

Full-Disclosure: RE: [Full-Disclosure] Microsoft urging users to buy Harware Firewalls

RE: [Full-Disclosure] Microsoft urging users to buy Harware Firewalls

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-08/0791.html>

From: Richard M. Smith (*rms_at_computerbytesman.com*)

Date: 08/14/03

To: <full-disclosure@lists.netsys.com>

Date: Wed, 13 Aug 2003 23:13:17 -0400

Tens of millions of home owners have already purchased NAT boxes and use them on a daily basis to share their cablemodem and DSL Internet connections between multiple computers. These products are extremely popular. Not sure what all these problems that are you complaining about. In my experiance, these boxes just work.

Richard

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

From: full-disclosure-admin@lists.netsys.com

[mailto:full-disclosure-admin@lists.netsys.com] On Behalf Of Thilo Schulz

Sent: Wednesday, August 13, 2003 10:00 PM

To: full-disclosure@lists.netsys.com

Subject: Re: [Full-Disclosure] Microsoft urging users to buy Harware Firewalls

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

On Thursday 14 August 2003 02:04, Richard M. Smith wrote:

> *I agree with Microsoft's recommendation for a hardware firewall on all
> home PCs. A Linksys NAT router box is selling for only \$40 at Amazon
as
> we speak. Besides protecting against the MSBlaster worm, a hardware
> firewall blocks those annoying Windows pop-up spam messages which have
> become so common lately. A hardware firewall also protects a shared
> Windows directory from being accessed from the Internet. My only
> question is why aren't NAT routers built into all cable and DSL
modems.*

This is ridiculous. Before long, you get millions of windows private users complaining, why netmeeting, or their nice game server is not accessible

RE: [Full-Disclosure] Microsoft urging users to buy Harware Firewalls

Full-Disclosure: RE: [Full-Disclosure] Microsoft urging users to buy Hardware Firewalls

anymore. Nice – of course you also disabled the potentially "evil" services now. Then the user finds about port forwarding, and as soon as the user has done this, the computer is suddenly vulnerable again to flaws in the service that is being provided to the outside! who would have thought that? Also – the principle of masquerading is, that inbound connection attempts land at the router and cannot get to the computers in the local network. By default the router approves all connections from the inside to the outside. To be honest, I have preferred this solution in my home LAN, I would not want anything else to be set up. Trojans/worms that connect from inside the lan to a control channel in IRC or something like that are not hindered at all by the router/hardware firewall... – From the point of the user – one has bought some new hardware router and now has trouble with configuring the firewall (to make it possible for oneself to host games or something like that), or doing all the portforwarding stuff – all of it requiring time. Furthermore, I have seen many routers enough, that were unable to do some decent connection tracking, especially for UDP based games .. if the user has not put that hardware he bought into the trash can yet, he has some basic security. With port 135 and 139 and all the like closed and secure. What is wrong with this picture?

How about not opening these ports in question _AT_ALL_ on the private home machine? I mean – what the hell has a oversized bloated super server behind the port windows opens by default got to look for on a home computer? The popup spam is only a minor example ... I simply ask _why_ open the ports to the internet at all? I can understand if this is needed for file shares, etc... but why not leave the configuration of these matters in the hands of the users and only start to listen on these ports if the user explicitly tells windows to do so?

Full-Disclosure: RE: [Full-Disclosure] Microsoft urging users to buy Hardware Firewalls

If a user *really* wants these services be available to the world wide web and has a hardware firewall, he will do port forwarding, and we'd be back again where we started.

If Microsoft's general concept of "secure by default" installations is not going to change radically, we will face a vulnerability soon enough again.

CodeRed
Nimda
SQL slammer
Remote DoS against FileSharing
RPC

I think history speaks for itself. I want to annotate, that I am not happy either regarding the policy of many Linux distributions. But that microsoft expects home users to buy additional hardware to make up for microsoft's own faults is an outrage.

--
- Thilo Schulz

My public GnuPG key is available at
http://home.bawue.de/~arny/public_key.asc
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.2 (GNU/Linux)

iD8DBQE/Ou0oZx4hBtWQhI4RAIobAJ9Hrah8kwAEOA18ah+vBJUTVmCcKwCfejC6
TvBeDU5k3bOcrR1qYn4n7N4=
=dhyh
-----END PGP SIGNATURE-----

Full-Disclosure – We believe in it.
Charter: <http://lists.netsys.com/full-disclosure-charter.html>

Full-Disclosure – We believe in it.
Charter: <http://lists.netsys.com/full-disclosure-charter.html>

RE: [Full-Disclosure] Microsoft urging users to buy Hardware Firewalls