Computerwissen-Daily-Newsletter – Freitag, 20. Juli 2007

25 Jahre Computervirus - ein unrühmlicher Geburtstag

Es jährt sich ein Geburtstag - der Computer-Virus feiert dieser Tage seinen 25. Geburtstag - doch es besteht kein Grund zum Feiern.

1982 wurde von dem 15-jährigen US-Schüler Rich Skrenta ein Programm geschrieben, das sich selbst über Disketten auf Apple-II-Systemen verbreitete. Der Schüler wollte damit seine Freunde erschrecken, die ihn ständig nach neuen Computerspielen fragten. Das Programm verbreitete sich über Disketten, zeigte ein Gedicht an und ließ die befallenen Apple-Rechner ansonsten unversehrt. Das Programm hieß "Elk Cloner" und stellt den ersten Bootsektorvirus dar. "Allerdings gab es zuvor bereits Auftritte von Programmen mit viren- oder wurmähnlichem Verhalten, die geschrieben wurden um Updates und Patches für Drucker in Netzwerken zu verteilen", erklärt Candid Wüest, Virenexperte bei Symantec.

Die theoretischen Anfänge von Virensoftware gehen auf eine Arbeit von John Neumann aus dem Jahr 1949 zurück. Er stellte die These auf, dass sich ein Computerprogramm selbst wiederherstellen kann. Die praktische Umsetzung erfolgte mit dem Computerspiel "Darwin", das von Programmierern der Bell Labs entwickelt wurde. Dabei kamen zwei Programme zum Einsatz, die um die Kontrolle in einem System kämpften und versuchten, sich gegenseitig zu überschreiben. Im Roman "Der Schockwellenreiter" ahnte Autor John Brunner bereits die Gefahr von Internetviren voraus, die sich in den Computernetzen verbreiten.

Jürgen Kraus schrieb 1980 an der Universität Dortmund seine Diplomarbeit mit dem Thema "Selbstreproduktion bei Programmen". Darin konstatierte er, dass sich bestimmte Computerprogramme wie biologische Viren verhalten könnten. Dieser Vergleich machte Behörden hellhörig, als Konsequenz wurde die Verbreitung der Arbeit gestoppt. Erst seit 2006 ist sie wieder zugänglich. Der erste Virus für MS-DOS tauchte 1986 auf. "Zwei Brüder aus Pakistan nutzten den 'Brain' genannten Virus als Kopierschutz für ihre Software", erläutert Wüest. Der Virus schrieb die Bezeichnung des Datenträgers auf "(c)Brain" um und fügte einen Text in den Bootsektor ein.

Verglichen mit heutigen Schadprogrammen verbreitete sich Brian aber sehr langsam, denn sein Infektionsweg war der Tausch von Disketten. Und Brian wurde auch nur aktiv, wenn von der Diskette gebootet wurde, er war ein "Bootsektor-Virus". "Die ersten Viren waren noch recht harmlos und in den ersten zehn Jahren ging es dabei auch eher um die sportliche Herausforderung. Der Antrieb der Programmierer war es, der Erste zu sein, der ein System bezwingen kann, oder den ersten Virus zu schreiben, der sich massenhaft verbreitet. Die damaligen Programme enthielten kaum Schadroutinen", so Wüest.

Mitte der neunziger Jahre verschwanden mit den Disketten als Bootmedium auch die Bootsektor-Viren. Ab 1995 kamen dann Makro-Viren auf, die Sicherheitslücken in den frühen Windows-Versionen ausnutzten. Runde vier Jahre ärgerten im Wesentlichen Makro-Viren die PC-Anwender. Die Kommunikation per E-Mail brachte dann Ende der neunziger Jahre E-Mail-Würmer wie Loveletter alias ILOVEYOU, die großen finanziellen Schaden anrichteten.

Ende der 90er Jahre trat Melissa auf. Der Makrovirus mailte sich selbst an die ersten 50 Teilnehmer im Adressbuch des Opfers und erreichte so schnell eine weltweite Verbreitung. Im Mai 2000 verbreitete sich Loveletter explosionsartig per E-Mail. Der Wurm löschte auf infizierten Rechnern Dateien mit bestimmten Endungen und verursachte weltweit Schäden in Milliardenhöhe.

Ab 2001 begann das Zeitalter der Netzwerkwürmer. Nun konnte ein Schadprogramm einen Rechner übernehmen, ohne dass der Anwender irgend etwas dazu tun musste. Es reichte, einfach nur online zu sein und Sicherheitslücken im System zu haben oder ohne Schutzsoftware zu arbeiten. Netzwerkwürmer wie Sasser oder Blaster erreichten auch erstmals eine weltweite Verbreitung innerhalb von weniger als eine Stunde.

Ein interessantes Viren-Exemplar ist für Wüest der SQL-Slammer. Der Virus befiel den Microsoft SQL Server und infizierte im Januar 2003 innerhalb einer halben Stunde 75.000 Opfer, den Großteil davon in den ersten zehn Minuten. "Der SQL-Slammer war der erste Virus, der sich ohne Zutun des Benutzers verbreitet hat. Er hat eine Schwachstelle im SQL Server missbraucht und sich so verbreitet. Viele Anwender wussten nicht, dass sie das System auf ihren Rechner mit dem kompletten Office-Paket mitinstalliert hatten und waren sich deshalb der Gefahr auch nicht bewusst", erläutert Wüst.

"Etwa 2002 haben die Leute gemerkt, dass man Viren auch zu anderen Zwecken als zur Erlangung von Ruhm und Prestige nutzen kann. Spätestens seit zwei Jahren haben die Schadprogramme eindeutig kriminellen Hintergrund und versuchen persönliche Daten sowie andere Informationen auszuspionieren. Zudem werden E-Mail-Adressen gesammelt und an Spammer weiterverkauft", sagt Wüest. In Zukunft werden Viren zudem mobile Endgeräte wie Smartphones oder PDAs häufiger heimsuchen. "Derzeit sind uns etwa 300 Schädlinge für diesen Bereich bekannt", so der Virenexperte. Die Verbreitung und Entwicklung werde ähnlich wie in den vergangenen 25 Jahren ablaufen, jedoch bedeutend schneller. Bereits jetzt seien Handyviren im Umlauf, die beispielsweise SMS an Premiumdienste versenden oder teuere 0190-Nummern anrufen. "Die zunehmende Vernetzung dieser Geräte wird zur Beschleunigung der Verbreitung beitragen", ist Wüest überzeugt.

"Elk Cloner"-Autor Skrenta ist heute nicht mehr ganz so stolz auf seine Tat. Den Scherz aus Teenager-Tagen hat er in seinem Lebenslauf mit dem Zusatz "da war ich in der neunten Klasse!" vermerkt . Seitdem ist er als Programmierer für Unternehmen wie Sun, Netscape und AOL tätig gewesen und hat das Unternehmen Topix gegründet. Auf Journalistenfragen, ob er denn der Programmierer von Elk Cloner sei antwortet er: "Nicht zu fassen. Ich habe Adventure-Spiele, Compiler und ein Betriebsystem für den Apple-II programmiert. Und der dümmste Hack, den ich je geschrieben habe, hat am meisten Interesse erzeugt - bis heute."

Heute schätzt man die Zahl der Schadprogramme wie Viren, Würmer und Trojaner auf über 150.000, Tendenz weiter drastisch steigend. Dabei hat sich das Bedrohungspotenzial auch qualitativ erhöht. In frühen Jahren der Bedrohung mit Schadsoftware wurden Viren "im stillen Kämmerlein" eher aus Hobbyinteressen oder Geltungssucht in der Szene entwickelt. Heute stecken kriminelle Gruppierungen hinter modernen Schadsoftware-Attacken, denn "moderne" Schadsoftware hat in aller Regel eine ganz gezielte wirtschaftliche Zielsetzung, soll also auf illegalem Wege Geld verdienen.

Es kann heute sicher vorhergesagt werden, dass beispielsweise die große zukünftige Verbreitung von Funknetzwerken zu neuen Sicherheitslücken und Bedrohungspotenzialen führen wird. Wie aber ein Schadprogramm in 20 Jahren aussehen wird, weiß heute wirklich noch niemand.