Securing E-commerce Web Site's Against The Five Highest Security Threats

CNG-132 Information Security

Joseph Martinez

First Threat – Forces of Nature Policy

Of course my service provider will provide the necessary equipment and hardware concerning back-up generator lay-out and design, guaranteeing that my web-site will always be up and running in the event of an electrical failure. This first layer of threats is classified under physical security: the contracts and maintenance policies will be managed within operation management and will be highly classified confidential policy information due to national security.

Second Threat - Software Development Threats

During the construction and design phase of web-site development, one must consider the options: After much research I have decided not to trust anyone. I will be designing my own web-site using the software “Dream Weaver” which is published by many different companies of which will include many threats that must be addressed all to their own.

Threats during development

Threats during operation (both insider and external threats). Any software system that runs on a network-connected platform is likely to have its vulnerabilities exposed to attackers during its operation. Attacks may take advantage of publicly known but unpatched vulnerabilities, leading to memory corruption, execution of arbitrary exploit scripts, remote code execution, and buffer overflows. Software flaws can be exploited to install spyware, adware, and other malware on users' systems that can lie dormant until it is triggered to execute.

More experienced attackers often develop (and share) sophisticated, targeted attacks that exploit specific vulnerabilities. In addition, the nature of the risks is changing more rapidly than the software can be adapted to counteract those risks.

Solution

After securing my web site, I will implement several anti-virus and anti-malware software applications together, that are compatible together as I have now. First with web-design, the web-site should be:

User Friendly

- Immediately tell visitors on the site what the company does
- Get users to the information they want in two clicks
- Include headers and links that give the company’s logo, and show a "tree" branching from the homepage to the current page. Visitors will also know where they are within the website at all times
- Have extensive “Help” information with a real-time customer service link. Allow visitors to find answers to questions easily
- Implement users with disabilities software
- Pay special attention to the quality of information, graphics and ensure that the text is written well and spelled correctly
- Include a link to the homepage on every page so that in one click, users can be led there
- Develop visuals that are useful, not flashy and distracting. Useful visuals include illustrations or photos of products, graphics that separate categories of products, or maps with directions

Once I design my web-site, I will register my domain name to purchase a U.R.L. address. Once this is done I will be published and my website can began operations

Departments

At first all individual departments within the web-site will be ran by myself. As the company grows, I will hire with-in and outsource.

Accounting department

Web design development department

Legal department

Management department

Customer Service department

Before all written policies can be implemented **integral policies** must be applied:

All eCommerce systems must meet four integral requirements:

- Privacy Policy – information exchanged must be kept from unauthorized parties
- Integrity Policy – the exchanged information must not be altered or tampered with
- Authentication Policy – both sender and recipient must prove their identities to each other
- Non-repudiation Policy – proof is required that the exchanged information was indeed received

These basic maxims of eCommerce are fundamental to the conduct of secure business online.

Privacy Policy

Privacy has become a major concern for consumers with the rise of identity theft and impersonation, and any concern for consumers must be treated as a major concern for eCommerce providers. Privacy now forms an integral part of any e-commerce strategy and investment in privacy protection has been shown to increase consumers spending, trustworthiness and loyalty.

Integrity, Authentication & Non-Repudiation

In any e-commence system the factors of data integrity, customer & client authentication and non-repudiation are critical to the success of any online business. Data integrity is the assurance that data transmitted is consistent and correct, that is, it has not been tampered or altered in any way during transmission. Authentication is a means by which both parties in an online transaction can be confident that they are who they say they are and non-repudiation is the idea that no party can dispute that an actual event online took place. Proof of data integrity is typically the easiest of these factors to successfully accomplish. A data hash or checksum, such as protocols MD5 or CRC, is usually sufficient to establish that the likelihood of data being undetectably changed, notwithstanding these security measures, it is still possible to compromise data in transit through techniques such as phishing or man-in- the-middle attacks. These flaws have led to the need for the development of strong verification and security measurements such as digital signatures and public key infrastructures (PKI).

My Service provider will be providing protection against Malware, Phishing, Unauthorized Data Access, Denial of Service and providing security for E-mail services and Encryption. I will be using a separate Credit card service provider that also provides banking.

After securing my web site, I will began implementing of the many security policies that must be implemented for e-commerce:

Written Policies

Export policies, copyright polices, bulletin board policies, customer service policies, export, copyright, bulletin board, chat room and customer service policies.

Home Page

On the footer of the home page of the site, I will have a link to my privacy policy, my user agreement and terms and conditions, and my copyright notice.

Privacy Policy

If you collect any information from users of your site, using cookies or otherwise, the Federal Trade Commission requires you to have a privacy policy. The privacy policy should contain an explanation of how you collect the users' information, how and where the information is stored, how the user can delete or change the information, and to whom the information is disclosed and for what purpose. The European Union also has similar and strict regulations on collection of information via websites.

User Agreement

Having a user agreement or "terms and conditions" may be the most important part of a website. A user agreement requires each user to agree to be bound by a contract governing his or her use of the site by clicking "I agree" before being permitted to use the site. Be aware that simply posting your legal agreement without forcing the user to click "I agree" prior to use is unlikely to bind your users to the terms. The user must take an active step through which she agrees to the terms and must not be allowed to proceed to use the site without such step.

A user agreement allows a company to:

dictate how the site may be used (for example, for reading and printing materials)

dictate how the site may not be used (for example, reverse engineering the coding tricks, copying content, for illegal purposes)

dictate who may use the site (for example, persons over 18, US citizens)

dictate procedures or policies for the site (for example, return policies, complaint policies, notification of copyright infringement policies) dictate your company's waiver of implied legal warranties (for example, implied warranties of noninfringement, fitness for particular purposes, etc.)

dictate the limit of your company's liability for the site, other users postings on your site, sites you link to, etc.

dictate jurisdiction for any disputes relating to the site

Warranties

Statements on your website about your products and services are express warranties to customers. It is important to carefully review all website text to be sure that what your company promises is true and corresponds with its other policies and advertising. When you review, look for statements that are absolute statements which may be hard to prove or verify if the Federal Trade Commission were to request that you do so. Examples of such statements are: "Our printer works with all software," "Our services are the best," and "We guarantee that our product will always perform perfectly." Also, be aware that the FTC has specific guidelines that should be followed for use of the words "free" and "guarantee" in advertising or on your website.

Also, review your website to be sure that the text matches your regular business contracts. For example, your website should not promise a 60-day money-back guarantee if your contract states only a 30-day warranty.

Export

If persons from other countries use your site, then you are exporting.

If you sell to such persons, you are exporting the item you sell and entering into contracts with persons of other countries. If you use encryption on the site, then you are exporting technology regulated by the Department of Commerce and Defense. Various government departments regulate the countries with which U.S. companies may do business and when a company needs an export license to transmit items, technology or information abroad. Doing business with certain countries, such as Iraq, Iran, Cuba, North Korea, Syria, Yugoslavia and others, is severely restricted. Depending on the information on your site, what kind of business you do, the technology and information involved, your site may be subject to these regulations, and you should consult with your attorney about these business decisions.

Copyright

The footer of your site should display a copyright notice for the content of the site. The notice should read "© [date] [copyright owner name] All rights reserved." You should also deposit a copy of the site with the Copyright Office to record ownership of the site's content, look and feel. Finally, under the Digital Millennium Copyright Act, depending on the purpose and the users' activities on the site, your company may be eligible to register for limited liability offered by the act for the site. You should consult your attorney for review of the act and how to register.

Bulletin Boards, Chat Rooms, Etc.

Any posting ability by users should be subject to site submission rules and a user agreement. The rules should obtain users' consent not to post pornographic, defamatory or infringing materials and, through your user agreement, consent to your company not being liable for other users taking such actions.

Customer service policy

Because customers expect to be able to contact a company with questions, special requests or problems related to ordering, online businesses should offer an e-mail address or phone number for customer service inquiries. Not only is customer service a great way to build loyalty, but it's also a valuable feedback mechanism--customers are all too ready to sing your praises or call out improvements that need to be made to your product, service or image.

Security threats arise either because of somebody's malicious actions, or because of incorrect technical setup.

Further to the fundamental maxims of eCommerce above, eCommerce providers must also protect against a number of different external security threats:

Investigate

Identify the threats

Most common security threats to e-commerce websites are Malware, Phishing, Unauthorized Data Access, Denial of Service and Copyright Infringements

All threats will be protected for physical, personal, operations, information, communications and network security

Malware and Phishing

I have done extensive research on cyber-crime. It is estimated that 50% of all computers and servers are infected with malware, which means that someone other than the owner has ultimate control. This is very alarming and disturbing.

Tracking down malware and eliminating it from your network is frustrating and time-¬consuming. You often have to rebuild your machines from the ground up, reinstalling the operating system and software and restoring data from backup tapes. Lax security can lead to weeks of wasted time spent patching your network and fixing the wreckage.

Viruses can infect ecommerce website servers. Such malware infects users of the website by executing unintended actions such as downloading software without permission.

After investigating how phishing, viruses, Trojans and malware work on personal computers and websites I knew that my website must be continually updated against such threats on the server end. My service provider will provide these services.

Symptoms: How do you know when you’re affected with malware?

At any given time, roughly half of all computers are infected with "malware" — programs that can steal files and passwords, hold your machine hostage for purchase of bogus security software, or enlist it into a "botnet," a network that makes it secretly send out spam.

Phishing

To the accomplished criminal, it is easy to set up a website that looks exactly like your ecommerce website. Then it is only a matter of inviting a large number of users to this fake site. Some of them will fall for it and wrongly assume that they are on your ecommerce website while in reality they are on the criminal's site.

If you assume that you are on a genuine site, you will be more likely to part with information such as credit card information, personal identification information, user names, passwords, and he like. Once such sensitive information reaches the wrong hands, there is no telling how it will be misused.

Symptoms: How do you know when you are a victim of Phishing?

When you read email, use a social networking site (like Facebook) or surf the Internet or respond to pop-up advertising, you should be wary of scams that try to steal your personal information (identity theft), your money, or both. Many of these scams are known as "phishing scams" because they "fish" for your information.

If you think you are a victim you should:

Change the passwords or PINs on all your online accounts that you think might be compromised.

Place a fraud alert on your credit reports. Check with your bank or financial advisor if you're not sure how to do this.

Contact the bank or the online merchant directly. Do not follow the link in the fraudulent email message.

If you know of any accounts that were accessed or opened fraudulently, close those accounts.

Routinely review your bank and credit card statements monthly for unexplained charges or inquiries that you didn't initiate.

Unauthorized Data Access

Online discussion forums are flooded with criminals offering databases of credit card information. They promise that these databases contain accurate and complete information.

Using backdoors or cross site scripting (XSS), or other methods, hackers gain access to private information stored in the databases of ecommerce sites. A backdoor is a secret or undocumented means of getting into a computer system. Many programs have backdoors placed by the programmer to allow them to gain access to troubleshoot or change the program. Some backdoors are placed by hackers once they gain access to allow themselves an easier way in next time or in case their original entrance is discovered. Cross site scripting (XSS) refers to the ability to use some of the functionality of active scripting against the user by inserting malicious code into the HTML that will run code on the user's computer, redirect them to a site other than what they intended or steal passwords and personal information among other things.

It is up to the web site developer to ensure that user input is validated and checked for malicious code before executing it.

This threats must be secured to protect network security, data – software security and patron privacy.

To secure against Unauthorized Data Access:

Software patches, updates, and drivers are made available, often for free, to consumers to help keep a software program and operating systems running properly and secure.

Denial of Service

Denial of Service (DoS) or Distributed Denial of Service (DDoS) is a method used by hackers to send a large number of automated requests to an ecommerce website. To the website server, these requests seem to originate from genuine visitors. So the website server attempts to respond to the requests. But the sheer volume overwhelms the server.

The high volume of artificial traffic has the same effect as high volume of genuine traffic would, i.e., the server slows down, or worse, completely blocks out genuine visitors.

Protection: Use and configure router

All of these threats affect the physical, personal, operations, information, communications and network security. Physical, because it can damage hardware and software. Personnel because sensitive information can be compromised. Operations because operations can be halted. Information because information can be manipulated, stolen or destroyed. Communication and network security also for all of the above reasons.

% amount of chance of getting infected depends on amount of security that's implimented

Risk Assessment- Assign a Risk Rating – From 1 to 100, gets 95

Documenting the Risk Assessment

Risk Control Strategies – Once ranked and worksheet complete- must choose strategy-

I'm going to transfer the risk (transference)

Cost benefit analysis (CBA)

Avoidance: 3 methods of risk avoidance – application of policy, training and education and applying the technology

Threat Identificarion

Plan

To secure:

Implementing firewall software

Implementing encryption

Implementing intrusion and prevention software

Implementing anti-virus and anti-malware software

Maintenance

Change passwords frequently and automatic updates turned on

Copyright infringements

Relatively inexpensive software is available that allows a copyright owner to search the Internet and see if his content is being used illegally by another website. Additionally, many websites put digital tags on their pictures which allow them to track the use of the image. And sometimes, just placing a copyright symbol and date on the work is enough.

- Policy servicing for copyrights: My legal departments

Infringements.

Protection:

I have recognized the possibility of these threats, defined them and offered protection plans.

Call for action:

Create a network diagram. Ghant- chart (Blueprint)

One of the most useful exercises for understanding your security situation is creating a network diagram. A network diagram consists of symbols representing your hardware (PCs, servers, switches, routers, printers, etc.) and the connections between them. The diagram should also include some information about the model and configuration of each piece of hardware (e.g., name, IP address, function, etc.). For network connections, list the speed and protocol of each link. While you can map a small network with pencil and paper, it's hard to extend and update your diagram using this technique. Most network administrators employ software to help them map their networks.

Understand your situation. A network diagram goes hand-in-hand with an assessment and evaluation of everything that happens on your network. Who uses your network? What types of hardware and software do they use? What kind of Internet connection does your web-site have? Service provider will provide email service. Is your staff network separated from the service network? What types of security policies, procedures and equipment do you already have in place?

Review your technology plan. Review this document, if available, to determine the network services you're currently providing and the plans for your network's future.

Training policy: your IT staff or hire a consultant. You must make sure that either your IT staff receive appropriate training when it comes to network security or look for outside IT support that can offer the necessary knowledge to secure your network.

Email

Service provider will provide service

Credit card service

Integrate an online payment service. If a business doesn't have access to a merchant account or the fees are just too high, one solution is an online payment service, like PayPal . PayPal allows businesses to accept credit-card transactions and payments safely and conveniently. It also allows buyers to send payments directly from a bank account.

When a buyer indicates the desire to use PayPal during checkout, that person will be directed to sign into or sign up for a PayPal account to then complete the transaction.

For merchants there may be benefits for offering PayPal. There are no setup charges, monthly charges, minimums or gateway fees. PayPal charges a per-transaction fee, which ranges from 1.9 percent to 2.9 transactions are done safe on Pay Pal. - Credit card service providers –generating money – pay pal percent plus 30 cents per transaction. PayPal also actively fights chargebacks on behalf of online merchants. If a transaction meets all of the requirements of PayPal's Seller Protection Policy, then the merchant will not be liable to for the chargeback by the customer.

Ensuring Transaction Security

Online entrepreneurs have a responsibility to do all they can to ensure their websites offer a safe shopping experience. But they don't need to be information technology security experts to have a secure site--the techies already have developed security measures that any online Small business can adopt.

There are services in this space that bring together all the security measures that an online small business needs to have in place. PayPal enables businesses to set up a website that accepts credit cards without seeing or having to store the account numbers of its customers. This makes buyers feel even safer because they don't have to share their personal or financial information online. Gateway services like Authorizenet.com, Cyber Source or Pay ManTech will also handle credit card and electronic check payments securely.

Downloading Material

Handout Assignment #5

Chapter 29, Three Page Report

CNG 120- 01A

Joseph Martinez

The Six Common Security Threats

- Unauthorized access

Unauthorized access occurs when a user accesses resources in an unauthorized way.

- Data destruction, accidental or deliberate

Authorized access can lead to data destruction by users who do not intend to be malicious. When users have access to a file or database, they typically believe the system won't let them make any changes they are not authorized to make.

- Administrative access

Access control includes four interlinked areas requiring your attention: Physical security, authentication, users and groups, and security policies. Store computers with sensitive data in a locked room and never walk away from your computer while logged on. Accounts should be given permissions to access only what they need and no more. Unused accounts should be disabled.

Policies control permissions for activities, such as installing hardware, accessing a command prompt, or logging on at a particular time of the day. A policy is usually applied to a user account, computer account, or a group. Use the Local Security Policy tool to manage policies for an individual computer.

- Catastrophic hardware failures

Hardware failures happen, though the best defense is to perform data backups, so that when they do happen important information can be recovered.

- Malware

Malware includes grayware, spam, viruses, worms, macros, Trojan horses, and rootkits, all of which can wreak havoc on your system. Unsolicited e-mail is called spam. Never post your e-mail address on the internet; over 97% of spam goes to e-mail addresses posted online. A virus is a piece of malicious software that is passed from computer to computer and is designed to attach itself to another program on your computer. A worm is a freestanding program that takes advantage of security flaws and copies itself over and over again, thereby bogging down a network. A macro is any type of virus that exploits application macros to replicate and activate.

To help protect a computer from malware, make sure to run up-to-date antivirus software, use a firewall, and apply all security patches for your software and operating system. Run Windows Update automatically, or at least weekly if you choose to configure it for manual updates.

- Environmental threats

Power surges, dirty or humid air, extreme cold or hot room temperatures, moisture and toxic hazards are environmental threats.

One of the main causes for a power supply failure is dust build up on the power supply fan, it can build up to a point where the fan stops operating, thus causing the power supply to stop functioning.

The best defense is to inspect the inside of your computer and the power supply regularly and to clean the dust build up out with either compressed air or a vacuum.

User Security

The first step in securing data is authentication, through user name and password. Firewalls do a good job controlling information coming and going to and from the internet, though hackers can access user authentication if the information is not encrypted.

Windows uses user accounts and groups as the main definitions for access control. A user account is assigned to a group, such as Users, Power Users, or Administrators, and by association gets certain permissions on the computer. Using NTFS enables the highest level of control over data resources.

All of the default groups-Everyone, Guest, Users- define broad groups of users. Never use them unless you intend to permit all of those people access to a resource. If you use one of the default groups, remember to configure them with the proper permissions to prevent users from doing things you don’t want them to do with a shared resource.

Network Security

As an Administrator, all network operating systems provide you with capabilities to control hundreds of security parameters, under Policies. Policies are permissions for activities, as opposed to true permissions, which control access to resources. The tool that is used to set local policies on an individual system is called ‘Local Security Policy’. If you want to apply policy settings for a whole group, you need to use Windows Active Directory domain-based ‘Group Policy’ to control all network clients.

Cryptosystems use public keys, private keys to encrypt, digital signatures, random keys to decrypt.

Internet passports are used with username and passwords to access certain sites where a client has already registered.

Web blocking and parental controls limit internet access. Software can be installed to stop children from being able to access objectionable material. Software can be installed on individual computers or servers. Many countries around the world use Web blocking to block out news about democracy and religion. Many companies use Web blocking to block access to sites that contain pornography, racist and violent material.

Personal firewalls and proxy servers add much additional security and corporate firewalls protect the workplace.

Biometrics, iris and finger printing security systems are becoming popular in secure facilities and the work place, though people worry about invasion of privacy issues.

VPN (Virtual Private Network), using VPN to tunnel through the Internet is one way of network security. To connect to the VPN, client software must be running on the PC on one end of the tunnel. The client first encrypts each of the documents packets. They are then encapsulated inside a normal IP packet, as it travels to an OS or router, only the IP address is read. Once it arrives at its destination, it is decrypted.

When accessing the internet many networks consist of multiple networks linked together by some sort of private connection, usually some kind of WAN connection such as DSL or T1. Microsoft’s encryption method of choice for this type of network is called IPSec (IP Security). IPSec provides transparent encryption between the server and the client.

TCP/IP applications use encryption such as SSL (Secure Sockets Layer) security protocol, which is used to create secure Web sites. Microsoft incorporates SSL into its far reaching HTTPS (HTTP over SSL) protocol.

To make a secure connection, your Web browser and the Web server must encrypt their data. For the Web browser and the Web server to be able to encrypt and decrypt each other's data, the server sends a public key to your Web browser so that the browser knows how to decrypt incoming data. These public keys are sent in the form of a digital certificate. A number of companies issue digital certificates to Web sites, the most famous being VeriSign, Inc.

If you receive a certificate not listed in your browser, the browser will warn you and ask you if you want to accept the certificate.