CIRT Management:  
Rapid Alerts

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

The value of time is context dependent. For example, a minute saved during an emergency may be worth the expense of hours of planning, training and practice for the computer incident response team (CIRT). In this column, I review three important aspects of early warnings in CIRT management: notification of vulnerabilities, notification of threats and notifications of incidents.

_Vulnerabilities_

The CIRT relies on operations managers to maintain adequate defenses by maintaining up-to-date system and application software. The subject of patch management is complex and will be discussed in another series, but I can remind readers that there are many resources on which to draw for notification of new-found vulnerabilities. Each network-equipment and systems-software vendor generally provides a notification service; many organizations have one of their employees subscribe to these to keep up with the news. A better approach, less susceptible to interruption, is to set up a special e-mail address (e.g., alerts@yourfirm.com) for all the subscriptions and to assign one or more people to read that mail every day. If one of the team members is away on assignment or on vacation, be sure that a replacement person takes over the task of scanning the notices to spot anything that is relevant to your network configuration. Instead of forwarding the messages to an individuals mailbox, all of them can be kept in a separate mailbox accessible to everyone on the team.

There are also many newsletters that summarize vulnerabilities; I particularly like “@RISK: The Consensus Security Vulnerability Alert” from the System Administration and Network Security Institute (SANS); you can subscribe at no cost using <https://portal.sans.org>.

Finally, regular readers will recall that the Common Vulnerabilities and Exposures (CVE) dictionary <http://cve.mitre.org/> is a superb compendium of standardized names for vulnerabilities and exposures. MITRE writes, “CVE aspires to describe and name all publicly known facts about computer systems that could allow somebody to violate a reasonable security policy for that system.”<http://cve.mitre.org/about/terminology.html> MITRE also uses the term “exposure” and defines it as “security-related facts that may not be considered to be vulnerabilities by everyone.” You can download the CVE in various formats or you can use the ICAT Metabase <http://icat.nist.gov/icat.cfm> to search the CVE for various subsets of vulnerabilities (e.g., by product, version, type, and so on). At the time of writing (late June 2004) there were 6663 vulnerabilities in the CVE. As a side note, of these, 1383 involved buffer overflows (about one fifth).

_Threats_

There’s a wide range of resources keeping track of security threats. By staying up to date about
new threats, you can improve your defenses before you are attacked; e.g., if particular attacks are
growing in frequency and there are configuration changes or other measures you can take to
stave them off, early warning is a real help. Some of the more popular alert letters < and where
you can subscribe> include:


* Cybercrime-Alerts < http://www.freelists.org/cgi-bin/list?list_id=cybercrime-alerts >

* DHS/IAIP Daily Open Source Report < mailto:nipcdailyadmin@mail.nipc.osis.gov >

* Information Security This Week < security-subscribe@News.WebUrb.dk >

* NewsBits < http://www.newsbits.net/ >

* RISKS < mailto:risks-subscribe@csl.sri.com >

* SANS NewsBites < http://portal.sans.org/ >

* SC Infosecurity Newswire < http://content.hbpl.co.uk/subscribe1/?cmp=387 >

* Security Wire Daily, Security Wire Perspectives, Security Alert <
http://searchsecurity.techtarget.com/registerProfile/1,291003,sid14,00.html?Offer=ismagsite >

_Incidents_

Finally, it’s important to know when there’s an incident happening in your own system.
Intrusion detection systems should be configured to alert CIRT or network management
personnel at once when there are successful intrusions, disturbances of network performance,
equipment malfunctions and other incidents. There are systems available to coordinate output
from network and security systems for rapid notification; for example, the GFI LANguard
Security Event Monitor (S.E.L.M.) is described as follows < http://www.gfi.com/lanselm/ >:

>GFI LANguard Security Event Log Monitor (S.E.L.M.) performs event log based intrusion
detection and network-wide event log management. GFI LANguard S.E.L.M. archives and
analyzes the event logs of all network machines and alerts administrators in real time to security
issues, attacks and other critical events. GFI LANguard S.E.L.M.'s intelligent analysis means
network administrators need not be 'event gurus' to be able to:

* Monitor for critical security events network-wide, and detect attacks and malicious network
users
* Receive alerts about critical events on Exchange, ISA, SQL and IIS Servers
* Back up and clear event logs network-wide, and archive them to a central database.<

[Note: I have no financial interest whatsoever in the resources listed in this article. Mention of
specific products should not be interpreted as endorsement.]

** **
A Master’s degree in the management of information assurance in 18 months of online study from Norwich University – see <http://www3.norwich.edu/msia> for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2004 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.