Information Anarchy: The Blame Game?

M Edwards | Oct 23, 2001

Full disclosure of security risk information is still under fire—this time driven by the recent outbreak of malicious worms such as Code Red and Nimda. Last week, Microsoft published an essay written by Scott Culp, manager of the Microsoft Security Response Center. In the essay, Culp refers to full disclosure as "information anarchy" and says that Microsoft is working with other industry leaders to form a consensus protesting such information release. The company will ask its customers to support the adoption of the resulting consensus.

The central concern with full disclosure is that people often take vulnerability demonstration code—sometimes released in fully functional form—and use the code to create a weapon against unsuspecting users. "But regardless of whether the \[security vulnerability\] remediation takes the form of a patch or a workaround," Culp wrote, "an administrator doesn't need to know how a vulnerability works in order to understand how to protect against it, any more than a person needs to know how to cause a headache in order to take an aspirin." Although he's right to a certain extent, we need to consider a larger perspective.

Worms such as Code Red and Nimda definitely played upon well-known bugs for which patches had long since been available. Those worms showed us how many administrators don't consider security to be a priority in operating their systems. Granted, the worm writers seem malicious in releasing such nuisances, but is there a silver lining to those dark clouds? I think so. As a result of regularly demonstrated administrative complacency, Microsoft has adopted significant new policies and practices. The company has expanded its customer support

efforts and is committed to providing even more robust security in its products and more robust tools to help automate and manage security. For example, because of these worms, Microsoft is now giving in a bit to the habits and needs of its customers instead of the somewhat idealistic visions of its software architects. So who benefits in the overall scenario? Everyone does. Culp wrote, "Customers who are considering hiring security consultants can ask them what their policies are regarding information anarchy, and make an informed buying decision based on the answer. And security professionals only need to exercise some self-restraint."

In reality, Microsoft doesn't benefit by condemning the sharing of detailed vulnerability information. Instead, the company should be scolding the misguided focus and relative complacency of its customers' administrative efforts. It seems that Microsoft is doing that now indirectly with its new Strategic Technology Protection Program (STPP). The effects should benefit information security in general, but getting a new program fully operational takes time. Perhaps any new consensus is going a bit too far too soon. In any event, a new consensus will benefit Microsoft by buying the company some time to get STPP into full swing. So again, who benefits from any new consensus in the long run? As Culp pointed out, "Even in the best of conditions, it will still be possible to write worms." So a new consensus won't eliminate the core problems of administrative latency and faulty code.

The full-disclosure problem comes down to timing on three fronts: Researchers publish explicit details in many cases without enough consideration for the time required for companies to develop a patch and coax customers into loading the patch; users wait too long to apply patches, if they apply them at all; and Microsoft product cycles are probably still far too quick to market for effective code development.

What do you think about full disclosure? Is it a detriment or a benefit to

the user community, or does it seem to balance out fairly equally in the bigger picture? Go back to our home Web page and take the Instant Poll. We're eager to learn your perspective. And if you want to express detailed comments regarding any new consensus, you can post them in response to this editorial—you'll find a copy posted on our home page, too.