Intrusion Detection Resources

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

A reader wrote, "I would like to hear about "what to do when you are being attacked by hackers."

Here is a brief summary of some points to ponder plus some references to readings that you may find helpful on this matter. I may cover this matter in more detail in future columns.

The key elements of effective response to breaches of security (whether denial of service, intrusion or some other problem) are as follows:

--BEFORE there is a problem:
* constitution of a suitable Computer Emergency Response Team (CERT)
* implementation of effective intrusion/incident detection procedures and technology
* effective planning and rehearsal of responses to a wide range of scenarios as part of training and policy refinement

--DURING an incident
* discretion / secrecy of CERT actions
* careful safeguarding of evidence for forensic purposes
* collaboration with law enforcement authorities
* meticulous record-keeping of CERT and other actions (for later analysis)

--AFTER an incident
* analysis of vulnerabilities
* implementation of remedial measures to reduce likelihood of similar or related intrusions/attacks
* analysis of CERT responses and improvements to procedures.

Some resources for intrusion detection and response:

Computer Security Institute (CSI) Intrusion Detection System Resources
< http://www.gocsi.com/intrusion.htm >

ICSA Labs Intrusion Detection Systems Consortium
< http://www.icsa.net/html/communities/ids/membership/index.shtml >
with links to a white paper
< http://www.icsa.net/html/communities/ids/White%20paper/Intrusion1.pdf >
and a buyers' guide

<http://www.icsa.net/html/communities/ids/buyers_guide/index.shtml >

A search on the MIS Training Institute Web site
< http://www.misti.com >
finds the following events (among others) or courses that include intrusion detection or incident response:
* The MIS and IIA Annual Conference and Expo on Control & Audit of Information Technology, September (17) 18 - 20 (21), 2000, Chicago
* Network Intrusion Detection, September 25 - 27, 2000, Orlando
* Windows 2000 Security and Control Conference - London, September (25) 26 - 27 (28), 2000, London
* The Business Recovery Managers Symposium, October (30) 31, November (2) - 2, 2000, San Diego
* Network Intrusion Detection, November 6 - 8, 2000, Boston
* SuperStrategies 2000 - London, November (13) 14 - 15 (16), 2000, London
* The Business of eBusiness: Audit, Control and Accounting in a Dot.Com World, December (3) 4 (6) - 6, 2000, Las Vegas
* SecureWeb Symposium, December (4) 5 - 7 (8), 2000, Monterey
* SecureWeb Symposium, December (4) 5 - 7 (8), 2000, Monterey
* Network Intrusion Detection, December 11 - 13, 2000, San Antonio

SANS Guide to Intrusion Detection, Forensics, and Firewall Courses
< http://www.sans.org/newlook/events/guide.htm >

SANS Intrusion Detection FAQ
< http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm >

SANS Computer Security Incident Handling: Step-by-Step (paper)
< http://www.sansstore.org/Merchant/incident.htm >
and ordering on < http://www.sansstore.org/ >

Allen, J., A. Christie, W. Fithen, J. McHugh, J. Pickel, E. Stoner (2000). State of the Practice of Intrusion Detection Technologies. CERT-CC <
http://www.sei.cmu.edu/publications/documents/99.reports/99tr028/99tr028abstract.html >
PDF file at < http://www.sei.cmu.edu/pub/documents/99.reports/pdf/99tr028.pdf >

Amoroso, E. (1999). Intrusion Detection. Intrusion.Net Books (Sparta, NJ). ISBN 0-9666700-7-8. 218 pp. Index.

Bace, R. B. (1999). An Introduction to Intrusion Detection And Assessment.
http://www.icsa.net/html/communities/ids/White%20paper/index.shtml

Bace, R. B. (2000). Intrusion Detection. Macmillan Technical Publishing (Indianapolis, IN). ISBN 1-57870-185-6. xix + 339. Index.

Escamilla, T. (1998). Intrusion Detection: Network Security Beyond the Firewall. John Wiley

& Sons (New York). ISBN 0-471-29000-9. xx + 348. Index.

Hollander, Y. (2000). Intrusion Prevention: The Next Step in IT Security. ClickNet Security Technologies < http://www-west.clicknet.com/products/entercept/whitepapers/wp_intrusion.asp >

Icove, D., K. Seger, W. VonStorch (1995). Computer Crime: A Crime Fighter's Handbook. O'Reilly & Associates (Sebastopol, CA). ISBN 1-56592-086-4, $24.95 US.

CERT-CC < http://www.cert.org >

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses he would be delighted to deliver to your employees at your site and at your convenience.

AtomicTangerine is an independent Venture Consulting firm founded at SRI International, formerly known as Stanford Research Institute. AtomicTangerine's mission is to apply the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries. Headquartered in the San Francisco Bay Area, AtomicTangerine has more than 225 employees in eleven offices worldwide. Additional information on the company can be accessed via the Web at <http://www.atomictangerine.com>.