Pressemitteilung

PM 02 (2000)
Stand 05. Mai 2000

Schutz vor Internet-Wurm

„ILOVEYOU“ legt weltweit Rechner lahm

Am Donnerstag, den 4.5.2000 wurden in wenigen Stunden tausende PCs weltweit von einem neuen Software-„Wurm“ befallen. Dieses in der Programmiersprache „Visual Basic“ offenbar von einem Programmierer auf den Philippinen entwickelte und in die Welt gesetzte Programm, das sich über E-Mail-Nachrichten mit dem Betreff "ILOVEYOU" verbreitet, hat innerhalb eines Tages viele zehntausend Computer infiziert und allein in den USA einen geschätzten Schaden von mehreren Milliarden Dollar verursacht.

Ein solcher „Wurm“ unterscheidet sich von einem Computervirus dadurch, dass er keine „Wirtsdatei“ (wie ein Programm oder ein Textdokument) für seine Verbreitung benötigt. „Würmer“ verbreiten sich, wie der Name andeuten soll, aus eigener „Kraft“: Sie nutzen die Kommunikationsdienste des befallenen Computers, um sich in andere Systeme einzuschleichen. Diese aktive Komponente macht sie um ein Vielfaches gefährlicher als herkömmliche Viren, die sich nur über die Weitergabe der „Wirtsdatei“ durch einen Benutzer verbreiten können.

Die Technik, die der nach seinem Betreff „ILOVEYOU“ getaufte „Wurm“ verwendet, ist nicht neu; einen ähnlichen Mechanismus verwendete auch der "Melissa"-Wurm, der Mitte des vergangenen Jahres in die Schlagzeilen geriet, nachdem er bei einer Vielzahl großer Unternehmen, nicht zuletzt bei Microsoft, für Stunden die Kommunikation lahmlegte.

"ILOVEYOU" verbreitet sich, indem er automatisch an alle Adressen, die er im Adressbuch des E-Mail-Programms „Outlook“ auf einem befallenen Rechner findet, eine E-Mail sendet, an die er sich selbst als „Anhang“ anhängt. Die E-Mail enthält nur eine Textzeile mit folgendem Inhalt:

„kindly check the attached LOVELETTER coming from me."

Als Absender wird – infamerweise – die Adresse des Benutzers des befallenen Rechners verwendet: Dadurch entsteht beim Empfänger der Eindruck, er erhielte eine Nachricht von einem ihm bekannten (und vertrauenswürdigen) Sender.

Startet man die anhängende Visual Basic-Datei, wird der „Wurm" aktiv: Zunächst sorgt er für seine eigene Verbreitung, anschließend ruft er seine Schadensfunktion auf. Er ändert die Konfiguration des Internet-Explorer so, dass beim nächsten Programmaufruf automatisch ein ausführbares Programm namens "WIN-BUGSFIX.EXE" über das Internet geladen und beim darauffolgenden Neustart von Windows ausgeführt wird. Dieses Programm sammelt alle Windows-Passwörter des Benutzers und schickt sie per E-Mail an die E-Mail-Adresse „mailme@super.net.ph" (Philippinen).

Da viele Benutzer des weit verbreiteten E-Mail-Programms „Outlook" die Standardkonfiguration verwenden, bei der eine automatische Ausführung von E-Mail-Anhängen erfolgt, konnte sich der Wurm mit rasender Geschwindigkeit verbreiten: Schon das Öffnen der eingegangenen Nachricht aktiviert in diesem Fall den Wurm.

Noch am Tag des ersten Auftauchens von „ILOVEYOU" wurden zwei Varianten des Wurms im Internet verbreitet: Eine verwendet die Betreffzeile "Joke" oder "fwd: Joke"; der Anhang heisst "Very Funny.vbs". Die zweite Variante trägt die Betreffzeile "Funny News". Da der Wurm in einer recht einfachen Sprache programmiert wurde, muss davon ausgegangen werden, dass in Zukunft neue Varianten des Wurms auftauchen werden, möglicherweise mit schlimmeren Schadensfunktionen.

Maßnahmen zum Schutz vor „ILOVEYOU"-Wurm

Da der „ILOVEYOU"-Wurm in Visual Basic geschrieben ist, wird er nur auf Windows-Systemen ausgeführt, bei denen die Ausführung von Visual Basic-Skripts zugelassen ist. Ist "Windows Scripting Host" (WSH) abgeschaltet, kann der Wurm nicht aktiv werden.

Grundsätzlich sollte darauf geachtet werden, dass E-Mail-Programm und WWW-Browser unter Windows so konfiguriert sind, dass keine aktiven Komponenten ("Active Scripting"), weder auf Webseiten noch in E-Mail-Anhängen, ausgeführt werden. Gefahr geht dabei nicht nur von Visual Basic, sondern auch von JavaScript-Komponenten aus.

E-Mail-Anhänge mit der Endung „.exe“ sollten weder automatisch noch manuell gestartet werden, wenn nicht sichergestellt ist, dass es sich um kein schadenstiftendes Programm handelt. Bekannte Würmer lassen sich zudem an der Betreffzeile der E-Mail-Nachricht erkennen und sollten ungeöffnet gelöscht werden.

Im Internet werden derzeit Skripte verbreitet, die ein automatisches Löschen des Wurms von einem befallenen System versprechen. Da solche „Rettungsprogramme“ oft selbst Viren oder Würmer enthalten, ist hier äußerste Vorsicht geboten: Wenn die Herkunft der „Rettungsmaßnahme“ nicht vertrauenswürdig erscheint, sollte man von einer Ausführung dieser Programme unbedingt absehen – will man nicht vom Regen in die Traufe kommen.

Anti-Viren-Programme bieten einen weiteren Schutz, indem sie bekannte Würmer und Viren erkennen und deaktivieren. Alle Hersteller solcher Programme haben innerhalb von 24 Stunden aktualisierte Versionen ihrer Software veröffentlicht, die Schutz vor „ILOVEYOU“ und Varianten bieten.

Einer der schlimmsten Schäden, den ein Wurm verursacht, sind die Kosten, die durch die Beschäftigung mit dem Phänomen und seiner Beseitigung in hunderten oder tausenden von Unternehmen entstehen. Die verursachten Produktivitätsausfälle gehen auch in Deutschland zweifellos in die Millionen. Daher ist die Verbreitung solcher Programme kein Bubenstreich oder Kavaliersdelikt, sondern kriminelles Verhalten.

Dirk Fox, Stefan Kelm
Secorvo Security Consulting GmbH

(4710 Zeichen im Pressetext)

Weitere Informationen:

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe

Tel. +49 721 6105-452
Fax +49 721 6105-455
E-Mail info@secorvo.de
http://www.secorvo.de