Computers & Security (2004) **23**, 87—88

Computers & Security

www.elsevier.com/locate/cose

FROM THE EDITOR-IN-CHIEF

Incident response teams need to change

Dr Eugene Schultz, Principal Computer Engineer, University of California-Berkeley Lab

Every week I receive an email message from one of the many security incident response teams currently in existence informing me how many unauthorized vulnerability scans have targeted particular ports during the previous week. I never take the time to look at the content of any of the messages. After all, a large part of my job involves intrusion detection, something that already makes me aware of the current trends in port scanning. Additionally, if I need to, I can quickly go to the SANS Internet Storm Center site and locate much more detailed (and in all likelihood more accurate) data about scans as well as an abundance of other Internet security-related data and information. The U.S. government is paying what is certainly no small amount of money every year for response teams such as the one that dutifully sends me port scan data to duplicate what is already being done. The same is also true of many other governments in other countries. And the port scan data I mentioned serve as only one of many examples of this kind of redundancy and waste.

When incident response teams first surfaced they were a bold, novel experiment. Cliff Stoll, author of *The Cuckoo's Egg*, deserves credit for coming up with the concept. Shortly after Stoll published his legendary book, two vanguard teams were formed. These teams were soon followed by others, and then by the federation of response teams, ''CERT System'', later to be renamed ''FIRST'' (the Forum of Incident Response and Security Teams). Most incident response teams have historically provided support to those who have requested it—people whose systems have been compromised or are suspected of being compromised—and have issued bulletins describing vulnerabilities and fixes for them. These roles were appropriate in the early stages of the existence of these teams, but now they have for the most part become obsolete. Why? Response teams started to receive fewer and fewer requests for assistance over the years. Why? For one thing, the level of knowledge concerning incident handling (especially among system administrators) has substantially increased, due in large part to the widespread availability of incident response and forensics training. Additionally, many response teams have alienated their constituencies due to a variety of reasons—arrogant behavior of team members, failure to respond at all (earning certain response teams the dubious nickname of ''the black hole''), because certain teams have consistently provided inaccurate technical advice and direction, in many cases because the response teams and their constituencies were geographically too far apart from each other (creating, among other obstacles, communication problems due to differences in time zones) and betrayal i.e. leaking sensitive information about incidents to others without consent of persons who provided the information). Certain U.S. government agencies have reacted to the declining role of response teams by requiring that all security-related incidents be reported to the agency's response team—something that pretty much killed whatever enthusiasm remained for each such team among its constituents, but this has at least ensured a continuing role for the team, however petty.

Don't get me wrong—not all response teams play a petty role. Some actively seek evidence of incidents and notify their constituents rather than waiting for their constituents to report incidents to them. Some have developed extremely useful tools such as automated vulnerability assessment and remediation tools. I especially value CERT/CC's quarterly summary of the major types of Internet

doi:10.1016/j.cose.2004.01.009

attacks that occur. But I fear that these exemplary teams are more the exception to the rule than anything. As I have discussed in chapter four of *Incident Response: A Strategic Guide to Handling System and Network Security Breaches*, response teams can be characterized in terms of four stages: initial; critical (that is, will they serve a useful function or not?); established (that is, they have an ongoing, productive role that meets the needs of their constituencies); and post-established (that it, they develop advanced roles and functions). Most of today's government-sponsored teams (even teams that have been in existence for years) are either in the initial or critical stages. They wait for incident reports, simply copy (partially or entirely) other teams' bulletins, notify their constituents of new, important events many days or even weeks after their onset, and spew what effectively constitutes spam—counts of port scans, lists of countries from which attacks have ostensibly (but in all likelihood not really) originated and the like—to their indifferent constituents.

The current trend among response teams is to redefine team charters to transform the teams into ''analysis centers'' that gather data about threats, vulnerabilities and incidents, analyze and correlate these data, and then distribute them to the team's constituents and sponsors. Doing so makes sense, at least superficially, but with very few exceptions; what has in effect happened is that whatever operational capabilities each team has developed have eroded in favor of a bureaucratic orientation in which ''bean counting'' has become the norm. As a taxpayer, I strongly object, and as an embarrassed information security professional (and founder of one of the original response teams), I say that enough is enough.

In short, many if not most of today's government-sponsored incident response teams are badly in need of change. The major barrier to change is response team sponsors themselves, who are usually so badly out of touch with the community that each team is supposed to serve that they, too, rely on bean counting—statistics concerning the number of incidents handled, the number of port scan reports generated, and so on—to assess the worthiness of response team efforts. At some point the sponsors must ask the question: ''Would it really make a difference if the team we sponsor ceased to exist?'' The best solution is to mandate brutally thorough, independent audits of government response team efforts. The audit findings would serve as an almost too-perfect basis for either keeping a response team as is (as in the case of established and post-established teams) or to change a response team or to force the team to close shop (as in the case of teams that were founded years ago, but are still in the initial or critical stages of existence).

Dr Eugene Schultz
E-mail address: eeugeneschultz2@aol.com

17 January 2004