When Black Hats Are Really White

Linda Wilbanks, *US Department of Energy*

Each August, more than 4,000 IT administrators, industry experts, government officials, and hackers gather at a convention in Las Vegas. The Black Hat Briefings (www.blackhat.com), as that conference is known, started out many years ago as a hacker's convention, but it has evolved into the premier venue for technical information on cybersecurity and the latest security research.

I'm discussing it here in the CIO Corner not to promote attendance but to examine the critical conundrum in information security that this conference represents—one that my long experience with IT conferences suggests is truly unique. The conference is attended by people who work diligently to protect computer systems from unauthorized access, and they sit next to the very people they're working so hard to keep out of their systems: both groups recognize that the other is there, learning the same information about system vulnerabilities and how to protect against them.

Stealth Training

From the CIO perspective, cybersecurity is a very big issue that consumes significant resources, both personnel and monetary. From a success standpoint, the optimal case is to never suffer a successful breach or lose data, but how do you prove a negative? How do you truly know that your system hasn't been breached? After all, the bad guys are getting "badder," and we really don't know what they know or what they're capable of. Enter the Black Hat Briefings, which aim to train professionals in stealth cybersecurity, so that they can wear the white hats in their organizations.

Much of the conference is about training. Indeed, it offered an extensive number of multiple-day classes this year. The breadth of these courses is astounding—from cryptography, forensics, and reverse engineering to auditing, malware analysis, and system administration—but one class really caught my attention: Certified Ethical Hacker.

This is an actual certification with 63 modules that cover the latest hacking methodologies and technologies. I've been told that many companies really do have ethical hacker positions, although they generally use titles that are more along the lines of *computer security specialist*. The ethical hacker's objective is to help organizations take preemptive measures against malicious attacks by attacking the system themselves, but staying within the legal limits.

The Trusted Hacker

Although we might cringe at the idea of unleashing hackers in our companies' systems, we have, in fact, been doing so for years. We do it through software testing, looking for weaknesses before releasing applications as well as testing external vulnerabilities through red team activities. Yet, at this conference, it's called what it is: hacking.

Hacking involves creativity and out-of-the-box thinking, looking for different ways to get in—if not

(continued on p. 63)

 Published by the IEEE Computer Society 1520-9209/08/$25.00 © 2008 IEEE

(continued from p. 64)

the door, then the windows, any of them (no pun intended); if not the windows, then the duct work, or the basement or attic. You get the idea. The ethical hacker is a trusted employee hired to attempt to penetrate networks and computer systems using the same methods as hackers. Hacking is a felony in most countries, but it's legal when done by request and under a contract between the ethical hacker and the organization that owns the systems being hacked.

A certified ethical hacker is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems using the same knowledge and tools as a malicious hacker. Through this class, students are immersed in an interactive environment in which they learn to scan, test, hack, and secure their own systems. They will come to understand how perimeter defenses work, how to scan and attack their networks, and how intruders escalate privileges.

This is just one of the many classes advertised on the Black Hat site. Attendees believe the classes present a lot of important information about issues such as the vulnerabilities in Web 2.0 technologies, the Cisco IOS (Input/Output Services) rootkit, Google gadgets, and Microsoft products. Ellen Messmer of *NetworkWorld* refers to this conference as a "funhouse" where experts "seek to shock and amaze by poking holes in today's network technologies" (E. Messmer, "Black Hat/DefCon: Welcome to the Funhouse, *NetworkWorld*, 19 Aug. 2008). The conference also offers many other interesting presentations, including "How to Impress Girls with Browser Memory Bypasses," "The Internet Is Broken" (examining client-side threats), and "Get Rich or Die Trying" (about the profit potential in some online scams that aren't, strictly speaking, illegal—yet).

Cybersecurity issues impact everyone who puts anything on a computer other than games. Assuming that no one can maintain a computer without some personal information (even if only game-registration material), everyone is thus at risk and needs to address cybersecurity.

As Black Hat founder Jeff Moss says, security issues continue to get more challenging each year, and hacking is no longer child's play. "Over the past year, the attacks have gotten better. On the organized crime side, they have gotten better organized. The bad guys have continued to grow." (W. Jackson, "Overcoming the IT Security Learning Curve," *Government Computing News*, 5 Aug. 2008.) Nonetheless, I'm still intrigued that I just sent my head of cybersecurity to a conference with the very people he's working to keep out of our systems.

Linda Wilbanks *is CIO of the US Department of Energy. Contact her at linda.wilbanks@nnsa.doe.gov.*

IT Professional (ISSN 1520-9202) is published bimonthly by the IEEE Computer Society. IEEE Headquarters, Three Park Avenue, 17th Floor, New York, NY 10016-5997; IEEE Computer Society Publications Office, 10662 Los Vaqueros Circle, PO Box 3014, Los Alamitos, CA 90720-1314; voice +714 821 8380; fax +714 821 4010; IEEE Computer Society Headquarters, 1828 L St. NW, Suite 1202, Washington, DC 20036. Annual subscription: $40 in addition to any IEEE Computer Society dues. Nonmember rates are available on request. Back issues: $25 for members, $102 for nonmembers.

Postmaster: Send undelivered copies and address changes to *IT Professional*, Circulation Department, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08855. Periodicals Postage Paid at New York, NY, and at additional mailing offices. Canadian GST #125634188. Canada Post Corp. (Canadian distribution) Publications Mail Agreement #40013885. Return undeliverable Canadian addresses to 4960-2 Walker Road; Windsor, ON N9A 6J3. Printed in USA.

Editorial: Unless otherwise stated, bylined articles, as well as product and service descriptions, reflect the author's or firm's opinion. Inclusion in *IT Professional* does not necessarily constitute endorsement by the IEEE or the Computer Society. All submissions are subject to editing for style, clarity, and space.