make sure that you have proper security features already up and running. Having the security features running will stop the attacks that they are meant to stop, and they can alert you when you have been attacked. It is a good idea to meet up with your professional security team to have a plan or set of rules to follow if you find out that you have suffered an attack. You want to have a plan of action to take when you find out your system has been compromised. Sitting there and allowing the attack to go on is counterproductive to your business.

5. **What is a Malicious Code Attack?**

A malicious code attack is when code that is meant to damage or gain access to the server has been loaded onto the network. This code can come as a Virus, Worm, Trojan Horse, or Logic Bomb. A Virus or a Worm is meant to delete system files or it can wipeout the whole hard drive, while Trojan Horses and Logic Bombs are used to gain wireless access to a victims computer giving the hacker complete control of the machine.

6. **What is a Denial of Service Attack?**

A DoS attack is when a hacker or attacker sends a vast amount of requests to an E-commerce server. A server can only handle so many requests so if an attacker is constantly sending illegitimate requests, that added to the amount of actual legitimate requests, which will force the server to shut down. With the server shut down it can no longer take any requests, not even from legitimate users. A hacker or attacker will do this so the company cannot make any progress.

7. **How do you implement protection from these attacks?**

To protect yourself from a malicious code attack you should have a Firewall and a Network Intrusion Device. The Firewall will stop incoming malicious code packets from entering your network. If a disgruntled employee has loaded the malicious code from inside the network then the firewall will not stop it. That is where the Network Intrusion Device will alert you or your professional security team to tell you that a malicious code has entered your

network. The Firewall and the Network Intrusion Device will also protect against a DDoS attack, until they become successful that is. After a DDoS attack has become successful the only thing you can do is react to it. Your reaction to the DDoS attack should be your plan that you and your professional security team have sat down and come up with to get your E-commerce server back online.

Conclusion

In conclusion, I have looked at and described several possible threats that could pose trouble to an E-commerce server. I talked about Malicious coding, Denial of service attacks, and Phishing scams. I have also gone over some different ways to protect yourself from these attacks. The different types of protection I have gone over are Firewalls, Routers, Network Intrusion Devices, Encryption, Authentication, and VPNs. It is vital remember that while each of these security measures provide adequate protection, it would be a wise move to use more than just one of these security practices. You should use a combination of the different preventative strategies described in this paper. More than anything it is important to actively keep checking the securities you have put in place. You cannot just set them up and do nothing you must constantly monitor your security so you can make improvements where need be. Also, you should keep up on the changing elements of IT security because new attacks and defenses are being found and made up constantly.

References

1. IBM. "e-Commerce security: Attacks and preventive strategies."
http://www.ibm.com/developerworks/websphere/library/techarticles/0504_mckegney/0504_mckegney.html

2. E-Commerce Security: Attacks and Preventive Strategies
http://sallysspecialservices.wordpress.com/2010/07/29/e-commerce-security-attacks-and-preventive-strategies-2/

3. “Threats to E-Commerce Servers-Part II”
http://www.biometricnews.net/Publications/E-Commerce_Article_Part_II.pdf

4. The Beginners Guide to E-Commerce Security
http://www.brighthub.com/computing/smb-security/articles/28128.aspx

5. E-Commerce security: Attacksand preventive strategies
http://www.scribd.com/doc/91332192/Project-Paper

6. Strategies of Protection from Distributed Denial of Service (DDoS) Attacks
http://www.intruguard.com/strategies-of-protection-from-ddos-attacks.html

7. eCommerce Payments and Security
http://www.alimdco.net/writing/apa/ecomrce/payments_securities.pdf

8. Protective Strategies
http://tolga.saygi.org/is/is-e-commerce/protective-strategies-2.html

9. Disruptive Strategies
http://tolga.saygi.org/is/is-e-commerce/disruptive-strategies-2.html

10. Strategies for Reducing the Risk of eCommerce Fraud
http://www.firstdata.com/downloads/thought-leadership/ecommfraudwp.pdf

11. “Threats to E-Commerce Servers-Part I”
http://www.technologyexecutivesclub.com/Articles/security/artThreatstoEcommerceServers.php

12. MALWARE’S IMPACT ON E-BUSINESS & M-COMMERCE : THEY MEAN BUSINESS !

http://www.academia.edu/934928/MALWARES_IMPACT_ON_E-BUSINESS_and_M-COMMERCE_THEY_MEAN_BUSINESS_

13. What is a proxy server? How do I get proxy server information?

http://java.com/en/download/help/proxy_server.xml

14. Secure Sockets Layer (SSL)
http://searchsecurity.techtarget.com/definition/Secure-Sockets-Layer-SSL

15. Layer 2 Tunneling Protocol
http://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol