

SECURE ENTERPRISE

BUILDING TRUSTED BUSINESS

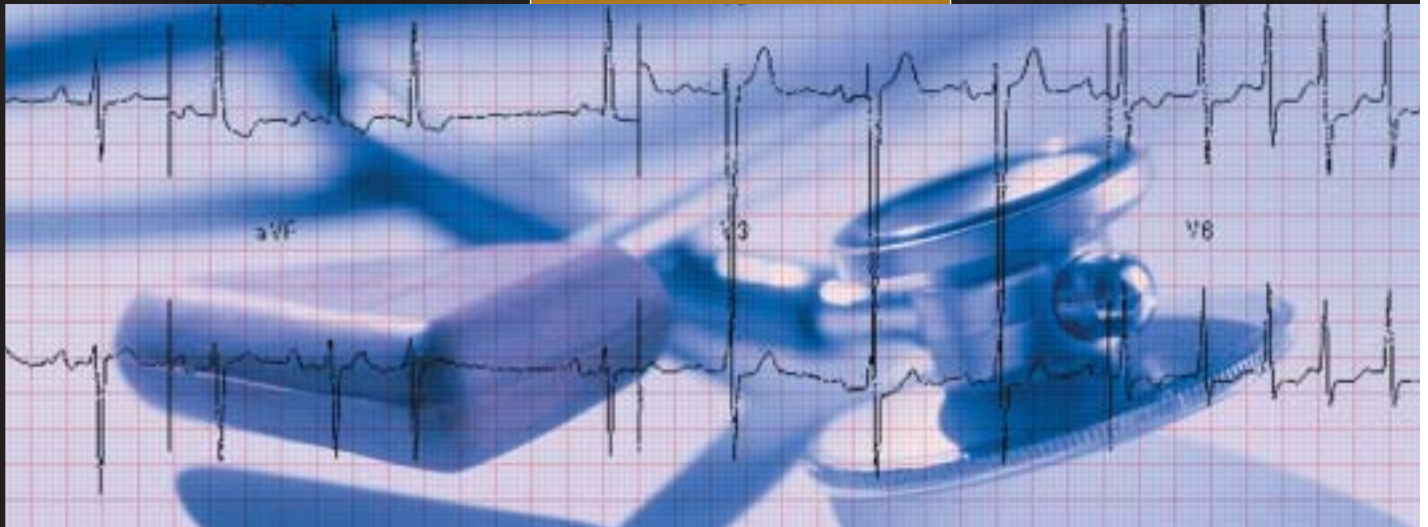
May 2004

THE PAYOFF

THE REGENCE GROUP

PORTLAND, ORE.

EVENT-LOG MONITORING



PHOTOGRAPH BY (NICK KOUJIS)/GETTY IMAGES

Watchful Eyes

Outsourcing event-log monitoring saves health insurer money and provides early warnings on network intruders

June 28, 2003, is a day David MacLeod remembers well. That's when an attacker just outside Peking tried to penetrate the network of The Regence Group, a health insurer that hired MacLeod as chief information security officer to fend off such attacks. The would-be intruder looked for an opening in the Web site Utah physicians use to submit Medicare claims.

"I'm absolutely convinced that whoever he was, he had no idea what Medicare is or who Regence Blue Cross and Blue Shield of Utah is," MacLeod says. "All he saw was an IP address on the Internet that he thought he'd take a shot at."

The attack failed. MacLeod credits Counterpane Internet Security, the Mountain View, Calif., company that monitors thousands of events logged each month by Regence's Web servers, firewalls, routers and intrusion-detection systems at the edge of the network.

Counterpane was able to tell MacLeod and his staff of the

attack, where it was coming from, and that it wouldn't be successful, MacLeod says. "For about 20 minutes, my IT folks and the Counterpane folks watched what was going on before we decided to repel the attack by shutting down the routes they were coming in on," he says.

The Regence Group, based in Portland, Ore., administers Blue Cross and Blue Shield health insurance policies in Utah, Oregon, Washington and Idaho. The organization has 3 million subscribers and manages \$6.4 billion in annual premiums. In 2000, the independent organizations from each state formed an affiliation, with one administration and one IT department.

The new coalition became a security nightmare because each state's unit had widely differing policies. Oregon, for instance, had centralized security administration. In Wyoming, security responsibilities were spread among different IT groups. One unit, for example, handled user accounts for systems running on Novell NetWare,

BY ANTONE GONSALVES

another focused on Windows NT and a third on Lotus Notes.

At about that time, large employers buying health insurance started asking Regence for guarantees that the group was complying with the federal Health Insurance Portability and Accountability Act, which regulates privacy for health-care records. Regence also planned to launch Web portals that would let physicians and brokers submit forms and get information online, and provide a variety of services to customers. Those portals, of course, must be secure. Against that backdrop, Regence hired Deloitte & Touche to help centralize its security infrastructure, administration and policies. The firm introduced Regence to Counterpane.

Outsourcing Option

Security-event monitoring was an obvious choice for outsourcing. Regence would have needed a staff of six people working 24/7 to sift through the 450,000 events generated each month on the network perimeter.

Besides what comes from its DMZs, Regence also generates event logs from apps that handle subscribers' personal records. This includes PeopleSoft financials, health-care systems for claims processing and record management.

To match Counterpane's service internally, Regence would have had to spend \$600,000 a year, most of it for salary and benefits, MacLeod says. This compares with about \$450,000 a year for the service. And Counterpane has years of experience monitoring security for organizations, which means it's more capable of determining whether an event is important or just the result of a software glitch.

Gartner analyst Kelly Kavanagh says a log-monitoring service provider can sometimes watch the client's network better than the client can because of its experience and knowledge gained from working with varied clients. Counterpane analyzes about 200,000 logged events sent from Regence each month. The number of events has been reduced over the years through improved configu-

ration of perimeter devices and by taking down services that weren't in use. For example, Counterpane found telnet connections that were no longer live.

Of those 200,000 events, Counterpane identifies about four per month that need Regence's attention. The vendor notifies the client immediately of a security breach and any unsuccessful intrusion attempts, which may include a repeated failed log-in, someone seeking unauthorized access to network services and attempted nighttime log-ins by those who work day hours.

Counterpane places on the customer's network a custom-configured security device called a Sentry, which encrypts the log data, compresses it and ships it to Counterpane's operations center for analysis. The logs are shipped as they're generated, and, in the case of Regence, move across dedicated circuits leased from a carrier. Counterpane's Socrates decrypts the log-carrying messages, and the data is correlated with threat information aggregated from other customers, as well as historical data about the normal operation of a customer's network.

Regence didn't lay off any employees in conjunction with this outsourcing, mainly because Regence hadn't been monitoring logs closely before.

Early Virus Warning

Besides watching for hackers, Counterpane has kept Regence up to date on virus attacks, notifying the company if dangerous viruses begin spreading and explaining what steps must be taken to prevent infection.

As a result, when the Bagle worm struck this year, the only computers infected at Regence were four laptops that employees had used to download personal e-mail remotely. Counterpane explained the virus threat to Regence, which took steps to plug the vulnerability in all desktops.

Regence regularly patches all the desktops on the network, but laptops aren't always available to patch. When laptop users connected to the Regence network, the virus tried to contact a remote Web site to download malware. The port it tried to use, however, had already been blocked. Counterpane reported the activity and Regence's IT staff located the machines and disinfected them.

"To me, four PCs that didn't actually get the [virus] code downloaded is not an infection or breach, because it didn't complete," MacLeod says. "We really haven't been breached in the last three years." MacLeod couldn't estimate what it would have cost had Bagle infected a large number of computers on his network. But a survey of businesses by ICSA Labs, the company that certifies antivirus products and is a closely held unit of TruSecure Corp., found that companies spent an average of \$100,000 in 2003 recovering from each virus "disaster," a 23 percent increase over the previous year. A virus disaster was defined as infections in at least 25 machines or an event that caused a significant dollar loss.

Antone Gonsalves is a freelance technology writer in San Francisco. Write to him at antoneg@pacbell.net.

