AZION

11 Techniques for Securing Your Website

With more people shopping, communicating, and working online than ever, many online sites are seeing unprecedented growth. However, the more visitors a website attracts, the bigger a target it becomes for bad bots, fraud, and other malicious activity.

That means it's absolutely critical for website owners to check for vulnerabilities and ensure that they're enforcing best security practices.

Use an SSL Certificate

Have you ever gotten a pop-up warning from your browser that the site you're trying to visit is not secure? Browsers use these warnings to signal when a website isn't protected by an SSL certificate.

SSL is a protocol for encrypting data as it travels from the website to the server. This not only protects the information users enter into a site, but also verifies ownership of the site, ensuring that users are accessing your site and not a fake version created by attackers. In addition, SSL certificates ensure more traffic reaches your site by providing you with an HTTPS address (the more secure version of HTTP).

Most crucially, it ensures that users visiting your site never encounter one of those frightening pop-up warnings, which could scare users away from your site before they've even had a chance to see it.

Azion lets you check, create, or update your SSL certificates through a Digital Certificate API.

Change Passwords Regularly

If you're reading up about website security, chances are you've already implemented a unique password that can't be easily guessed. However, the strength of that password could be compromised if you don't change it regularly.

Even hard-to-crack combinations of letters, numbers, and special characters could be recorded by surveillance technology that logs keystrokes, and hackers who have stolen a password can access a site indefinitely until its login credentials are changed.

By frequently changing your passwords, you limit their usefulness to anyone who gets a hold of them.

Make Sure Your Software Is Up to Date

Software updates don't just squash bugs or add new features; many of them are released specifically to address security vulnerabilities. This means the less you check for software updates—and the longer you wait to install those updates—the more you risk exposing yourself to hackers who've already cracked that software's vulnerabilities. In fact, 60% of security breaches last year occurred in situations where security patches were available, but not installed.

Always ensure that you're using the latest version of any plugins, ecommerce, or other software that might give hackers a foothold into your website, and arm yourself with security products from trusted experts who can help you to recover from any attacks.

Perform Daily Backups

Not all hackers are looking to profit off of their crime; some simply want to sow chaos. And the more work you put into your site, the more devastating it would be to lose that work to malicious code or data destruction.

To minimize the fallout from such an attack, keep daily backups of your site on a third-party location that is separate from your website's server. This will ensure that if data loss does occur, you won't be forced to build everything again from scratch.

Protect Against DDoS Attacks

For sites big and small, DDoS attacks have been skyrocketing since the start of the pandemic. DDoS, which stands for distributed denial of service, is a type of attack designed to take a website offline by overwhelming it with fake traffic.

By shutting down your site, hackers not only prevent the access of legitimate users, but damage your reputation by making you seem unreliable. Not only are DDoS attacks occurring more and more frequently, they're constantly growing in size and complexity, leveraging different types of devices and targeting different parts of the target's network.

That's why Azion's DDoS Protection lets you choose the level of protection you want, offering anywhere from 5Gbps to unlimited protection against attacks of any size. In addition, all levels of Azion's DDoS Protection provide always-on mitigation with Deep Packet Inspection and advanced algorithms to immediately detect and block malicious traffic.

Protect Against Web Application Attacks

Two of the most common web application attacks are cross-site scripting (XSS) and SQL injections. Cross-site scripting is a type of attack where web applications inject malicious code into your site, passing it on to your users to infect their computers and capture their data.

SQL Injections are attacks that insert code into a server's SQL database, allowing hackers to destroy, alter, or steal data, or even become an administrator of the database server.

The reputation-damaging consequences of these attacks are enormous. Azion's Web Application Firewall guards against these and other common web application attacks with protection against Top 10 OWASP threats.

Block Brute Force Attacks

Brute force attacks are when hackers try to crack login credentials or encrypted data by systematically trying every possible combination of letters and numbers until they finally land on the right one. One of the easiest ways to prevent these attacks is by automatically blocking users after too many incorrect attempts.

Azion's Network Layer Protection enables this through rate limiting, which lets you control how many times users can attempt to log in before being locked out and how long users need to wait before trying again.

Prevent Spam

Finding spam in your email is annoying; seeing it all over your site's comments and message boards is horrifying. Spam is another way hackers can turn users away from your site. Not only are these obnoxious comments sure to put off some users, others may fail to reach your site altogether, since Google factors spam into SEO rankings.

Just like rate limiting can be used to stop brute force attacks, it can be used to prevent bots attempting to spam a site by limiting the number of times a bot (or a truly obnoxious user) can comment, making our Network Layer Protection a useful tool against spam.

Use a Seal of Trust

While a seal of trust may sound similar to an SSL certificate, it is actually a separate security measure that indicates additional security measures beyond data encryption.

Trust seals are usually displayed on the site's main page as an icon containing the words "Secure" or "Verified," sometimes alongside the name of a security partner. This icon indicates that the site is working with a third-party company to further secure particularly sensitive data like payment information. Clicking on the trust seal will take users to the security firm's verification page, confirming the badge is legitimate.

For ecommerce sites, the presence or absence of these badges can make or break a sale, as many users won't buy from a site that doesn't have one. For any type of site, however, a seal of trust can assure users that you're doing everything you can to keep their information secure.

Check for Malware Regularly

Even a quick glance at a site can provide a world of information about its security. Defacements, suspicious pop-ups, malvertising, and phishing kits that redirect users from your site to another are all signs that your site has been infected with malware.

Performing regular checks for these red flags can ensure that you are able to quickly eliminate malware before it drives away users and infect their devices.

To avoid reputation-damaging malware altogether, Azion's Origin Shield allows you to build a secure perimeter around your source infrastructure, blocking any traffic outside of specific IP addresses.

Build Multiple Layers of Security

Given the frequency and sophistication of cyber attacks today, it would be naive to assume that hackers will never find a vulnerability in your website. That's why it's important to have multi-layer security, preventing a single point of failure from disrupting your entire website.

This means a firewall or other protective measure to keep attackers from getting into your site, visibility and monitoring for users on your site, and a solution for responding to attacks—and Azion's multi-layer security platform is designed to do just that. In addition to our Network Layer Protection, Web Application Firewall, and DDoS Protection products, we offer additional visibility tools such as Data Streaming and Real Time Metrics to keep track of suspicious activity and gain the insight to make sure your site is as secure as possible.

Securing your site isn't just a one-time activity; it's an ongoing process. Hackers are constantly finding new ways to infiltrate websites, so it's important to always stay up-to-date on security trends and practices and periodically check your site for potential threats and vulnerabilities.

Count on Azion to implement all cybersecurity techniques in your business!

Contact us