In coming weeks, I will be reviewing the information security resources upon which I rely most often. In the first few issues of the new series, we will look at alerts and vulnerabilities.

I hope that any readers who don’t know about the Computer Emergency Response Team Coordination Center or CERT/CC at the Software Engineering Institute of Carnegie-Mellon University <http://www.cert.org> will immediately go to their Web site for an introductory exploration.

CERT/CC was developed in the wake of the Morris Worm of 2 November 1988, when it became clear that the Internet community needed some sort of central data repository and communications service to ensure rapid and effective response to emergencies affecting the Internet.

The CERT/CC resource is a extraordinary source of unbiased, technically advanced information about security vulnerabilities, exploits, and patches. All network administrators should ensure that someone in their group is formally tasked with the responsibility of monitoring bulletins from CERT/CC. The latest Advisories are always listed at <http://www.cert.org/advisories/>; these documents provide an overview of current important security problems and usually provide an overview, description, impact analysis, solutions, vendor information and references. For example, at the time of writing, the latest Advisories included "CA-2001-12: Superfluous Decoding Vulnerability in IIS" and "CA-2000-11: sadmind/IIS Worm."

The CERT/CC Summaries <http://www.cert.org/summaries/> are extensive documents published four to six times a year and provide a wide-ranging review of key issues as seen by the organization’s expert staff. The latest Summary is “CS-2001-02,” published May 29, 2001; it includes the usual summary of recent activity and a list of recent updates to the CERT/CC Web site.

Two less well-known resources are the CERT/CC Incident Notes <http://www.cert.org/incident_notes/> and the Vulnerability Notes < > which are described as, “as an informal means for giving the Internet community timely information relating to the security of its sites. Incident notes describe current intruder activities that have been reported to the CERT/CC incident response team. Vulnerability notes describe weaknesses in Internet-related systems that could be exploited but that do not meet the criteria for advisories.” The Incident Notes are usually short reports on particular exploits and sometimes include source code to illustrate how the attacks work. The latest Incident Notes listed at the time of writing were "IN-2001-05: The cheese Worm" and "IN-2001-04: Carko Distributed Denial-of-Service Tool."

Subscriptions to all these publications are free; details are available at the end of each document.
In addition to the publications described above, CERT/CC also provides a wealth of data in other forms. There are courses, books, and White Papers enough to keep any security-happy network manager fully occupied. For example, Julie Allen of CERT/CC has just published a new book entitled _The CERT Guide to System and Network Security Practices_ (Addison-Wesley, ISBN 0-2017-3723-X) which I hope to review soon. Details are at <http://www.cert.org/nav/index_green.html#feature>.

CERT/CC are currently introducing the OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) self-directed risk evaluation method which provides a three-phase framework for workshop-based security analysis for organizations. See <http://www.cert.org/octave/> for details.

Live courses offered by staff of the CERT/CC are described at <http://www.cert.org/training/>. Courses include, for example,

- Concepts and Trends in Information Security
- Information Security for Technical Staff
- Managing Risks to Information Assets
- Executive Role in Information Security: Risk and Survivability
- Creating a Computer Security Incident Response Team
- Managing Computer Security Incident Response Teams (CSIRTs)
- Computer Security Incident Handling for Technical Staff (Intro)
- Computer Security Incident Handling for Technical Staff (Adv)
- Overview of Managing a CSIRT.

CERT/CC is also involved in ongoing research. I urge readers to look into participating in necessary data-gathering by reporting computer security incidents and vulnerabilities promptly; see <http://www.cert.org/contact_cert/contactinfo.html> for the appropriate forms.

* * *

The next article in this series will focus on the Common Vulnerabilities and Exposures Dictionary.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from our Information Security University project, see <http://infosecu.com>.

For information about AtomicTangerine, visit <http://www.atomictangerine.com>.

Copyright © 2001 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.