SearchSecurityChannel.com
The Web's best resource for security channel professionals

INFORMATION SECURITY THREATS

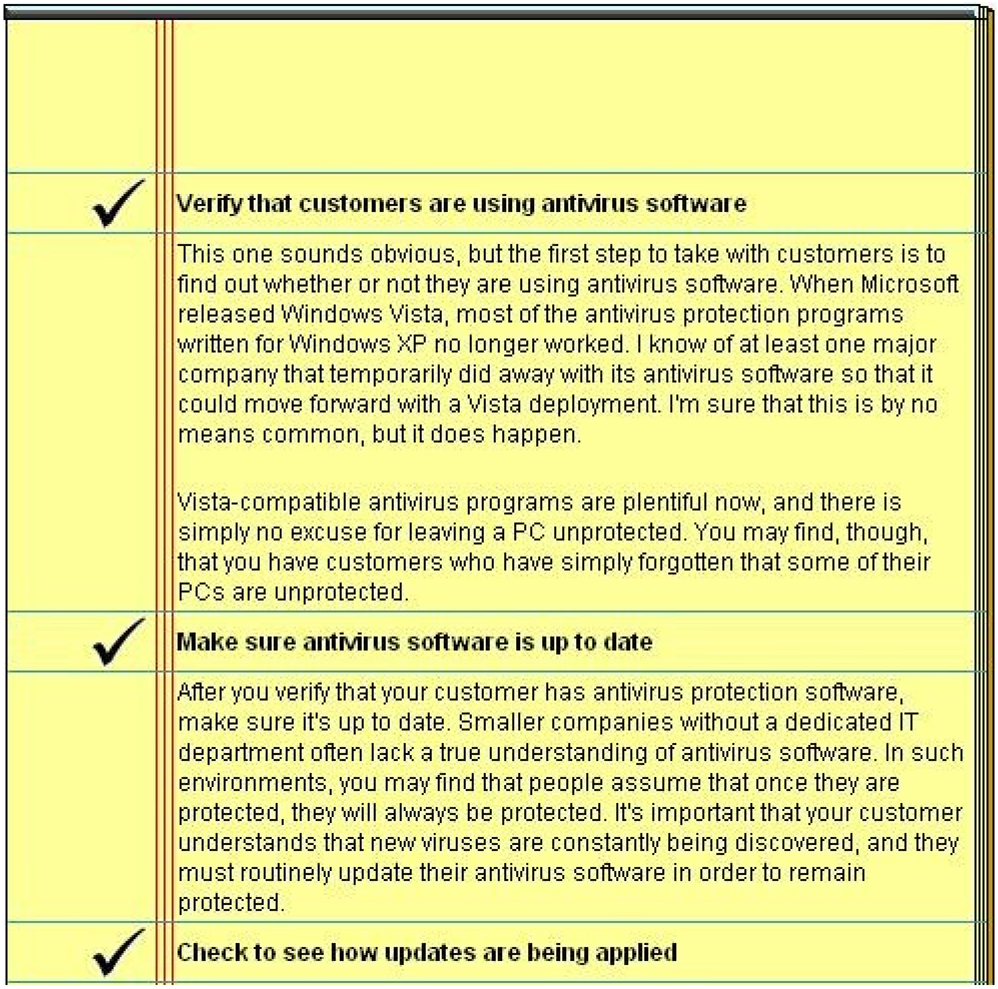
Checklist: Five steps to assessing a customer's antivirus protection

Brien M. Posey

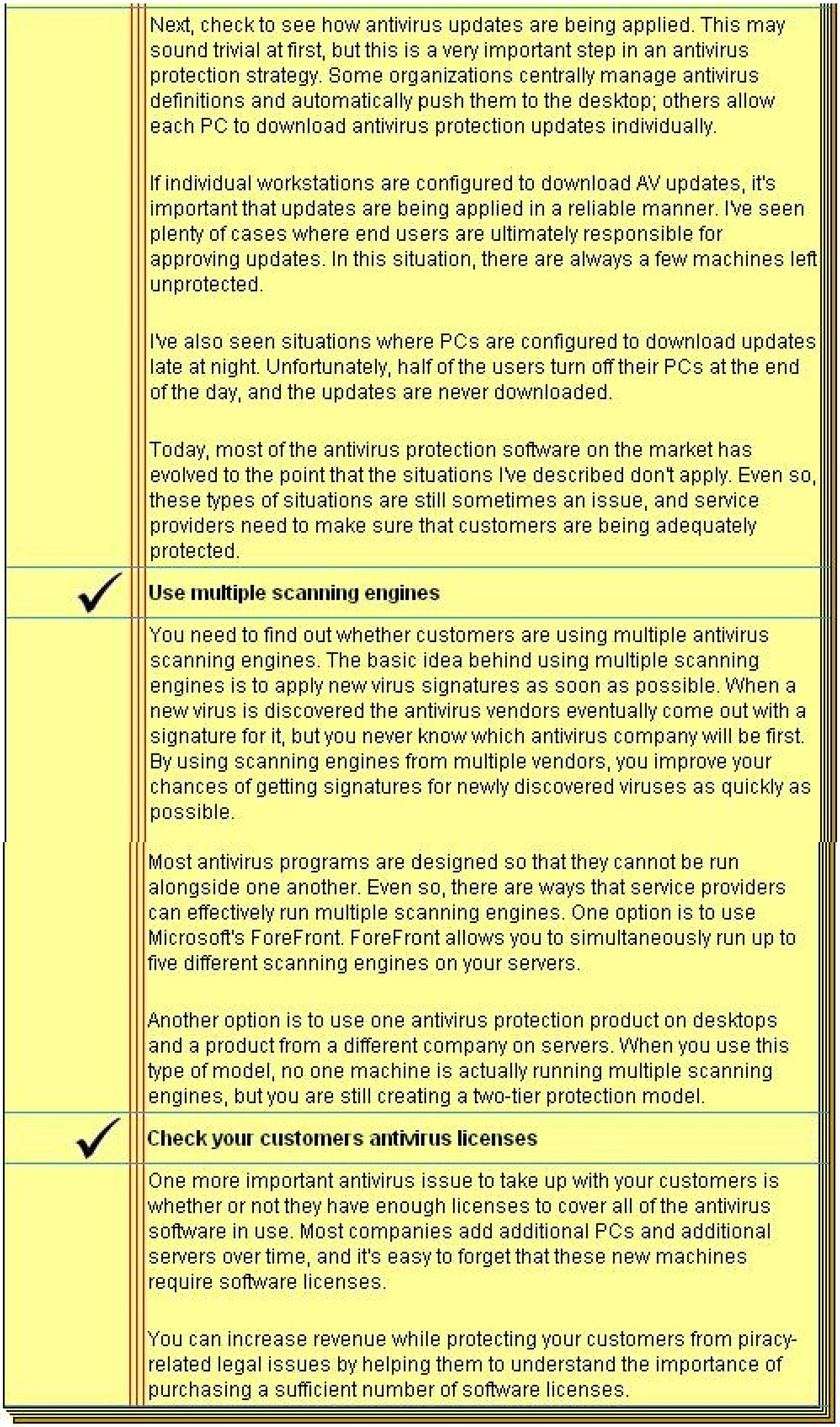
01.25.2008

Service provider takeaway: Service providers and value-added resellers can strengthen customers' antivirus protection strategies by taking these five steps.

One of the most important security issues service providers and value-added resellers (VARs) can discuss with customers is their antivirus protection strategy. After all, viruses are an indiscriminate security threat. A lot of smaller companies don't worry about security because they are not likely targets for hackers. Viruses are so common, though, that infections can occur in big companies, small companies and at home. This Channel Checklist provides five steps to walk through with customers to gain a better understanding of their antivirus protection strategy and to help correct deficiencies.



✓	**Verify that customers are using antivirus software**
	This one sounds obvious, but the first step to take with customers is to find out whether or not they are using antivirus software. When Microsoft released Windows Vista, most of the antivirus protection programs written for Windows XP no longer worked. I know of at least one major company that temporarily did away with its antivirus software so that it could move forward with a Vista deployment. I'm sure that this is by no means common, but it does happen. Vista-compatible antivirus programs are plentiful now, and there is simply no excuse for leaving a PC unprotected. You may find, though, that you have customers who have simply forgotten that some of their PCs are unprotected.
✓	**Make sure antivirus software is up to date**
	After you verify that your customer has antivirus protection software, make sure it's up to date. Smaller companies without a dedicated IT department often lack a true understanding of antivirus software. In such environments, you may find that people assume that once they are protected, they will always be protected. It's important that your customer understands that new viruses are constantly being discovered, and they must routinely update their antivirus software in order to remain protected.
✓	**Check to see how updates are being applied**



Next, check to see how antivirus updates are being applied. This may sound trivial at first, but this is a very important step in an antivirus protection strategy. Some organizations centrally manage antivirus definitions and automatically push them to the desktop; others allow each PC to download antivirus protection updates individually.

If individual workstations are configured to download AV updates, it's important that updates are being applied in a reliable manner. I've seen plenty of cases where end users are ultimately responsible for approving updates. In this situation, there are always a few machines left unprotected.

I've also seen situations where PCs are configured to download updates late at night. Unfortunately, half of the users turn off their PCs at the end of the day, and the updates are never downloaded.

Today, most of the antivirus protection software on the market has evolved to the point that the situations I've described don't apply. Even so, these types of situations are still sometimes an issue, and service providers need to make sure that customers are being adequately protected.

✓ **Use multiple scanning engines**

You need to find out whether customers are using multiple antivirus scanning engines. The basic idea behind using multiple scanning engines is to apply new virus signatures as soon as possible. When a new virus is discovered the antivirus vendors eventually come out with a signature for it, but you never know which antivirus company will be first. By using scanning engines from multiple vendors, you improve your chances of getting signatures for newly discovered viruses as quickly as possible.

Most antivirus programs are designed so that they cannot be run alongside one another. Even so, there are ways that service providers can effectively run multiple scanning engines. One option is to use Microsoft's ForeFront. ForeFront allows you to simultaneously run up to five different scanning engines on your servers.

Another option is to use one antivirus protection product on desktops and a product from a different company on servers. When you use this type of model, no one machine is actually running multiple scanning engines, but you are still creating a two-tier protection model.

✓ **Check your customers antivirus licenses**

One more important antivirus issue to take up with your customers is whether or not they have enough licenses to cover all of the antivirus software in use. Most companies add additional PCs and additional servers over time, and it's easy to forget that these new machines require software licenses.

You can increase revenue while protecting your customers from piracy-related legal issues by helping them to understand the importance of purchasing a sufficient number of software licenses.

About the author

Brien M. Posey, MCSE, is a Microsoft Most Valuable Professional for his work with Windows 2000 Server and IIS. Brien has served as the CIO for a nationwide chain of hospitals and was once in charge of IT security for Fort Knox. As a freelance technical writer he has written for Microsoft, TechTarget, CNET, ZDNet, MSD2D, Relevant Technologies and other technology companies.