

FIREWALLS

This week I will attempt to bring down one of the cornerstones of internet security, namely the need for a software firewall solution. This sacred cow comes under my knife because, on the whole, firewall programs are giant, fat behemoths, which suck up system resources under the guise of “protecting you from hackers”. Not only that, but software firewalls are one of the leading causes of our service jobs. Most commonly the program stops allowing internet access altogether, either because the user didn’t know how to configure it properly or, more commonly, it is just a bad program. Learn to live without one, I have never had a software firewall installed on any of my PCs.

First, there are no hackers. You heard me. To be more precise, there are no hackers that want on your ubiquitous box, there’s nothing there that he really wants. On the other hand, if your son’s best friend considers himself a “h4X0r” be afraid, very afraid. With direct access to your system in your house there are any number of things he can do to ruin your day.

To bring us to the next point, outside of your house there is almost nothing an enterprising hacker can do to get on your box.

I am not kidding.

I can’t “hack” my way onto your Windows machine, and you can’t “hack” mine, because by default there are simply no services running to allow it. On the other hand, if I sent you a server program that you installed because you trusted me, it would give me complete access to your machine. Or if you decided to “network” your two PCs with file and print sharing by plugging them into a switch or hub, along with your high speed modem, you would be essentially turning your network inside out for the whole world to see. Bad move, I actually know two guys here in town that run computer stores that have done this.

I wasn’t completely honest about never having had a software firewall. Back in the day (1997) I had a Linux standalone firewall, a PC which shared my internet connection to my other Windows PCs. Linux is a user-supported operating system with a great deal of power. It is endlessly configurable and we use it primarily for its server capabilities (NOTE: I personally find Linux entirely useless in every other regard). Unfortunately, some hacker from California ended up “rooting” the box (taking control of it) by using a known exploit of the QPop server, a program we used for serving up our emails. The point is, hackers can only exploit boxes with server capabilities, like Linux or Windows Server, not client machines. This is the only actual case of “hacking” I have ever seen in nine years of business.

I am not preaching complete abstinence, particularly for those on cable. High speed routers with built in firewalls cost as little as \$59 these days. They are primarily used for sharing internet between multiple PCs, but they work just fine with even one PC. Uninstall that piece of junk Zone Alarms or Norton Internet Security and give your Windows a little breathing space.

If you have question or comments, I can always be reached via email sean@intrex.ca or join our forums at <http://intrex.ca> for more in-depth conversations.