

How to Reduce Web Vulnerability Scanning Times



It shouldn't be surprising cyber crime is costly to any business. Between the cost of lost productivity, the cost associated with the resultant fallout from any compromised data, as well as the hit the reputation your business will take – it's no wonder many businesses fail, or come close to it after a major security breach. And that's before you even consider the costs associated with clean up and recovery.

Cost of A Business Cyber Attack

According to the 2014 Ponemon Cost of Cyber Crime Study, the cost of cyber crime ranged from \$1.6 million to \$61 million, with an annual average of \$12.7 million. These figures are 10% higher than 2013's numbers, but most concerning is the fact that it took an average of 170 days to discover a malicious security breach had even occurred in the first place. The study found it took businesses an average of 45 days to clean up after an attack as well.

That's why the importance of not just using a powerful tool such as Acunetix's Web Vulnerability Scanner is a must, understanding how to use it by working with trained Acunetix experts with Alliance Technology Partners, and then knowing how to

get the most out of your scans and scan times is vital to your business operations.

Things That Cause Slow Web Vulnerability Scanning Times

The quality of your server has a lot to do with how quickly or slowly your web vulnerability scanning takes. A good server response time is considered to be anything less than 200ms (0.2 second), while a response time over 300ms (0.3 second) is considered to be prohibitively large – which causes scans to drag on for dozens of hours, if not days.

Keep in mind, there are any number of other things that can cause slow scan times, such as:

- Firewall issues
- Issues with your Internet Service Provider (not on a high enough plan, service down, etc.)
- Issues with your database

The good news is that there are multiple options for you to take advantage of to reduce the amount of time it takes for your web vulnerability scan to complete and ensure the digital security of your business.

“According to the 2014 Ponemon Cost of Cyber Crime Study, the cost of cyber crime ranged from \$1.6 million to \$61 million, with an annual average of \$12.7 million.”

Reducing Web Vulnerability Scanning Time

Now that you know slow web vulnerability scanning times are typically caused by issues with your server, we can take steps to speed things up.

The first thing you will want to do is check things such as your CPU, memory and hard disk success to find out if there are issues that are impacting your server and database performance. Some times simply cleaning up and optimizing your database will resolve slow response times because there aren't as many queries your system has to go through each and every time a response is requested.

If cleaning up and optimizing your database doesn't fully resolve the issue of slow scan times, upgrading your server should be your priority. With servers, you typically get what you pay for so don't upgrade to something that won't meet the needs of your business and be sure you're working with Alliance Technology Partners' team of engineers to ensure a successful upgrade.

It Only Takes One Successful Attack

Those trying to break into your company digitally only need to be successful one time,

whereas you need to successfully protect your data from attackers every single time.

No amount of investment in security can guarantee your company won't ever be the victim of a cyber attack, but arming yourself with the right tools and making sure you have the resources and people in place to prevent attacks and respond to attacks when they happen is a critical piece of the puzzle.

To learn how you can leverage the full potential of Acunetix Web Vulnerability Scanning, contact our team of Acunetix trained engineers today.



CORPORATE HEADQUARTERS

18102 Chesterfield Airport Rd. Suite E
Chesterfield, MO 63005

Phone: **888 891 8885**

sales@alliancetechnpartners.com