Managing Vulnerability Disclosure

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

In a couple of recent columns, I have looked at the practice of trying to get companies to pay money for information about vulnerabilities and the related issue of threatening to publish vulnerabilities unless companies respond according to an imposed timetable.

Corporations have to shoulder their share of the blame for the frustration felt by users who fruitlessly batter at their doors to get a hearing. Yes, corporations do have priorities for using limited resources, but the frustration comes from not being listened to. From experience in technical support, I'd say that the critical elements in gaining the cooperation of users who are experiencing difficulties are

* paying attention to the calls for help or for repairs;

* having a systematic method for tracking all calls and correlating problems so that you know what is causing most of the trouble;

* a system for assigning priorities to specific fixes or repairs;

* reliable, frequent communications with the people who called in the trouble report;

* involving the callers in solving the problem if possible.

The worst thing a company can do is brush off a trouble report; the next worst is to claim that they will resolve the problem when in fact there is no intention to do so. Honesty is essential in all our work, and especially when dealing with clients and with the public at large.

When I was an operating-systems and performance specialist for Hewlett Packard in the early 1980s, it always seemed wonderful to me that HP consistently published a complete list of all the known problems they had registered for their products. The _Systems Status Bulletin_ was published quarterly, with biweekly updates; it was a compendium of all the problems that had been localized in every software product the company made, with patch numbers for those that were fixed, release numbers for patches that had been integrated into installation releases, and workarounds if possible for those problems that were not yet fixed.

I recommend this honest and complete approach to all companies, especially those working with security products.

Finally, users and specialists should understand that using the threat of publishing detailed exploits – or actually publishing them – is a crude, extreme and unprofessional approach to resolving a problem. Instead, try to build pressure using a graded series of actions instead of jumping to threats:

*
* define a timetable for acceptable responses that takes into account the severity of the security hole – don't ask for instant repairs on a minor item;

* contact higher levels of management at the vendor firm to discuss the issue;

* get the cooperation of upper management in your own firms, if appropriate;

* arrange for face-to-face meetings between the top managers of your firm and those of the vendor firm;

* contact your professional colleagues for joint letters pressing for a solution;

* raise the issues in professional forums (USENET, mailing lists, professional association meetings) without giving enough details in public that would allow instant exploits by the black-hat crowd;

* set up a BOF (birds-of-a-feather group) at an upcoming meeting specifically to discuss solutions and workarounds to a longstanding or fundamental design problem;

* look for alternative suppliers – and make sure that you do so openly by telling your supplier you are not satisfied with their product quality or their service;

* contact certifying bodies to withdraw certification of products that remain unrepaired for a long time after notification;

* get your corporate counsel involved to discuss possible legal action for breach of contract if possible;

* publish information about the problem, again without giving away so much detail that you make the problem worse than it already is. The last thing you want is to give some twisted ten-year-old script kiddie (or a twenty-year-old with the same level of moral development as a ten-year-old) a prefabricated attack script.

In summary, I think that a sound approach to preventing extortion in our business involves making it unnecessary. We should establish norms for professional, collaborative responses to reports of vulnerabilities. The other powerful tool we can use is peer pressure: let's establish a consensus about not trying to extort compliance with our own priorities when we run into trouble with software and systems. But in any case, demanding money to avoid publication of a vulnerability is just plain sleazy.

In the world of INFOSEC, we need people who are the equivalent of blood donors, not blood suckers.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.
