Pressedokumentation - Symantec

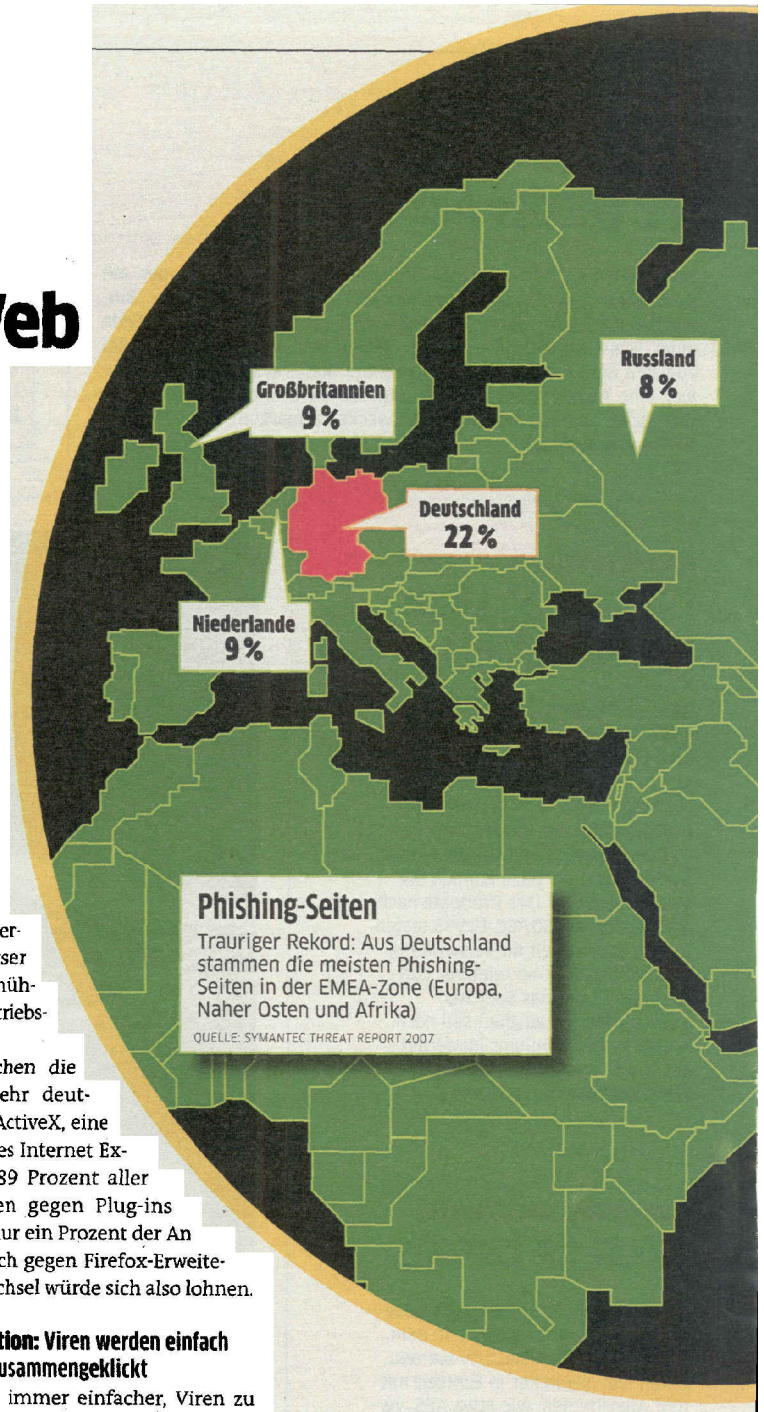
Medium (Print)	Erscheinung (Ausgabe)	Seite	Auflage (gedruckt)	Auflage (verbreitet)
CHIP	04/08	38	638.205	431.000

Brennpunkt: Gefahr aus dem Web

Angriff der Schädlinge

Es ist **EINE FLUT**, der sich kaum noch jemand in den Weg stellen kann: Allein im Jahr 2007 verdoppelte sich die Anzahl der Malware. Immer öfter spähen Datendiebe die Rechner ihrer Opfer aus

VON **AXEL SCHOEN**



Vielleicht sollte man sich einfach daran gewöhnen. An wild blinkende Internet-Warnprogramme, an Virenscanner, die im Hintergrund die halbe Rechenleistung des PCs beanspruchen. Und an nervige Rückfragen des Betriebssystems. Denn sicher ist: Die aktuelle Virenschwemme im Web wird so bald nicht abebben. Im Jahr 2007 bedrohten laut F-Secure rund 500.000 Schädlinge die Sicherheit von Computern. Selbst Anti-Viren-Programmierer können da kaum noch mithalten und haben Probleme, die Signaturen für Scantools rechtzeitig zu erneuern.

Den Surfern selbst bleibt wenig, um die eigene Sicherheit zu erhöhen: Klar, man könnte auf exotische Betriebssysteme oder Browser setzen – Apples Mac OS beispielsweise oder Opera. Webbrowser wie Opera und Safari (Mac) haben laut der Consulting-Firma Janco einen Marktanteil von rund einem Prozent. Bei einer so geringen Verbreitung lohnen sich für Hacker die Angriffe nicht.

Einfallstor: Vor allem Windows XP und der Internet Explorer ziehen Angriffe auf sich

Das beliebteste Opfer von Hack-Attacken bleibt laut F-Secure Windows XP mit einem Marktanteil von über 75 Prozent. Und Windows Vista – mit einem wachsenden Umsatzanteil von inzwischen knapp 12 Prozent – entwickelt sich zu einem immer wichtigeren Angriffsziel. Doch wer wechselt schon für ein bisschen mehr gefühlte Sicherheit den vertrauten Browser oder gar das mühsam erlernte Betriebssystem?

Dabei sprechen die Zahlen eine sehr deutliche Sprache: ActiveX, eine Komponente des Internet Explorers, zieht 89 Prozent aller Hacker-Attacken gegen Plug-ins auf sich. Aber nur ein Prozent der Angriffe richtet sich gegen Firefox-Erweiterungen. Ein Wechsel würde sich also lohnen.

Massenproduktion: Viren werden einfach per Baukasten zusammengeklickt

Zudem wird es immer einfacher, Viren zu schreiben: Profis und Laien nutzen Baukästen wie etwa MPack, die für rund 1.000 US-Dollar in zwielichtigen Foren angeboten werden. Vor allem chinesische Hacker basteln so immer wieder neue Varianten des gleichen Schädlings. Schnell, billig, mit wenig Aufwand – eine Art Massenproduktion.

Die Sicherheitsunternehmen reagieren auf die Virenschwemme: Neuerdings sollen die Schutzprogramme das Verhalten der Schädlinge erkennen, analysieren und sie dann stoppen. Durch die sogenannte „behaviour control" können auch Schad-Tools erkannt werden, die noch nicht in die Datenbanken der Sicherheitshersteller aufgenom-

DIE GESCHICHTE DES VIRUS

Der Begriff „Virus" wurde 1981 in einem Gespräch zwischen Dr. Fred Cohen und Professor Leonard M. Adleman das erste Mal verwendet.

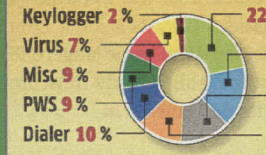
John von Neumann entwickelte die Theorie der „selbstreproduzierenden Automaten". Und bildete damit die **theoretische Basis** für alle Viren.

1949

men sind. Auch Candid Wüest, Sicherheitsexperte bei Symantec, ist überzeugt: „Die meisten Viren verraten sich durch ihr Verhalten." Das funktioniert beispielsweise ausgezeichnet bei „Drive-by-Downloads", die immer dem gleichen Muster folgen: Zunächst bringt eine Website den Internet Explorer zum Absturz, dann installiert sie einen Downloader und der lädt schließlich die Schaddaten aus dem Netz. So etwas kann man ganz einfach erkennen und stoppen. Es gibt da nur ein kleines Problem mit sehr simplen, fast schon altertümlichen Schädlingen: Um einen ganz normalen Virus an seinem Verhalten zu erkennen, muss dieser Virus auch etwas tun. Ein paar Dateien löschen, zum Beispiel. Und gerade das sollte ein Anti-Viren-Programm ja eigentlich verhindern. Abhilfe wird wohl erst die nächste Generation der Sicherheitsprogramme schaffen. Die sollen nämlich, so die Idee der Entwickler, Downloads zuerst in einer Sandbox ausführen. In diesem gesicherten Bereich wird dann geprüft, ob die Dateien halten, was sie versprechen – oder ob sie auf Zerstörung programmiert sind.

Malware-Trend

Trojaner und Downloader verdrängen die bekannten klassischen Viren.

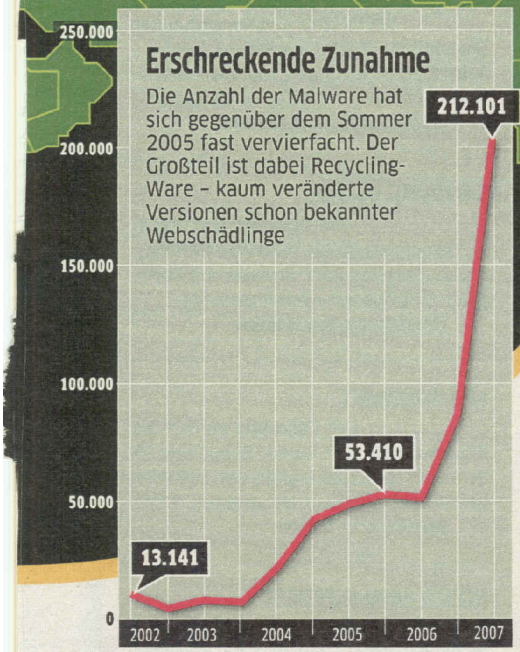


QUELLE: IBM INTERNET SECURITY SYSTEMS 2006

29 % der Botnetze weltweit sind in China

Erschreckende Zunahme

Die Anzahl der Malware hat sich gegenüber dem Sommer 2005 fast vervierfacht. Der Großteil ist dabei Recycling-Ware – kaum veränderte Versionen schon bekannter Webschädlinge



QUELLE: SYMANTEC THREAT REPORT 2007

STECKBRIEF
Die schlimmsten Internet-Betrüger

Michael Buen
Philippinischer Student und Autor des „I love You"-Virus
Der Virus richtete einen Schaden von rund drei Milliarden Euro an und nutzte Outlook zur Verbreitung

David L. Smith
Amerikanischer Programmierer des „Melissa"-Wurms
Der Makrovirus verursachte allein in den USA einen Schaden von über 80 Millionen Dollar

Tariq Al-Daour
Der Al-Qaida-Unterstützer entwickelte „Storm"
Der Student erbeutete zirka 37.000 Kreditkarten und kaufte Waren im Wert von rund 2,4 Millionen Euro ein

STECKBRIEF
Die besten Jäger der Anti-Viren Firmen

Eugene Kaspersky
Leiter der Kaspersky Lab Anti-Viren-Forschung
Er gründete 1997 Kaspersky Lab und ist Mitglied der Organisation der Computervirenforscher (CARO)

Candid Wüest
Virenforscher und Sicherheitsexperte bei Symantec
Candid Wüest ist Virenjäger bei Symantec und durchleuchtet im Forschungszentrum neue Schad-Tools

Mikko H. Hyppönen
Chief Research Officer bei F-Secure
Sein Team spürte Würmer wie beispielsweise „Sobig.F" auf, warnte vor „Sasser" und stoppte „Zotob"

1983 – Der Forscher Fred Cohen definierte in seiner Doktorarbeit „Computer Viruses – Theory and Experiment" erstmals die grundlegenden **Funktionen von Viren**.

1986 – Ein PC-Händler verbreitete mit „Brain" den ersten **MS-DOS-Virus**.

1990 – „Chameleon" war der erste **polymorphe** Virus. Er verändert sich bei jeder Infektion und war mit 9 KBit der größte speicherresistente Virus mit Tarnkappenfunktion.

2004 – Ein 18 Jahre alter Student aus Norddeutschland lässt den Sasser-Wurm auf das Internet los. Microsoft lobt sogar 250.000 Euro für Hinweise auf den Täter aus.

2005 – „Sober" war ein Massenmailer-Wurm, der sich über eine eigene **SMTP-Maschine** mit gefälschten Absenderadressen verbreitete. Er deaktivierte Anti-Viren-Tools.