Top Best Practices for Increasing Website Security

Website security threats can affect any business. With cyber-attacks growing in sophistication, speed, and intensity, companies need to focus more on when an attack can compromise their websites and not “if it will happen”.

An unsecured website is vulnerable to multiple attacks, threatening the integrity of the organization and the privacy and security of the users.

The following are the most effective practices to observe today.

1. Use HTTPS protocols to increase website security

HTTPS protocol should be a priority for all website owners.

Not only is it vital for ensuring secure communication between a web server and a client, but it also improves the basic security standard for all websites.

First, it reassures users that all communications done through the website are secure. HTTPS protocol essentially tells the website visitors that the information they request or view from the webserver cannot be intercepted nor altered by third parties.

Second, web browsers like Google Chrome identify and mark all websites that lack HTTPS security protocols. Any time a visitor accesses the website, they receive a notification that it is not secure. Some visitors would be reluctant to continue accessing the services of a website marked as not secure. This can discourage new visitors from visiting the site resulting in decreased online interactions with customers.

Also, HTTPS security prevents hackers from accessing any of the codes used to develop the website. Attackers sometimes change the code of a website without HTTP security to monitor and access all the information visitors provide while interacting with the website. The information can include personal details like credit card information, passwords and usernames, and date of births.

More importantly, an HTTPS protocol allows a website to enhance its SEO rankings. A search engine like Google uses HTTPS security measures to reward websites by ranking them higher in search results.

An organization can complement the HTTPS security measures by deploying a Secure Socket Layer (SSL) certificate. An SSL certificate encrypts all communication between a server and a website user. As such, it does not prevent hackers from distributing malware or from executing attacks. Instead, it encrypts information to ensure it is inaccessible in the event of a successful attack.

By implementing SSL security, user data remains protected against attacks like man in the middle (MITM) attacks. SSL certifications are especially required for websites handling a lot of personal data like eCommerce platforms.

However, all companies should secure their websites using HTTPS and SSL certifications irrespective of the services they provide through the sites.

2. *Make frequent software updates*

Websites require the use of various software tools to run effectively. They include content management systems (CMSs), website plugins, WordPress software, among others.

Updating software tools is vital to ensuring website security.

Other than fixing glitches and bugs that inhibit a website’s performance, software updates also install the latest security measures and patches. Cyber adversaries can target outdated software tools to exploit their vulnerabilities, thus gaining an entry point for executing attacks on a website.

Besides, hackers also leverage technologies like artificial intelligence to automate cyber-attacks. This is by creating intelligent bots that continuously scan for vulnerable websites and execute attacks to exploit them.

Failing to implement the latest updates only provides hackers with more vulnerabilities to execute. This exposes a website to more security risks, jeopardizing the security and privacy of all services and information. Website owners should consider using automated solutions that check for and install software updates as soon as they are released. By doing so, businesses can ensure that all their website software tools are updated and do not contain exploitable vulnerabilities.

3. *Use sufficient password management*

The need to adopt effective password management solutions cannot be stressed enough.

Despite passwords being the easiest way of maintaining website security, they also provide the highest security risks if not managed properly. A study showed that 25% of created passwords could be cracked in under three seconds is an eye-opener as to why website owners should take their password management practices seriously.

Any individual with basic skills can use hacking tools like John the Ripper to hack a password. Keeping this in mind, what are the recommended password security practices that can enable a business to enhance its website’s security?

First, frequently changing passwords is a top password security practice. Website administrators, for example, should periodically change their passwords to lower the risks of an adversary cracking the password. Also, it is essential to use strong passwords. The passwords should be complex enough not to be cracked, yet simple enough to memorize. However, creating complicated passwords with numerous letterings like alpha-numerals and special characters can be challenging to remember. That's why a password manager tool like 1Password comes into play. The tools can allow the creation of long, complex passwords and securely store them for secure usage.

More importantly, a business should only use the services of a web hosting company that uses two-factor authentication or multi-factor authentication.

Such authentication schemes provide an additional security layer. Anyone can provide a valid username and password, but only the legitimate user can provide the required authenticators.

For example, before gaining access, a user can be required to provide a unique code that is only accessible to the legitimate user. A common example of two-factor authentication requires the input of a code that is sent by SMS to the user's cell phone. In this case, the user will need to know the username and password and have the cell phone in their possession. This is considered two-factor authentication because signing in requires both **"something you know"** and **"something you have"**. This prevents insiders with access to the passwords of their colleagues from using them for unauthorized activities that can compromise the website's security.

4. Secure personal devices

Many organizations concentrate on deploying recommended website security practices, forgetting that their personal devices can threaten their sites' security.

Hackers often target personal computers to gain a foothold into a secured website. For instance, by stealing the FTP logins, cyber actors can use malware to inject malicious data and files into a website. Moreover, hackers deem it easier to execute website attacks by using personal computers as a gateway. Therefore, securing a personal computer should be a priority website security practice.

There are several ways through which businesses can secure any personal computers. They include the use of antivirus and antimalware products. Although some might question the viability of such products in countering current threats, they are essential. They protect a user in an online community by preventing the download or installation of malicious files. Also, they can promptly identify malware present in an inserted USB stick or hard drive, thus blocking them from accessing the computer. Using firewalls with strict firewall rules can block incoming malicious connections that hackers use to deliver malware. The security of a website is highly dependent on protected personal devices, and as such, website owners and administrators must ensure maximum protection.

5. Ensure adequate access control measures

Access control is integral to the success of any security program. The same applies to website protection.

Businesses operating a website should define the access permissions for different users who can access the website. The need for strong access controls arises from the fact that human activities are the highest cause of cyber-attacks.

A recent research study that identified that 95% of cyber-attacks are due to human causes echoes this statement. Employees with access permissions to specific website areas can make errors that result in disastrous attacks. To address the risks, website owners need to deploy robust access control mechanisms.

Access controls enhance website security by limiting the number of individuals whose activities can result in errors. By identifying that not all employees should access a website, a business can create role-based access control policies. This would ensure that website access is limited to users with specific roles.

For example, there would be no need to allow a content creator to access the website's coded part. Only a developer or a website administrator should access it. The same applies to all roles, including external developers, guest bloggers, consultants, or designers.

A least access privilege, commonly referred to as the principle of minimal privilege or least authority, is an essential control. It permits employees or outsourced labor only to access the part they need to get the job done. For an individual requiring specific access, applying the principle ensures that the person only accesses the part for the specified time and purpose. This eliminates the chance of an erroneous mistake that can lead to unwanted website security incidences.

6. Change the default configuration settings

Changing the default security settings is a security practice that many companies tend to overlook.

As previously mentioned, cyber attackers often create bots designed to perform automated scans on vulnerable websites. The bots are also used to scan for websites that use software tools that contain default configuration security settings.

Default settings may not provide the security and protection needed to meet a given environment's unique needs. As a result, programs using the default settings are highly vulnerable to attacks.

Attackers can use bots to identify websites that contain the same default settings such that they can be exploited using the same virus or malware. After deploying a website, businesses should ensure to change the default settings of, say, a content management site. Some of the settings to consider changing include but not limited to:

- User controls
- File permissions
- Comments settings
- Information visibility

7. Make Frequent website backups

The basic premise for all security procedures is to stay prepared for the worst.

Companies should always be ready to be the victim of an attack. A website attack can lead to its compromise and subsequent unavailability, and obviously, no company would desire to be in such a situation.

Regularly backing up a website is not just a good idea, but it is an essential measure for preserving the privacy and security of any associated information. A website backup consists of a snapshot of all the essential site components. It allows a website owner to retain and restore critical data when an attack takes down a website.

Essential components to include in a website backup includes themes, plugins, databases, and essential files.

Furthermore, backups are vital to website security. They permit the restoration of a website's clean version if a hack leads to loss and destruction or if a software update results in a crashed website.

Backups should be a top website security practice since they are both easy and essential to maintaining integrity, availability, and confidentiality.

Most website hosts provide organizations with simple ways through which they can create and manage their backups. They can use the panels provided for customer control to maintain the backups or use backup plugins located in tools such as WordPress.

8. Use continuous monitoring

Website owners are unable to identify malware and viruses since they are capable of hiding and are elusive. This contributes to why malware programs are considered to be among the most prevalent threats to website security.

However, with continuous and consistent monitoring, businesses can identify activities that indicate the presence of malware or other illicit programs.

The following are some of the crucial signs that indicate website security issues requiring to be addressed:

a. The login information of user accounts is done without their consent
b. The website files are modified or deleted without the owner's knowledge or consent
c. If the website repeatedly freezes and crashes
d. When search engine results indicate noticeable changes like warnings on harmful content or blacklisting
e. If there is a rapid increase or drop in the website's traffic

The presence of the above signs can signify that a website is infected. A business can opt for a manual monitoring process, where security personnel handles the responsibility of visually monitoring the website's activities. But this can be ineffective. It can be impossible for human operators to monitor a website 24/7, resulting in some security incidences going unnoticed. As such, it is highly recommended to use automated monitoring processes.

An automated scanner is a more effective security solution since it can continuously monitor a website and still allow the website to operate normally. It also eliminates the high costs and inefficiencies involved in manual monitoring. In any case, some monitoring tools are designed to identify anomalous behavior and deploy corrective actions.

Many services can scan websites for common vulnerabilities. These services are useful because they can check to ensure that the website's security precautions are properly implemented.

It is good to run a new vulnerability scan anytime that a change is done to the website. Changes can introduce new vulnerabilities, and a website scanner can help to identify them.

Some free online website security scanners can help detect security flaws. These scanners check for vulnerabilities and tell you if the site is susceptible to things like cross-site scripting and SQL injection attacks.

The free scanning services have value and are highly recommended. However, paid versions of these tools do deeper and more comprehensive scans.

9. Deploy firewalls for website security

Using firewalls is one of the most widely applied website security measures.

A firewall protects a website by blocking malicious connections that can compromise its security. Companies create and maintain security rules created to meet the security needs in the context of the companies' services and environment.

For example, the firewall rules created for an eCommerce platform are different from those defined for a registration portal. There are two types of firewalls used to enhance website security. These are network and web application firewalls.

Network firewalls are usually used by organizations that manage their servers and by web hosting providers. The firewalls ensure website security by identifying and blocking malicious scripts between web servers running within a network.

On the other hand, web application firewalls are used to secure a specific website. A web application firewall prevents malicious scripts from accessing a web server, thus securing a website from being compromised. Blocking malicious traffic secures a website and saves the bandwidth and load time of the web hosting account.

10. Validate all user input

Validating user input protects against attacks like SQL injection. An SQL injection attack is where a hacker enters SQL code into an input field on your website. For example, your website may have a field where a user can sign up for an account. Instead of entering a name, the hacker will enter a computer code that can trick your website into outputting your database's contents. This might give the hacker information, including all of your users' passwords, email addresses, and potentially even social security numbers and other data that may be stored.

It is relatively easy to guard against this potential vulnerability. The data that a user enters into your website must be validated to ensure that it is safe. This validation can be done at the client-side and the server-side. Server-side validation is more secure because hackers have the ability to circumvent client-side validation.

Many websites were vulnerable to SQL injection attacks in earlier days of the internet. SQL injection attacks were commonplace because there was less of an emphasis on website security. But even today, these attacks are widely used because they still work. Any website that does not validate all user input is at risk of being breached.

11. Understand third party security issues

Virtually all websites depend on third parties. The third party might be the hosting company, the company that created the content management system (Ie. WordPress, Joomla, etc.), the companies that create plugins, or even the designer hired to help create the website.

Each of these third parties introduces risk and potential vulnerabilities to a website. For example, if the website is built using WordPress, it is susceptible to any vulnerabilities that WordPress may have. Any plugins or third-party code that is used in the website may also introduce attack vectors for hackers.

The website hosting company is a third-party risk. Hosting companies are often the target of cyberattacks that can affect all of the websites on their platform. Hosting companies are well aware of these risks, and they often take measures to ensure that their customers are not negatively affected by attacks. Despite these efforts, it is not uncommon for hosting companies to be taken down by malicious actors. A recent example includes an attack where hackers used ransomware to take down the entire web hosting infrastructure of web host company Managed.com.

12. Create a website security blueprint

To sum up the top website security practices, it is essential to develop and maintain a plan for implementing them. More often than not, organizations follow a disorganized approach for managing website security processes, resulting in minimal accomplishment.

Therefore, before deploying any security measure, it is vital to develop an actionable and detailed website security plan. The plan should outline the objectives the organization wants to achieve by implementing security measures.

For instance, the main objective would be enhancing the website's overall compliance or to enhance the security of the website. A website security blueprint should further identify the applications whose security requires prioritizing and the processes that will be applied in testing their security. Although the website security blueprints of different organizations can differ, the following six-step checklist can be applied.

1. Gathering information on main security issues
2. Planning a countering process
3. Executing the plan to discover vulnerabilities, if any
4. Document the results
5. Address the identified security vulnerabilities by remediating appropriately
6. Verify the website's security