www.sec-xtreme.com

honeyBox®

Constant Network Control

MIT SPECK FÄNGT MAN MÄUSE!

Mit der **honeyBox** unerwünschte Besucher in Ihrem Netzwerk.

honeyBox®

constant network control

Mit der honeyBox, basierend auf der Honeypot-Technologie, Sicherheitsrisiken nachhaltig unter Kontrolle halten.

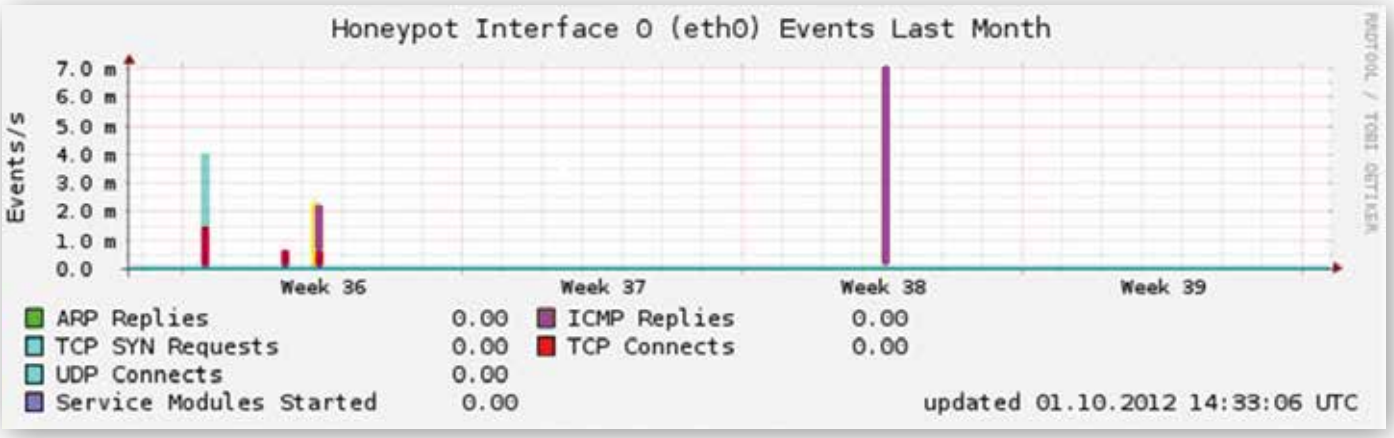
Schutzmechanismen im Netz sind meistens aktiv, sie gehen direkt gegen Angriffe vor oder versuchen Fehlverhalten zu unterbinden. Einen anderen Ansatz verfolgen Honeypots. Sie laden Angreifer geradezu ein, sich mit ihnen zu beschäftigen und geben Administratoren so Zeit, Attacken zu erkennen und abzuwehren. Die honeyBox passt auch sehr gut in industrielle Steuerungsnetzwerke.

Wie funktioniert die honeyBox?

Die honeyBox stellt eine große Anzahl virtueller Honeypots zur Verfügung. Die Sicherheitsmeldungen der honeyBox werden zentral gesammelt und der Administrator alarmiert. Über eine sichere HTTPS-Verbindung im Browser können die Meldungen über verschiedene Kriterien ausgewertet werden. Damit steht die Möglichkeit für einen gezielten Drill-down zur Verfügung. Zudem können die Meldungen an Drittsysteme (z. B. per syslog) weitergeleitet werden.

„A honeypot is a system who's value is being probed, attacked or compromised, you want the bad guys to interact with your honeypot."

Quelle: „The Honeynet Project FAQ"



Angriff mit System: Honeypots binden Ressourcen des Angreifers in wichtigen Phasen der Attacke

Die honeyBox überwacht nicht den Inhalt, sondern das Verhalten des Angreifers. Durch die virtuellen Honeypots können mehrere Stufen des Angriffs erkannt und gemeldet werden. Dazu gehört der erste Scan auf verfügbare IP-Adressen und Ports sowie die Suche nach verwundbaren Systemen, um auf diese Zugriff zu erlangen.

Einfaches Prinzip: Virtuelle Köder sollen Angreifer anziehen und herausfordern.

Angriff mit der honeyBox erkennen:

1. Informationsrecherche im Internet
2. Scannen (ARP, Ping, Ports, Betriebssysteme)
3. Erkunden (Dienste, Benutzer, Software)
4. Auf Systeme zugreifen

honeyBox

5. Privilegien ausbauen
6. Suche nach Vertrauensbeziehungen
7. Hintertüren einbauen
8. Spuren verwischen

Ablauf eines typischen Cyber-Angriffes

honeyBox®

constant network control

Sicherheitsrisiken nachhaltig mit der honeyBox eindämmen, passend zu industriellem wie Office-Umfeld.

Einsatzszenario Office-Umgebung

Als Betreiber eines großen Netzwerkes, haben Sie keine flächendeckende Überwachung im Einsatz. Sie haben zusätzliche DMZs eingefügt, jedoch kann das IPS eine Ausbreitung innerhalb der DMZ nicht mehr erkennen und verhindern, falls ein Angreifer eines der DMZ-Systeme übernommen hat. Verlässliche und flächendeckende Daten über den Sicherheitsstatus Ihres Netzwerkes bekommen Sie mit IDS/IPS nicht. Für diese Anforderungen benötigen Sie eine zusätzliche Lösung.

Interview mit Behördenspiegel 2/2014:

Behördenspiegel: Kann es passieren, dass klassische Lösungen Ausfälle verursachen oder den Datenverkehr stören?

Scheucher: Ja, das kann leider der Fall sein. Die Verfügbarkeit als ein Teilziel der IT-Sicherheit besitzt meistens sehr hohe Priorität. Firewalls und IPS stehen direkt im Datenstrom. Somit kommen neue Ausfallrisiken hinzu. Durch diese Funktionsweise kann es zudem sein, dass Datenverkehr nach einem Update, der davor noch einwandfrei übertragen wurde, danach gestört ist.

Das Interview wurde geführt von: Guido Gehrt, Redakteur „Behördenspiegel"

Wie ein Boot auf steinigem Boden? Für die Industrie sind andere Lösungen als im Office-Bereich erforderlich!

Einsatzszenario industrielles Umfeld

Auch industrielle Netzwerke können Ziele von Attacken sein und müssen daher durch Erkennungsmechanismen geschützt werden. So können Servicemitarbeiter, denen Sie für Ihre Computer einen Zugang zum Steuerungssystem verschaffen müssen, Ursache einer Infektion sein. Störungen können zu massiven Problemen in der Produktion führen. Durch den Einsatz der honeyBox industrial verfügen Sie über das Potential auch unbekannte Angriffe zu erkennen und aufzuzeichnen. So können Sie Angriffe zeitnah eindämmen und auch infizierte Systeme schnell identifizieren. Veränderungen an der Netzwerkstruktur sind dabei nicht notwendig.

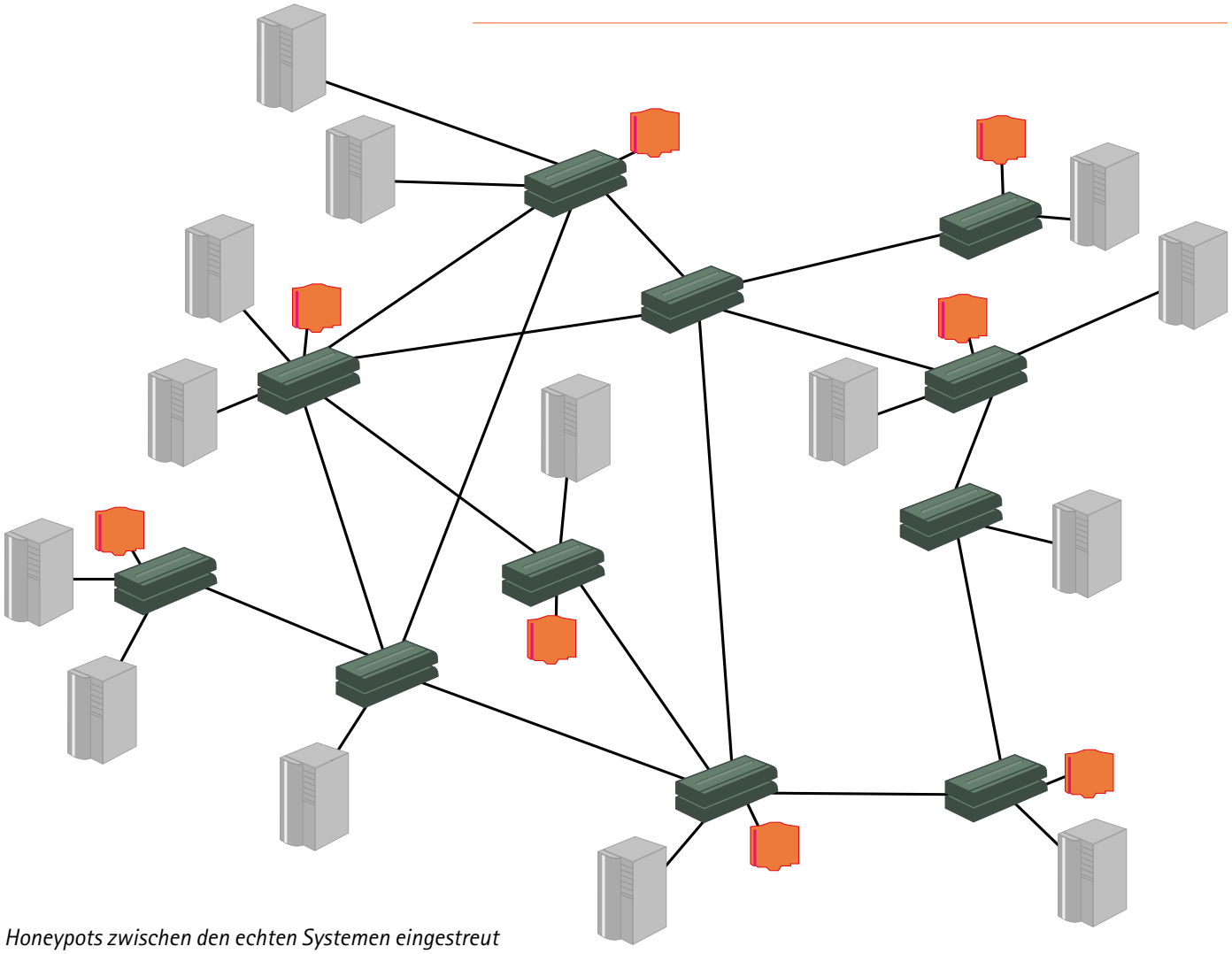
honeyBox®

constant network control

Honeypots im LAN

„Die professionelle Implementierung und die technische Kompetenz von secXtreme haben uns gezeigt, dass die Entscheidung für die honeyBox richtig war".

Kundenmeinung von Reinhard Görtner, Leiter IT & Services RTL II



Honeypots zwischen den echten Systemen eingestreut

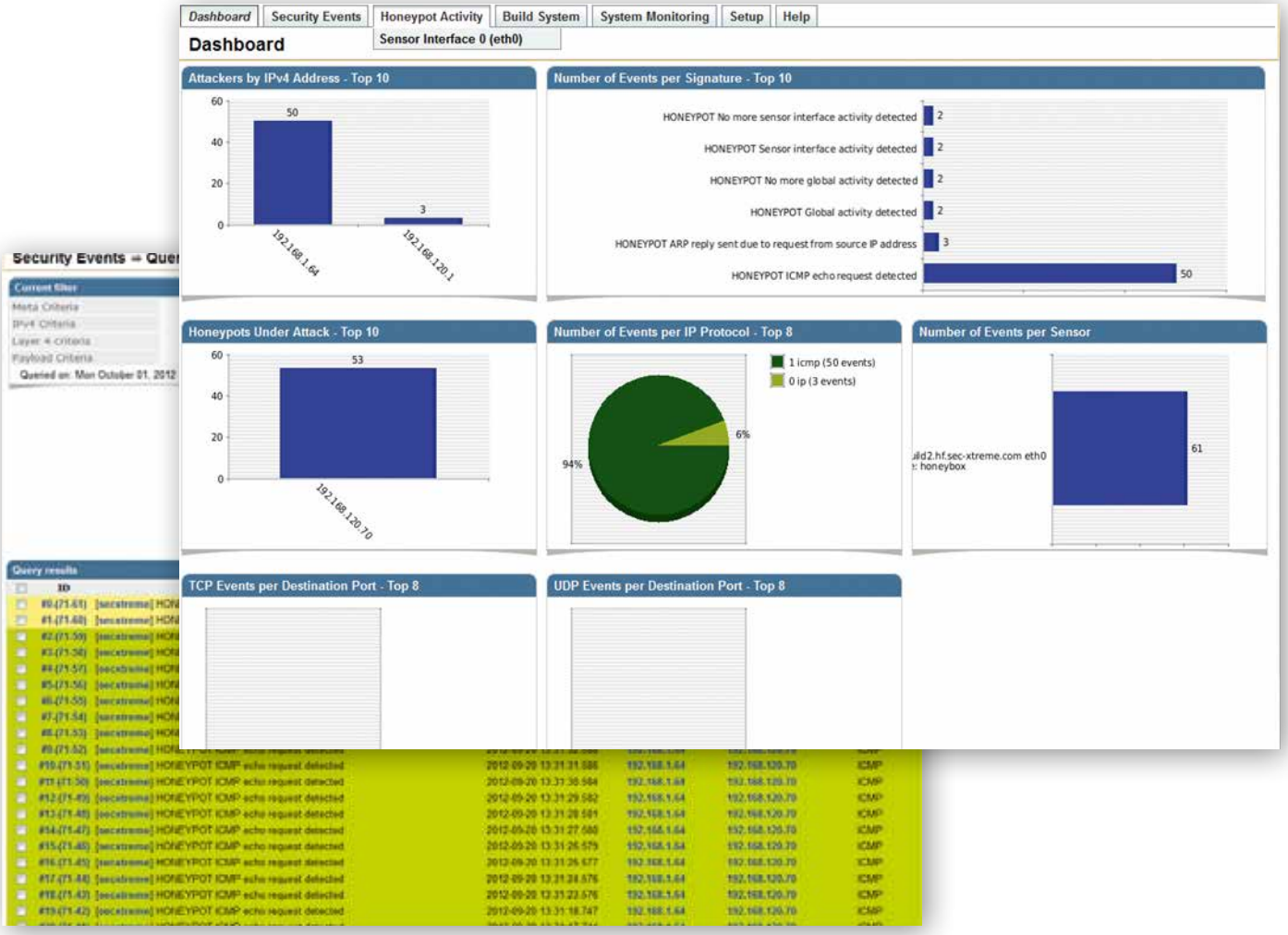
Technische Informationen

Hardware	honeyBox industrial 1-Port	honeyBox industrial 2-Port	honeyBox 4-Port-Version Generation 2	honeyBox enterprise
				
CPU	AMD Geode LX-800, 500 MHz	Intel Atom D525, 1,8 GHz, 2 Kerne, Hyperthreading	Intel Celeron M 440, 2,0 GHz	Intel Xeon E5-2620, 6-Core, 2,0 GHz
Arbeitsspeicher	512 MB DDR SDRAM	1 GB DDR2 SDRAM	1 GB DDR3 SDRAM, Non-ECC	8 GB Registered DIMMs PC3-10600R
Netzwerk	1 x 10/100 Kupfer	2 x 10/100/1000 Kupfer	4 x 10/100/1000 Kupfer	4 x 10/100/1000 Kupfer
USB	2 x USB 2.0	4 x USB 2.0	2 x USB 2.0	7 x USB 2.0
Speichermedium	4 GB Industrie-CompactFlash-Karte	64 GB 1,8 Zoll S-ATA MLC SSD	250 GB, SATA-II, 7200 RPM	2 x 146 GB, 6G SAS, 15 000 RPM (RAID 1)
RS232	2 x DB9	3 x DB9	1 x RJ45	1 x DB9
Spannungsversorgung	DC 12 - 24 Volt, max. 15 % Toleranz	DC 10 - 30 Volt	110 - 240 VAC, 50 - 60 HZ, 4,2 A	2 x 100 - 240 VAC, 50 - 60 HZ, 4,5 - 2,2 A
Leistungsaufnahme	7 Watt typ.	min. 17 Watt typ. 45 Watt	200 Watt max.	160 Watt typ. 750 Watt max.
Betriebstemperatur	0 bis +50 °C	-20 bis +55 °C	0 bis +40 °C	+10 bis +35 °C
Luftfeuchte	5 % - 95 % nicht kondensierend	0 % - 85 % nicht kondensierend	5 % - 95 % nicht kondensierend	10 % - 90 % nicht kondensierend
Abmessungen	48 x 123 x 135 mm (BxHxT)	163 x 111 x 83 mm (BxHxT)	426 x 44 x 366 mm (BxHxT)	434,7 x 43,2 x 698,5 mm (BxHxT)
Zertifizierungen	CE, FCC, RoHS	CE, FCC, RoHS	CE, FCC, RoHS	CISPR 22, EN55022, EN55024, FCC u. a.

honeyBox®

constant network control

honeyBox – Mit Sicherheit mehr Kontrolle über Ihr Netzwerk.



Technische Informationen

Funktionen	Funktionsdetails	honeyBox industrial 1-Port	honeyBox industrial 2-Port	honeyBox 4-Port-Version Generation 2	honeyBox enterprise	Management
Honeypot Sensor	max. Anzahl der Honeypots je Appliance	250	500	4.000	40.000	○
	max. Anzahl der Honeypots je Netzwerkschnittstelle	250	250	1.000	500	○
	Anzahl der Netzwerkschnittstellen	1	2	4	4	○
	Max. VLANS	○	○	○	80	○
	Anzahl spezielle Services	19+	19+	19+	19+	○
	Anzahl Honeypot Templates	40+	40+	40+	40+	○
	Netzwerk-Daten-Recorder	○	●	●	●	○
Honeypot Management	Monitoring Web-GUI	●	●	●	●	●
	Alarmauswertung auf zentralem Management	●	●	●	●	●
	Management-Komponente enthalten	○	●	●	●	●
	Setup über SSHv2 und seriell	●	●	●	●	●
	Alert-System (E-Mail, Pager, Syslog (CSV und CEF), Datenbank, Logfiles)	●	●	●	●	●
	Backup/Restore/Recovery	●	●	●	●	●
	Watchdog	●	●	●	●	●
	Hardware - Monitoring	●	●	●	●	○
Installation	ISO - Image	○	○	○	○	●
	USB-Stick	●	●	●	●	○
Integration	digital signierte Updates über Internet	●	●	●	●	●
	NTPv3 Zeitsynchronisation	●	●	●	●	●
Sicherheit	gehärtetes Debian Linux	●	●	●	●	●
	SSHv2	●	●	●	●	●
	HTTPS (lokale CA)	●	●	●	●	●
	Filesystem-Integrity-Checks	●	●	●	●	●
	Security-Baselining	●	●	●	●	●
	lokale Firewall	●	●	●	●	●
	signierte Software-Pakete	●	●	●	●	●
Support	5x8 per Telefon und E-Mail (dt. & eng.)	●	●	●	●	●
Hardwaretausch	Standardgewährleistung Hardwaretausch	2 Jahre	2 Jahre	1 Jahr	3 Jahre	○
	Verlängerbar bis	○	○	5 Jahre	5 Jahre	○
	Keep-Your-Hard/Flash-Disk-Option	●	●	●	●	○
	NBD-Service möglich (länderabhängig)	○	○	●	●	○

● *unterstützt*
○ *nicht unterstützt*

honeyBox®

constant network control

Die Honeypot-Appliance ermöglicht einen sehr hohen Nutzen bezüglich Sicherheit, Realisierungszeit, Investition und Betriebskosten.

Die honeyBox kann Ihnen bieten:

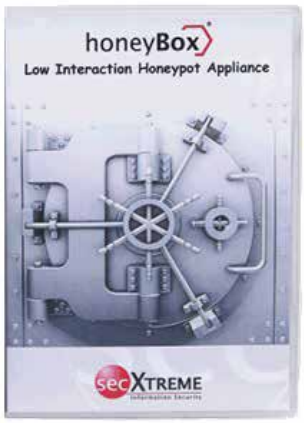
- eine zuverlässige Erkennung von Angriffen im Netz und eine sehr schnelle Detektion von Wurmausbrüchen bei einer Überwachung von bis zu 80 Subnetzen auf einem Gerät (honeyBox enterprise mit VLAN-Unterstützung)
- keine Beeinträchtigung der Verfügbarkeit des Netzwerkes bei so gut wie keinen Fehlalarmen
- einfache Integration, geringer Betriebsaufwand und keine Änderung der Netzwerkinfrastruktur nötig

Die honeyBox wurde mit dem Bayerischen Sicherheitspreis 2009 ausgezeichnet.

Im Innovationspreis der Initiative Mittelstand errang sie 2009 und 2010 vordere Plätze und wurde 2013 und 2014 mit dem BEST-OF-Zertifikat ausgezeichnet.

honeyBox Modelle

honeyBox industrial 2-Port



honeyBox-Management

honeyBox industrial 1-Port

honeyBox 4-Port-Version Generation 2

honeyBox enterprise

honeyBox®

constant network control

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
Telefon: +49 89 18 90 80 68-0
Telefax: +49 89 18 90 80 68-77
E-Mail: info@sec-xtreme.com
www.sec-xtreme.com

Überreicht durch secXtreme Partner:

INNOVATIONSPREIS-IT BEST OF 2014 initiative mittelstand IT-SECURITY

INNOVATIONSPREIS-IT BEST OF 2013 initiative mittelstand IT-SECURITY

TOP 2011 IT-Lösung ITBestenliste.de

INNOVATIONSPREIS-IT 2010 initiative mittelstand QUALIFIZIERT

TOP 2010 IT-Lösung ITBestenliste.de

QUALIFIZIERT initiative mittelstand 2009 INNOVATIONSPREIS-IT