10 security problems you might not realize you have

Takeaway: It's easy to get distracted by high profile security threats and let more subtle — but equally destructive — risks fall through the cracks.

IT administrators are often so busy just trying to keep up with the obvious security threats that many more problems fly under the radar. Here are 10 security risks you may have in your organization that you are not aware of.

1: Your employees

Your own employees are your biggest source of security risks. Sometimes, it is deliberate; sometimes, it is not. Employees have the most access and the most time. We expend a lot of effort worrying about external threats, but in all honesty, all it takes is an employee bringing in a virus from a home PC on a USB drive to nullify all your forward-facing firewalls and measures. Disgruntled employees sometimes express their anger by hurting your computer systems. And of course, it is possible for a well-meaning employee to make a major mistake. Good governance, education, setting (and enforcing) policies, and knowing your employees are your best steps to closing the holes here.

2: Common coding mistakes

Certain mistakes in programming *still* get made despite years of warnings and education. Most common are SQL injection and cross-site scripting vulnerabilities. I still see these issues from time to time even in major software packages that you would think are trustworthy (WordPress is a good example). It's hard to change software once you've installed it, so you need to keep these packages up to date even though it is quite a hassle.

3: Unauthorized machines

I've seen this one too many times. Someone decides to bring in an old PC and put it on the network to do something your existing infrastructure doesn't allow them to do. They think that they are being helpful, working around the limitations of the IT department. After all, if IT won't build a Web site for their group, it's just "doing them a favor" to set up an old PC in the corner with a Web server on it, right? Wrong. The best way I've found to keep these rogue machines in line is with rigorous IP address audits and policies and scanning the network to create a list of machines. If machines can't get IP addresses, they can't do much harm.

4: Ancient "rock solid" servers

We all have them — that server buried deep in the data room that "just won't quit." Usually, it's running some software package that is impossible to migrate to another machine. Sadly, these machines are often major security risks because they typically are no longer getting patches or we fail to patch them out of fear of breaking them. In addition, those older versions of operating systems often come with inherent security holes that no patching can fix. You need to replace these servers one way or the other. The best first step is to virtualize them. From there, it is a lot easier to try to update them.

5: Legacy applications

It's not just the old servers that are big security risks; it is also the applications running on them, as well as other legacy applications you may have running. These applications would be a lot less problematic if they were current with their patches, but usually they aren't. All too often, we miss a major version update because the upgrade is so difficult, and then we're so far behind the ball that it's impossible to catch up. Or perhaps the applications are completely discontinued. It's painful to say it, but the best thing you can do is find a migration path to a recent version or another package entirely.

6: Local admins

We all know the dangers of allowing users to run with escalated privileges. Still, we occasionally end up with users being granted local admin rights inappropriately. In my experience, this often happens while troubleshooting a problem: We make the user a local admin to see if it fixes a problem and we forget to undo it. Regardless of how it occurs, it is a ticking time bomb for security. Use your central administration tools to make sure that the local admin list gets reset on a regular basis to the proper users and groups.

7: Incorrect share/file permissions

File permissions are tricky things, and most users are not even aware of how to set them. So what happens? Users create sensitive files in their usual networked location and those files get the default permissions, which are "collaboration friendly" to say the least. The next thing you know, everyone can read the documents, which are supposed to be confidential. Your best weapon is to pre- establish a share and file structure with the correct permissions. For example, give everyone a home directory for personal documents and create shares or directories around roles, projects, and teams with the appropriate permissions. The hard part is then educating them to use the correct locations — but that is much easier than trying to teach them permissions.

8: Hidden servers within applications

I have seen more and more applications lately that use a local Web server as an administration console. Sometimes, these applications are installed by users without permission. But

occasionally, the IT department just does not realize what comes with an application. While these servers can be locked down so that they are not a risk (and with luck, they get installed like that), you need to verify that the applications are secured properly before allowing them to be installed on users' machines.

9: VPN clients

Some users figure out how to set up VPN access on their personal machines. For a power user, it isn't too hard to do. But you have no control over that machine, and once it is on the VPN, problems with the unauthorized machine can easily spill over onto the VPN. One thing you can do is audit the VPN systems to see who is connecting from what PCs and compare it to your list of authorized systems. Also, you can put additional firewalls around VPN clients to quarantine them. Finally, there are various systems to ensure that the clients connecting are on a preapproved list.

10: Disabled security software

Security software often puts up roadblocks to getting work done, so the "logical response" from many users is to find a way to work around it. For example, I've seen people set up anonymizers at home to sidestep IT policies. Power users (especially developers and system administrators) often know how to circumvent security tools. They may also be local administrators because of a technical need, which makes disabling software and changing settings even easier.

Combatting this is tough because these users often assume that they are "too smart" to be a security risk. What they fail to realize is that the modern crop of security threats do not require the user to make a mistake, like going to an obviously suspect Web site or downloading pirated software. Every Acrobat file, for example, is a potential plague rat at this point. Start looking for unusual trends, like large amounts of consistent traffic to an IP address and use centralized tools to ensure that settings are at the right levels and are reset periodically. Also, take any unnecessary local administration rights and firewall entire groups onto their own network segment to limit damage if those groups have a legitimate need for lower security.