Security Goes Virtual

Establishing appropriate safeguards has always been recognized as an important part of data processing. Whether in terms of controlling different levels of user access, or in terms of protecting corporate information from outside threats, computer security features have always been part of the picture. Its critical nature may not be appreciated by personal computer users, since studies have shown that home users don't always keep their virus protection up to date and may be overly casual about IDs and passwords. However, it is something that business users understand, given the financial and public relations impact of data breaches.

With society's increasing dependence on mobility, traditional models of security are breaking down. These days, it's not enough to rely on a strong perimeter defense and protected enterprise gateways. Just as a PBX can no longer monitor and control telephone traffic, gateways can no longer monitor and control computer networks. We already have ubiquitous connectivity for telephones, and we'll soon have the same for laptops. Today, a company's computing environment can't be considered in terms of its physical facilities alone.

There's also a larger social trend toward virtualization in general, in which dedicated, device-oriented approaches are being replaced by software-based alternatives. Traditionally, computer security has been deliberate, local and self-administered, much like an old-fashioned answering machine. There was a time when everyone had individual answering machines, but few people do today. The widespread acceptance of voicemail is a good model for understanding the benefits of virtualization. The same trend can be seen in home entertainment, as streaming video-on-demand services begin to offer serious competition for DVD players.

The Hackers are Out There

The simple truth is that a virtualized approach to computer security issues can deliver a more robust mode of protection, with less involvement from the user. That's quite a good value proposition, since computer crime is going to be with us for the foreseeable future. The methods and tools used by computer hackers are in a constant state of evolution. Hackers are drawn by the value of personal information that can be looted from various applications, and the relative ease with which it can be captured. The increasing use of botnets makes hackers harder to find, and they're never more than a few steps behind the latest anti-malware developments.

In computer security area, over-reliance on familiar countermeasures is the kiss of death. Every change in infrastructure, operating systems, software or hacker technique warrants a response on the user side. Perimeter security features and local firewalls made good sense in 1993, but make less sense in 2009. Even a properly-secured machine offers no defense against phishing, pharming and other social engineering ploys. Unfortunately, every PC user needs to step up to the job of becoming their own security administrator, or choose to ignore the risks and hope for the best. Things are changing though, with the introduction of virtual security options.

Today, there's a convergence in telecommunications and computing technology. Telephones are becoming more like computers, and computers are becoming more like nodes of a network and less like stand-alone devices. As this happens, there is an opportunity to do a better job when it comes to managing security requirements. There are many components involved in managing PC security, including registry scanners, virus blockers, spam blockers and URL filters. In a typical home there might be four or five PCs, and every one will need its own security services software and local administration. The very complexity of a localized approach to security makes it inherently unsecure.

A virtual approach to security is much better than this centralized "every man for himself" model. It offers users some relief from the constant vigilance that's needed, and protect computers from threats that originate within the network. Now that floppy disks have largely disappeared, the network connection is the biggest threat. Improvements in software patching and auto-update utilities are helping, but the proliferation of always-on broadband connections puts people at greater risk. Securing the network connection from the network side can also make upgrading easier.

AT&T is Moving Forward

AT&T is building out its virtualized security options to cover current and future needs. It already offers virtual security features/services for its VPN customers through the AT&T Network Based Firewall Service. Next, it will design and deploy virtual firewalls for managed Internet service customers. Soon, the same kind of policy control and environment will be available for DSL customers.

Virtualization offers the opportunity for a better approach to security, without the need for constant user intervention. It eliminates the need for (and cost of) local hardware, as well as the time required for security administration. It frees users from worrying about arcane technical details, and eliminates the need for constant attention. Like voicemail, virtualized security delivers results in a simple, low-maintenance way. It's a better way to address security requirements, and an option that makes sense.

For more information contact your AT&T Representative or visit us at www.att.com/business.

at&t
Your world. Delivered.