

RE: home wireless router good practices for security

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-12/0574.html>

From: Preston, Tony (*Tony.Preston_at_acs-inc.com*)

Date: 12/31/03

To: security-basics@securityfocus.com

Date: Wed, 31 Dec 2003 08:37:09 -0500

I also have the Linksys, it is a great buy.

To answer some of your questions... Yes, enabling the encryption will not only hurt your performance, it is a pain to get right with different machines (I have a Win ME, 3 Win XP boxes on my network). It will work with a bit of work. I never did any benchmarks, but I think it was PC world magazine that did and it seemed to have about a 10-20% penalty associated with it.

You want to use an odd SSID, not the default and disable the broadcast. I also changed the channel from the default and while it only uses that in machine to machine communications (I have game players in the house), I never like leaving defaults...

You should run a firewall on each machine. I also suggest that using MAC filtering is a good thing and would have prevented your neighbor's access.

My son has a laptop with a wireless card and went to his girl friend's house. She was not home yet so he sat outside on their porch waiting and had minor problems attaching to their wireless network (which he setup for them). He found that he could easily attach to the neighbor's wireless network (directly across the street) and use their connection while he waited. Most people do not lock their connection down either out of ignorance or deliberately.

I prefer to lock mine down with what little I can... I have blocked several ports at the router (135-139, ect...) which is an option on the Linksys router. My son plays online games and has had no problems with the blocks.

I *KNOW* the router is not secure so I run AVG, Kerio personal firewall, Ad-aware, and Spybot S&D on my system and track things to prevent problems. My worst nightmare has occurred, my daughter is back from school with her laptop and wireless card and she is dangerous...:) always running things sent to her in email, downloading stupid programs... I think she is almost

SecurityFocus BASICS: RE: home wireless router good practices for security

cured of that (she got infected once), but who knows..., but that is one of the reasons I run a firewall and check its logs.

Tony Preston
Systems Engineer, AS&T Inc.
Division of L3 Corporation
(609) 485-0205 x 181

-----Original Message-----

From: Steve [mailto:securityfocus@delahunty.com]
Sent: Tuesday, December 30, 2003 1:33 PM
To: security-basics@securityfocus.com
Subject: home wireless router good practices for security

So I went out and purchased a wireless router (Linksys 802.11b) for home since it was so inexpensive and actually less cost than the wireless access points I was trying to get via eBay. Got it home, installed my wireless network card (SMC), powered on the router, attached it to a port on my other wired linksys router, and boom it worked great. Then about 5 minutes after I sent an instant message to my neighbor (fellow IT friend) he was on my network. So I took the steps that Linksys recommends below, seems good (to me).

- Change the default SSID
- Disable SSID Broadcasts
- Change the default password for the Administrator account
- Enable WEP 128-bit Encryption

Linksys also recommends these other measures, I have not implemented:

- Enable MAC Address Filtering
- Change the SSID periodically
- Change the WEP encryption keys periodically.

My Questions:

- 1) Anyone know how much enabling 128-bit encryption will hurt my wireless performance?
- 2) Does setting the SSID for my wireless NIC then keep me from getting onto other wireless networks like when traveling? I ask since that setting was set to ANY before I changed it to the SSID that I set for my wireless router.
- 3) What else should I really do to protect my home network?

