4 Effective Tips to Keep the Dedicated Servers Secure and Inaccessible by Preeti

Article published on January 18th 2012 | Web Hosting

Many webmasters prefer to host their business websites on dedicated servers to avoid the risk of storing multiple services onto a single web server. Despite of the high cost of hosting the websites on the Windows dedicated server or Linux dedicated server, these servers are popular among companies due to their effective in keeping the website secure and inaccessible various types of malware attacks and hackers. However, you must remember that all the text and multimedia files, software programs and hardware required for running you business website are stored on a single system. Therefore, a number of effective measures need to be implemented to provide the server with a much higher level of protection and security.

1. Impose Restrictions on Server Room Entry:

The information and data stored on the web server can be damaged in an intentional as well as accidental manner. Therefore, you must place the server inside a secure and locked room. It is also very much important to implement a string password policy for the persons authorized to access the system. Further, you must clearly mention the consequences of violating the information security rules and sharing individual system passwords. These measures will be effective in protecting your business website from intentional and accidental damages.

2. Apply the Security Patches and Critical Updates Immediately:

The software program and operating system manufacturers frequently released security patches and critical updates. If you have subscribed to the Windows dedicated server or Linux dedicated server maintenance services, it is critical to ensure that the service provider installs these security patches and critical updates without causing any slight delay. Similarly, the server administrator deployed by your company must be instructed to install the patches and updates immediately to eliminate the security loopholes and other exposures.

3. Indentify and Remove the Irrelevant Services:

When you decide to use specific systems as dedicates server, some measures must be taken to optimize the performance and security of the computer. Sometimes the unneeded and unused services running on the web server of you company can lead to inherent security exposures. You must identify and turn off these irrelevant services to allow the essential services to run and boost the performance of the server. For instance, if the server is going to manage the email account of your organization, you can turn off the file transfer protocol (FTP) feature. You can even get the system checked by a network security technician to turn off these unnecessary services.

4. Regularly Conduct Sever Audits:

In addition to the precautionary measures, you must audit and inspect the server on a random basis. You can always concentrate on finding some normal irregularities like passwords, suspicious user identification and intrusion attempts. Further, you also need to check whether any unnecessary service is activated recently. The occasional server audit will alert the responsible staff and also ensure the security of the dedicated web server.

However, the safety and security of the dedicated servers is an ongoing issue. You must prepare and implement a proper security policy by considering these effective measures.

Article Source:
http://www.articleside.com/web-hosting-articles/4-effective-tips-to-keep-the-dedicated-servers-secure-and-inaccessible.htm - Article Side

Preeti - About Author:
SRE Global Infotech, a a SEO India Comapny is handling SEO campaign for SuperSeedbox, provides you with the best and top notch quality internet services. Your search for a Seedbox, Windows and Linux a Dedicated Servers and Semi Dediacted Server ends here.

Article Keywords:
Seedbox,Seedboxes,Dedicated Seedbox Hosting,Cheap and Best Seedbox,Dedicated Servers,Managed Dedicated Servers,Cheap Windows And Linux Dedicated Server

You can find more free articles on Article Side. Sign up today and share your knowledge to the community! It is completely FREE!