BANK TECHNOLOGY NEWS

NOVEMBER 14, 2013 TECHNOLOGY INNOVATION. BUSINESS RESULTS. banktechnews.com

Virus Attack Prompts Wyoming Bank to Change Security Software

by Penny Crosman

In the small mountain town of Lander, Wyoming, Travis Homi runs a one-man IT department at Central Bank & Trust. Recently a virus infected the bank's network and caused significant damage, bringing a huge loss in productivity and new business.

"We have a main network share where we keep all shared files for all our branches," Homi explains. "The virus affected that and files were unavailable." As soon as he saw the problem, Homi knew it was caused by some kind of virus or malware.

The $161 million-asset bank had a "big-name" antivirus software product in place that failed to detect or prevent the virus. "That prompted us to look for an antivirus solution that worked, because we had one that didn't work," he says.

External auditors that audit the bank's network every 18 months recommended a product called LanGuard for managing system patches. Homi implemented it and found it worked far better than the bank's existing patch management software, which worked in a piecemeal fashion. "When I look into the web console, I can see the entire network," he says. "I can see what systems are missing patches, not just Windows patches, but for all the major software we have. You can push them directly out from the console — I really like that feature."

This experience made Homi consider the company that makes LanGuard, GFI Software, in his search for a new antivirus solution. He ended up choosing GFI Cloud IT security software. Despite the word "cloud" in the name, the software needed to be installed on each of the bank's Windows-based machines. But it can be managed through a single web console.

It can be hard to know whether antivirus software is working until something goes terribly wrong. But Homi saw signs right away.

"After we installed it, it discovered some viruses that were on the network that my previous product didn't catch," he says. "It gets updated with [new virus] definitions constantly."

Next on Homi's security software to-do list is purchasing new web protection software that would block sites he doesn't want employees accessing.

A devastating virus attack drove Travis Homi to make some changes to ditch the "big name" antivirus software his bank was using.

"One thing I've struggled with here in our bank is tracking down who the bandwidth hogs are," he says.

The bank blocks YouTube, Facebook and other websites that are considered time wasters.

The software Homi is thinking of buying, which is also from GFI, would let him give certain staff, such as those in the marketing department, access to the social network sites they need, while blocking those that management feels don't need it.

What worries Homi most about security is … everything.

"It's a multi-headed beast, isn't it?" he says. "Internally, keeping our systems as secure as possible — that means keeping everything patched and up to date, having antivirus software that's reliable. I don't want to imply I'm not concerned about DDoS, phishing, and social engineering. I'm concerned about all of it, so I don't know if I can pinpoint one thing that's a main concern. The things I have most control over are internal security and employee training."

And control in this context is relative.

"You can tell your customers and employees to watch for certain things, but the real challenge is, are they listening and are they following your direction?" Homi says.