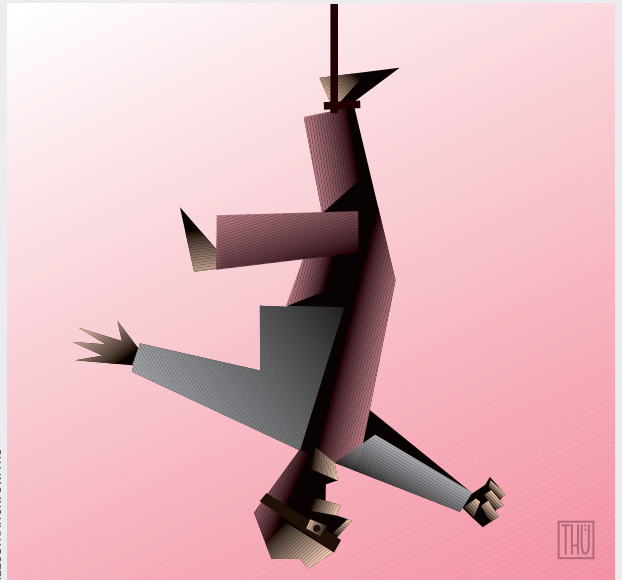


IT-SECURITY

Fallenstellen mit System

Jede Woche beantworten Sicherheits-
experten Leserfragen und geben
Ratschläge, wie sich die Sicherheit in
einem Unternehmen erhöhen lässt.

ILLUSTRATION: CW/THU



Frage: Was ist ein Honeynet und wozu dient es?

Ein Honeynet ist ein hochinteraktives Netzwerk, das speziell entwickelt wurde, um Informationen über «Gegner» (Cracker und Hacker) zu sammeln. In der Vergangenheit wurden Honeynets nur zur Irreführung oder zur Erkennung von einzelnen oder spezifischen Angriffen benutzt. Heutzutage sind Honeynets zwar ähnlich aufgebaut wie früher – was bedeutet, dass noch immer Systeme, bekannte Dienste und Schwachstellen emuliert oder aber beschränkte Umgebungen zur Verfügung gestellt werden. Aber die Zielsetzung hat sich verändert. Der Zweck bezieht sich nicht mehr hauptsächlich auf das Aufspüren (Tracking) oder das Irreführen von Angreifern, sondern auf das Sammeln von Informationen über zukünftige Bedrohungen, sprich über Methoden und Mittel der Hacker Community.

Hinsichtlich der Definition unterscheiden sich heutige Honeynets: Entweder werden die Services nur emuliert (z.B. mit Honeyd), oder es werden reale Systeme, bestehend aus Servern und Netzwerkkomponenten bereitgestellt, welche Services anbieten, wie sie in

gleicher oder ähnlicher Form auch in den produktiven Netzen vorkommen:

Den Angreifern wird ein ganzes Netzwerk mit mehreren Systemen und Anwendungen «zur Verfügung gestellt» oder nur emuliert, um somit eine realistische Situation erzeugen zu können (produktives Netz). Im Honeynet selber können verschiedene Systeme gleichzeitig im Betrieb sein. Damit wird eine realistische Simulation eines produktiven Netzwerkes erzeugt. Je unterschiedlicher die Systeme und Anwendungen im

Entweder werden die Services nur emuliert oder es werden reale Systeme, bestehend aus Servern und Netzwerkkomponenten bereitgestellt.

Honeynet sind, umso mehr Angriffsmethoden, Werkzeuge und Vorgehensweisen können in Erfahrung gebracht werden.

Ein Honeynet besteht aus Standardsystemen – Systemsetups wie sie hundertfach im Internet gefunden werden können. Die Schwachstellen sind in einem Honeynet genau gleich wie in einem normalen produktiven Netz, es werden also keine speziellen Dienste emuliert und die Systeme werden nicht mit Sicherheitslücken präpariert,

welche das System angreifbarer machen. Ein Honeynet läuft somit parallel und unter den gleichen Bedingungen wie das produktive Netzwerk. Ein heutiges Honeynet ist ein Forschungswerkzeug im Security-Umfeld, um einerseits das produktive Netzwerk parallel updaten zu können und es somit so sicher wie möglich betreiben zu können. Andererseits ist es ein Know-how-Spender, um den «Gegner» kennen zu lernen.

Security Systeme, wie sie in vielen Firmen eingesetzt werden, sind rein defensiv. Der Sinn

Bereitstellen einer vermeintlich produktiven Umgebung anzulocken um damit Erkenntnisse über Angriffsmuster und Motive, wie auch Werkzeuge und Code-Segmente zu erhalten. Die dadurch gewonnenen Informationen können danach dazu verwendet werden, die eigenen produktiven Systeme vor derartigen Angriffen besser zu wappnen.

So gesehen ist ein Honeynet ein Werkzeug mit vielen Facetten. Hier möchten wir es dazu benutzen, um schneller auf heutige und zukünftige Bedrohungen reagieren zu können. Denn durch die Analyse kompromittierter (geknackter) Systeme, welche in einem Honeynet immer wieder vorkommen, hat man alle Antworten, die man braucht, um sich zu schützen und Angreifern die Stirn zu bieten. ■



Der Autor
Oliver Gruskovnjak ist Consultant und OPST bei der Sicherheitsberaterin Oneconsult, Bern. www.oneconsult.com

Unsere Experten beantworten Ihre Fragen. Schreiben Sie uns: it-security@computerworld.ch

Ein Archiv der Helpdeskartikel finden Sie im Internet: www.computerworld.ch