Microsoft in the News

While it is not my intention to indulge in Microsoft–bashing, several items about Microsoft in the news are worthy of comment. Let us begin with the most serious.

Yesterday’s USA Today had a front page (below the fold) story about attempts to exploit various weaknesses in Microsoft Office. These attacks have been aimed at government agencies, and many seem to come from China. The most egregious incident was a May incident in the US State Department. An employee clicked on a malware Word document that exploited an unpatched security hole; Microsoft issued a patch eight weeks later.

USA Today offers the following advice, not in a complete sentence, and without attribution: “The best protection: keeping Office security patches updated.” This is not good advice; the weakness was in the employee who allowed the attacker in. The analogy here is saying that college dormitories need to keep their locks up-to-date, ignoring the fact that residents leave the door propped open so their friends can get in.

Microsoft’s response was that the attacks are “very targeted and very limited.” This is correct: the targets were limited to corporations and government entities that had something of value to steal. Willie Sutton (of “… because that’s where the money is” fame) will not carjack you. In my mind, this makes the attacks more frightening not less so. Microsoft also offers the sensible advice urging workers “to absolutely extend extreme caution” when opening Office files in e-mail.

OK, while we’re on Microsoft, a couple of items from slashdot.com:

1. Microsoft says that Apple’s iPhone will be “irrelevant” to business, because it is closed-source (yes, the pot can call the kettle black!). Of course, lots of phones run Windows Mobile, and they want to keep that market.

This particular article (ZD Australia) did not address the ubiquity of Research In Motion’s BlackBerry and its many imitators. And remember that the financial world came to a near standstill last week when RIM suffered a still unexplained service interruption.

[from eWEEK.com] Microsoft claims that the Messaging and Security Feature Pack for WM offered “… existing security features in the software platform, such as end-to-end encryption over a virtual private network, application certification, and a range of third-party anti-virus and file encryption solutions.”

“Gartner analysts acknowledge some security improvements in the platform, including certificate support and a remote management utility that lets an Exchange administrator wipe the device’s main memory after too many failed password attempts.
“A separate facility has also been added to allow an administrator to instruct the device to wipe itself the next time it connects via TCP/IP to the server.”

Also, Symantec announced a couple of weeks ago that it is preparing to launch a mobile-security suite for WM devices that will offer the “same level of security for handhelds as is standard for PCs.”

Still, I can’t help but be reminded that Bill Gates dismissed the internet as an irrelevant fad.

2. [This is pure gloating.] Dell has reintroduced Windows systems at its website, an indication that consumers are rejecting Vista.

CERT

CERT, for Computer Emergency Readiness Team, was originally a project of Carnegie–Mellon University, and is now hosted by the government at //http://www.us-cert.gov/. It was started after the Morris worm disrupted internet/ARPAnet service in 1990. The Morris worm exploited a UNIX vulnerability in that one could access a host’s mail directory without any authentication, but the providing client ran as a superuser. Once the work had access, it also had email addresses, and spread through emails.

CERT is funded by the Department of Defense and the Department of Homeland Security. CERT collects information on vulnerabilities and patches, as well as offering advice on what to do while you wait. A typical recent VU can be seen at http://www.kb.cert.org/vuls/id/448745;

this concerns a possible buffer overflow in Apple’s QuickTime software. Apple identified the problem and alerted CERT, whose advice was to disable automatic opening of Quicktime until the proper security patch was installed.

A naïve user might ignore this: what harm is there in looking at a movie trailer or news story? The issue is that this, like many buffer overflow attacks, might allow an intruder to run arbitrary code with the user’s privileges. If the user has wheel privileges (or whatever the equivalent is in other operating systems), the intruder has full access.

Here are some recent telephone and mobile device vulnerabilities.

• Some systems use Caller ID for authentication (you may have bumped into this activating a credit card), but VoIP makes it very easy to spoof Caller ID.

• There is a denial of service of attack affecting Handspring Visor phones. The attack involves sending a large SMS message. (Service can be restored by a reset, but as a former Handspring user let me assure you that a reset is a major pain. I went through several of these in trying out a purchased(!) navigation module that insisted on reporting South longitudes. It crashed my PDA while travelling and, since I did not have the sync dock with me, I was without PDA service for the entire trip.)

• Yahoo!’s [yes, that is the correct punctuation] mobile services had a vulnerability that allowed an attack to view random queries, which may include recent web pages that include user credentials.