

Forum:[Hack Forums](#)

Thread: [Legal Questions needed answered. internet security/comp security/program security](#)

GhostlySam - September 10, 2011, 1:21 pm

After some research I have learned about many ways to protect yourself, your server, and your internet to be online.. I am posting this because of legality reasons and thought I would get a lot of feedback in this forum, if you believe it could be posted in a different forum as well, please tell me and I will do so.

I was wondering, on a legal stand point, if I owned a company, and what we did was put a server with an automated program online to stop specific illegal activity. If we put a server online that automates a process to stop the specific illegal activity, then our IP will be shown and then possible hackers could try and disrupt the service or shut down the internet/server/or inject something of our server or even our VPN... Right?

On a legal stand point to protect ourselves, our machines, and our programs. What do you think would be the best way, legally, to protect everything, and I mean everything.

Botnets seem good for illegal activity, but connecting through zombies seems bad if you have a legitimate company. Right?

What would you recommend, internet security, server security and program security wise to be almost "impenetrable"? I was thinking a Linux box to start off with because less viruses are made for Linux as well.

I am looking for all answers from the pros, black, white and grey hats honestly. Everyone who has experience in any one of those fields. This is something we want to protect, in any way, shape or form. So we can be online 24/7 and know our machines, product, internet and our information is protected at all times.

We might have a website, but we were going to get a different host for the website, which is not connected to our main server where the program is running online, for potential security reasons. Does that seem like a valid idea?

I am asking everything there is to know, from the pros or experienced members on every part of every subject... Yes, it is a lot, but I am looking forward to hearing all the feedback, hopeful debates and security guru's talking about every aspect.

Go Go Go! Thanks in advance everyone!

v3xr - September 22, 2011, 11:18 pm

Well, if you're asking for the best way to secure a server, I would say yes go with Linux, an up-to-date and personally secured version. Yes, Linux doesn't have a large threat to malware, but a virus isn't your worry as a server/website owner anyway, it's vulnerabilities. Whether its http or something else, there are usually vulnerabilities in everything, and the key is making sure you keep your software up to date. This includes yes your kernel, but also the structure and functions of your website, and the various other programs accessing the internet as well. For websites this goes for file inclusion, file uploads, directory permissions and index-less directories, all info passed through GET should be sanitized, as well as all forms and input boxes, and anything else input related.

Anything with a potential vulnerability should be either removed, or updated beyond the range of the vulnerability.

The next thing after that would be firewalls. You should employ both a software, and hardware firewall to secure your server. Setup the rules for both to best fit your server, allowing ports for necessary programs, and denying all else unless approved by an admin.

Also, on passwords-- make them long, alphanumerical passcodes, not just phrases. Anything short or simple can be easily bruteforced/dictionary'ed. Having password reset dates can be very helpful too. If an attacker manages to get a password without you knowing, a 10 day password reset can prevent them from saving the password for future use.

Hopefully this answers your question ?