Warm and Fuzzy, but Insecure: One School's Journey To the Cutting Edge

By Gerald Wilson, Ph.D.
Nov 6 2008 7:58PM
URL:http://www.techlearning.com/article/14364

from Educators' eZine

Walking into the school the atmosphere felt comfortable, but a bit chaotic. Not too different from other schools we had been in over the years. The students seemed friendly, the administrators and teachers had a long list of IT tasks to accomplish, but this also was no different than any other organization. We had only the slightest hint that we were crossing into a battle zone.

The school is an inner-city charter school in California. Although the building is not new, it has been recently renovated, so that the facilities were good. It is not a high income area, but most of the students are here to learn, and the discipline problems are not far from the norm. The teachers were all enthusiastic users of technology.

The school has already purchased, or has had donated, more than 50 computers, has a reasonably high-speed internet connection and a variety of software. The teachers and staff have the usual mix of people ranging from technology savvy (very few) to those who are mostly lost, but most are able to work their way around the computer and the network. As usual, many of the students were far more computer literate than their teachers.

Our initial main assignment was to help the school adhere to district regulations and appropriate laws with regard to internet controls. The secondary assignment was to protect the school network, computers and network assets from the standard maladies(viruses, worms, spyware, trojan horses, and other malware), protect the students from accessing inappropriate network sites, and repair computers that were not working properly. From experience, we also know that the unspoken part of the job is to help educate the faculty and administration about the current nature of the Internet and Internet threats as well as how to protect themselves from data loss, plus there are always problems that come up that are not anticipated. We felt we were well prepared for the assignment and ready to go. Little did we know!

Soon after we started our work, we started to see hints of some deeper problems. First, every laptop and desktop that teachers or administrators brought to us was heavily infested with viruses, worms, and all sorts of other malware. Some could not start at all, some couldn't run specific applications, and all were not running properly. We and the school administrators believed that with a proper firewall, good Internet filtering tools, and installation of virus and spyware fighting tools, these problems could be addressed and things would improve fairly rapidly. It was a good plan.

The first steps of the plan were to install the firewall and the network filtering tools so that improved protection was in place. Once they were in place, we then tuned their internal rules to match the needs of the school, including differentiation between the students and staff. It didn't take very long before the firewall and filtering were up and running, and the staff noticed a small improvement in network performance almost immediately. We were going in the right direction, but there was still more investigation and tuning to be done.

We started to work on repairing the problems of individual computers, but within days the administration office started to complain that the network performance had once again degraded. In addition, some teachers were complaining that they could not get to network sites they had been using. With the help of the principal, we had a meeting with the faculty to explain what we had done, what we would like to do, and get a better understanding of what changes were having negative impacts. Some teachers did not understand why the network was so heavily loaded. Others did not want the network filtered, even though they understood that the students needed to be kept from going to inappropriate sites. Neither faculty nor staff understood how either the firewall the network filtering work. Everyone felt that the biggest problem to solve quickly was the network performance.

Improving network performance can be complicated. With 50 or more computers in the school doing various activities there can be many potential network hogs. At the same time, performance is dependent on the networking equipment between the computers and the firewall. The performance is also determined by the Internet Service Provider (ISP), the limitations of the connection between the ISP and the firewall, and the quality of the firewall and filtering tools. Fortunately, the informational tools that come with the Sidewinder firewall we had installed were a big help in letting us track both the sites being accessed, the amount of traffic coming and going to between the school and the various sites, and the routing information associated with each connection. Using this information, we were able to plan the next set of tuning adjustments.

Our analysis indicated that almost 90% of the network traffic from the school was being directed at MySpace and YouTube(utube). In addition, the total network traffic was near 100% of the maximum capacity of the network connection. After discussion with the administration, it did not appear that these sites were being used by the faculty, or as a result of class assignments. Thus, the next tuning step we took was to block access to both MySpace and YouTube. This had the almost immediate effect of reducing the total network traffic to less than 30% of the maximum capacity. Suddenly the administration and faculty could access the network, send mail, and do other routine tasks as they needed. We felt that we were winning the battle for network performance.

This improvement did not last long. Within days, the network performance deteriorated again. More detective work revealed that in fact access to YouTube and MySpace was again flooding the network, but the question was how? The firewall and filtering rules had not changed, and the faculty was not using these sites. It was the students! They had in fact found a method to circumvent the web filter and were once again waging war on the network.

The next strategy the students developed was to use their home machines to act as DNS (domain name server -- a type of network directory service that translates from English names to IP addresses) sources, so that the students could go where ever they wanted on the Web regardless of the filtering and firewalls on the school network. Once again the students were winning the battle, but we were not throwing in the towel!

The next actions were a set of moves and counter moves between us and the students. We added rules to block access to their home machines from inside the school. The students researched their alternatives and found sites in eastern Europe that could provide “gopher proxy” services, which are software tools that allow one machine to act as a conduit for other machines. Using these, the students would connect from a machine inside the school network to the IP address of a gopher proxy, and then they could connect to anywhere they wanted. As we discovered the IP addresses of the gopher sites, we blocked those sites, only to discover that the sites had hundreds of different addresses that they changed randomly. The students had downloaded special software which they brought to school on their iPods and loaded into school machines. This software allowed them to automatically try all of the available addresses of the gopher proxies until they were able to connect. As our next step we found ways to block these rogue sites as a group, which defeated the students search software. We were briefly winning, but not for long.

The students retaliated by installing programs onto several school machines and setting them up so that these programs would download very large files from allowed sites (ones which were intended to be left open for use) starting at 10:00 a.m. every morning. So, until we were able to identify and track these network activities, the school network would work properly with relatively light loads up until 10:00 a.m., then come to a massive slowdown for a couple of hours, and then suddenly return to light loading. It wasn't clear whether the high activity was coming from machines in the office, machines in classrooms, or rouge machines somehow getting onto the school network. The administrators blamed the teachers and students, the teachers blamed the administrators, and both groups were yelling at us to do something.

It took several days of monitoring and tracking, but we finally identified the machines involved and temporarily isolated them from the network to prove our theory. Once proven, the problem was to find a way to block these rouge activities without damaging the other legitimate uses of the network. Working with the administration, we temporarily blocked access to the sites being used for the downloads. Things once again returned to normal, for a while. The next battle came when the students were able to get the passwords needed to unblock the web filter on specific machines. These passwords were set up at the request of the administration so that teachers could go to sites normally blocked. The students managed the get the passwords by convincing the teachers they needed to get to a blocked site for legitimate reasons. The teachers would then, in full view of the students, log into the web filter and enter the bypass password. The students simply watched the teachers a few times until they were able to understand the process and obtain the password by watching the teachers as they typed. Once again the heavy download use was back in business.

We were able to counter their move by reconfiguring the firewall to use only a specific, well protected, DNS site for all queries, and then adding rules to exclude “network anonymizer” to the SmartFilter web filters. A network anonymizer is a site that pretends to be a valid site but which can be used to allow another machine access to otherwise blocked sites. By adding the exclusion rules to SmartFilter, we were able to block sites, which had been automatically identified as anonymizer sites by the TrustedSource.com site to be blocked. With this set of moves and counter moves, we had once again come out a step ahead of the students. In fact, our latest moves had made it so difficult for them to get to the rouge sites and do any damaging downloads, that they resorted to a different tactic completely, namely direct sabotage of machines by installing viruses and other malware onto machines from inside the school.

The students approach was very simple but temporarily effective. They recognized that they were permitted to connect their iPods to the school network for use during break times. They told the teachers they were downloading music, but they were in fact loading viruses and malware into their iPods at home, and then using the iPods to load these bad items into the school machines while supposedly downloading music. The plan was incapacitating school machines one by one until we found a new solution. We changed the school routers so that only machines known to be school machines were allowed to connect on the network, thus preventing the iPods from connecting. Finally, we had achieved a stable network usable by all!

Over the months since this series of battles many other network security events occurred. Keeping a network and the associated collection of computers running properly is a never ending task. Operating system companies (like Microsoft and Apple) keep releasing new patches and upgrades. Security threats keep changing. But most of all, some students take it as a challenge to see how far they can push the system. Keeping school networks running properly requires constant attention, but the rewards are worth the trouble.

Gerald A. Wilson, Ph.D. is the CEO of OmniSoft, Inc., a company specializing in network security and risk management with special attention to K-12 education. Dr. Wilson has more than 25 years of experience in a broad variety of networking systems design and analysis. He currently does technical consulting, project management consulting, and lecturing.