

Monitoring bandwidth and HTTP

The case for controlling Internet use **Interviewed by Troy Sympson**

Everything about business has gotten faster with the advent of the Internet. Accessing the World Wide Web for advertising, research, marketing, recruiting, data hosting and hundreds of other things has quickly moved business into the 21st century and beyond. While the Internet has made life and business easier, it's also opened the door to a host of new problems.

"An inherent part of being connected is dealing with the ever-changing threats that bombard an organization," says Bob Hochmuth, vice president of SLPowers. "Lately, spyware via your standard HTTP connection has become the threat of choice for hackers and wrongdoers because it can be very difficult to stop. It acts like normal Web content but can bring a computer or an entire network down in just moments."

Smart Business spoke with Hochmuth about the perils of the Internet and how bandwidth management and HTTP filtering can be very beneficial to an organization.

Why does a business have to be concerned with controlling Internet use within its organization?

Computer use in organizations has grown from only the information worker in the past to almost everyone in the organization today. We've seen that roughly 40 percent of a business's Internet traffic is dedicated to Web browsing. The fastest-growing challenge, however, is the other 60 percent of traffic — the portion that is being used for Internet dependent applications. The challenge is that some of these applications are highly critical, like Voice over Internet Protocol (VoIP), online CRM tools, banking and remote access, while others are noncritical or detrimental, like peer-to-peer downloads, instant messaging, streaming music and video, or recreational file downloads.

What are the costs of ignoring this issue?

Unfortunately, along with increased Internet use comes increased Internet misuse, traffic congestion and new threats to



Bob Hochmuth
Vice president
SLPowers

the organization via spyware, viruses and malware attached to Internet pages. At today's salaries, every minute not spent being effective adds up to serious money. Lost productivity can never be regained. Threats allowed into the business can be catastrophic. Corporate informational assets can be transferred through the network, causing loss of market share and lost revenue. Legal issues can befall a company by not protecting the corporate information. It's interesting how many organizations simply think that they need more bandwidth when in actuality, they have plenty. It is just being misused.

What can an organization do to combat the issues?

The biggest issue we see is that many companies leave the wide-open Internet problem unaddressed or underaddressed. Organizations are starting to realize they need to control traffic to regain business performance and productivity, and to mitigate threats and legal issues. Failure to control Internet traffic will cost organizations hard money. Many companies try to control some of this through 'acceptable use' policies and Web filtering software. There are myriad secure Web gateway

devices on the market that will allow you to control browsing access to some extent. Most of them will keep nonthreatening users out of trouble from inappropriate content. But organizations need to protect themselves from the traffic that users generate and the malicious users that are trying to get past the standard safeguards. Controlling this jumble of applications takes sophisticated hardware and software, and it needs to be managed.

What are the best ways to manage bandwidth and content?

An organization needs to understand what is happening out there and 'see' its Internet traffic to create the proper defense. We have an increase of social networking and streaming media entering the organization. We have IM where corporate information can flow unseen. Much of this could be legitimate use of the Internet, but users are becoming more sophisticated and have been able to bypass systems in place and fool employers.

Preferred solutions, which truly allow you to 'see' your traffic, perform a deep packet inspection, report the results of both content and application, and correlate by user, group, time of day, upload/download size, etc. Once you have gathered this information, you can set the solution to meet your policies. Some filtering solutions offer an 'on or off' approach to traffic. The better ones can prioritize an application and dedicate a minimum and maximum amount of bandwidth to it.

Make sure you're looking at all components of your Internet bandwidth. Make sure you can manage bandwidth, HTTP content, and the applications that access your Internet connection. Also, let the employees know the safeguards you deploy to protect them and the company's assets. When evaluating technology, be aware of the actual capabilities of the solution.

BOB HOCHMUTH is vice president of SLPowers, with offices serving South Florida and Metro Atlanta. Reach him at (561) 718-7203 or bhochmuth@slpowers.com.

Insights Technology is brought to you by SLPowers