ON SITE · DAVID STROM

Global TV makes its decision at last: All three products are worth the cost

I'VE BEEN DESCRIBING my tests of several security products at two networks of a New York media conglomerate that I call Global TV. (See Oct. 31, page 97; Nov. 7, page 72; and Nov. 14, page 126.)

One network at the sales office has plenty of security holes (indeed, you might say that very little of the network is secure), the other at an operating division is more secure.

For the most part both Ted Smith (a pseudonym for the IS support person working with me at Global TV) and I were impressed with what all three products found. We tested Kane Security Analyst (KSA), a reporting tool from Intrusion Detection Inc., in New York; and two monitoring tools called SmartPass (from e.g. Software Inc., in Portland, Ore.) and Audit Track (from On Technology Corp., in Cambridge, Mass.).

Part of the reason for examining Global's network with these three products is that tracking down security is a multi-dimensional problem. There isn't a single parameter you can change to turn an insecure network into a secure one (although the reverse is probably true, if you pick an easy target, such as the supervisor password or the server console access design). That's one of the things that I liked about KSA: Its long-winded report was essential to understanding all the various nooks and crannies of NetWare security.

None of the products caught one big problem: the RConsole access had no password whatsoever, in keeping with the theme of this insecure network. This means that anyone who knows how to spell the word could gain instant access to the server's console and do all sorts of dastardly things, including disconnect it from the network or run any server-based utility he or she so desired. All of the products should check for this situation and report on it.

Ted and I had some other concerns with the products. First was the way KSA's logic is set up, especially in the reports concerning password control. Consider the situation of a user who has no password. KSA's report would give that user a passing mark for periodically changing the password. It makes more sense to report a failure when users don't have passwords.

KSA, SmartPass win the comparison

Strom's pick: KSA

- **Biggest positive:** Reports from KSA are top-quality. There are so many places to lock down, that most network installers won't remember all of them. Provides fairly comprehensive view of network security in a format even a VP can understand.
- **Biggest negative:** Not easy to manipulate different data sets.

Global's pick: SmartPass

- **Biggest positive:** What it does, it does well.
- **Biggest negative:** SmartPass' reports include users' passwords, a security gap itself.

Second, the reports from all three products consistently use the log-in names, which both Ted and I found somewhat dense. At Global's sales network, user IDs and network identities are the same: the three initials of each user's name. Of course, this is another security no-no. Both of Ted and I would rather have seen the "real" user's names in addition to the log-in names on the reports.

Third is an issue I have with how reports are specified in Audit Track. The documentation on setting up the right kind of report to check for specific violations is sparse. And the user interface (which is run at the server's console) is somewhat klunky, combining the worst aspects of character-based menus and multiscreen pick-lists. This could be improved to make the product more usable.

Fourth, I would recommend that SmartPass use a separate "auditor" ID, independent of any of the NetWare log-in accounts. Indeed, this separate auditor account is required by Audit Track when it is installed. And a nice thing about Audit Track is that you can lock its console screen after a certain amount of inactivity, so users with access to the server console can't snoop around or review the reports.

My fifth and final concern is with the overall design of KSA's data analysis. The software is designed to be run on a single network, and stores all of its data in preset files. But Ted wanted to install the product on all servers and carry a laptop around to do periodic assessments, a reasonable expectation.

It can be done, but you have to manually copy data files and run an undocumented command. It should be easier.

Would Global buy all three products, knowing what it knows now? Yes, says Ted. "We see two primary markets within the company: First, for those installations that have poor security and need to tighten up. And second, for those installations that have high security needs."

Ted likes all three products. For the two monitoring tools.

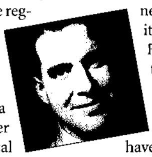
"It would be worth the money for us to get information down the road, after the network has been running for some time. It could certainly pay for itself in places that have poor security," he says.

I agree. These products are well worth their cost. As Ted says, "Every network installer makes some mistakes. KSA will help us sniff them out before a hacker can find them. And Audit Track is a great tool if you are trying to do some detective work."

David Strom is president of his own consulting firm in Port Washington, N.Y. Each week he writes about his experiences installing and testing network products at reader sites. If you have a product or a problem you would like David to tackle, send him E-mail at david@strom.com on the Internet.

LAN TALK · PAUL MERENBLOOM

Now that everyone has a laptop, it's time to plan your dial-in strategy



WITH ALL OF THE hubbub of Comdex now over, it's time to address one of the hot issues that IS managers have to face. It seems most users now have (or want) a laptop computer, complete with 14.4Kbps fax/modem and the regular cadre of software. But they also want E-mail and access to "their" LAN-based files from any town, city, or airport.

Although this may sound like a simple request, it opens yet another Pandora's box filled with technical surprises (the products don't work straight from the box), demands on creativity (yours, getting all of the components working together without proper documentation), and financial bliss (this is will cost *way* more than you'd expected).

The first order of business is devising a plan to expand the network and make provisions for remote access. What's key here is how the definition of "remote access" has changed. A few years ago it meant use of X.25 service, technology from companies such as Shiva Corp. or Digital Communications Associates Inc., or the use of products that provided remote control, such as Microcom Inc.'s Carbon Copy or Symantec Corp.'s pcAnywhere. Not anymore.

To borrow a line from Sun Microsystems Inc.'s Scott McNealy, "The network is the computer." It really is true.

With the advent of LANs, many of the resources we employ (programs, data files, and so on) reside on the network (file servers, remote hosts, and so on), not on the user's local machine. In many cases information resources (news services, stock market tickers, and the like) may enter an organization over several different LAN segments, all interconnected via a WAN. To the user, though, it's "just on my computer."

From a remote-access point of view, the remote-control approach used by Carbon Copy and pcAnywhere may or may not fit the bill today. Users want to work off-line and still have access to "their stuff."

So, implementing remote access is no longer a simple task.

Often the first question that crosses planners minds is "How should I set up remote access?" I'd suggest a twist on this. "How" is important, but even more crucial is "what." What does the remote user need access to?

The usual response is E-mail, fax gateways, file services (access to user-specific data located on a unique file server), and network services (things that live on the bigger LAN or WAN).

Determining the specific needs first is important because not all of these applications and services support the same access mechanisms. Your E-mail server may be equipped to deal with asynchronous dial-in/dial-out for remote users but may not support across-the-wire (in-band, networked) access. Conversely, fax servers may only support in-band transmission.

Depending on the systems (file servers, minicomputers, and/or mainframes), you may have several access alternatives, including TCP/IP, dial-up asynchronous, or other access support.

Starting with your list of functional needs, make notes on the various types of off-premises access each will support (including frequency). You might want to create columns titled "LAN-to-LAN" (private virtual circuits), ISDN, X.25, Frame Relay, and asynchronous (direct dial) access and place an "X" in the appropriate boxes.

As you evaluate the user needs/desires, you'll probably reach the same conclusion I did. There are really two solutions — one for E-mail and another for everything else. Because E-mail is a store-and-forward process, speed isn't as critical a factor. So those 14.4Kbps modems will work fine for your E-Mail solution.

The best solution for higher bandwidth access to your LAN and WAN resources is, in my opinion, ISDN.

Offering 56Kbps (or 64Kbps) at very affordable rates, it's a no-brainer. Unfortunately, ISDN isn't ubiquitous — yet. There are still many areas without ISDN service and more than a few problems exist getting long-distance ISDN service (inter-LATA, Local Access and Transport Area), especially when crossing Regional Bell Operating Company territories. Besides, equipment prices aren't exactly cheap.

This, then, forces us into the asynchronous world. Here the choices are plentiful. As we look at the technology, the best on the street are the V.Fast modems offering 28.8Kbps connection rates (or half the bandwidth of a typical ISDN circuit). More popular (and less expensive) are the V.32bis units supporting 14.4Kbps and V.32 modems rated at 9,600 bps.

Despite the expense of the best solution, my recommendation is "go for it!" Buy the V.Fast units, at least for your access hub. Field units can always be upgraded on an incremental basis, but you'll appreciate not having to touch the central communications equipment for a long time.

Finally, users aren't going to want to use four or five different network access tools. So you'll have a lot of work to do keeping the real stuff invisible, leaving users with the "just click here" approach to access.

Paul Merenbloom is vice president, technology research at Piper Jaffray, in Minneapolis. Send comments to him via MCI Mail at PAULM; CompuServe 75663,2032, or the Internet at paulm@mcimail.com.