TECHNOLOGY

Deep Packet Inspection

Column: The Bleeding Edge

Nov. 01, 2008

From the Nov. 2008 Issue

When it comes to morality, technologies tend to be pretty neutral. Only when people make use of the technologies do they tend to emerge as good or evil. Nuclear technology produced both power plants and powerful bombs. Gutenberg's printing press enabled the mass production of Bibles and of pornography.

And then there is Deep Packet Inspection (DPI). DPI is a technology used to inspect the packets of information that travel across the Internet. A more extensive examination than a simple "Packet Inspection," which looks only at the headers of each packet for information, DPI is increasingly used to examine the protocols and data within each packet.

Such deep packet inspections can be used for enormous good. They can spot spam and viruses, shuttling them off the network for further inspection or quarantine, thus making them an essential defense against increasingly sophisticated Internet attacks. But the same deep inspection can be used for targeted advertising, data mining, eavesdropping and censorship.

And that's a problem for tax and accounting professionals in private practice.

Accountants, like many other professionals, rely heavily on their guarantees of confidentiality. Even when using web-based accounting and payroll tools, there is an understanding and bond that requires that client data be safeguarded.

But Congress is wrestling with the extent to which deep packet inspection can and should be used in support of law enforcement (with or without a warrant) and other activities. This means that in the very near future it may be possible for anyone to identify and read packets of information over the Internet. And while this doesn't yet mean that they can piece together data to read a complete tax return or filing, the possibility can't be ruled out for the future.

The prudent accountant, particularly one who uses the public Internet for client communications and web-based accounting services, should begin now to look for ways to protect the bond of client confidentiality. And that generally means making use of three technologies for data protection:

E-mail Encryption. Back when Congress first began to authorize the perusal of Internet e-mail, Phillip Zimmerman created a handy little program called "Pretty Good Privacy," or PGP. The joke was that the e-mail encryption tool was more than pretty good — it was so good that the U.S. government tried to send Zimmerman to prison for it. Zimmerman beat the rap, and PGP is now a de facto standard. No one is suggesting that every e-mail (or even every e-mail to clients) needs to be encrypted. But now would be a good time to start learning how it works and how to use it. Zimmerman sold the product, and you can find a lot of information at the PGP corporate website at www.pgp.com.

File Encryption. While at the PGP site, you may want to also check into their programs for archive and file encryption. After all, files that are encrypted can't be read. You don't have to use PGP's technology for this. There are plenty of other vendors with competing products that are just as good, and even Microsoft provides some of these tools with

its operating systems. I'm more wary of these products because the companies involved may have other, conflicting priorities that would include breaking the encryption to help police copyrights. The point is that this is, again, a good time to start learning about the technologies of file encryption, because you will likely need them … and sooner rather than later.

Virtual Private Networking. VPNs, as they are known, are a kind of virtual, invisible tunnel through a network that opens when needed, is virtually impenetrable and closes without a trace when the communication is complete. VPNs are widely used for corporate and government communications but don't entail rocket science. Microsoft includes a basic VPN client with its operating systems, and setting up a VPN server at the office is relatively straightforward. And again, there are plenty of third-party providers should you choose not to use Microsoft.

I'm admittedly a little spooky about all of this stuff. I don't much care for how Congress keeps hinting that it will open up networks for increased use of deep packet inspection. I'm concerned that Congress has authorized the Department of Justice to snoop through phone and Internet files without bothering to get a warrant. And I am even more concerned that the Inspector General of the Federal Bureau of Investigation reported this summer that warrantless searches have been repeatedly and systematically abused by agents of that organization.

The bond of confidentiality doesn't hold when the client is engaged in a criminal activity and is the target of an investigation by law enforcement. But at what point is confidentiality terminated if there is no formal investigation and no warrant? Or if the investigation is conducted not by law enforcement, but by a third party using Deep Packet Inspection technologies?

Those questions must ultimately be settled by Congress and the courts. But in the mean time, prudent accountants will prepare to deploy the technologies

that will safeguard both their clients and their practices.

Technology • Article

CPAPA is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.