Your security online is only as good as the weakest link in the security chain. This means that you must protect your own website, update your web applications regularly, protect network with firewalls and take into account the cyber security of your hosting agent or server.

Your online security is only as good as the weakest link in the chain. That means you need to protect your own website; regularly update the web applications you use; protect your network with firewalls; and consider the security of your server or hosting agent.

## Steps to Secure a Server

If you want a stable and secure server, then you should follow the steps below:

### Review Your Server Status

Regular and routine monitoring of your server is a crucial point in cybersecurity. The more you check your server status, the better you are aware of your server's stability. You would know if there is any problem with your RAM, CPU, disk usage, running processes, and other metrics by conducting a server status. Furthermore, you should check your database logs and site access logs to see any suspicious entry in your server.

### Update Security Patches

Public vulnerabilities don't give you much time to encounter them. Thus, another essential thing for cybersecurity is that you should regularly update your security patches. It is better if you automate your security updates so that you can minimize public vulnerability.

### Use Encrypted Information Transfer

You should avoid insecure communication protocols because it is very easy for intruders to intercept the communication path. Thus, you should use encrypted information paths that are secure such as FTPs, HTTP, and SSH. A web server that supports any of these protocols will ensure that your message is encrypted when it goes to and fro the network.

### Set Up Perimeter Security with Firewalls

A firewall plays a very important role in cybersecurity because it can block any automated attacks, malicious traffic, known threats, DDoS filters, and untrusted networks. Furthermore, a local firewall can also monitor SSH password guessing and block any security threats.

### Remove Unnecessary Services

Some unnecessary services are a threat to your server, so it is best to remove such unnecessary services. Some examples of these not secure and unnecessary services are Remote Registry Services, Print Server Service, RAS. If such ports are left open, then they are vulnerable to attack and can serve as a threat to your cybersecurity.

### Restrict Access

You should always limit the access of your files and directories to only those who need them. You can control and minimize the amount of risk and damage by limiting access to your files.

## Conclusion

If you are looking to secure your server, then consider the steps mentioned above. To achieve cybersecurity, be vigilant with the protection level of your server.