

Re: Hijack well-known ports

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2004-04/0142.html>

From: Bluto (*arf-arf_at_doubleclick.net*)

Date: 04/03/04

Date: Fri, 02 Apr 2004 20:55:16 -0500

Duane Arnold wrote:

<BIG SNIP>

> *I do know that if I was to walk into System and the Security departments and
> say let's implement personal FW solutions on all the workstations company
> wide, they would laugh at me and proceed to kick me out of the departments,
> hollering *where is the cost justification for this nonsense*. <g>*

I'm sure you are right.

I'm also sure that it's those companies who are having 100's of machines compromised with new viruses and so on. I don't see them attacking my servers, because they have multiple gateways and firewalls, and can clamp outgoing attacks pretty quickly. This keeps the internal compromise off upper management's radar and out of the news (usually).

In turn, that makes it possible for the CTO to say things like, "Yeah, we had a few boxes get infected with MyDoom (or Bagle, or whatever), but we've got it under control . . . while the CTO's techies are frantically running around fixing things (after pulling an all-nighter), blowing the timetable on other projects and so on.

I realize that there's a point where security costs more than it's worth. I realize — and this is not just true of IT — that it's easier to justify capital expenditures (a \$15K firewall device) than it is to justify maintenance expenses (\$3K of Kerio 2.1.5 plus \$3K of installation plus \$3k in likely additional annual support). But, I also realize that the REAL cost of security failures gets buried.

I can tell you for certain, that the CTO of a major financial company didn't call me personally, just to make me feel better, after I recieved porno spam on an one-off email address that ONLY his company possessed. Nor, was his concern to find out about the breach that led to the spammer gaining access to the address — he already knew about that. And they already knew about the spam, too. But my situation — because I could prove

that the spam was a result of a security breach — scared him to death. So, his concern was to reduce the chance that I would talk to the media or HIS boss.

You can be VERY sure, that the cost of that episode never became a line item in the accounting records!

And, I think his behavior is more the rule, than the exception. So, I don't doubt that the "hollering" you describe is common, but I don't doubt that it's dumb, either.

- > *The implementation of a personal FW on machines on a secure company LAN with*
- > *rules implemented to allow traffic on the Win Networking ports for all LAN*
- > *IP(s) serves no purpose and is a waste of time and resources, IMHO.*

"serves no purpose" ?

I don't know whether you have no experience or no knowledge or no regard for the truth, but it's one of the three. If you'd said "serves no *sufficient* purpose", well, I'd probably disagree, but you could argue the point. But, "no purpose"?

All I can say is that I hope you aren't involved with network security on behalf of any company I do business with! A "secure company LAN" is only as secure as the weakest link, anywhere on the network.

All it would take, to totally compromise such a network, is ONE road warrior with a laptop that's allowed back on the network, without a total scan for viruses AND trojans AND unknown processes.