Is the disclosure of security flaws the best way to make vendors fix software?

Full disclosure

For Microsoft systems administrators, it was the summer of 'Code Red'. After a major bug in Microsoft's web server was exposed – and then exploited by virus writers – systems administrators around the world scrambled to download patches and to decontaminate their networks. But, could the outbreak have been avoided if (and it's a big if) no one had actually publicly documented the flaw in Microsoft's software? Or, alternatively, would non-disclosure have ultimately resulted in a far wider contamination of servers at companies that were oblivious to the threat?

Some analysts are in no doubt. "What we've learned over the past few years is that full disclosure [of bugs by suppliers of packaged software or by security agencies] helps much more than it hurts," says Bruce Schneier, founder of Counterpane Internet Security. "Since full disclosure has become the norm, companies that once ignored and belittled security now that fixes vulnerabilities as quickly as possible."

PATCHING PRESSURES

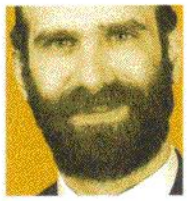
Much of the pressure has come not from software vendors but from agencies. Until CERT, the US government-funded Computer Emergency Response Team, started publishing details of flaws, vendors had little motivation to disclose bugs in their software – or indeed fix them. As a result, malicious hackers continued to break into systems – often using weaknesses discovered years earlier – with customers often unaware of the problems.

> "Full disclosure helps much more than it hurts."

Today, customer awareness of bugs is much more acute, and it puts pressure on vendors to produce fixes. CERT, which estimates it saw 3,000 vulnerabilities this year, issues bug reports to the US government and the Internet Security Alliance, giving the relevant vendor 45 days to develop a patch for the problem before it publishes details of the flaw.

But the devil is in the detail, say many software vendors, and the level of detail published by CERT and other agencies actually fuels malicious hacking. Russ Cooper, moderator of the NTBugtraq email group, argues that although Code Red exploited a weakness that had not previously been known, the publishing of in-depth details of the flaw resulted in the greater virulence of its successor, Code Red 2.

Others argue that the short period of time given to vendors to produce a patch means such 'fixes' are anything but that. In June 2001, Microsoft twice had to re-issue a patch for the same hole in its Exchange groupware server after a error in the patch caused servers to hang.



Bruce Schneier, Counterpane

VAGUE STATEMENTS

Schneier believes that only full disclosure will make vendors fix their mistakes. "If a researcher just publishes vague statements, the vendor can claim [a report of a bug] it is not true," he points out.

But some argue that the issue of disclosure is fraught with legal risk.

Never afraid to court controversy, Microsoft, meanwhile, is working on an alliance with a handful of major suppliers of security software and services designed to prevent bug information getting out into the public domain in the first place. Members – which include security software companies Network Associates and Internet Security Systems – say they will exercise "best efforts" for 30 days from the initial discovery to avoid disclosing details that can be used to exploit a vulnerability. Put another way, they will tell neither the potential hackers nor the users of their software products. After that, further details may be released, although not enough to allow the exploitation of the flaw. Code that might allow organisations to test their vulnerability to the weakness would also be suppressed.

The scheme will cause major problems for Microsoft's partners and customers. Would any CIO employ a security firm that has made a commitment to Microsoft not to reveal any of the flaws found in the Microsoft software running within the organisation, for example?

As Code Red showed, malicious hackers can find vulnerabilities in software before vendors can locate and patch them. Unless CIOs know how vulnerable their systems are to attack, and that security patches will be quickly available, they cannot entrust their data to them.

Even then, they can only hope that vendors are quicker than hackers and good enough at writing code, both for patches and for the original product, so that the chance of a security breach is minimal.

CONTACT
Rob Buckley **rbuckley@infoconomy.com**

SECURITY MYSTERY

In August 2001, Novell come up with one of the strangest compromises between full and zero disclosure of security problems so far. The company sent an email to its GroupWise 5.5 Enhancement Pack and GroupWise 6 users, asking them to apply a fix to their servers immediately because of an extremely serious security flaw. But the company then refused to reveal the nature of the bug – just in case hackers exploited the problem.

Novell executives insist that no hackers actually found and exploited the flaw, but admit that the problem was so severe, "it needed a whole different kind of response" from the standard practice of disclosure.