LINUX MAGAZIN 12/09

LINUX MAGAZIN

Mit **DELUG-DVD**
Doppelte Kapazität - 7,5 GByte

Asterisk-Appliance
Final-Versi… d
Telefonanl…

NST 2…
ISO und Sof… Appliance
der „Network Security Toolkit"-Distribution

…, Python
Zwei komplette E-Books

Linuxcon 2009
3,5 Stunden Linus T. & Co.

Sonderdruck

Bash-Stümperei mit Passwörtern und »/tmp« S. 100

Hallo?
Ein proprietäres Plugin dockt Asterisk jetzt an die Skype-Welt an. S. 62

Linux and the City

Großer GPS-Wegweiser: Freie Karten und Tools für Handys und Netbooks

Moderne E-Mail

- Charly archiviert seine Inbox S. 67
- Caldav organisiert Push und Sync von Termindaten S. 68
- Lemonade-Standard: IMAP-Extensions für mobile Clients S. 74
- Thunderbird 3 im Anflug S. 78

KDE: Die Landung der Plasmoide

Programmier-Workshop zur geglückten Invasion der Plasma-Widgets. S. 110

Deutschland € 8,50 | Österreich € 9,35 | Schweiz sfr 17,- | Benelux € 9,85 | Spanien € 11,05 | Italien € 11,05

4 196892 708509 12

Infotainment
Datenträger enthält nur Lehr- oder Infoprogramme

Honeybox-Appliance von Secxtreme im Test

Lockstoff

Intrusion Detection gilt Admins als wartungsintensive Technik, da sie viele Fehlalarme auslöst. Meldet sich hingegen ein Honeypot zu Wort, hat tatsächlich ein unberechtigter Zugriff stattgefunden. Bislang galten die klebrigen Fallen aber als aufwändig zu konfigurieren. Die Honeybox von Secxtreme tritt an, das zu ändern. Jörg Fritsch


© Richard Blaker, Fotolia.com

Seit spätestens 2006 ist es um Honeypots ruhig geworden. Der Hersteller Symantec beispielsweise hat sein kommerzielles Produkt Mantrap eingestellt [1], andere betreiben noch Webseiten, auf denen Kunden veraltete Produkte aus dem Jahr 2004 bestellen können, oft für Windows. Ähnlich ist es den zahlreichen Open-Source-Varianten ergangen, die in dieser Zeit versucht haben, das damals vorhandene Verlangen nach den hippen Honeypots zu stillen [2]. Ihre Befürworter positionierten diese Technik als ein Werkzeug, um den Netzwerk-Perimeter, also den Übergang zwischen wohlbehütetem internen Netz und dem gefahrvollen Internet zu verteidigen.

Sie wollten Angreifer wie in einem Spionageroman beobachten. Doch bald kamen Netzverantwortliche zu dem Schluss, dass durch Extranets, mobile Benutzer und komplexe Internetanwendungen der Perimeter immer mehr an Bedeutung verliert. Schließlich gilt es, nicht primär den Netzübergang zu schützen, sondern die Daten, ganz egal, wo sie sind.

Mit martialischer Perimeter-Verteidigung war es aus – und auch fast mit den Honigtöpfen. Einzig das Honeyd-Projekt [3] hat überlebt und versucht sich in Literatur und experimenteller Praxis als Alternative zu herkömmlichen Intrusion-Detection- und Intrusion-Prevention-Systemen (IDS/IPS) zu definieren [4].

Betriebsfertiger Honigtopf

Seit Anfang 2009 bietet das Münchner Unternehmen Secxtreme die auf dem Honeyd basierende Honeybox-Appliance an [5]. Sie versteht sich als Gegenentwurf zur Intrustion Detection. Der Hersteller behauptet, dass Netzadmins durch ihren Einsatz bessere Resultate bei niedrigeren Preisen erzielen als mit IDS/IPS-Systemen. Das Linux-Magazin hat sich in seinem Testlabor eine Woche lang mit der Honeybox auseinandergesetzt, um das zu überprüfen.

Die Appliance (siehe Abbildung 1) setzt nach der Konfiguration eine Anzahl virtueller Low-Interaction-Honeypots auf

Secxtreme Honeybox

- **Hersteller:** Secxtreme, Taufkirchen [5]
- **Sensor-Appliance:** Grundmodell ist eine 19-Zoll-Hardware-Appliance mit vier Netzwerkports. Sie baut auf einer Nexcom NSA1042N8 auf, hat eine Intel-Celeron-M370-CPU mit 1,5-GHz, 1 GByte DDR2-SDRAM und eine 160-GByte-SATA-II-Festplatte.
- **Management:** Das Verwaltungs-GUI ist für größere Installationen auch ohne Sensoren als so genannte 0-Port-Variante und als reine Softwarelösung erhältlich. Verteilte Sensoren senden ihre Logs an solche Stationen.
- **Lieferumfang:** Die Hardware-Appliance kommt zusammen mit einem seriellen Kabel, vier Ethernet-Kabeln, Installationszubehör und einem USB-Stick mit Recovery-Funktion, einem 200-seitigen Handbuch als PDF sowie weiteren Unterlagen zur Hardware. Die Softwareversion, die nur Management beherrscht, liefert Secxtreme auf CD-ROM aus.
- **Virtualisierung:** Die Softwarevariante startet von CD und installiert ein gehärtetes Debian-System. Der Einsatz als virtuelles Image ist vom Hersteller nicht offiziell supportet.
- **Wartung:** Enthält Zugang zum Updateserver, der Debian-Pakete und eigene Software aktualisiert. Support per Telefon und E-Mail.
- **Preise:** Secxtreme verkauft die Honeybox durch Partner im Rahmen individueller Projekte. Der Listenpreis für die 4-Port-Appliance inklusive einem Jahr Wartung ist 8925 Euro brutto, jedes Folgejahr kostet 1190 Euro, die Softwarevariante 3451 Euro. Eine Gewährleistungsverlängerung auf drei Jahre kostet 357 Euro, ein Austausch am nächsten Tag 1012 Euro für den gleichen Zeitraum.

Abbildung 1: Die Honeybox von Secxtreme gibt es als Software- und Hardware-Appliance. Das Standardmodell besitzt vier Netzwerkports.

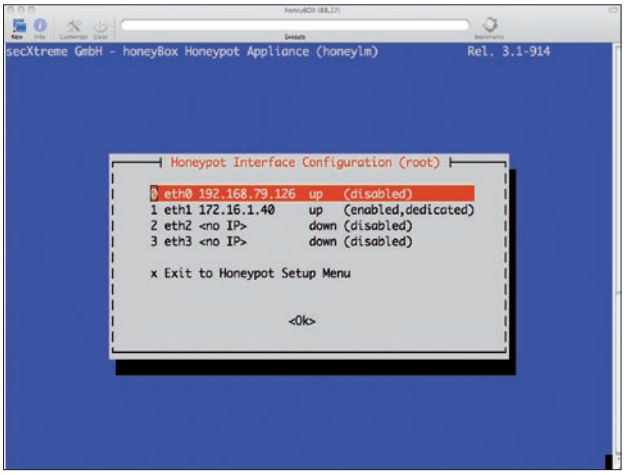

Abbildung 2: Eingangs konfiguriert der Admin die Überwachungsports der Honeybox-Appliance. Interface »eth0« ist das Out-of-Band-Interface für das Management, die anderen stehen als Sensoren zur Verfügung.

(siehe Kasten „Honeypots in allen Geschmacksrichtungen“). Dabei lassen sich auf einem physikalischem Sensorinterface mehrere Hundert virtuelle Honeypots mit jeweils eigenen IP-Adressen konfigurieren, die für den Angreifer zunächst wie echte Systeme aussehen.

Die Erstinstallation der Honeybox erfolgt über das serielle Interface mit einem Setup-Tool, dessen Benutzerführung ähnlich einem Debian-Installer (die Appliance basiert auf Debian) oder Yast von Open Suse funktioniert. Als Hürde erwies sich, dass Debian mit UTF-8 als Zeichensatz arbeitet und die Masken und Menüs des Installers bei älteren Terminalprogrammen mit einem anderen Encoding nicht zu erkennen sind. Der Hersteller hat auf Nachfrage hier weitergeholfen und auf Seite 126 seines Handbuchs verwiesen. Netzwerk- und Sicherheitsadministratoren, die mit virtuellen Honeypots vertraut sind, konfigurieren die Honeybox danach ohne weitere Hürden.

Bis auf die Lizenz ist alles vorinstalliert und der Systemverwalter konfiguriert lediglich die Honeybox für ihre zukünftige Umgebung. Er richtet ein Out-of-Band-Administrationsinterface und bis zu drei Sensorinterfaces in dedizierte Subnetze ein. Abbildung 2 zeigt den Honeypot mit einem Out-of-Band-Interface mit deaktivierten Funktionen und einem aktiven Sensorinterface.

Wenn bei der Installation etwas schiefgeht, darf der Admin die Appliance mit dem mitgelieferten USB-Stick auf die Fabrikeinstellungen zurücksetzen. Ist die Installation geglückt, aktualisiert die Software der Appliance sich per HTTP vom Updateserver des Herstellers. Dazu benötigt sie natürlich eine bestehende Internetverbindung.

Fühler austrecken

Auf jedem Sensorinterface darf der Admin mehrere virtuelle Honeypots mit eigenen virtuellen IP-Adressen konfigurieren. Alle Honeypots auf einem Interface müssen sich dasselbe Subnetz teilen, können aber verschiedene Systeme emulieren. So lässt sich zum Beispiel eine Lockfalle konfigurieren, die einen IIS-Webserver vorgaukelt, und eine andere, die vorgibt, ein Cisco-Router zu sein. Der Admin bestimmt durch das Zuweisen von Templates, welcher virtuelle Honeypot was emuliert. In der getesteten Version 3.1-914 der Honeybox gab es 22 verschiedene Templates (siehe Tabelle 1).

Laut Hersteller sollten Anwender Honeyboxen in demilitarisierten Zonen (DMZ), in der Nähe der Firewall oder in vertrauenswürdigen internen Segmenten des LAN einsetzen. Dort erkennt das Frühwarnsystem Angreifer, aktive Trojaner, Viren oder Würmer, sobald sie auf einen der virtuellen Köder anbeißen.

Aufgrund der Position im Netzwerk und des Prinzips von Honeypots meldet die Honeybox nur echte Angreifer, echte Viren oder Trojaner, die unerkannt im Netzwerk aktiv sind. Die Honeybox liefert also keine falschen Alarme. Im Gegensatz zu vielen IDS/IPS-Systemen ist ihr Normalzustand, dass sich nichts tut und sie keine Arbeit macht. Auch haben es die Tester als angenehm empfunden, dass die Honeypots keine Policy und kein Tuning erfordern. In der Praxis ist das eine wertvolle Eigenschaft.

Zum Test hat das Linux-Magazin die Honeybox einige Tage ungeschützt ins

Tabelle 1: Emulierte Profile

Menü	Emuliertes System	Menü	Emuliertes System
cisco	Cisco IOS 12.1	sol27	Sun Solaris 2.7 Host
cray	Cray Super Computer	sol28	Sun Solaris 2.8 Host
default	Generisches Default-Template	win2k2e	Windows 2000 Server mit SP2 und MS Exchange
hplj	HP Laserjet Printer	win2k2	Windows 2000 Server mit SP2 und Default-Services
hppc	HP Procurve Switch	win2k3	Windows 2000 Server mit SP3 und Default-Services
stealth	Stealth-Template (antwortet nicht, simuliert eine Drop-Policy)	win2k4i	Windows 2000 Server mit SP4 und IIS
suse10	Suse Linux System, Version 10.0	win2k4	Windows 2000 Server mit SP4 und Default-Services
suse7	Suse Linux System, Version 7.0	win2k1i	Windows 2000 Server mit SP1 und IIS5, SSH
suse8	Suse Linux System, Version 8.0	win2k1s	Windows 2003 Server mit SP1 und SSHv2
suse82	Suse Linux System, Version 8.2	win2k4ws	Windows 2000 Professional Workstation mit SP4
osx10	Macintosh mit Mac OS X	winxp1	Windows XP Workstation mit SP1

Honeypots in allen Geschmacksrichtungen

Die Literatur teilt die verführerischen Fallen in mehrere Kategorien ein. Physikalische Honeypots sind konkrete Systeme, die keine Anwendungen emulieren. Alle Dienste, die potenzielle Angreifer anlocken, laufen tatsächlich auf dem System. Angreifer kommunizieren mit ihnen wie mit einem echten System. Im Gegenzug hat der neugierige Netzüberwacher die Möglichkeit, das Vorgehen und die Tools von Angreifern detailliert zu überwachen.

Obwohl Admins mittels Xen oder KVM pseudo-physikalische Honeypots vergleichsweise einfach einrichten und überwachen, stellt sich die Frage, wer ernsthaft daran interessiert ist, die Vorgehensweise von Angreifern zu erforschen. Da dies Zeit, Aufmerksamkeit und damit Geld kostet, ist die weite Verbreitung dieser Varianten ungewiss.

Virtuelle Honeypots simulieren reale Server. Low-Interaction-Honeypots beschränken sich dabei nur auf einen Teil eines echten Systems und emulieren zumeist den Networkstack, die MAC-Adresse und bestimmte Daemons. Sie lassen sich nicht dazu verwenden, um Angreifer auszuspionieren. Mit der Installation von Low-Interaction-Honeypots erkauft sich der Admin aber Zeit, die er dazu nutzen kann, um zum Beispiel seine Produktivumgebung in Sicherheit zu bringen: Während ein ungebetener Gast versucht einen erfolgreichen Angriff beim Honeypot zu landen, spielt der Admin schleunigst die fehlenden Sicherheitspatches ein. Wie lange sich der Angreifer mit einem Honeypot aufhält, hängt erfahrungsgemäß selten davon ab, ob es sich um einen virtuellen oder einen physikalischen Honeypot handelt.

Internet gestellt, um Logeinträge und Screenshots zu erhalten. Als Ergebnis meldete das System pro Tag rund sechs Angreifer, von denen sich zwei längere Zeit mit dem Honypot beschäftigt haben. Die Appliance überwacht alle konfigurierten virtuellen Honeypots und schreibt für jede versuchte Kontaktaufnahme, sei es mittels ICMP, ARP oder durch den Zugriff auf emulierte Daemons und Services, einen Eintrag ins eigene Logfile.

Alarm nur bei Angriff

Ihre Alarme verschickt die Honeybox zusätzlich auf Wunsch per E-Mail, sendet sie an einen Syslog-Server oder zeigt sie über das Webfrontend auf dem OOB-Interface an (siehe Abbildung 3). Der Hersteller hat in die Oberfläche die BASE-Engine integriert [6], mit der Systemverwalter die Zugriffsversuche auswerten (siehe Abbildungen 4 und 5). Secxtreme hat die BASE-Engine erweitert und angepasst, denn sie verarbeitet normalerweise nur Snort-Alarme. Die Version auf der Appliance geht jedoch auch mit den Alarmen des Honeyd um.

Im Testverlauf hat die konfigurierte Appliance mit ihren virtuellen Honeypots zuverlässig funktioniert. Lediglich bei der Neukonfiguration oder beim Ändern von bestehenden virtuellen Honeypots gab es gelegentlich Abstürze des Systems. Auf Nachfrage erklärte der Hersteller, dass es sich hier um einen bekannten Bug im Tool »whiptail« handelt, das in den Menüs den Fortschrittsbalken erzeugt. Er versicherte, bereits daran zu arbeiten, das Problem zu beheben.

Die getestete Honeybox besitzt vier Sensorinterfaces, die ihr Betreiber dazu konfigurieren kann, zum Beispiel drei verschiedene DMZs oder zwei DMZs und das interne Netz mit Honeypots auszustatten. Die Möglichkeiten, mit dem Honeypot zu kommunizieren, sind bei Low-Interaction-Honeypots beschränkt: Ein Angreifer kann sich zum Beispiel nicht über einen emulierten Telnetd einloggen.

Abkürzung für Eindringlinge

Dennoch ist es für den Admin ratsam, einige Überlegungen zur Sicherheit anzustellen, bevor er sich dazu entscheidet, mehrere DMZs gleichzeitig zu überwachen. Eine Verwundbarkeit der Honeybox oder des Honeyd selbst würde nämlich ungewollt die Segmentierungsfunk-

Zero-Day-Attacken

Mit der Sicherheit betraute Anwender fürchten besonders Angriffe, die eine Schwachstelle ausnutzen, deren Ursache bis dato nicht bekannt ist. So greifen musterbasierte Schutzprogramme nicht. In den Jahren 2005 bis 2007 gab es einen großen Hype um die Zero Day Attacks genannten Angriffe, und viele Hersteller von IDS-Systemen, AV-Scannern und anderer Sicherheitssoftware haben in der Folge damit geworben, vor ihnen dennoch zu schützen.

Seit 2007 ist es auch um diese Variante der Angriffe ruhig geworden. Es ist schwer zu beurteilen, ob es sich dabei je um eine reale Gefahr für Unternehmen handelte – oder eher um ein gutes Verkaufsargument der Anbieter. Somit wäre es schon eine kleine Sensation, wenn sich in der Praxis durch den Einsatz von virtuellen Honeypots zeigen würde, dass Zero Day Attacks existieren und die Anwendergemeinde verlässliche Zahlen für deren Verbreitung bekäme.

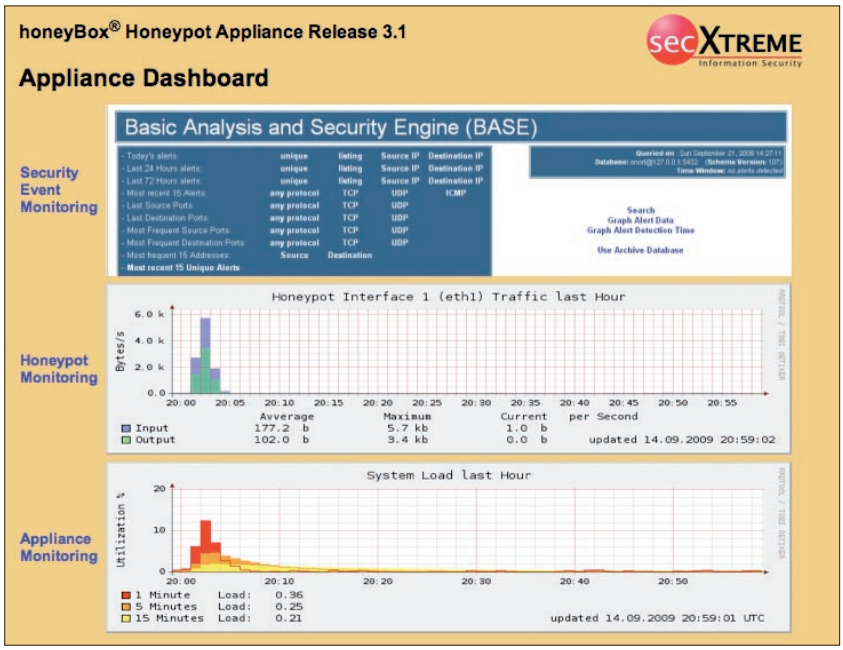

Abbildung 3: Vom Dashboard der Honeybox aus überblickt der Systemverantwortliche den technischen Status der Honeybox und hat so den Überblick der verwendeten Bandbreiten oder der CPU-Last.

tion der Firewall aushebeln: Wer mit der Honeybox mehrere DMZs gleichzeitig überwacht (siehe Abbildung 6), baut so durch den Honeyd eine Brücke zwischen den einzelnen DMZs. Die Segmentierung ist dann von der Sicherheit des Honeyd selbst abhängig. In der Theorie kann auch der Honeyd Schwachstellen aufweisen, die ein Angreifer womöglich dazu nutzt, sich zuerst Zutritt zur Appliance und danach zu anderen DMZs zu verschaffen.

Stolperdrähte spannen

Obwohl der Hersteller Secxtreme in die Appliance Tripwire integriert, um ihre mögliche Kompromittierung frühzeitig zu entdecken [7], erscheint es nicht ratsam, mit einer physikalischen Honeybox verschiedene Sicherheitszonen zu überwachen. Empfehlenswert ist hingegen, mehrere Subnetze des gleichen Sicherheitsniveaus im Auge zu behalten (siehe

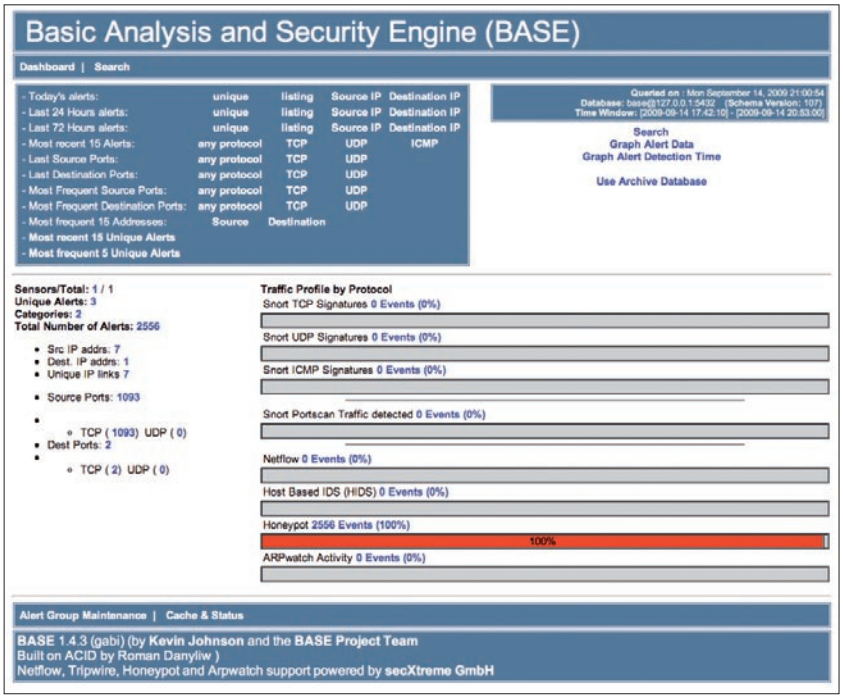

Abbildung 4: Das Dashboard der BASE-Engine zeigt eine Übersicht aller bisherigen Logeinträge und Alarme an. Die Web-basierte Software ermöglicht vielfältige Auswertungen und Statistiken.

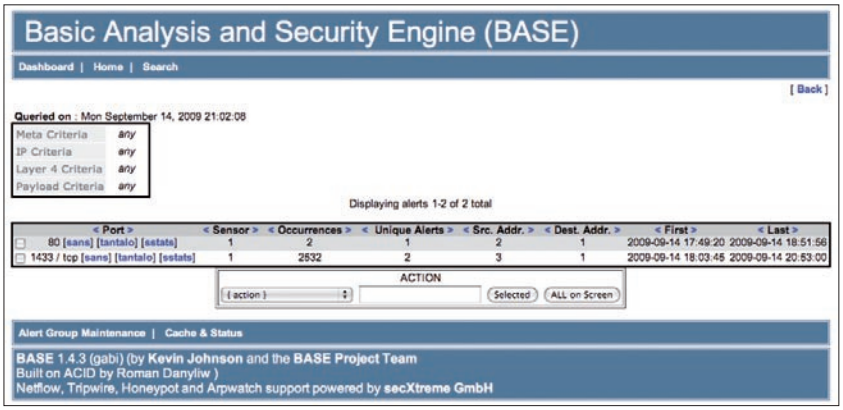

Abbildung 5: Die Aktionen eines Angreifers betrachtet der Systemverantwortliche in einer Detailansicht.

Abbildung 7). Mit virtuellen Honeypots sind auch ungewöhnliche Topologien abbildbar: So wäre ein Admin in der Lage, in einem internen Subnetz einige Hundert unterschiedliche Honeypots zu konfigurieren und darunter einen einzigen Produktionsserver zu verstecken.

Der Hersteller gibt zusätzlich an, die Honeybox-Appliance erkenne im internen LAN Würmer oder Viren: Solche Schadsoftware würde vermutlich versuchen die Systeme in ihrer Umgebung zu infizieren, also auch die Honeypots. Was die aber als Alarm melden würden, und zwar auch dann, wenn der Virus völlig neu ist und es dafür noch keine Antivirus-Patterns bei den Herstellern gibt, also wenn es sich um einen im Kasten „Zero Day Attacks" beschriebenen Angriff handelt. Da die Honeyboxen ja keinerlei produktive Aufgaben haben, ist definitionsgemäß jeder Kontaktversuch mindestens als Fehler, wenn nicht als Angriff zu werten.

Ökonomische Innovation

Die Honeybox ist eine echte Innovation der vergangenen Jahre und hat dafür den zweiten Platz des Bayerischen Sicherheitspreises 2009 belegt. Um den Einsatz der Honeybox möglichst ökonomisch zu gestalten, wäre es wünschenswert, wenn sie mehrere Sicherheitsniveaus mit einem einzigen Gerät überwachen könnte. Wünschenswert wäre weiterhin, wenn nun das Bundesamt für Sicherheit (BSI) mit einer EAL-Zertifizierung der Honeybox nachlegen würde.

Für Anwender ist die Honeybox eine Alternative zu IDS-Systemen. Wer dort nichts als Alarme sieht und deswegen schon gar nicht mehr hinschaut, für den lohnt es sich, die Honeybox anzusehen. Positiv fällt auf, dass Anwender bei Internetverbindungen oder internen Netzen mit hohen Bandbreiten (bis 10 GBit/s) keine Hochleistungshardware benötigen, wie es zum Beispiel bei der IDS/IPS-Technik der Fall ist. Sie versetzt sonst die Preise für Sicherheit ins Astronomische. Das macht die Appliance auch für große Betriebe und ISPs interessant. *(mg)* ■

Infos

[1] Symantec stellt Mantrap ein: [http://www.symantec.com/business/support/release_details.jsp?pid=52775]
[2] Gorecki, Göbel, Engelberth, Trinius, „Einbrüche im High Interaction Honeynet beobachten": Linux-Magazin 02/09, S. 54
[3] Honeyd: [http://www.honeyd.org]
[4] Niels Provos, Thorsten Holz, „Virtual Honeypots: From Botnet Tracking to Intrusion Detection": Addison-Wesley Longman, 2007
[5] Honeybox von Secxtreme: [http://www.sec-xtreme.com/honeypot.html]
[6] BASE-Engine: [http://base.secureideas.net]
[7] Tripwire: [http://sf.net/projects/tripwire/]

Der Autor

Jörg Fritsch studierte Chemie und arbeitete in der Software-Entwicklung und der IT-Sicherheit. Seit 2003 ist er Engineer Communication & Information Security bei der Nato-C3-Agentur. Er ist Autor zahlreicher Fachbeiträge zu den Themen Load Balancing, TCP/IP und Security.

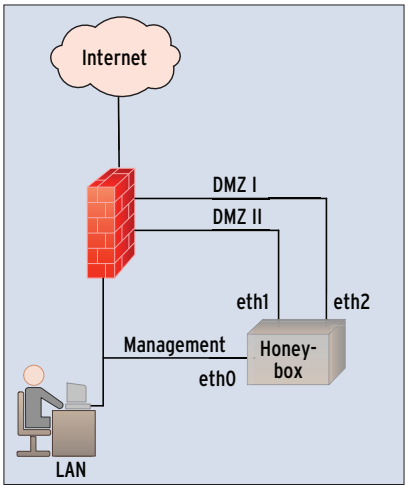

Abbildung 6: Eine Honeybox mit zwei Sensor- und einem OOB-Interface überwacht zwei unabhängige demilitarisierte Zonen. Der Aufbau beeinträchtigt schlimmstenfalls die Segmentierung der Zonen und öffnet Angreifern möglicherweise eine Hintertür.

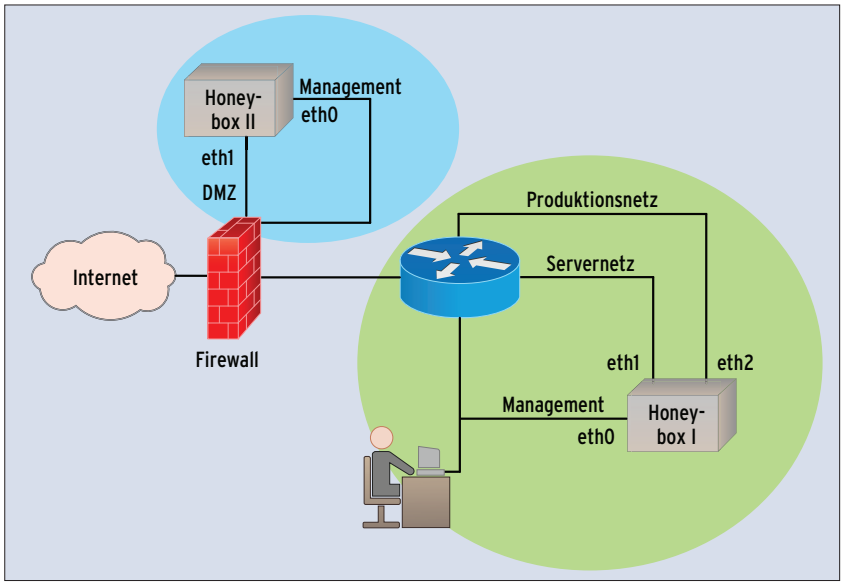

Abbildung 7: Mehrere Honeyboxen untersuchen die unterschiedlichen Sicherheitszonen (blau, grün). Jedes Sensorinterface überwacht jeweils ein anderes Subnetz mit gleichem Sicherheitsniveau.