Bangalore, India (Head Office) - #27, Ambalipura, Bellandur Road, Bangalore 560103, India.
Phone : +91 80 4131 7700

California, USA | Texas, USA | New York, USA | Doha, Qatar
www.instacarma.com

How an e-commerce host could improve sales through PCI compliance, with InstaCarma's help.

This post is intended to share how we at InstaCarma were able to help one of our clients in achieving PCI Compliance and hence increase their customer base.
This client* is basically a provider of e-commerce based hosting solutions. They deal with plenty of sensitive and important data. Hence, becoming PCI Compliant was mandatory for them. Recently they were getting too many potential customer queries whether they are PCI Compliant.

What is PCI Compliance?

A PCI Scan tells you what could be potentially insecure about your server. This is particularly important where storage of sensitive data occurs. Therefore, PCI Compliance is something which is preferred by most credit-card companies these days.
The PCI Security Standards Council talks about 12 basic requirements broadly divided into 6 categories. This is called the PCI-DSS (Payment Card Industry Data Security Standard)
This is required in order to avoid data frauds where card information is stored.

The approach

Following are the important steps that we took in order to ensure that their cPanel servers pass the PCI Scan: -
Installed a firewall: A server is not likely to pass the PCI Scan if there are unnecessary open ports. We installed CSF on the server. Alternatively, APF can also be used. We closed all the ports except for the ones required for the essential services. Certain standard ports like 2082, 2086 and 2095 could produce a negative result. So, we configured WHM to use the secure ports only.
Updated the packages: Just run /scripts/upcp to update all the packages. Also, we had to make sure that Apache, PHP and MySQL were running the latest version.
The suggested versions are:
MySQL 4.1.22 or above
PHP 5.2.5 or above
Apache 1.3.39 or above (Certain scans might require Apache 2.0.x)
OpenSSL 0.9.7j or above
cPanel suggests that you should keep cPAddons up to date as well. We did all the above on their servers.

Disabled mod_userdir: If a site on the server can be accessed as http://serverip/~username then it means that mod_userdir is 'enabled'. For PCI Compliance, this should be disabled and that is exactly what we did. It can be done via WHM > Security Center > Apache mod_userdir Tweak

Installed SSL: At least, one SSL certificate from a recognized certificate authority is required. We installed SSL for Apache. SSL can be installed for other services as well.

Apache Setup should not be revealed: We all have seen the '404 Error' page at some point. Information about the Apache Setup should not be available on that page. We did this by adding the following lines to the 'httpd.conf' file :

1. ServerSignature Off
2. ServerTokens Prod
3. FileETag None

Disabled SSLv2 and other weak encryption methods: Some services don't allow you to choose between SSL protocols but most PCI Scan overlook it.

The Weak SSL cipher issue has been a headache for people who want to pass the scan. We disabled SSLv2 on the servers.

mod FrontPage – It is likely to cause a scan failure. Therefore, we kept it disabled.

2 factor authentication – This is another suggestion by cPanel that we adopted. A 2-factor authentication procedure which requires a key and a pass-phrase.

It is a wonderful freely available tool to find any vulnerabilities on your server. You can find the details on the official Nessus website – http://nessus.org

Nessus basically consists of two parts, the server and the client. Once you are done with the two installations you need to add a user for the scanner and then you can start a scan on any remote server. The scan might take a while. It will give you a detailed report about all the package related vulnerabilities and any security loopholes. The best thing about Nessus is that it will also give you suggestions on how to fix those.

Thus, Nessus will tell you almost everything that needs to be done in order to achieve PCI Compliance. We got a list of vulnerabilities as the result of the scan. We then went ahead and fixed them one by one. This was of immense help in our goal to get the servers PCI Compliant.

The result

What else? The client achieved PCI Compliance. Achieving this has helped them grow their business by almost 50% in last couple of quarters. The trust that the customers had in the company increased. Word of mouth is the best mode of publicity. That is exactly what happened here resulting in quick and

sustained growth. Note that different scan companies have a different approach. Hence, the requirements vary and they might have many more than the ones mentioned above. But these are the very basic ones that need to implemented for sure. We hope that this write-up would be of some help to those looking forward to achieve PCI Compliance.

* *Name of the client cannot be revealed as per the NDA (Non-disclosure Agreement). References and testimonials are available.*