

i/OS Security Warnings: Like Talking to a Brick Wall

By Alex Woodie

What if you were the president of a company and somebody told you that the locks to your building were broken. You would fix them instead of taking the chance millions of dollars worth of goods would be stolen, right? Now instead of physical locks, say you were told the security mechanisms that protected your company's data weren't working. You'd fix those too, right? Actually, if you're a typical System i shop, you would do very little to address the problem year after year, according to the latest security survey from PowerTech.

Despite decades of warnings about the lack of security in default i/OS configurations, System i users continue to largely fail to do anything about it. Instead, they go about business, day by day, with their data and applications unnecessarily exposed to cyber criminals, malicious employees, and accidental deletion.

This is the only reasonable conclusion that one can come to after reading PowerTech's latest *State of IBM i Security 2010* report, which was published last month by the respected i/OS security software and services company.

The problem is, little has changed. Year in and year out, the System i customers that participate in PowerTech's survey show the same types and levels of security exposures. The folks at PowerTech are understandably diplomatic about the lack of progress on the security front among IBM midrange shops, but the truth is that preaching good i/OS security practices to them is like talking to a brick wall. They just don't seem to get it.

Consider some of these not-at-all fun facts about the average i/OS shop from the *State of Security* report:

- **23**--the percentage of System i shops running at security level 30 (which has well-known security exposures) or lower
- **67**--the average number of user profiles with *ALLOBJ authority (experts recommend no more than 10)
- **57**--the percentage of System i shops that have no exit programs in place to monitor network exit points
- **11**--the median number of user profiles in place with default passwords (which, in i/OS, is the user name)
- **61**--the percentage of user profiles that have unrestricted access to data or the authority to change it

Since PowerTech's annual surveys aren't scientific (that is, they're not drawn from a randomly selected sample), you could make the case that the numbers don't mean much. You could say that, because the 200 or so survey respondents came to PowerTech to take the survey last year, that

they're either more concerned about security than the average customer, or that they are knowingly deficient.

Both of these conditions are true, and they skew the data in opposite directions, admits Robin Tatam, director of security technologies for PowerTech. But even if you threw out the top and bottom 10 percent of data, and just looked at that 80 percent in the middle, the numbers still tell the same tale. "We've surveyed over 1,500 systems at this point," Tatam says. "I think at some point, you could start making some fairly valid assumptions that this is a pretty good representation of the iSeries base."

The survey results indicate that System i shops simply aren't getting the message on security, Tatam agrees. "On the one hand, it's interesting to see that it doesn't really change a lot year over year," he says. "The new systems we're looking at are typically not any better configured than the ones we looked at last year and the year before that."

Take network security, for example. PowerTech has eased off the message about the huge security problems that protocols like FTP and ODBC pose for System i servers, instead focusing its marketing and advertising on automating other i/OS security activities, like tracking the QAUDJRN for signs of unauthorized access or cracking down on excessive authorities in individual and group user profiles, both of which it sells solutions for.

"We had kind of turned away from that message [about network security] a little bit, just based on the fact that it's been almost 20 years. We figured it was old news," Tatam says. "We found that, in our best attended Webinars, that there are a lot of customers that are completely blindsided when you tell them that people can come in through these mechanisms."

The network security problem is actually worse than it appears. While 43 percent of i/OS shops are using exit programs--either their own homegrown software or tools such as PowerTech's Network Security software--to monitor or block network access through i/OS exit points, 25 percent of these customers had only one or two exit programs in place, usually for FTP and ODBC. That leaves dozens of other exit points unprotected, and that's in the most security-conscious System i shops.

Jill Martin, product support manager for PowerTech, was putting it kindly when she said "There isn't a broad understanding of what these exit points are covering and why they should be activated and turned on."

The big question is why. Why are i/OS administrators leaving dozens of unprotected routes into their System i servers? Are they under the impression that, if they are not actively using a network access route, that hackers could not use it to get into their System i server?

"I think that's part of it," Tatam says. "I think the other part is, if they're not using an interface, they don't even know that it's there."

To be fair, i/OS administrators may have switched off the various network "servers" that exit points are designed to protect. With the service turned off, the thinking may go, the security risk is lessened.

In fact, that's not quite true. "Maybe they have the service turned off, and they're confident with that. But when you have a number of users with the *IOSYSCFG user profile, where they can go turn on those services, simply turning them off is not necessarily good enough," Martin says.

Hopefully, those powerful user profiles are protected with a password that is easier to guess than "i." But that might be wishful thinking. "We're still seeing a few systems out there that have a minimum password length of one," Martin says. "It could be 'A' today and 'B' tomorrow."

Unfortunately, this is not a joke. How can a company defend a password policy that would allow a hacker to guess a password with a minimum of 26 tries (52 if capital letters are enabled)? (That's assuming that they even have a policy in the first place; many System i shops still don't have an overall security policy).

Tatam chalks it up to a legacy mindset. "What I find when I talk to customers about having a password length of one, they dismiss it as 'Management says we don't want to deal with it.' That is pretty staggering in this day and age, from a management standpoint, that they're not looking to enforce integrity of the access to their systems."

The platform's "set it and forget it" reputation is clearly part of the problem here. Whereas many Windows and Unix implementations require gaggles of specialized personnel to run, the average System i server is maintained by a jack-of-all-trades administrator who's responsible for a dozen other IT disciplines. Just as there are few specialized database administrators on the platform, there are few trained security administrators.

"We still find the accountant maintaining the system and putting the backup tape in at night, because there's really no maintenance to be done," Tatam says. "So they don't have specialized experts that are extremely knowledgeable on the platform. We still run across people who are not trained in that field."

Paradoxically, the System i platform's deserved reputation as a bullet-proof and secure server also contributes to poor security configurations in the real world.

"The message that we're trying to present the customer is that the system is very securable, and it doesn't necessarily come that way out of the box," Martin says. "There are a lot of tools and facilities in place that come with the system that can make your environment very secure, but it doesn't mean that they're implemented and in use on day one. I think there's a misconception, that people don't understand that they have to do some work to be able to take advantage of what's provided in the operating system. And then of course the vendor tools like ours that are available to help make their lives easier."

The more you hear about the state of i/OS security, the more you become afraid that too many companies are unknowingly taking a big risk with the integrity of their businesses, their employees, and their customers. Unfortunately, the companies that lack the requisite skills to fortify their System i servers are also failing to obtain the services from ISVs or consultants that do have the skills. This, apparently, because they don't know any better. But that doesn't cut it.

It is one thing to take advantage of "security through obscurity" if you have done your homework, have locked down your system, and are confident that others will not have the knowledge of the skill to penetrate through the layers of security that you have laid down to reach the inner core of this proprietary computer. But it's something else entirely when the obscurity is your own ignorance on the matter of i/OS security. That's just dangerous and inexcusable.

You can register to read PowerTech's *State of IBM i Security 2010* report, or view the recent Webinar where Tatam and Martin discuss the report, by visiting PowerTech's Web site at www.powertech.com.