Web hosting security practices

XANTHI, THRACE, GREECE, November 15, 2022 /EINPresswire.com/ -- While the Internet has many advantages, one disadvantage is that the more people do business online, the more vulnerable their information is to those who want to access our data through malicious attacks and fraud.

Web hosting myip.gr

In recent years, billions of people have had their information compromised through attacks on high-profile companies like Yahoo, Equifax, and Uber.

Small business owners may think that because of the more low-profile nature of their businesses, their websites are not attractive targets for cybercriminals and hackers, but this is not the case. If starting a new website or just looking for a new web hosting host, check out MyIP hosting packages.

> MyIP has been active in the field of Datacenter services since 2003. The main service we offer is website hosting. Today MyIP offers a wide range of services regarding Internet and Datacenter."
>
> *Haris Alatas*

According to a 2021 report, small businesses account for 43% of data breach victims. Small businesses must take their website security seriously, as data breaches can have serious and long-lasting consequences.

Malicious attacks can cause a website to be temporarily or permanently disabled, cost businesses thousands of euros, and erode customer trust if their personal information is exposed through a website. Choosing a web hosting provider that takes website security seriously is key to protecting a business, a website, and its customers.

Below, web hosting security best practices are outlined to look for when choosing a provider for a website, as well as some steps to take to protect a website. Security is a major concern when considering a web hosting plan. But there is no single feature that makes one hosting platform more secure than any other.

Instead, a set of individual factors contribute to the overall security of web hosting. Most web hosting companies engage in at least some of the standard security practices, but that doesn't tell how secure they are compared to the competition. It is important to consider several different security measures that a web hosting company may take to keep a website secure.

Web hosting security practices

When buying web hosting services, the main thing purchased is the server space to host the files that make up a website. Ensuring that physical servers are protected from threats is the first step to feeling confident that the data stored on those servers is safe.

ssl certificate - myip.gr - Web hosting security

The data centers where the servers are physically located should be secure, with access granted only to the web hosting company's personnel responsible for installing and maintaining the hardware. Best practices include controlled access points, security cameras, motion detectors, and secure cabinet mounts that prevent bad actions from physically compromising servers.

Server rooms are also vulnerable to natural and man-made disasters such as power outages, fires, floods, and more. To mitigate these problems, server rooms should be waterproof and fireproof, equipped with backup generators, and hardware racks should be bolted to the floor, ceilings, or walls.

Companies that back up data at off-site locations add an extra layer of protection. Always take into consideration where a company's data centers are located and try to avoid areas that are prone to natural disasters such as earthquakes, hurricanes, and tornadoes.

Consistent threat monitoring is critical to quickly identifying and resolving issues before escalating into more serious attacks and breaches. Just as web hosts should limit who has

physical access to their servers, getting virtual access should also be limited. Being careless about who can connect to a server and what information can be seen, can easily lead to data breaches.

Web hosting providers should use the Secure Socket Shell (SSH) network protocol or an equivalent for login access. SSH uses strong password authentication, public key authentication, and encrypted data communications to facilitate remote and secure management of systems and applications. Many web hosting providers will clearly state whether they allow SSH access.

Secure Sockets Layer (SSL) encryption ensures that if someone tries to intercept data as it is transmitted over the web, garbled, unintelligible characters will only be seen. SSL encryption is such an integral part of website security, especially for e-commerce sites, that many web hosting providers now include a free SSL certificate in their hosting packages.

If not, all business owners should obtain an SSL certificate separately. Not only does this help protect a business and its customers, but search engines are increasingly labeling sites without SSL certificates as "unsecured," which could turn visitors away.

Web application firewalls (WAFs) provide additional protection for web applications by filtering and monitoring HTTP traffic and protecting web applications from attacks. Look for web hosting providers that offer host-level or cloud-based WAF.

MyIP net-Works O.E.
MyIP.gr
+30 215 215 4722
email us here
Visit us on social media:
Facebook
Twitter
