Nevis NETWORKS

Exclusive to Communications News

http://www.comnews.com/features/2008_September/0908_association_web.aspx

The Government Employees Health Association Uses Network Access Control as Key Element of Compliance with HIPAA Regulations

An unauthorized user had just gained access to the LAN at the Government Employees Health Association (GEHA) in Independence, Missouri. Justin Gerharter, the senior systems engineer at GEHA, discovered the breach by accident. “One day the guy sitting next to me happened to be going through DHCP scopes and saw an unfamiliar network name associated with an IP address,” Gerharter recalls. “Sure enough, it was a consultant who had plugged in a laptop.”

The incident was innocent enough, but it raised two important questions: How often does this type of unauthorized access occur, and how might the network’s resources or patient privacy be compromised when it does? “That single incident drove home the need for network access control,” says Gerharter.

As the second-largest national health insurance plan serving federal employees and retirees and their families, GEHA (www.geha.com) operates under strict guidelines established by the Health Insurance Portability and Accountability Act (HIPAA), which in part requires control over individual user access to network resources. HIPAA also requires an ability to distinguish between corporate-owned and guest assets seeking access to the network. Given the sensitivity of patient privacy for GEHA’s 221,000 health plan members and their dependents—a total of some 400,000 patients—the Association had already implemented strict security provisions for its IT resources. But the incident that day made Gerharter realize more measures were needed.

Show Me

"Not knowing the identity of every user and what resources they are authorized to access on a network as sensitive as ours was the trigger point for investigating NAC solutions," Gerharter says. "But despite all of the hype surrounding NAC, it was surprising to discover just how few solutions there are that appear to be mature enough to integrate easily into a large enterprise environment like ours without requiring fundamental changes to the network infrastructure or impacting network performance."

Perhaps it is fitting that such skepticism should exist in Missouri, the "Show Me" state. GEHA's criteria for an identify-driven LAN security solution quickly narrowed down the field of vendor options. "We realized early on that we needed more functionality than traditional 'NAC solution' vendors were even talking about," Gerharter explains.

The goal, at a minimum, was to ensure that all devices accessing the network were authorized to do so. "If they were on, we wanted to make sure we had control over where they could go," says Gerharter. These fundamental capabilities seemed simple enough for a NAC solution, but Gerharter was about to encounter some serious reluctance from at least one vendor to prove it.

Being new to NAC, Gerharter sought advice from Steve Allen, security manager at DPSciences Corporation (www.dpsciences.com) in Cincinnati, Ohio. Allen was a trusted advisor to GEHA, and DPSciences was a Silver Certified Cisco partner, as well as a certified reseller of LANenforcer products from Nevis Networks.

DPSciences believed solutions from both Cisco and Nevis should be able to handle GEHA's application. Nevis fully cooperated, and the test of its LANenforcer 2024 Security Appliance at DPSciences' demonstration lab was an unqualified success. But for whatever reason, DPSciences could not get Cisco to schedule a similar test. "We tried several times to get a demo of the solution, but we were unable to find anyone to show us a working implementation or even a demo in a lab," Gerharter recalls.

GEHA Goes with Nevis

Gerharter liked the fact that the LANenforcer transparently enforces identity-based policies in real-time within the network fabric, tightly controlling who can access the network and which resources are permitted for use. "Nevis brought us an integrated, identity-driven LAN security solution, complete with an identity firewall capability for controlling user access to sensitive resources, as well as inline intrusion prevention," Gerharter notes. "We soon discovered that complete integration of these services was necessary to adequately enforce our security policies."

With the confidence gained from the successful test at DPSciences, Gerharter decided to proceed with a full-scale implementation of the LANenforcer 2024 Security Appliance.

The deployment involved nearly 1,600 access switch ports, together providing secure access control for some 800 users.

“We found the implementation to be very simple and straightforward,” Gerharter says. As an in-line appliance, the LANenforcer is installed between edge and core switches. The use of port pairs made it easy for Gerharter to unplug each line on the core switch, plug it into the LANenforcer instead, then add a short patch cable from the LANenforcer to the core switch. “You just plug the edge switch into the top port and the core switch into the bottom port of the same port pair,” Gerharter explains. “It’s that simple.”

The next step was to create policies using the LANsight management system. Although the Nevis solution supports fairly elaborate policies, Gerharter decided to keep it simple initially. GEHA already had several layers of security for its applications, but to prevent any additional unauthorized access to the LAN, he provided guests with Internet access only. For employees on company-owned systems, the LANenforcer was configured merely to monitor and log activity.

“Can You Hear Me Now?”

Gerharter initially experienced what appeared to be a pretty serious problem with GEHA’s Voice over IP (VoIP) system: the phones didn’t work. The access control policy was set, naturally enough, to recognize all VoIP phones by their MAC addresses, and restrict access exclusively to the VoIP VLAN. But when the Avaya phones boot up, they must have temporary access beyond the VoIP VLAN to register with the PBX and receive configuration information. Because these phones were blocked from reaching the PBX, they were unable to boot up.

The problem was solved by changing policy to grant these phones access to a separate VLAN. According to Gerharter, “We were making the network more secure than we needed to, and for these phones that created a problem.”

No other problems were experienced during the implementation or since, although there have been a few surprises. “We discovered things we never thought about as far as what people are doing and where they’re going,” says Gerharter. For example, the anti-virus software was routinely authenticating in a manner that had not been understood very well. “It’s allowed us to understand some of our applications and processes a little better,” he adds.

The restrictive guest access policy recently proved to be behaving as expected when an employee brought in her personal laptop because she had been experiencing problems connecting to the Citrix system while away from the office. “How would we know how often that’s happening without a very watchful eye and constantly looking at this stuff?” Gerharter wonders.

Getting the Knack of Identity-Driven LAN Security

In the future, after getting more comfortable with the system, Gerharter plans to use LANenforcer's endpoint scanning capabilities. A trial of such a configuration is already underway on the access switch serving the network operations center. Gerharter also has plans to take advantage of the LANenforcer's granularity to create policies that establish which users can access which servers and applications. This should be particularly beneficial for proving conformance with HIPAA regulations.

GEHA recently installed the latest release of the LANenforcer operating software, and Gerharter and others in the IT organization are now coming up to speed on some the enhanced capabilities. For example, the new software has a policy evaluation tool for running "what if" scenarios for policy troubleshooting and planning purposes. The new posture-check dashboard provides real-time monitoring, while the new customizable reporting tool can be used to answer critical questions, such as "Who (by user name) accessed various servers and applications over the last month?" Gerharter is even contemplating using the new dissolvable endpoint messaging agent to strengthen pre-connect access control for guests.

Summarizing his impressions of the solution, Gerharter concludes: "Its cost-per-user is exceptional and our deployment confirms complete interoperability with our network infrastructure. The great thing about the solution is that it's vendor agnostic. It doesn't care what switch vendor or firewall vendor we use. It only cares about the traffic sent to or from these devices. The more I learn about the LANenforcer 2024, the happier I am with the decision we made."

# # #