Some friends of mine recently told me about new LCD projectors that were installed at their university over the summer. Seems the information technology (IT) group ordered a bunch of projectors, installed them in the ceilings of classrooms at great expense, and then discovered an unpleasant feature in each projector.

Anyone could set a password on the projector to lock out further configuration changes.

The configuration includes such essential elements as the input source; i.e., whether the signal is coming from a computer, a DVD player or a VCR. If someone locks the configuration, at least two of the sources won’t work. Neither will such essential controls as the color balance settings, adjustments for ensuring a rectangular image, and so on.

Wouldn’t you know it? Some unknown person locked one of the $5,000 projectors the day before classes were due to start.

When my friends called the manufacturer for help, it turned out to be a mess. They had to send proof of ownership by fax and then had to wait almost the whole day before they got an unlock code for that specific projector. Imagine if that had happened on a class day.

They gently suggested to the manufacturer's tech support that letting unauthorized personnel apply a configuration lock was perhaps not the brightest idea in the world. The tech cheerfully responded, “Oh, but you can disable that feature in the configuration.” Yes, you can, but the unauthorized personnel can equally cheerfully re-enable the feature before locking down the projector. Can you say, “denial of service?”

Now they have to obtain and file the unlock codes for all their new projectors so that they can unlock them on demand. What they're actually going to do is to return all of those projectors as soon as they have replacements from a different manufacturer whose engineers were a little more thoughtful in their security design.

So what does this have to do with network security?

Many organizations configure their user’s company-owned PCs or workstations using centralized policies. Operating system parameters, network configurations, firewall policies and antivirus rules are potentially legitimate targets for centralized controls. For example, in some circumstances, firewall configurations can usefully be determined in advance to prevent naïve users from allowing all possible network traffic. Many personal firewalls let the user allow or disallow inbound or outbound traffic for specific processes. Some users unfortunately click “yes” for everything. After a while, their firewalls become tools that reduce bandwidth but offer no security.

Similarly, some users notice that turning off the antivirus scan when transferring large numbers
of files between computers can significantly increase speed; unfortunately, it's easy to forget to turn the scan back on. These are the people who discover they have seven viruses resident in memory when they bring their computer to the shop complaining that it’s “acting funny” because all the letters are falling to the bottom of the screen while they’re typing text.

If you do decide to control such tools, be sure to apply appropriate access controls to the configurations for two reasons: first, to prevent users from changing the configurations; and second, to prevent users from locking _you_ (or even themselves) out of the configurations if you have to fix something for them.

There are dangers in locking such tools. The most serious is that inadequate analysis can produce a dysfunctional setup that reduces user productivity or even stops work altogether. For example, a simple error in firewall configuration can deny access to an internal network that the technician forgot about but that the user desperately needs right now – yes, now. Similarly, an overzealous but impractical technician can configure an antivirus product to perform an obligatory scan of all data files on the system at every boot up. This policy works may work flawlessly and take only a few seconds on the technician’s test system (with its 100 data files), only to take 20 minutes on the user's system (which has 25,000 data files the tech didn’t know about).

So before you go locking locks, be sure you have figured out which ones to lock.

* * *

A Master’s degree in the management of information assurance in 18 months of online study from Norwich University – see <http://www3.norwich.edu/msia> for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2004 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.