

New user a security nightmare

Contributed by Linux
Tuesday, 08 August 2006

Safe computing outside the corporate perimeter
Employees logging into corporate networks from home PCs over public broadband
connections are now commonplace. As a result, security software and hardware that once
did a fine job of guarding sensitive systems looks increasingly vulnerable. That's because all
these remote networkers, be they employees or partners, are no longer snugly
inside the "official" data-security perimeter.

Safe computing outside the corporate perimeter
Employees logging into corporate networks from home PCs over public broadband
connections are now commonplace. As a result, security software and hardware that once
did a fine job of guarding sensitive systems looks increasingly vulnerable. That's because all
these remote networkers, be they employees or partners, are no longer snugly
inside the "official" data-security perimeter.

Also, persistent worm-virus outbreaks, such as Nimda, explain why more and more
corporations are going through the considerable hassle of putting security software--firewall,
intrusion detection systems, antivirus software--on every desktop machine. Companies with
end-to-end protection remain in the minority, but they won't be for long as it
becomes easier to link up fleets of desktops with central control consoles that not only talk to
the big, heavy-duty security appliances but also to the thousands of small programs guarding
the road warriors' machines.

Identity theft goes berserk online
Call in the copycats. When well-organized ID thieves convinced a clerk at a Long
Island (N.Y.) software company to give them access to tens of thousands of credit
reports using his company's password, they illustrated how the Net makes the part of ID theft
that was hard until now--accumulating the information--much easier. With widely available
credit reports such an integral part of American business, it's hard to imagine how
the credit agencies can quickly and simply limit access to the reports without impeding the flow
of commerce.

With easy access to credit reports available to thousands of people throughout the
U.S., expect blockbuster ID thefts in 2003 and beyond. Whereas credit-card
numbers were traded freely on the Internet in the past, now the bad guys will trade entire personal
dossiers. And fixing the problem will be much harder because it's pretty easy to screen
out someone who has picked up one of your credit-card numbers but much harder
when it comes to a rogue who has that, your bank-account number, your social security number,
and the last five addresses you have called home.

Of course, this little list is just the beginning. I haven't even touched on still-early
trends such as merging physical and online security: Companies are starting to look
at guarding these assets in coordination because often computer-security breaches start with
physical breaches.

Likewise, more and more businesses are installing software that tracks theft of
sensitive, high-end intellectual property. Once ham-fisted, the second generation of these systems
works much better, according to Gartner security analyst John Pescatore.

All told, computer security remains one of the more dynamic areas of the moribund
IT sector. And it'll get only more interesting in the coming year.

Lock down
The entire event was documented and submitted to upper management. Now the IT department had to decide what action to take. It decided that the associate's PC would have to be locked down better, and that IT would need to monitor the machine and the new associate closely. The administrator password was reset using Winternals System Commander 2002. Next, Debra removed the ability to boot from floppy and CD-ROM and set a password on the system BIOS. She knew the BIOS could potentially be reset with a jumper or possibly by removing the system battery. To prevent this, or at least make it difficult to open the system, she added a lock to the case.

On the software side, she enabled auditing on the PC and began checking the logs on a daily basis. Several days later, she remembered a TechRepublic article that mentioned a tool known as SELM, or Security Event Log Monitor. She installed the SELM product -- which can e-mail alerts as well as create reports for later review -- so that she wouldn't have to manually check the logs every day. In addition, she monitored the PCAnywhere service on this PC.

In a meeting, the new associate apologised for his actions. He explained he was working very late and did not want to bother anyone at that hour. He had some software that he wanted to install for the project he was working on and needed administrator access to install it. The IT manager went on to explain the policies the company has in place restricting anyone from installing software without IT involvement. He further explained that IT was on-call after hours for any problems or needs that might arise. The new associate decided that he did not want to work on the project anymore.

More problems
During a routine check the next day, the new associate's PC did not appear to be connected to the network. A call to his office confirmed that he had not arrived for work yet. Debra was given access to his office and discovered he had disconnected his PC from its network jack and had connected his Linux box to that jack instead. She disconnected the Linux box and reconnected his PC.

The next day, the same scenario played out again. His PC was gone from the network. Debra couldn't gain access to his office, so she entered the wiring closet where his network jacks were connected and viewed the status of the switch ports. One port had an active connection. Since she knew his PC was not connected, the only possibility was his Linux box. The patch cable was disconnected, and the entire incident was again reported to upper management. He was asked to remove his Linux box from the premises. He indicated he would comply, and his other PC was reconnected to the network.

Debra realised that she needed some way to be sure that his Linux box was truly off the network. Again, she remembered a TechRepublic article about various net admin tools. One of those tools was the GFI free network scanner called LANguard. She installed LANguard and scanned her entire network. It did a pretty good job of identifying the types of systems it found. It recognised a Red Hat Linux system as "probably UNIX," but it recognised one of Debra's Mandrake boxes as "Linux Mandrake." After running a scan, LANguard can sort the results by OS, which makes it easy to view what has been discovered. In addition to listing the OS, it indicates all the open ports on a system and points out known vulnerabilities. Debra now runs scans daily and reviews to see whether any new systems show up. The registered version offers a comparison feature that allows comparison of two scans to note any differences.

Once a hacker
Things were pretty quiet for a while. Then the SELM software sent a few alerts with the new associate's name. If you have used security auditing in NT, you already know the security event log can have some pretty cryptic messages. Nevertheless, after doing a bit of research, Debra figured out that the new associate had downloaded some software and was stopped dead because of the lack of admin privileges. Looking closer at the machine, she found that several services had been stopped; one was the antivirus software, and another was the PCAnywhere service. The associate was again confronted, and he told IT what it had suspected: He had attempted to install software on his PC but was unsuccessful because of the lack of administrator rights.

Next, the IT department turned to the System Policy Editor. It wanted to disable access to several Control Panel applets, especially the Services applet. IT was already using system policies to perform change control, such as limiting access to the Display applet in the Control Panel and use of the Run command and the registry editing tools.

Although the System Policy Editor in NT has no built-in controls for limiting the Control Panel except for the Display applet, you can customise it by creating your own ADM files with the proper registry tweaks. So Debra created a custom ADM file that removed the Devices, System, Services, Server, and Network applets from Control Panel.

Object lesson
The entire event was exactly what Debra's IT department needed to test its current security policies and find out the strengths and weaknesses of its internal security. Sometimes, a problem such as this is ideal for evaluating your security practices, as long as you have the right stuff to fight the problem -- and most important, to keep a similar problem from popping up in the future. In this battle, Debra and her IT department mainly acted reactively. But it led them to look at their policies and practices and try to be more proactive and prevent similar incidents from occurring. They are still revising their security policies and making changes to keep their network secure and their data protected.