From: www.cio.com

New Security Services and Tools to Intercept Online Villains

– Karen D. Schwartz, CIO

April 15, 2001

Eddie Schwartz likes to be proactive. As the former chief security information officer for Nationwide Insurance Cos. in Columbus, Ohio, Schwartz spent his days investigating security issues and researching new products that could help the company's executives rest more easily.

Security managers and executives at other companies around the globe are thinking more like Schwartz, who is now the senior vice president of operations for Waltham, Mass.-based system security vendor Guardent, every day. And with security on everyone's mind, vendors are lining up with new tools for keeping invaders at bay. From intrusion detection tools to XML-based security options, the choices increase--and become more sophisticated--each year. Boston-based consultancy Yankee Group predicts the market for network and computer security to reach more than $10 billion by 2003, up from $2.3 billion in 1998.

For a global company like Nationwide, the most important aspect of security is finding a way to lock down its network perimeter. The company's complicated and far-reaching array of wide area networks, extranets and servers--not to mention its 50,000 employees--helped create an environment vulnerable to visits from unauthorized users, viruses and malicious attacks.

"We used to assume we were like a castle where you could draw a big moat around [the network] and only lower the drawbridge when you wanted the good guys to come in," Schwartz says. But today's reality--which includes Internet businesses and extranet B2B relationships--forced Nationwide to provide access to systems that were previously hidden behind walls.

To deal with potential new chinks in the network armor, last year Schwartz chose LogiKeep Intelligence Alert, a tool that warns companies about security threats before they become dire. The service, from Dublin, Ohio-based LogiKeep (which was recently purchased by another vendor, Parsippany, N.J.-based Vigilinx), scours a variety of websites to identify potential threats, such as viruses and software security holes, as quickly as possible. It then disseminates that information to its customers so that they can take immediate action. To customize the service, LogiKeep requires that clients fill out templates that describe the operating systems, hardware, applications, firewalls and other technology employed in the company's networks.

Before implementing the LogiKeep product, Nationwide "might not have known something was wrong until somebody started complaining," Schwartz notes. "Now the company can eliminate a lot of problems before they happen because the information is provided in a timely manner and has been adequately analyzed and thought through."

Nationwide's adoption of LogiKeep is just the kind of proactive thinking more companies should pursue,

says Matthew Kovar, director of security solutions and services for e-networks and broadband access at The Yankee Group. Tools like those from LogiKeep and competitors Para-Protect Services in Centreville, Va., and iDefense in Fairfax, Va., are at the forefront of the proactive security trend, he says.

Out Of Your Control

LogiKeep's managed services products touch only parts of a company's overall security system, but other vendors are taking the concept to the extreme. Today's dearth of trained security personnel has led some vendors, such as Guardent and Santa Clara, Calif.-based MyCIO.com (now called McAfee ASaP after recently being reabsorbed by its parent company, Network Associates), to offer truly outsourced managed security services--from monitoring to virus protection to firewalls.

DPR Construction, a Redwood City, Calif.-based construction company with 1,500 employees in 18 locations throughout the country, has successfully deployed MyCIO VirusScan to more than 1,500 workstations.

Before turning to VirusScan, DPR was always behind the curve regarding virus protection, Network Manager Lee Rocklage says. When the "I Love You" virus hit last year, for example, only 300 of the company's 1,200 workstations were up to date with the latest virus definitions. Now all workstations are protected; anytime employees access the network or the company's intranet, they receive the most recent protection for their machines.

In addition to giving Rocklage peace of mind, outsourcing the security headache to someone else allows him to focus on other things. "It's an unbelievable relief to get some of this off of our plates because we don't want to spend our days fighting viruses when we've got so much else to do," he says. Rocklage notes that with this workload easing in mind, DPR has now adopted other MyCIO services as well.

Intruder Alert!

All-in-one security services aren't the only newcomers to the security scene. Intrusion-detection software--which seeks to identify when unauthorized users access a network by pinpointing and reporting suspicious activity, such as repeated attempts to enter incorrect passwords and denial-of-service attacks--has also become a hot topic.

Everett Carter, director of security at BankServ, a provider of Internet payment services based in San Francisco, uses a combination of the ICEpac Security Suite from San Mateo, Calif.-based Network ICE and Network Flight Recorder from NFR Security in Rockville, Md., to protect the company's $2 billion in daily transactions.

The products are intended to protect against a comprehensive list of security breaches, and they send an alarm when any are detected. They also allow security analysts to audit network traffic so that they can reconstruct it at the time the breach occurs, helping identify exactly what events happened during the attack and providing clues about ways to prevent similar events.

Like Carter, protecting large sums of money is something Chris Smith knows a lot about. As vice president of computer information systems at EasCorp (Eastern Corporate Federal Credit Union) of Woburn, Mass., Smith is charged with ensuring that the organization, with 100 employees and more than 250 credit union customers, is fully secure.

For EasCorp, the most important part of the security puzzle is authentication. To solve the problem, at least in part, EasCorp uses RSA Security's Keon PKI Certificate Authority software, which allows the company to act as its own certificate authority and issue certificates for customers.

That's fine as far as it goes, but Smith says it's simply not adequate when dealing with such large sums of money. If someone passing by an employee's PC sees the user ID and password, for example, he has unlocked the key to the digital certificate. "That's not strong enough to perform a $1 million wire transfer," Smith notes.

To address the problem, EasCorp has just purchased SafeWord, a handheld token-based security device from Secure Computing. EasCorp plans to use the device as a multifactor authentication system. When paired with the digital certificate, the physical token device will generate a random number, which the user will key in during the process of releasing the wire transfer for processing. By combining digital certificates with multifactor authentication systems such as a token-based system, a smart card or a

biometric-based system, "you end up with much stronger certainty that the person is who they say they are," Smith says.

Future Uncertainty

The future of security is both bright and dark--bright for the myriad vendors providing new ways to keep miscreants with modems at bay and dark for the CIOs who feel compelled to keep buying the resulting products. But there is some hope. All-in-one security services can provide companies with 24/7 outsource system protection that's constantly taking advantage of the latest products. And companies that would rather retain more control of their security systems while still simplifying the process, new all-in-one security systems (such as those from Zone Labs and Okena) combine firewall, antivirus, intrusion detection and other security necessities into a single product that's easier to manage than integrated multiple tools.

Even the ubiquitous XML may get in on the security act. Nationwide is investigating the opportunity to use XML to deposit better information from its Web-based knowledge into a central security site and then act on it in a more timely manner. Schwartz says that although the concept is brand new, he talked to some vendors, including Guardent, about how they might develop such products.

"We looked closely at how we can use XML to do things like data classification. You've got websites for the general public and sites you want to keep more confidential containing your customers' private information, and XML could be a great way to deal with that," he says.