Bundestrojaner zu Bundeswürmern

„Wurm statt Windows-Update“ titelt der Heise-Newsticker. Eine typische Microsoft-Idee: Um einen Schädling zu entfernen, schleust man einen anderen Schädling ein, der zwar ein „Nützling“ ist, aber auch nur durch ein Leck im Betriebssystem eindringen kann. Die Methode ist nicht neu. Vor fünf Jahren lasen wir den hübschen Titel „Wurm jagt Wurm“. Auch da gruselt es den sicherheitsbewussten Computer-Nutzer: „Wenn der Wurm den Original-Blaster auf dem befallenen Rechner entdeckt, beendet er den zugehörigen Prozess, löscht die Wurmdatei msblast.exe und versucht den Microsoft-Patch zu installieren. Danach startet er den Rechner neu und macht sich auf die Jagd nach weiteren Opfern.“ Igitt.

Milan Vojnovic hat ein Papier dazu publiziert [„On the race of worms, alerts and patches“, with A. Ganesh, journal submission, 2006 (conf ver ACM WORM 05)], das aber schön älter ist. Bruce Schneier wettert gegen die Idee („Benevolent Worms“) an sich, was zu erwarten war und womit er sicher Recht hat. Er bezieht sich auf einen Artikel der New Scientist.com: „Friendly ‚worms‘ could spread software fixes“. „Milan

Vojnović and colleagues from Microsoft Research in Cambridge, UK, want to make useful pieces of information such as software updates behave more like computer worms: spreading between computers instead of being downloaded from central servers. The research may also help defend against malicious types of worm, the researchers say."

Statt permanent „Patches" und neue „Sicherheitsupdates" in den löchrigen Käse zu stopfen, möchte das Microsoft durch „gute" Würmer erledigen lassen. Das erschließt sich mir theoretisch nicht ganz: Ein Wurm dringt prinzipiell über Schwachstellen im System (Windows!) ein. „Würmer warten andererseits nicht passiv darauf, dass sie mit infizierten Dateien weitergegeben werden. Sie versuchen auf unterschiedliche Art, aktiv via Netzwerk weitere Computer zu infizieren. Aber auch ein Wurm kann – wie ein Virus – in vertrauenswürdigen Dateien getarnt integriert sein, in diesem Fall hat man evtl. beide Übertragungsarten und daher eine Mischform. Als dritte Art gibt es noch die Trojaner (Trojanisches Pferd), diese zeichnen sich vor allem dadurch aus, dass sie eine Hintertür auf dem System installieren, über welche die Versender (etwa die Programmierer) Zugriff auf den kompromittierten Rechner haben. Heutzutage sind häufig Mischformen (Trojanerwürmer und Trojanerviren) anzutreffen."

Sollen die Windows-Benutzer bestimmte Sicherheitslücken jetzt bewusst offen lassen, damit die gutartigen und von Kleinweich autorisierten Würmer die bösen Würmer angreifen und auf dem Rechner eine digitalen Wurmkrieg beginnen? Schneier schreibt: „Giving the user more choice, making installation flexible and universal, allowing for uninstallation – all of these make worms harder to propagate. Designing a better software distribution mechanism, makes it a worse worm, and vice versa. On the other hand, making the worm quieter and less obvious to the user, making it smaller and easier to propagate, and making it impossible to contain, all make for bad software distribution."

Vielleicht denkt Microsoft ganz kommerziell? Wäre ein angeblich gutartiger Wurm nicht ein Exportartikel nach Deutschland? Bundestrojaner zu Bundeswürmern!