InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

Public In The Dark About 95% Of Software Bugs, IBM Says

An IBM security director is estimating that the 7,247 software vulnerabilities disclosed last year are a fraction of the 132,115 that actually were discovered.

By Sharon Gaudin, InformationWeek
June 5, 2007
URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=199901292

Most people are grossly underestimating the number of vulnerabilities in the software they're using at home and at work, according to a security director at IBM.

Gunter Ollmann, director of security strategy at IBM's Internet Security Systems, said in a blog that 7,247 software bugs were publicly disclosed last year. The issue, though, is that he estimates that there actually were 132,115 vulnerabilities discovered last year. That means only 5.48% of them were disclosed to the public.

"To be sure, 139,262 new vulnerabilities in a single year is a colossal number, but is it wrong?" asked Ollmann in his blog entry. "Too many people underestimate the number of vulnerabilities in the software they use at home and in the enterprise office. Public vulnerability disclosures provide only a small window into the total number of vulnerabilities uncovered on an annual basis."

What does that mean to the IT or security manager trying to protect their network?

"If you're basing your protection strategy upon keeping up solely with public vulnerability disclosures, you're missing almost 95% of the vulnerabilities actually out there (this year)," said Ollmann. "If your defense systems are designed to protect against specific vulnerabilities (i.e. signature-based), it probably means that it was designed to protect a subset of publicly disclosed vulnerabilities. Preemptive protection engines are needed for the remaining 97% of annual vulnerabilities."

Where's the disconnect between bugs discovered and bugs reported?

Ollmann said it's a multipronged problem. Sometimes, for instance, vulnerabilities discovered internally by the vendor are generally patched silently. And flaws often are reported to the vendor who then keeps quiet about them until they can come up with a fix for them. Sometimes researchers simply think a bug is too "lame" to bother reporting.

While Ollmann listed several other reasons behind the discrepancy, he said the largest contributing factor is that security consultants and researchers find bugs while they're contracted to do penetration testing and vulnerability discoveries. He added that he "guesstimates" that an average consulting penetration-tester/researcher would uncover about five to 10 new vulnerabilities per day. If they're testing a typical, nonfinancial Web application, then the number jumps to more than 40 bugs found in a single day.

Now, if the contractors do find five vulnerabilities per working day, that quickly adds up to about 3,750,000 vulnerabilities per year, according to Ollmann. That number won't stand, though, since many contractors will be finding the same bugs. Even if 90% of the bugs discovered by contractors are repeats, that means they're still finding 125,000 newly discovered flaws every year.

"The bigger the application, the more vulnerabilities will be discovered," Ollmann noted. "For example, in some of the larger engagements I've worked on in the past, a four-man team working for five days has uncovered over 600 vulnerabilities in a

single commercial application."