

Virtuelle
Honeypots locken
Eindringlinge ins
eigene Netzwerk,
um ihre ver-
räterischen Spuren
zu speichern.

Honeypots: Schädlingsfalle im Internet

**Mit virtuellen
Honigtöpfen lassen
sich Daten über
unerwünschte
EINDRINGLINGE
sammeln – und über
Mitarbeiter, die sich
im eigenen Netz allzu
neugierig umsehen.**

TEXT: LUCY TRAUHMÜLLER

Die süßesten Früchte werden nicht nur von den großen Tieren gefressen: Oft erweisen sie sich auch als giftig. Dass das im Internet nicht anders ist als im Leben, überrascht vielleicht weniger als die Tatsache, dass eine ganze Technologie auf dieser Wahrheit beruht. Honeypots – virtuelle Honigtöpfe – täuschen Server oder Programme vor, die ungeschützt im Internet stehen und Angreifer anziehen sollen wie der Honig das Insekt. Dabei werden den Ködern IP-Adressen (Adressen von Rechnern im Internet) zugewiesen, die der normale, sprich berechnete, Nutzer nicht verwendet. Wer auf einem Honeypot landet, outet sich also per se als unerwünschter Eindringling, der das IT-System nach Schwachstellen abklopft. Doch anstatt sein Ziel zu erreichen, das darin besteht, Informationen aus dem System zu fischen, hinterlässt der ungebetene Gast Spuren: Seine Daten werden – meist im Rahmen von wissenschaftlichen Projekten – protokolliert und ausgewertet, wodurch wertvolle Auskünfte über Viren und Würmer im Netz gewonnen werden. Der akademische Erkenntnisgewinn ist hoch, doch benötigen Unternehmen Honeypot-Systeme für ihre Si-

cherheit? Für große Institutionen, die überdurchschnittlich exponiert sind, können Honeypots interessant sein, berichtet Christian Mock, technischer Leiter des auf Sicherheitslösungen spezialisierten Unternehmens Coretec. Mit seiner Lösung zur Erkennung von Eindringlingen, in die Honeypot-Elemente integriert sind, zählt er Krankenhäuser und Ministerien zu seinen Kunden. Kostenpunkt: 16.000 Euro. Und eine Nummer kleiner geht nicht: „Es gibt keine Honeypot-Suites von der Stange, und in Österreich bietet niemand Honeypots allein zum Verkauf an“, erklärt Josef Pichlmayr, Geschäftsführer des Security-Software-Anbieters Ikarus.

Billiger mit Open Source. Wer es dennoch mit Honeypots versuchen will, kann auf Open-Source-Produkte zurückgreifen. Das bekannteste ist honeyd, das unter www.honeyd.org kostenlos heruntergeladen werden kann und ein leicht angreifbares Netzwerk simuliert. „Ein kompetenter IT-Mitarbeiter benötigt für die Installation zirka einen Tag, und vermutlich kann es auch jedes Systemhaus aufsetzen“, so Jürgen Stöger, Security-Consultant beim Unternehmen Secur Data. Doch die Installation ist erst der Anfang. Um Angriffsmuster erkennen zu können, müssen die Daten aus-

gewertet werden. Der damit verbundene Aufwand ist schwer festzulegen, denn Sicherheit kann, um es mit Bernhard Fischer, IT-Security-Dozent an der FH St. Pölten, zu sagen, „ganz oberflächlich oder à la Fort Knox sein. Honeypots sind aber auf jeden Fall ein weiteres System, das am Laufen gehalten werden muss.“ Ohne Betreuung läuft also gar nichts – nicht gerade verlockend für KMU mit wenig IT-Personal. „Wer Honeypots installiert, exponiert sich automatisch, denn er ist ja daran interessiert, sich möglichst viele Viren ins Netz zu holen, gibt Pichlmayr ebenfalls zu bedenken.

Interne Spione fangen. Für Unternehmen interessant können Honeypots sein, die firmenintern eingesetzt werden, um allzu neugierige Insider, in der Regel eigene Mitarbeiter, zu fangen. Hierzu wird ein Honeypot im internen Netz platziert, der vor Zugriffen von außen – dem Internet – sicher ist. „Wenn ein Mitarbeiter das interne Netz durchstöbert, kann dieser Honeypot aber gefunden werden und einen Alarm auslösen“, erläutert Christopher Kruegel, Dozent an der Technischen Universität Wien. „Interne Honeypots sind in größeren Unternehmen mit hoher Nutzeranzahl bereits im Einsatz – auch in österreichischen.“ ■