CSIRTM Discussion: Triage

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

From June through mid-August 2007, I was delighted to lead a six-credit, eleven-week graduate course on Computer Security Incident Response Team Management (CSIRTM) in the Master of Science in Information Assurance (MSIA) program in the School of Graduate Studies of Norwich University. The course used material I wrote for this column over several years and which I collected in a monograph available on my Web site. Our courses have three weekly online discussion topics from weeks one through ten and I am always on the lookout for publishable work our students have created. Mani Akella and Rick Tuttle took up my suggestion that they compile commentary from a number of students of diverse backgrounds in our cohort (class) into a usable series for this column. Mani and Richard worked with their fellow students to ensure corporate approval from all the employers and this is the first in three short articles resulting from their work. As always, I have edited the students’ work for publication.

Today’s topic is triage.

* * *

For this cohort, many represented organizations that do not have a separate formal CSIRT. Instead, organizations use the IT Help Desk (HD) and associated incident-escalation process to perform CSIRT response functions. For those cases where a separate CSIRT exists, organizations often utilize a single HD as point-of-contact (POC) for all incidents. HD staff then use the triage process to assign the incident response to the appropriate functional team.<Grance, Tim et al. (2004) _Computer Security Incident Handling Guide_ http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf p 3-14; quoted by Timothy Dzierzak in discussion >

The prime business of the organization takes the leading role in determining the response and escalation process. For example, credit card data loss is a high priority incident for a financial organization. For these organizations, the response activity affects, and possibly stops, all other CSIRT members’ work tasks until the incident is resolved. For a retailer, the same data loss may only affect the functional area controlling transactions and sales. Management attention to the incident parallels the group response as they view the incident in terms of its disruption either of the entire organization or of the individual group.

Cohort members agreed that training is vital to successful CSIRT operation. Because the HD is the POC, CSIRT-provided training ensures that HD staff capture all relevant information when creating the incident report. Training also ensures that the triage process functions appropriately. In addition, the training helps ensure that the response team captures all relevant information and evidence in a forensically correct fashion to preserve the chain of evidence.

An interesting parallel was the triage processes for a medical emergency as compared to the triage process for a CSIRT. Although the individual processes may differ, the core thinking
processes are the same. Student Stanley Jamrog commented,

“It (triage) is a wonderful system in emergency scenarios, and adapts well to Computer Emergency Response. Now triage generally comes into play when you have a lot of casualties, although it is also done whenever you have multiple patients. Generally, you prioritize your patients. You have those that can wait, those who need emergency and immediate care, and those who are too far gone to bother helping. It seems cruel, but to save some people you can't bother treating those who are going to die anyways.

So you do a quick evaluation of each patient. Can they wait in the treatment area? Do they need to be treated before they are shipped, or do they need to be loaded in the helicopter and shipped immediately?

CSIRT can benefit from such an arrangement. During busy times and major incidents you need to prioritize your responses so that you can make the best use of your time. What systems and incidents need treating immediately and which can wait until you can get to them? After all you have to seal the intrusion holes before you fix the servers, or you will just be doing it again later.

Triage is very appropriate in my opinion, and works well for most types of emergency response. Taking a few minutes to analyze the situation and prioritize your responses.”

Student Timothy Dzierzek responded,

“I think that no matter how great an organization's procedures are, every incident will be different. That point probably is obvious, but even with a single, simple incident, a CSIRT needs to look at and see how their procedures fit into the response. In a mass incident, it gets much trickier. You have probably seen this on the medical side, though I hope not. There are not enough responders to go around. A CSIRT cannot possibly fix everything at once. So having a CSIRT that is skilled at triage is extremely important.


“Triage is an essential element of any incident management capability, particularly for any established CSIRT...This process can help to identify potential security problems and prioritize the workload.”

In the next segment of the discussion, coming in the next column, the students looked at problem-tracking software.

* * *

Mani Akella, CISSP is President and Technical Director at Consultantgurus, a Bridgewater, NJ organization focused on providing Information Assurance and Surveillance services to its clients. He can be reached via email at <mani@consultantgurus.com>. His personal blog is at <http://akellamani.blogspot.com>.
Rick Tuttle is a project manager at Sasol North America Inc., a Houston, TX based chemical manufacturing company. He manages desktop software deployment, including security patches and updates, and supports the company’s business continuity and compliance efforts. Rick can be reached by e-mail at RangerRickT@netscape.net.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.graduate.norwich.edu/infoassurance/> and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2007 M. Akella, R. Tuttle & 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.