E-BUSINESS THREATS AND SOLUTIONS
E-BUSINESS THREATS AND SOLUTIONS

E-business has forever revolutionized the way business is done. Retail has now a long way from the days of physical transactions that were time consuming and prone to errors.

However, eCommerce has unavoidably invited its share of trouble makers. As much as E-business simplifies transactions, it is occasionally plagued by serious concerns that jeopardize its security as a medium of exchanging money and information.

(1) The Threats Posed to E-Commerce Servers.
(2) The Security Issues with E-Commerce-The Human Element.

(1) The direct threats to E-Commerce servers can be classified as either :

(a) MALICIOUS CODE THREATS: -

Viruses and Worms
The most common threats under this category are the worms and viruses. In the media today, we keep hearing about these words on almost a daily basis, and there is confusion that the two are related, and synonymous. However, the two are very different. A virus needs a host of some sort in order to cause damage to the system.

The exact definition is “... a virus attaches itself to executable code and is executed when the software program begins to run or an infected file is opened.” So for example, a virus needs a file in which to attach itself to. Once that file is opened, the virus can then cause the damage. This damage can range from the deletion of some files to the total reformatting of the hard drive. The key to thing to remember about viruses is that they cannot by themselves spread - they require a host file.

However, worms are very much different. A worm does not need a host to replicate. Rather, the worm replicates itself through the Internet, and can literally infect millions of computers on a global basis in just a matter of hours. A perfect example of this is once again the MS Blaster worm. Worms by themselves do not cause damage to a system like a virus does. However, 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. A question that is often asked about worms and viruses is which of the two are worse. This is a difficult question to answer, as the criteria for which is worse depends upon the business environment. However, one thing is certain: in terms of the rate of propagation and multiplicity, worms are much worse than viruses.

Trojan Horses

A Trojan Horse is a piece of programming code that is layered behind another program, and can perform covert, malicious functions. For example, your E-Commerce server can display a “cool-looking” screensaver, but behind that could be a piece of hidden code, causing damage to your system. One way to get a Trojan Horse attack is by downloading software from the Internet. This is where you need to be very careful. There will be times (and it could be often) that patches and other software code fixes (such as Service packs) will need to be downloaded and applied onto your E-Commerce server. Make sure that whatever software is downloaded comes from an authentic and verified source, and that all defense mechanisms are activated on your server.
Logic Bombs

A Logic Bomb is a version of a Trojan horse, however, it is event or time specific. For example, a logic bomb will release malicious or rogue code in an E-Commerce server after some specific time has elapsed or a particular event in application or processing has occurred.

(b) TRANSMISSION THREATS -

Denial of Service Attacks

With a Denial of Service Attack, the main intention is to deny your customers the services provided on your E-Commerce server. There is no actual intent to cause damage to files or to the system, but the goal is to literally shut the server down. This happens when a massive amount of invalid data is sent to the server. Because the server can handle and process so much information at any given time, it is unable to keep with the information and data overflow. As a result, the server becomes “confused”, and subsequently shuts down. Another type of Denial of Service Attack is called the Distributed Denial of Service Attack. In this scenario, many computers are used to launch an attack on a particular E-Commerce server. The computers that are used to launch the attack are called “zombies.” These “zombies” are controlled by a master host computer. It is the master host computer which instructs the “zombie” computers to launch the attack on the E-Commerce Server. As a result, the server shuts down because of the massive bombardment of bad information and data being sent from the “zombie” computers. A Distributed Denial of Service Attack is diagrammed as follows:

Ping of Death

When we surf the Web, or send E-Mail, the communications between our computer and the server takes place via the data packet. It is the data packet that contains the information and the request for information that is sent from our computer to other computers over the Internet. The communication protocol which is used to govern the flow of data packets is called Transmission Control Protocol/Internet Protocol or TCP/IP for short. The TCP/IP protocol allows for data packets to be as large as 65,535 bytes. However, the data packet size that is transmitted across the Internet is about 1,500 bytes. With a Ping of Death Attack, a massive data packet is sent-65,536 bytes. As a result, the memory buffers of the E-Commerce Server are totally overloaded, thus causing it to crash.
SYN Flooding

When we open up a Web Browser and type in a Web address, or click “Send” to transmit that E-Mail from our own computer (referred to as in this section as the “client computer”), a set of messages is exchanged between the server and the client computer. These set of exchanges is what establishes the Internet connection from the client computer to the server, and vice versa. This is also known as a “handshake.” To initiate this Internet connection, a SYN (or synchronization) message is sent from the client computer to the server, and the server replies back to the client computer with a SYN ACK (or synchronization acknowledgement) message. To complete the Internet connection, the client computer sends back an ACK (or acknowledgement) message to the server. 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.

(2) Threats to Your E-Commerce Customers the Human Element -

Phishing Attack-

One of the biggest threats to your E-Commerce customers is that of Phishing. Specifically, Phishing can be defined as- “the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.”

So, for example, fraudulent e-mail could be sent to your customers claiming that their online account is about to expire, or their username and password has been compromised in some fashion, or that there is a security upgrade that will take place affecting their online account. After they are tricked into believing the content of the Phishing e-mail, the customer then clicks on the link, and submits all of their confidential information. All Phishing e-mail contains a link, or a web address, in which the customer clicks on thinking that they are going to secure and legitimate site (people who launch Phishing schemes [also known as “Phishers”] can copy the HTML code from your E-Commerce site, making it look authentic in the eyes of the customer). The truth is, all of the confidential information submitted is collected by the “Phisher”, who is bent upon creating havoc and damage to your E-Commerce business.

Other Threats To E-Commerce Servers

Data Packet Sniffing

This refers to the use of Data Packet Sniffers, also known simply as “sniffers.” While it is an invaluable tool to the Network Administrator for troubleshooting and diagnosis, an attacker can also use a sniffer to intercept the data packet flow and analyze the individual data packets. Usernames, passwords, and other confidential customer data can then be hijacked from the E-Commerce server. This is a very serious problem, especially in wireless networks, as the data packets literally leave the confines of the network cabling and travel in the air. Ultimately, Data Packet Sniffing can lead to hijacking sessions. This is when the attacker eventually takes control over the network connection, kicks off legitimate users (such as your customers) from the E-Commerce server, and ultimately gains control of it.
IP Spoofing

The intent here is to change the source address of a data packet to give it the appearance that it originated from another computer. With IP Spoofing, it is difficult to identify the real attacker, since all E-Commerce server logs will show connections from a legitimate source. IP Spoofing is typically used to start the launch of a Denial of Service Attack.

Port Scanning

This is listening to the network ports of the E-Commerce server. When conducting such a scan, an attacker can figure out what kind of services are running on the E-Commerce server, and from that point figure out the vulnerabilities of the system in order to cause the greatest damage possible.

Trapdoors/Backdoors

In developing the code for an E-Commerce site, developers often leave “trapdoors” or “backdoors” to monitor the code as it is developed. Instead of implementing a secure protocol in which to access the code, backdoors provide a quick way into the code. While it is convenient, trapdoors can lead to major security threats if they are not completely removed prior to the launch of the E-Commerce site. Remember, an attacker (HACKER) is always looking first for vulnerabilities in the E-Commerce server. Trapdoors provide a very easy vulnerability for the attacker to get into, and cause system wide damage to the E-Commerce server.
There is but one solution to all issues that at times dent the security of eCommerce services. Strict vigil on malicious intruders. Easier said than done? So is every preventive measure. However, with online transactions, progress in security has been overwhelming.

The solution includes two prospective: Wireless prospective and Hard wired prospective -

(1) Solutions to Threats from a Wireless Perspective:

* A Technical Discussion of the Data Packet.

* Threats from Wireless: Social Engineering and Man in the Middle Attacks.

* A Solution: Authentication-The Use of Secure Sockets Layer.

* A Solution: Encryption-The Use of Secure Shell

* A Solution: Tunneling-The Use of Virtual Private Networks

(2) Solutions to Threats from a Hard Wired Perspective:

* A Solution: The Use of Firewalls.

* A Solution: The Use of Routers.

*A Solution: The Use of Network Intrusion Devices.

Authentication

Most notable are the advances in identification and elimination of non-genuine users. Ecommerce service designers now use multi-level identification protocols like security questions, encrypted passwords (Encryption), biometrics and others to confirm the identity of their customers. These steps have found wide favor all around due to their effectiveness in weeding out unwelcome access.

Intrusion Check

The issue of tackling viruses and their like has also seen rapid development with anti-virus vendors releasing strong anti-viruses. These are developed by expert programmers who are a notch above the hackers and crackers themselves.

Firewalls are another common way of implementing security measures. These programs restrict access to and from the system to pre-checked users/access points.
Educating Users

E-Commerce is run primarily by users. Thus, eCommerce service providers have also turned to educating users about safe practices that make the entire operation trouble free. Recent issues like Phishing have been tackled to a good extent by informing genuine users of the perils of publishing their confidential information to unauthorized information seekers.