Ignorance or Lies

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
ADARIO, Inc.

Kevin Mitnick published a letter in *The Guardian* newspaper and perhaps others on the 22nd of February 2000. I won't comment today on his opinions concerning his guilt or innocence, other writers, the news media, and the justice system. Today I want to focus on exactly one question in his letter: "What threat did I present when I hacked into Sun Microsystems' computers?"

Criminal hackers and their supporters often use this flawed defense as an excuse after breaking into other people's systems without permission. They seem to think that as long as they don't modify information, they haven't done anything wrong. Some of them proclaim "Information wants to be free" and imply that there is something wrong with confidentiality, especially confidentiality of corporate communications and documents.

I suspect that most of the people who excuse unauthorized access to computers and networks have never worked with production systems. A production system is one whose functions are essential for the operations of its owners. For example, a real-time process-control computer in a factory is a production system; so are the computer and the network underlying a hospital registration system. Breaking into a production system without authorization process that production system into limbo. We can no longer trust the data or the programs in the compromised system.

Think about it this way: suppose you came home to find that someone had left a note on your pantry saying, in that childish character-substitution code of theirs, "Y0ur fr0n7 d00r 10ck w4s 34sy f0r m3 70 pick, s0 I br0k3 in70 y0ur h0us3. Fix y0ur d00r 10ck 0r I wi11 7311 3v3ryb0dy 31s3 h0w 70 br34k in70 y0ur h0us3. 14m3rs 1ik3 y0u d3s3rv3 n07hing bu7 c0n73mp7 fr0m us 31337 crimin41 h4ck3rs. I didn'7 d0 4ny7hing b4d 70 y0ur sys73m, 7h0ugh." [Your front door lock was easy for me to pick, so I broke into your house. Fix your door lock or I will tell everybody else how to break into your house. Lamers like you deserve nothing but contempt from us elite criminal hackers. I didn't do anything bad to your system, though."] Tell me, would you trust the food left in your pantry? Would you take such a person's word that he or she "didn't do anything?" Or would you be concerned about the safety of your family if you ate the food after a stranger -- and not a very nice stranger, at that, judging from the note -- had access to it?

Suppose you got the same kind of note or none at all after a stranger broke into your car? Would you assume that your brakes were still safe to use or that your fuel were still uncontaminated? You don't have to be paranoid to be concerned about trusting someone who violates your property and doesn't even identify himself or herself with a name, let alone an address, that would allow you to trace them.

The managers and staff responsible for production systems are in the position of someone contemplating that possibly-contaminated food or that possibly-damaged car. We have to check all the data and all the programs on the product system to ensure their integrity and authenticity. As a side note, this concern certainly provides support for security systems that allow systems management to maintain cryptographic checksums on all executables and data to insure program and data integrity and provide proof that only authorized software was used for making changes and additions. Databases and log files really ought to include message authentication codes as a matter of course so that no one with a debug utility can alter data without leaving tell-tale evidence of their changes.

When I was an operations manager in the 1980's, my staff and I at the large data center where we worked would treat the new operating system tapes in a way that may surprise some of you readers. We habitually spent five nights working from midnight to six in the morning testing the new versions of our mainframe operating system. We would replace the disk packs and work on a copy of the production systems data overnight, trying to show that we could break the new version in any way except through privileged utilities. By Friday, if we had not succeeded in breaking the operating system, we would decide whether to go into weekend testing with representatives from the 28 client companies using our systems. By Sunday noon, we would know whether we had enough confidence in the operating system to allow it to go live on Monday morning.

If we were willing to do all this work to test software from a major manufacturers even though system failures were something that happened only a few times a month or a quarter, how do you think we would have felt had there been unauthorized access to our systems? The operating system version could be backed out; our log files would provide the basis for backing out transactions and recovering them if necessary. But at least a faulty operating system would not be suspected of malice, and its installation could be delayed until after thorough acceptance testing. If an intruder had walked through our system — or our operations center, for that matter — we would have been in serious trouble.

All unauthorized access to production systems _always_ damages trust in our programs and in our data. When our customers, employees, patients, or the public depend on our systems, we _may not_ ignore break-ins. The criminal hackers and their supporters are guilty of either ignorance or of deliberately lying when they tell us that their depredations are harmless.

I urge all of us in the security field to get the word out to our friends, our families, fellow employees, and especially to the press: criminal hackers _always cause harm_ when they break into our production systems, no matter what they say.

* * *

M. E. Kabay, PhD, CISSP can be reached by e-mail at <mekabay@gmail.com>.

ADARIO, Inc. provides full-spectrum e-business strategy, planning and implementation; Web development and design; software development and integration; information security services; network architecture and planning; and change management. Visit the new Web site at < http://www.adario.com >.