community.spiceworks.com

Knowing what you don't know: How a logging class turned into an IT SWAT team

Spiceworks, Inc.

4 minutes

This is the 314th article in the Spotlight on IT series. If you'd be interested in writing an article on the subject of backup, security, storage, virtualization, mobile, networking, wireless, cloud and SaaS, or MSPs for the series PM Eric to get started.

It was a sweltering hot summer day, as summer days tend to get in the DC metro area, and I was locked in a training class teaching some network and security wonks about log data and log data management. A little lethargic in the stuffy classroom after lunch, we launched into a discussion of Network Activity Monitoring.

We were using live data siphoned off a log management appliance that had recently been put into production. When I asked the students to take a look at firewall traffic report, one of my students perked up a bit and asked, “Where did you get this log data? It looks like it’s from our firewalls.” A supposition I confirmed. My student, with a very concerned and somewhat annoyed look on his face, said to me, “Well, then, there’s a major bug in your software!”

Having taught this course dozens if not hundreds of times, I was

skeptical that any true, fundamental issue had been discovered and immediately leapt to the conclusion that there was likely some misunderstanding based on his unfamiliarity with the software.

With a bit of doubt in my voice, I asked, “What did you find?”

Turns out, I had leapt to the wrong conclusion. With full clarity of understanding the report just generated my student said, “This report is showing FTP traffic, but we don’t have any FTP servers.”

“Whoa! What? Are you sure you don’t have FTP traffic, because I’m fairly certain that my product isn’t generating phantom FTP data.” After a little scurrying we determined that the logs were indeed showing quite unexpected FTP traffic.

Neither of us totally sure what was happening, I suggested we investigate this as we would if it had happened outside the classroom.

Our first step was to expand our reporting range from the day of the class to the prior month and discovered that FTP traffic commenced about two weeks prior and over 20GB of data had been exfiltrated! We also expanded the device range to include other firewalls and VPNs to see if there were other affected devices and determined that the rogue activity was confined to a specific subnet. Armed with these basic findings we then called into the NOC & SOC to get corroboration of our findings. In just a few minutes we had gone from groggy training class attendees to a SWAT team feverishly banging away on keyboards and manically dialing cell phones.

Pretty much, that was the end of training class as my attendees entered into a full-blown crisis management situation. Perhaps the most effective training class I had ever run, but one I’m not sure I’d

want to duplicate!

The key message we all took away from this event was the old “know what you know and know what you don’t know” adage.

This organization knew that they had disable FTP access, so didn’t bother to monitor for FTP traffic. In many security and compliance situations, you have to not only test weaknesses you know about, but also you have to test to make sure everything you locked down stays locked down. Imagine if the training class had been scheduled just a few weeks sooner. How would they have discovered this policy violation?