Too Much of a Good Thing:  
Web Site Content & Security

by M. E. Kabay, PhD, CISSP  
Associate Professor, Computer Information Systems  
Norwich University, Northfield VT

The National Infrastructure Protection Center (NIPC, http://www.nipc.gov) publishes several valuable reports of interest to network managers (see http://www.nipc.gov/publications/publications.htm for a list). _Cybernotes_, published every two weeks, covers vulnerabilities, exploits, hacking trends, virus information and infrastructure-protection best practices. The monthly _Highlights_ provides high-level overviews of security issues particularly appropriate for managers to read. The _Information Bulletins_ appear irregularly with major news of infrastructure vulnerabilities. The most recent Bulletin had the following interesting news:

“A computer that belonged to an individual with indirect links to USAMA BIN LADIN contained structural architecture computer programs that suggested the individual was interested in structural engineering as it related to dams and other water-retaining structures. The computer programs included CATIGE, BEAM, AUTOCAD 2000 and MICROSTRAN, as well as programs used to identify and classify soils using the UNIFIED SOIL CLASSIFICATION SYSTEM.

“In addition, US law enforcement and intelligence agencies have received indications that Al-Qa'ida members have sought information on Supervisory Control And Data Acquisition (SCADA) systems available on multiple SCADA-related Web sites. They specifically sought information on water supply and wastewater management practices in the US and abroad. There has also been interest in insecticides and pest control products at several Web sites.

“Recipients can find additional information regarding posting sensitive infrastructure-related information on Internet Web sites in NIPC Advisory 02-001 issued on 17 January 2002 at <http://www.nipc.gov/warnings/advisories/2002/02-001.htm>. The intent of this advisory was to encourage Internet content providers to review the sensitivity of the data they provide online.”

The article raises an important point too often forgotten by busy Web masters: the information posted on a Web site is truly public, and so one ought to think carefully about whether specific details belong where anyone, including potential attackers, can find them. For example, details of personnel such as titles, explicit project titles and descriptions, specific buildings, offices and telephone numbers likely do not belong on a public Web site. Job openings, for example, sometimes have far too much detail about particular research projects, manufacturing processes or dependencies on particular software. Security-related information such as details of how systems are protected against intrusion or abuse likely have no place on such a site. All of these facts can be abused by hackers who use social engineering techniques to give themselves a false air of internal knowledge and credibility (“Hi Susan, this is Kamal from the Process Engineering Group – you know, we’re in Building 42? Yeah, so I was wondering if you could tell me when the Supervisor of Quality Control – what was his name? Oh thanks – Bill Davidson. Yeah, anyway. . . . .”)
Network security staff should review the current content of their organization’s Web site(s) and develop and implement a collaborative review process with the Webmaster(s) to reduce the risk of giving away valuable secrets.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@compuserve.com>. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at <http://www.mekabay.com/index.htm> for papers and course materials on information technology, security and management.

Copyright © 2002 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.