Feind liest mit - Geheime Lauschangriffe können entdeckt werden

08.04.2008, 12:16 | IT, New Media & Software

Pressemitteilung von: *Fachverlag für Computerwissen*

Bonn – Im Internet herrscht Krieg. Allein in deutschen Unternehmen sind schätzungsweise eine Dreiviertel Million PCs von Spionage-Trojanern unterwandert. Ihr Ziel: unbemerkt sensible Geschäftsdaten ausspähen und sie an den Angreifer senden, ohne dass die Übertragung zurückverfolgt werden kann.

Schuld sind die Angegriffenen häufig selbst, berichtet der IT-Sicherheits-informationsdienst „mIT Sicherheit“ (www.mit-sicherheit.de) aus dem Fachverlag für Computerwissen. „Die meisten Infektionen mit Spyware sind das Resultat zu hoher Benutzerrechte, mit denen Anwender im Alltag arbeiten.“ Der Rat des Infodienstes an Systemverantwortliche: „Achten Sie penibel darauf, dass Benutzer grundsätzlich nur unter User-Rechten arbeiten. Dies erschwert es Spionagesoftware enorm, sich zu installieren.“

In diesem Zusammenhang hält „mIT Sicherheit“ die erregte Diskussion um den Bundestrojaner für Panikmache. „Auch die Entwickler dieser staatlichen Schnüffel-Software können sich nicht über die Grenzen der Technik hinwegsetzen.“ Sie müssten damit leben, dass Spionagesoftware mit Tarnkappenmechanismus auffindbar ist.

Mittlerweile gebe es ein ganzes Waffenarsenal, um Schadsoftware zu enttarnen, auch wenn sie sich per Rootkit-Techniken tief im System verankert. Ausgangsbasis der Suche nach Spyware ist der Einsatz eines Virenscanners, der auch Rootkits entdecken kann. Außerdem sollte die Firewall so eingestellt werden, dass wirklich nur die Daten gesendet werden können, die man selbst benötigt.

Als nützliche Waffe gegen verdeckte Spyware hat sich nach Erfahrungen von „mIT Sicherheit“ der kostenlose „RootkitRevealer“ von Sysinternals (www.sysinternals.com) erwiesen. Das kostenpflichtige Programm „EnCase“ entdeckt sogar gelöschte und vor dem Betriebssystem versteckte Dateien. Der kostenlose „Rootkit Unhooker“ entdeckt und entfernt getarnte Software, die sich an der API-Schnittstelle von Windows zu schaffen macht.

Die Tools haben laut „mIT Sicherheit“ allerdings selbst alle einen schwachen Punkt: Sie liefern sehr schnell Fehlalarme. So werden z.B. oft Treiber als potenzielle Rootkits angezeigt. Eine unüberlegte Deaktivierung kann dann den Absturz des Computers zur Folge haben.

mIT Sicherheit
Fachverlag für Computerwissen
08.04.2008

"mIT Sicherheit" informiert monatlich auf 12 Seiten über alle relevanten Entwicklungen zum Thema Netzwerk-, IT- und Internetsicherheit. Erhältlich ist die Zeitschrift im gut sortierten Fachbuchhandel oder beim Kundenservice des Verlags unter info@computerwissen.de bzw. unter der Telefonnummer 0228 / 9555 01 90.
Weitere Bestellinformationen finden Sie unter www.mit-sicherheit.de

Portrait

Über Fachverlag für Computerwissen:
Der Fachverlag für Computerwissen gehört zur Verlagsgruppe des Verlag für die Deutsche Wirtschaft AG, zu der insgesamt 10 Fachverlage zählen. Die
Loseblattzeitschriften, Informationsdienste und Online-Portale des Verlages ergänzen und flankieren individuelle Beratung und Seminarangebote. Gemeinsam mit dem Schwesterunternehmen, dem FID Verlag GmbH Fachverlag für Informationsdienste, belegte der Verlag für die Deutsche Wirtschaft AG laut Ranking des Buchreportes vom März 2008 "Die 100 größten deutschen Verlage" mit Rang 6 wieder einen Platz unter den Top 10 der Fachverlage und Rang 12 unter allen deutschen Verlagen.

News-ID: 201857 • Views: 1366 (Stand: 29.07.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/201857/Feind-liest-mit-Geheime-Lauschangriffe-koennen-entdeckt-werden.html