Dr Slammer, or How I Learned to Love Downtime

Network World Fusion Security Newsletter by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

My friend and colleague Jim Reavis recently sent me the latest issue of his _CSOinformer_ security newsletter and I was so taken by his comments on the recent Slammer incident that I asked him for permission to republish it here. He has very kindly allowed me to print the following essay (lightly edited) from his excellent publication. “I” refers to Jim, so please direct your praise (or abuse) to him <mailto:jim@reavis.org> with a copy to me <mailto:mkabay@norwich.edu> when responding to any controversial bits below.

* * *

The Slammer (or Sapphire) worm has come and is mostly gone. This worm halted the Internet in many parts of the world and stopped many critical business functions within corporations. How do I grade the players in this latest saga? Let’s take a look:

* Microsoft: B-. Seriously, how much blame can we ascribe to Redmond when they released a security advisory six months before the attack, complete with a patch for the affected SQL Servers? They cannot get an “A” because they released the insecure product in the first place; they get the minus for having a lot of security advisories to wade through and for making the process for patching computers so painful, as I’ll discuss at the end of this column.

* Information Security Industry: D. If there is going to be an information security industry in the long run, these are the moments in which it needs to shine. Vulnerability assessment companies can claim that they warned you, but they didn’t do too much to help you. Many companies claimed that they could help – the next time Slammer attacked. There were some very good examples of smaller companies who trapped Slammer with anomaly detection technology or prevented it with patch management. But the big guys – the security companies most of us have standardized on - seemed to have very few answers.

* Systems Administrators: F. We all need to take personal responsibility for the security of our networks. The underlying vulnerability for Slammer was announced on July 24, 2002 by Microsoft bulletin MS02-039 and given the maximum severity rating. History tells us that nearly all wide-scale attacks are based upon known vulnerabilities. Microsoft released 72 security bulletins in 2002, not a tiny number, but not exactly the population of Hong Kong either. A systems administrator reading MS02-039 should have seen the hallmarks of a potential problem: specifically, the vulnerability could be automatically exploited without any local interaction. However, most chose not to apply the patch.

Clearly, what is needed is sophisticated patch management technologies to aid organizations in managing updates, which will only increase in frequency. Among the key needs:

* Scalability to accurately identify vulnerabilities in large networks;
* Regression testing and the ability to pilot patches;
* Wisdom to know which patches should be installed and when;
* Ability to simply roll back patches that have unintended side effects;
* Work-around information for vulnerabilities lacking a suitable patch;
* Ability to integrate patch management into enterprise systems-management consoles.

Everyone makes the same comment: Patching is difficult. Rarely does anyone explore why. What’s the main reason, the specific detailed single reason why patches do not get installed? Because, for most patches applied, the system must be rebooted. When you reboot a computer, a hundred different things can happen and only one of them is good. The Reboot Dilemma is the undoing of many a systems administrator. Anyone who has worked in the business for more than a year has their own personal horror story of an upgrade gone awry, and a two-hour project turning into a lost weekend. We need to figure out how to install service packs and hotfixes dynamically – without requiring a reboot. If any of the nascent patch management companies could figure this out, I’ll stand in line for their IPO.

---

_CSOinformer_ is edited by Jim Reavis <mailto:jim@reavis.org>, founder of SecurityPortal and longtime industry analyst. For full details about the publication, including subscriptions and site licenses, visit <http://www.reavis.org> or download <http://www.reavis.org/csoi.pdf>.

---

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


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2003 Jim Reavis. All rights reserved.

Permission is hereby granted to *Network World* to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.