;login:

THE MAGAZINE OF USENIX & SAGE

December 2001 • Volume 26 • Number 8

inside:

SYSADMIN

Do You Know What's in Your Firewall?

By Tom Limoncelli

USENIX & SAGE

The Advanced Computing Systems Association &
The System Administrators Guild

do you know what's in your firewall?

by Tom Limoncelli

Tom Limoncelli is director of operations at Lumeta Corp. and co-author with Christine Hogan of *The Practice of System and Network Administration*.

tal@lumeta.com

[Tom has shared with us some of the thoughts from his new system administration book. – RK]

I was surprised when Bob (not his real name) told me that he didn't have access to the rule sets installed on the firewalls at his company. He didn't mean that he didn't have easy access, or convenient access, or that it wasn't his job, or that he wasn't technically skilled enough to read a rule set. I mean he didn't have access. Nobody at his company did.

The company that he worked for, a major company whose name you would recognize, outsourced its firewall management to their Managed Service Provider (an MSP is an ISP with a larger feature set). This "managed service" was part of a package of convenient "value added" services. The ISP/MSP, I should mention, is also a name you would recognize.

How could customers not have access to their own firewall rules? The rule set is the critical list of filter rules that protects, or possibly fails to protect, a corporation's infrastructure! A minor typo is the difference between protection and Code Red.

The answer is simple. The MSP considered those rules to be their own intellectual property. Much to the customer's chagrin, the contract that they had signed agreed with this assertion.

I think outsourcing has many benefits. It can save money, it can let you focus on your business instead of the business of recruiting and retaining technical talent, and so on. However, you should always remember that when you outsource a task, you become responsible for checking the quality of the vendor's work.

My mother used to run a sandwich shop. She didn't bake her own bread. A local baker supplied bread to her and the other local restaurants. She was not responsible for making sure that the dough was properly mixed, prepared, baked, stored, and so on. Her job was quality assurance. When the bread arrived she had to make sure that it was the right type, quantity, and quality. Quality was the most important factor. Her customers took it for granted that she had the right type and quantity but she would lose business if the quality fell below expectations. If someone didn't like the bread, "I didn't make it" was no excuse. It was still bad bread. Of course, if she became dissatisfied with the bread, she could switch to another bakery.

The same is true for outsourcing services. You don't have to recruit employees, train them, and so on. You no longer have to mix the dough. Your job is now to make sure that the MSP is providing the quality of service that you need.

And that brings us back to Bob, my customer who didn't have access to the firewall rules that were protecting his company. I work for a company that makes a firewall rule set analyzer (see Wool, "Architecting the Lumeta Firewall Analyzer"). Bob hired us. After signing a Non-Disclosure Agreement, Bob went off to get his firewall rule set from his MSP so that it could be analyzed. He was denied.

If the customer wanted to know the rule set, the MSP argued, they should have kept track of every single change request submitted, guessed at what changes the MSP would be making as a result, and assumed their guesses were right. Of course, you paid for the MSP by laying off the person who could have done such duties. No offense, Bob.

An MSP has one very selfish reason not to reveal the rule sets in place: without the rule set, it's difficult for you to change MSPs.

An MSP has one very selfish reason not to reveal the rule sets in place: without the rule set, it's difficult for you to change MSPs. How could you guess your way through reinventing the rule set? Not without many trials and errors, outages, and pain.

There's another reason an MSP wouldn't reveal the rule sets. Chances are, they're very ugly. While the rule set began clean and pretty, the change requests that you've made were likely in the form of "Permit port FOO to host BAR" and "Block port FOO to host BAR." The easiest way to make such changes is always to add them to the front of the rule set. This requires very little thinking and is largely not prone to errors. However, after 500 requests, your rule set is 500 lines longer than the initial configuration. On the other hand, a carefully manicured rule set wouldn't be so large since each rule would have been installed with the kindest of care, with painstaking choice of where to insert the rule set for optimum performance, combining like rules to eliminate clutter, entered carefully at the keyboard by white-gloved hands while angels sing and cherubs toss rose petals into the air to create a beautiful and fragrant scene.

For an MSP to be profitable, there will be no white gloves, angels, or cherubs. Add the rule. Move to next customer.

In defense of MSPs, a rule set is intellectual property. There may be special filtering techniques in the rule set that are proprietary: how anti-spoofing is done, rules that permit special monitoring and Quality of Service protocols through, and so on. As part of any rule set modification, better firewall engineers do a highly sophisticated analysis that is on a par with the complexity of writing software. The MSP may have invested in special software that manipulates rule sets automatically.

All security-related systems need auditing. In *The Practice of System and Network Administration*, we discuss the benefits of self-auditing, and the very different role of external auditing, that is, audits by external groups. Both are needed. However, we never considered the ramifications of using MSPs. In this case, you are auditing yourself but really auditing someone else's efforts too. Auditing outsourced security services is just as critical, if not more critical, than auditing your own systems. Intellectual property issues must not get in the way!

What's the solution? Some companies have a policy that no firewall (or packet filtering device) will have write access by non-employees. This includes contractors, consultants, vendors, and ISP/MSPs. Such companies go to extremes. If their ISP places a router on their site, and the ISP requires access to said router, the company adds a router (or firewall) between the ISP's router and their network so that they have exclusive control of the filtering. This extra router can be expensive.

Alternatively, you can insert language in your contract that classifies the rule sets and configurations to be your intellectual property, to be revealed to you in a reasonable time frame, with financial penalties for non-compliance. If your MSP will not agree to that, at least put in the contract that you have the right to audit the configuration on a regular basis.

Having the ability to audit your firewall and actually doing the audits are two separate things. Establish a policy that sets down a schedule for regular audits, whether they are in-house or external. I know there is at least one fine company that provides this service. Check your business pages under "L".

Maybe we're dealing with the wrong problem. Maybe the problem is that we believe the promise of MSPs that offer soup-to-nuts solutions. They sound great but maybe we should only let them do parts of the project: the installation, the software upgrades, and most importantly, the monitoring. Leave the policy for us to directly manage; while they may generate SLA (Service Level Agreement) statistics, it is our responsibility to validate and monitor those statistics. I once claimed jokingly that outsourcing works best when you outsource the boring parts (monitoring) but keep the fun parts (design and implementation) to yourself. Maybe that wasn't a joke.

If our auditing service does nothing but help companies realize they have signed contacts that hide their own firewall rule sets, we will have made the world a better place.

Ultimately, security is nothing more than risk management. Security for security's sake doesn't make sense. Business objectives (set by your CEO) must be translated to security policy (set by your CIO or someone who reports to your CIO), which should then be translated into firewall rule sets, access systems configurations, host configurations, and so on. Trusting someone else to manage your firewall is a risk, and it may be an acceptable risk based on the business objectives of your company. Blindly trusting someone to do this without having the ability to audit their work is both dangerous and irresponsible.

The next time someone tries to sell you MSP services with no right to audit the configuration, sit them down and tell them about my mother's sandwich shop.

P.S. Bob did eventually get the rule set out of his MSP. It required a three-way Non-Disclosure Agreement to be signed between us, the client, and the MSP. The audit then proceeded without a hitch.

Bibliography

Avishai Wool, "Architecting the Lumeta Firewall Analyzer," *Proceedings of the 10th USENIX Security Symposium*, August 2001, Washington, D.C.

Thomas A. Limoncelli and Christine Hogan, *The Practice of System and Network Administration*, Addison-Wesley, 2002, ISBN 0201702711.