honeyBox®

enterprise

Angriffserkennung und Alarmierung

EINSATZSZENARIEN

Überwachung Ihres LANs auf Angreifer

Situation: Sie betreiben ein großes Netzwerk, haben aber keine flächendeckende Überwachung im Einsatz. Angriffe auf Ihre internen Systeme können jedoch großen Schaden anrichten.
Umsetzung: Mit dem Einsatz der Honeypot-Appliances erhalten Sie in kurzer Zeit eine Lösung, die speziell zum Erkennen interner Angriffe in Ihrem LAN eingesetzt wird. Veränderungen an der Netzwerkstruktur sind dabei nicht notwendig.
Ergebnis: Über die Erkennung und mögliche Aufzeichnung von Angriffen erhalten Sie jederzeit einen aktuellen Informationsstand darüber, ob Angreifer oder Würmer in Ihrem Netzwerk aktiv sind. Sie können dann gegebenenfalls Maßnahmen ergreifen, um den Angriff einzudämmen und zu analysieren.

Zusätzliche Überwachung Ihrer DMZs

Situation: Sie setzen vor den Systemen in Ihren DMZs IPS ein. Wenn allerdings ein Angreifer eines der DMZ-Systeme übernommen hat, kann das IPS eine Ausbreitung innerhalb der DMZ nicht mehr erkennen und verhindern.
Umsetzung: Sie installieren eine Honeypot Appliance, deren Sensor-Interfaces in die einzelnen DMZs gepatcht werden. Sobald die virtuellen Honeypots angegriffen werden, können Sie Gegenmaßnahmen ergreifen.
Ergebnis: deutliche Verbesserung der Sicherheit und Verfügbarkeit Ihrer DMZs

- zuverlässige Erkennung von Angreifern im Netz
- sehr schnelle Detektion von Wurmausbrüchen
- so gut wie keine Fehlalarme (False-Positives)
- eine Appliance kann bereits bis zu 80 Subnetze überwachen
- einfache Integration in das Netzwerk
- keine Änderung der Netzwerkinfrastruktur notwendig
- VLAN-Unterstützung
- Einsatz beeinflusst die (Hoch-)Verfügbarkeit des Netzwerks nicht
- sehr geringer Betriebsaufwand

Aufgabenstellung

Unternehmen benötigen verlässliche Daten über den Sicherheitsstatus Ihres Netzwerks. Mit IDS/IPS ist das in der Fläche nicht realisierbar. Im Gegensatz dazu können mit Honeypots auch in der Fläche unerlaubte Zugriffe erkannt werden. Erkannte Angriffsversuche werden zentral protokolliert und es können Alarme abgesetzt werden.

Lösung

secXtreme hat für diese Aufgabe die honeyBox®-Honeypot-Appliance entwickelt, die diese Anforderungen kostengünstig abdeckt. Durch die geeignete Auswahl der Funktionen auf der Appliance wird ein sehr hoher Nutzen bezüglich Sicherheit, Realisierungszeit, Investition und Betriebskosten erreicht.
Die Honeypot-Appliance basiert auf der Generischen Software-Security-Appliance von secXtreme. Alle Funktionen dieses Systems sind auch in der Honeypot-Appliance enthalten und ermöglichen so einen sicheren und rechenzentrumstauglichen Betrieb out-of-the-box.

secXTREME Information Security

Funktionen und Eigenschaften

FUNKTIONEN

Honeypot
- 4 Interfaces
- bis zu 80 VLANs
- bis zu 500 virtuelle Honeypots je VLAN möglich
- 40+ Honeypot-Templates
- 19+ spezielle Services
- Netzwerk-Daten-Recorder

Sicherheit
- gehärtetes Debian Linux
- SSHv2
- HTTPS (lokale CA)
- Filesystem-Integrity-Checks
- Security-Baselining
- lokale Firewall
- signierte Software-Pakete

Management
- Monitoring Web-GUI
- Setup über SSHv2 und seriell
- Alert-System (E-Mail, Pager, Syslog, Datenbank, Logfiles)
- Backup/Restore/Recovery
- Watchdog
- Hardware-Monitoring

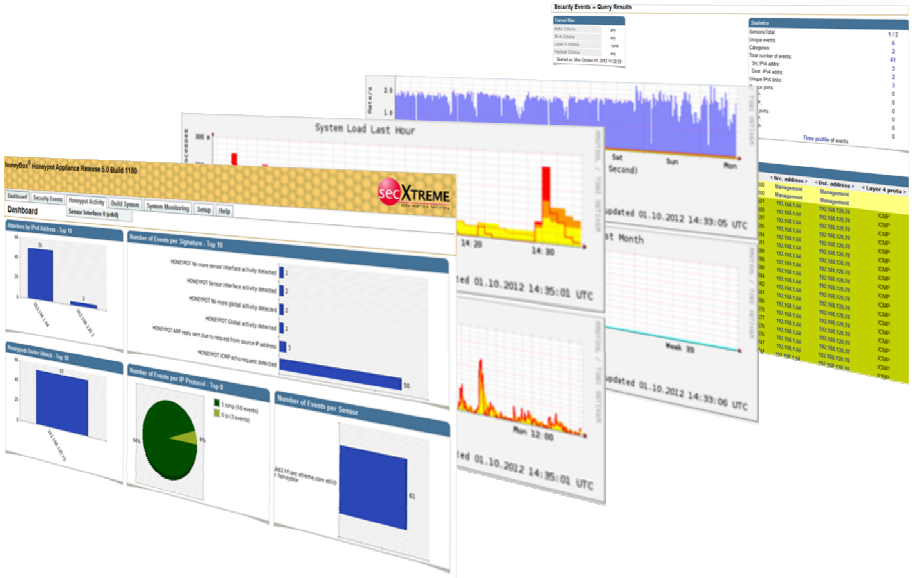
Installation
- CD-ROM

Integration
- sichere Updates über Internet
- NTPv3 Zeitsynchronisation
- E-Mail
- Syslog (CSV und CEF)

Support
- 5x8 per Telefon und E-Mail

Hardwaretausch
- NBD-Tausch für bis zu 5 Jahre
- Keep-Your-Hard-Disk-Option

Die honeyBox® enterprise-Appliance kann als Stand-alone-Lösung betrieben werden. Dabei werden Alarme im zentralen Repository gesammelt und über eine sichere HTTPS-Verbindung im Browser ausgewertet. Die Appliance kann auch als Managementsystem bei größeren Installationen mit mehreren honeyBox® Systemen eingesetzt werden. Sie arbeitet dann mit den Appliances zusammen, die die Sensorfunktionen übernehmen. Die Auswertung nach verschiedenen Kriterien ist möglich. Damit kann ein gezielter Drill-down durchgeführt werden.



Hardware	
CPU	Intel Xeon E5-2620 6-Core / 2,0 GHz
Arbeitsspeicher	8 GB Registered DIMMs PC3-10600R
Netzwerk	4 x 1 Gbit Kupfer (Fiber 1 Gbit od. 10 Gbit opt.)
USB	7 x USB 2.0
Speichermedium	2 x 146 GB, 6G SAS, 15 000 RPM (RAID 1)
RS232	1 x serial DB9
Spannungsversorgung	2 x 100-240 VAC, 50-60 HZ, 4,5 - 2,2 A
Leistungsaufnahme (typ.)	160 Watt typ., 750 Watt max.
Betriebstemperatur	+10 bis +35 °C,
Luftfeuchte	10 % - 90 % nicht kondensierend
Abmessungen	434,7 mm x 43,2 mm x 698,5 mm (BxHxT)
Zertifizierungen	CISPR 22, EN55022, EN55024, FCC u. a.

Auszeichnungen für die honeyBox® Appliance Familie

Über secXtreme: Die secXtreme GmbH hat sich auf die Sicherheit Ihrer Informationen spezialisiert. Dazu gehören die Bereiche Audit, Penetration Testing, Sicherheitsanalysen und Trainings. Neben diesen Bereichen entwickelt secXtreme Sonderlösungen im Sicherheitsumfeld. secXtreme ist Mitglied im Deutschen CERT-Verbund und unterstützt seine Kunden bei Incident-Management- und Forensik-Aufgaben.

secXtreme Information Security

secXtreme GmbH
Kiefernstraße 38
D-85649 Brunnthal-Hofolding

Tel. +49(0)89-18 90 80 68-0
Fax.+49(0)89-18 90 80 68-77
E-Mail: info@sec-xtreme.com
WWW: www.sec-xtreme.com