

Re: Which Router for VPN and Webhosting

Source: <http://www.derkeiler.com/Newsgroups/alt.computer.security/2003-09/1258.html>

From: Eirik Seim (*eirik_at_mi.uib.no*)

Date: 09/20/03

Date: 20 Sep 2003 20:36:24 GMT

On Sat, 20 Sep 2003 16:31:30 GMT, David wrote:

- > *It's hard to say. In either case it is simply a matter of whether the black*
- > *hats find the vulnerabilities before the white hats do. Even with MS's piss*
- > *poor reputation in regards to dealing with reported vulnerabilities, they do*
- > *seem to get most of their holes patched before the exploits hit the net.*

In most cases yes. I don't think they ever patched that IGMP problem with Windows 98SE (and earlier). The problem is rather the amount of patches. Once there is a patch that is a bit harder than usual to install (like the MS-SQL hole exploited by the Slammer worm), it is skipped and forgotten until networks start to go down.

- > *There are several security outfits looking for windows vulnerabilities right*
- > *now because there is money to made in doing so.*

Which is great! :)

- > *On the other hand I have seen a lot of open source vulnerabilities that are*
- > *being discovered after the exploits show up. OpenSSH for example just fixed*
- > *two holes one right after the other which it looks like were only discovered*
- > *after several systems had reportedly been hacked. And this is not an obscure*
- > *open source project.*

There will always be bugs in complex software. Most of them are found and fixed before an exploit is out, but yes I see your point. The sword cuts both ways.

- > *There is a lot of open source stuff out there that is not getting audited.*
- > *And there is a bunch of PHP and perl stuff for websites which is full of*
- > *exploitable code. Take a look at many of the open source web application*
- > *projects and you will probably find exploitable scripts and or SQL injection*
- > *vulnerabilities.*

Poorly written web applications will become even more of a problem in the future. There is an infinite amount of bad programmers out there who took a one-year "web programming" course[1], and keep making the same mistakes instead of reusing mature code, and follow the recommended guides for things like input checking[2].

– Eirik

1. And others, of course. A CS degree don't have to help, either.
2. The last case I reported was actually at my local MENSA website, which was kind of amusing in a way..

--

New and exciting signature!