Anti-hacking method of full disclosure under attack from a part of the security industry

FOR MORE THAN three years, we have strived to use this space to inform you about the latest tools and techniques from the security world. Our weekly toil was a wholehearted attempt to educate you about the importance of security and to demonstrate how easy it is both for others to compromise and for you to tighten security at your site. We recommend the tack, first realized by Dan Farmer and Wietse Venema, of securing your site by breaking into it. Although at first glance this path seems calamitous, it has earned great popularity.

Based on the feedback we get daily, nearly all of you have appreciated our efforts in this column and our security book, Hacking Exposed. Many of you have written us to relate your successes in convincing your CIOs to take a serious look at the bursting security artery in your companies. Sometimes the information we provide is the system administrator's last hope in motivating upper management to take security at their site seriously. In spite of all our good intentions, a small faction in the security industry has done a 180-degree turn in their stance on full disclosure over the past year. This faction has determined that the material we and others in the industry possess should be illegal.

The main argument goes something like this:

Security researchers are liable for the information they release because when it is used to harm others it can have deleterious effects. According to this logic, the Ginsu steak knife company would be liable for any and all misuses of their technology as well. This is beyond absurd.

The consequences of such logic would force us and others in the industry to go underground. The underground would continue to expose vulnerabilities, but only to the underground, and not to the public, keeping this vital information away from the system administrators who most need it. You tell us which is more effective, telling your IT manager you're insecure and asking for money for security or showing him his cracked password and then asking for the money.

The long-term effects of suppressing information have historically proven to be a recipe for disaster. The underground elite become intoxicated with their power and authority and soon turn those who would have been a benefit to society against it, creating a powerful force that would make today's current pool of bad guys seem emaciated. The way to fight a regime of terror is to fight it with information -- via full disclosure.

People need to be held responsible for their actions, not for the communication of ideas. How can we blame the people who disseminate information with the intention of educating the public? The result of

RELATED LINKS

» Bush's 2008 IT budget focuses on cybersecurity

» FTC: Identity theft remains top consumer complaint

» Baich: Data theft problem no easy fix

» Security RSS feed

>> MORE

such a policy would be the suppression of vital information, specifically in the security industry, that for the first time ever can get an IT manager or administrator to wake up to the nightmare that security at their site can turn into. The only rational solution is to make the script kiddies responsible for their actions, as we do with all criminals.

Here's another argument against full disclosure: Full disclosure today has never been more widely practiced, and yet the number of security break-ins has only increased. This is proof that the dissemination of security information is not helping. The irrationality here ignores the massive increase in the size of the target due to the exponential growth of the Internet. Even if the number of attacks has multiplied by 10 during the past five years (which is doubtful), the number of systems connected to networks throughout the world has grown by many times that number in the same time.

Like any system, full disclosure is not perfect. People do occasionally get hurt when it is abused for personal aggrandizement, corporate marketing, or plain old malice. The solution to these minor bumps in the road is more education. Teaching the general public the techniques and tools the underground uses is important, but so is teaching the fixes or countermeasures as we try to do regarding every vulnerability. Almost as important is to teach the moral responsibility that comes with such knowledge. How do you feel about publicly discussing the tools and

techniques of the underground?

The people who take the stance against disclosure are usually those who have been personally affected in some manner. For example, someone whose personal computer has been hacked tends to be much more sensitive about the subject, and we understand the sensitivities surrounding the issue. One of us recently had all his possessions stolen from a moving company. But our personal antipathy for moving companies brought on by this traumatic event did not motivate us to lobby Congress to get all moving companies banned from the United States. Neither do we feel that all movers should be vigorously sued until they decide to abandon the industry altogether. An argument based on emotions such as this is fundamentally flawed. Emotions typically leave objectivity and rationality out on the ledge. As such, we hope the arguments made against the dissemination of security information or full disclosure will soon die off, but until then, be wary of short-term appeals to your emotions.