CHIP-Testlabor bestätigt Berichte über den Killer-Virus

Windows-Virus "CIH" verursacht teure Schäden am PC

Ein äußerst gefährlicher Virus aus Taiwan ist in Deutschland aufgetaucht: CIH überschreibt am 26. eines Monats Teile des Startprogramms im Flash-BIOS eines Rechners und macht damit die Hauptplatine unbenutzbar, verhindert also den Neustart des Rechners. Zusätzlich überschreibt der Virus die Festplatte. Dies haben Versuche der Experten im CHIP-Testlabor bestätigt.

Die Folge der BIOS-Attacke: Beim Einschalten "hängt" der PC, noch bevor Text am Bildschirm erscheint - nur die Festplatte läuft an. Solange der Flash-Baustein nicht ausgetauscht wird, kann der Rechner nicht mehr gebootet werden. CIH ist damit der erste Virus, der es zur Beseitigung seiner Folgen erforderlich macht, den Rechner zu öffnen.
Sofern überhaupt möglich, funktioniert nach dem kostspieligen Austausch des BIOS-Bausteins über Fachhandel oder Hersteller der Rechner zwar wieder, aber der Eigentümer wird wenig Freude daran haben, weil der aus Taiwan stammende Virus auch die Daten und Systembereiche auf der Festplatte zerstört. Der nur etwa ein Kilobyte große Virus infiziert EXE-Dateien unter Windows 95 und Windows 98 und ist in Deutschland bereits auf raubkopierten CD-ROM mit Windows 98 und Office 97 gesichtet worden. Deutsche und englische Antivirenfirmen haben vereinzelte Meldungen über das Auftreten des Virus bekommen.

Wie der Virus infiziert
Der Virus ist unter Windows 95 oder 98 immer aktiv im Speicher. Dabei nutzt er eine komplizierte Technik, bei der er sich von der Anwendungsebene ("Ring 3") sofort in die abgeschottete Windows-System-Speicherbereiche ("Ring 0") einnistet, auf die er eigentlich keinen Zugriff haben sollte: Möglich machen das eine Reihe von Fehlern in Windows 95 und Windows 98. Dort kann er praktisch unsichtbar sein schädliches Werk treiben: Er infiziert jede Programmdatei, die geöffnet wird, egal aus welchen Grund. Dabei geht er sehr trickreich vor und versteckt sich in den "Hohlräumen" des von ihm infizierten Programms, also in unbenutzten Programmbereichen. Aufgrund dieser Technik ändert sich die Dateilänge der infizierten Programme nicht. Weil der Virus sich bei Bedarf auch in Stücke teilt, um mehrere Hohlräume eines Programms zu nutzen, ist er relativ schwer zu entfernen. Auch eine Folge dieser "Injektionstechnik" ist, daß im Hintergrund laufende Antivirenprogramme (die VXD-Module) den Virus mit großer Wahrscheinlichkeit übersehen. Der Grund: Mit Rücksicht auf die Performanz analysieren sie oft die Dateien nicht so gründlich wie die Festplattenscanner desselben Herstellers es tun.

Was der Virus zerstört
Die Schadensfunktion von CIH tritt jeden 26. eines Monats auf, bei einigen Versionen nur am 26. Tag eines bestimmten Monats (April, Juni). Dabei versucht er Teile des Flash-BIOS auf dem Motherboard (Hauptplatine) zu überschreiben. Gelingt ihm dies, wird der BIOS-Baustein dadurch unbrauchbar. Obwohl er physikalisch nicht zerstört ist, muß er ausgetauscht werden.
Der Virus macht in diesem Zusammenhang zusätzlich Programme und Daten auf allen lokalen Festplatten unbrauchbar, indem er die Partitionstabelle überschreibt - dies auch, falls sein Versuch, das BIOS zu überschreiben mißlingt. Die Festplatte muß danach frisch partitioniert (eingerichtet) werden, das Betriebssystem, die Anwendungen und alle Daten neu aufgespielt werden. Weitere Details siehe Anhang "Technische Einzelheiten" unten.

Fazit:
Weil einige Hersteller ein paar Pfennige an der falschen Stelle eingespart haben, ist CIH zu einer echten Gefahr für PC geworden. Denn Flash-BIOS-Chips befinden sich auch auf vielen Grafikkarten, Modems und sogar Festplatten. Das Know-how darüber, wie solche Bausteine umprogrammiert werden, ist derzeit noch nicht so weit verbreitet, doch können Assembler-kundige Virenprogrammierer diese Wissenslücke leicht schließen. Es steht zu befürchten, daß wir künftig noch mehr solcher Low-level-Attacken sehen werden. Wirklichen Schutz könnte nur Hardware-Gegenmaßnahmen wie Schreibschutzschalter bieten.

Karlhorst Klotz

Zur technischen Klärung haben beigetragen:

CHIP-Testlabor
Ieta Chi, Trend Micro (Taiwan)
Uwe Dormann, AWARD Software
Paul Ducklin, Sophos
Mikko Hypponen DataFellows
Eugene Kaspersky, KAMI
Andreas Marx, VHM & CHIP
Uwe von der Weiden, Asus

CHIP-Testlabor bestätigt Berichte über den Killer-Virus

So können Sie den Virus erkennen und entfernen

Die gängigen Virenscanner bieten noch keinen zuverlässigen Schutz gegen den Killer-Virus. Das haben Tests im CHIP-Labor ergeben.

http://www.avp.ch/

http://www.avp.ch/Nach Informationen von **CHIP online** ist das Antivirenprogramm AVP in der Version 3.0 Build 1.20 in der Lage, die derzeit drei Varianten des Virus problemlos zu erkennen. Nicht zufriedenstellend funktioniert allerdings die Reinigung, es bleiben unter Umständen Reste des Virus in Dateien zurück, so daß die Programme nicht mehr lauffähig sind. Dr Solomon's bietet einen Extra-Treiber an, um den Virus zu erkennen. jedoch nach Tests von CHIP ebenfalls nicht rückstandsfrei desinfiziert. Sophos Sweep in der Version vom Juli kann den Virus erst nachweisen, wenn die für den CIH-Virus charakteristische IDE-Ergänzungsdatei geladen wird. Von F-Prot ist noch kein Update erschienen.

CHIP-Testlabor bestätigt Berichte über den Killer-Virus

So können Sie sich schützen

Auf manchen Motherboards ist ein Schreibschutz-Jumper vorhanden, der verhindern soll, daß sich das Flash-BIOS verändern läßt. Wie Versuche im CHIP-Testcenter jedoch zeigten, funktioniert dieser jedoch nicht immer wie erwartet.

Der Anwender wiegt sich oft in falscher Sicherheit: Auf manchen Motherboards ist ein Schreibschutz-Jumper vorhanden, der verhindern soll, daß sich das Flash-BIOS verändern läßt. Wie Versuche im CHIP-Testcenter jedoch zeigten, funktioniert dieser jedoch nicht immer wie erwartet. Andere Motherboards besitzen den Jumper auch gar nicht mehr - oder man kann den Schreibschutz nur per Software einstellen.

CHIP-Empfehlung 1:
Falls vorhanden, sollte der Schreibschutz-Jumper aktiviert werden - schaden kann das nicht, und wenn es wirkt, ist der Rechner damit auch gegen Attacken von CIH-Varianten oder -Nachfolgern sicher, die vielleicht künftig auftauchen.

Da die Hardware keinen sicheren Schutz bietet, sollte immer aufmerksam gescannt werden, besonders wenn neue Windows-95- oder -98-Anwendungen aus unsicherer Quelle (z.B. Internet) auf dem Rechner installiert werden.

CHIP-Empfehlung 2:
Verlassen Sie sich nicht auf Ihre Hintergrund-Scanner. Überprüfen Sie neue Windows-Programme vor und nach der Installation, indem Sie die Festplatte scannen.

CHIP-Testlabor bestätigt Berichte über den Killer-Virus

Diese Faktoren beeinflussen den "Erfolg" der BIOS-Attacke

Für eine erfolgreiche BIOS-Attacke müssen offensichtlich mehrere Faktoren zusammenspielen:

1. Die Funktion des Motherboard-Chipsets
Manche Hersteller integrieren spezielle Hardware-Schutzschaltungen, so daß das Standard-Verfahren zum Schreiben des Flash-EPROMs nicht funktioniert.

2. Die Funktion des Flash-EPROM-Chips
CIH benutzt ein Kommando um einen Speicherblock zu löschen, das mindestens auf den EPROM Chips Intel 28F010 und dem Macronics MXIC funktioniert. Welche anderen Flash-EPROM-Typen betroffen sind, steht derzeit noch nicht fest.

3. Das BIOS-Programm
Auch wenn der Virus immer die gleichen BIOS-Adressen überschreibt, können die Effekte bei verschiedenen BIOS-Familien (AWARD, AMI, Phoenix) unterschiedlich sein, da an derselben Adresse unterschiedliche Routinen stehen können und nicht alle Routinen zum Start des Rechners benötigt werden.

4. Die Spannungsversorgung für das Flash-EPROM
Manche Chips brauchen 12 Volt zum Schreiben, werden sie per Jumper-Stellung nur mit 5 Volt versorgt, sind sie vor dem Überschreiben geschützt. Andere Chips können bei beiden Spannungen beschrieben werden. Einige Hersteller liefern ihre Systeme grundsätzlich im beschreibbaren Zustand aus.

5. Schreibschutz-Jumper
Falls überhaupt ein Schreibschutz-Jumper vorhanden ist, wirkt er trotzdem nicht immer. Manche Flash-EPROM-Typen werten Schreibschutz-Signale an Steuerleitungen aus, andere nicht. Generelle Aussagen über Motherboard-Typen sind nicht möglich, denn selbst bei der Produktion einer Motherboard-Serie werden je nach Verfügbarkeit und Preis verschiedene Flash-EPROM-Bausteine eingesetzt.

6. Das Timing
Üblicherweise "flashen" die Hersteller nicht von Windows aus, weil beim Schreiben auf die genaue zeitliche Abfolge geachtet werden muß, was unter Windows nicht gewährleistet ist. Der CIH-Virus läuft unter Windows und könnte deshalb gelegentlich Probleme haben, das BIOS zu überschreiben, weil die Ausführung durch den Windows-Overhead zeitlich nicht korrekt abläuft.