

Re: Please help me "sell" the idea of a more secure network

Source:

http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active_directory/2006-07/msg00024.html

- *From:* "Kurt" <lorentzenkurt@xxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 4 Jul 2006 08:05:52 -0700
-

You'll have a hard time selling it to management because setting up that way was their idea. It makes things simple for them because they have no in-house support (their "IT Guy" is a manager, handy employee or somebody's kid, right?). Write up a security assessment, present it in both printed and electronic form (email a Word doc and send a copy certified mail) with links to a few articles written for the public, not techie stuff (to back up your position). Make broad threat assessments ("Your password policy leaves you very vulnerable") and offer your phone number to discuss the problems in detail (you can do the selling then if they bite). Make sure you get a receipt for the email and store it along with the original in your client records, and the certification of delivery for the snail-mail in the filing cabinet. You might get a short-term job cleaning up the mess, or maybe even a long-term support contract. At the very least, when the lawsuit threats come ("These guys never said a word to us about..."), you're covered.

....kurt

"JM" <jm@xxxxxxxxx> wrote in message
[news:OJlpg.1715\\$u11.1616@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](news:OJlpg.1715$u11.1616@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

My company does mostly telecom interconnect work, and some data. Typically, we bring in a networking person from a partner company to do the actual technical stuff. However, it's often our job to educate the customer on why certain things are needed. And I need some help on a current situation.

The client has Windows 2003 Server Standard Edition, with about 15-18 XP Pro computers. They have AD setup, with their core company software running on the server. Most of the clients are joined to the domain, but several employee laptops simply operate in a workgroup sharing internet and POP3 email, with their email being hosted by a local network services/website design company.

Some users log on using a unique username, but ALL users use the same password. In fact, this "master" password can be found almost anywhere and on anything that requires a password, including their individual email

Re: Please help me "sell" the idea of a more secure network

accounts, websites, and who knows what else. Other domain users login in with generic logins like "CompanyNameUser," again using the universal password.

To make matters worse – at least in my non-expert view – is the wireless router they leave on 24/7, completely open, for anyone and everyone to use. They have literally hundreds of customers coming and going daily, and the wireless internet access is a courtesy they offer.

Finally, they have no comprehensive, system-wide security solutions, whatsoever. Their anti-virus "protection," for example, consists of various products, releases, life cycles, etc, all on the individual clients. Some have Norton, others McAfee, AVG Free (yeah, I know), with some being in-date, out-of-date, and some with nothing at all. There are various free malware killers, pop-up blockers, and the like, installed by whomever, whenever, because they have no group policies or other domain security policies in place enforcing who can and cannot install software.

I know this is a huge issue, and I'm not asking for anyone to spend a lot of time on it, but I need some concise ideas for these people. The problem is that up to this point nothing devastating has happened, so they are totally blissful in their ignorance. If I sell too hard, given their current good luck, they will think I'm doing Chicken Little or trying to make a buck.

The fact is, I'm really concerned about my clients, and I know their current situation is going to get them in trouble. I'm just not sure how to approach it.

thank you,

jm