SC MAGAZINE

FOR IT SECURITY PROFESSIONALS

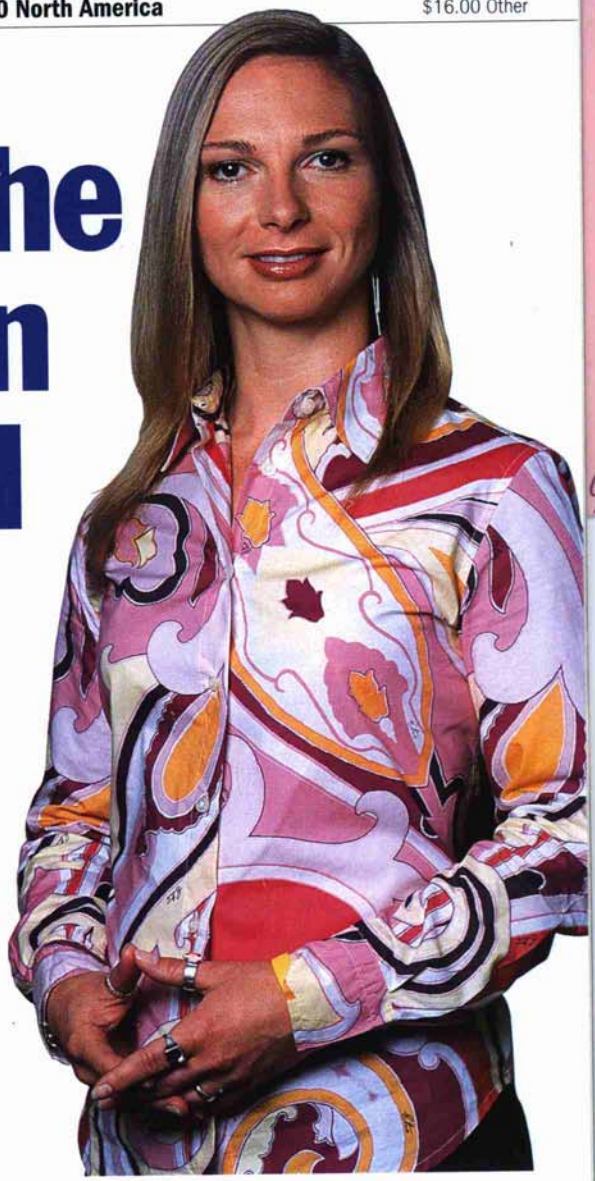
September 2004 | $8.00 North America | $16.00 Other

www.scmagazine.com

INTERVIEW

Meet the woman behind SP2

Why **Rebecca Norlander** made attitudes change in Redmond p18



Reviewed in this issue

Gateway

SentryPilot's clever management interface makes it a winner p49

Update management

UpdateEXPERT offers larger organizations a comprehensive solution to patch deployment p54

Network access control

The DSA-3100 is a cost-effective choice at departmental level p55

Page 26

Is IM busting your security?

IM can be a valuable tool, but you need to weigh the risks with the advantages

Page 34

Been hit? How to track down the evidence

Don't destroy forensic data in the rush to restore your systems

GROUP TESTS

IM security

Tools that will monitor and analyze your instant messaging communications p56

Forensic tools

These products will make the complex task of catching cybercriminals a lot easier p64

VOLUME 15 No.9

PRINTED IN THE USA

But in the past six months, the unnamed DOD agency had a significant problem with a hack that had compromised many systems by proliferating throughout the infrastructure more quickly than IT professionals could keep pace with. So it decided to wipe out hundreds of computers, re-baseline them, and then put them back in use.

"It took about a week, and everybody lost their emails, all their work, all their documents and what-not. While these systems were getting re-baselined, [they] were inaccessible," recalls Colbert. "The end result was about two hours after going back online, they were hacked again with the same hack."

The story is emblematic of the unfortunate way most organizations go about recovering from an incident, he adds. Choosing what he calls the patch-and-proceed method of recovering from an incident, which entails re-baselining the system, patching the problem, and then proceeding without ever learning the hack's root, might not cure the trouble.

"An organization is better off trying to find the root of the problem, determining how to actually correct that problem, and then doing some type of a compromise assessment across their network to look for any other systems that are affected," he says.

Failing that, a company might spend weeks or months attempting to recover from the episode, much like the DOD agency as a result of its recent attack.

"The Department of Defense is just as vulnerable as any Fortune 500 company. As for this incident, we support those investigative organizations out there, but we don't actually run those investigations," explains Captain Robert Renko, operations chief for the Defense Computer Forensics Lab, a division of the Defense Cyber Crime Center (DC3), which is part of the Air Force Office of Special Investigations. The Center provides computer forensics support to the DOD's various military criminal investigative organizations, such as the Navy's NCIS or the Air Force's Office of Special Investigations.

Guidance's Colbert says that the DOD agency is "still trying to determine exactly what the intent was, but it was definitely a compromise of the systems." So what is the most effective way to prepare for an attack before it hits?

Getting back up and running fast and collecting data and evidence to both learn from the incident and possibly pursue litigation are far from diametrically opposed goals, especially if you have a response plan in place.

As long as organizations have clear procedures on what is done when a breach occurs, and which employees are directly involved, the two aims can be met, contends Christopher Painter, deputy chief with the Department of Justice's Computer Crime and Intellectual Property Section. And part of achieving these ends means ensuring from the start that companies and their systems operators understand that while they are remediating their systems, they must retain pertinent data in such a way that it can be trusted and used in both internal and, possibly, law enforcement-driven investigations.

"The obvious next step is to think about some best practices. We have some of those [that were developed through the G8 Justice and Home Affairs Ministers' Subgroup on High Tech Crime] and we're working on more of them all the time," says Painter (see Incident recovery best practices from the G8 on p44).

But it is not enough simply to draft a response plan and maintain a corporate IT security policy that informs staff of their everyday infosec responsibilities, contends Curtis Tomlinson, manager of investigations for AMD, the California-based chip maker. Corporate security professionals must stay educated about infosec goings-on and maintain connections with peers. Doing this will keep them apprised of trends in the industry and, sometimes, offer a heads-up to various new attack methods.

"It's not enough now to develop a policy that looks sound, [then] put it in place and leave it there. It's something that has to evolve over time, depending on what's occurring in the immediate environment," he explains, noting that such continuous development applies to both overall IT security policies and investigative procedures.

Procedures and policies are living, he says, and should avoid being peppered with vague directives. Planning and people are critical; without them, the first reaction will always be to fix the problem immediately and/or take the system off-line, which might lead to evidence being compromised. Network administrators, infosec professionals, those who know about forensics practices, public relations specialists and corporate lawyers all play roles when a

When is a security breach also a crime?

The key to helping organizations understand when a breach is actually against the law requires a great deal of outreach and consumer/business education, says Joel Schwarz, a trial attorney with the U.S. Department of Justice's Computer Crime and Intellectual Property Section in Washington D.C.

As a result, adds Schwarz, the European Union has paid to publish a handbook that spells out precisely which cybercrimes are criminalized by different countries.

APEC (the Asia Pacific Economic Cooperation), which is comprised of 21 "member economies," is an inter-governmental group that works

Schwarz: power to the people

to "facilitate economic growth, cooperation, trade and investment in the Asia-Pacific region," according to the official web site (*www.apec.org*).

The organization's e-security task group "has been working with individual economies to develop and refine their cybercrime laws," says Schwarz, as well as fine-tune procedural laws, which empower law enforcement officials to gather electronic evidence.

The U.S., an APEC member, has also been doing its part for other participating economies in the group, he continues.

"So far this year, we have provided one-on-one training to the Philippines and Indonesia, [and] numerous others [are] scheduled for later this year," he explains. These include Thailand, Peru, Vietnam and Chinese Taipei.

● A summary of the laws of many APEC economies has now been put up on its website; visit *www.apectelwg.org/apec/alos/data/consolidatedresponse.doc*.