www.honeybox.com

honeyBox

Detection · Deception · Mitigation

MIT SPECK FÄNGT MAN MÄUSE!

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

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.

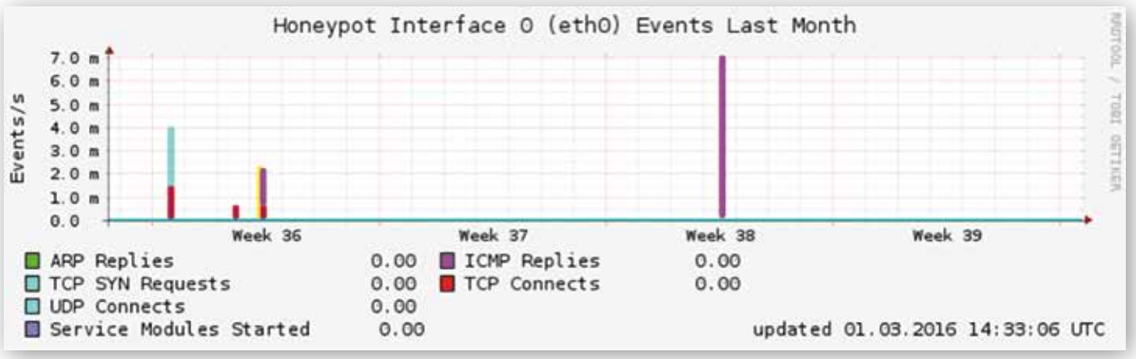
Wie funktioniert die honeyBox®?

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"

Signifikante Ereignisse auf einen Blick erkennbar:



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.

1. Informationsrecherche im Internet
2. **Scannen (ARP, ICMP, Ports, Betriebssysteme)**
3. **Erkunden (Dienste, Benutzer, Software)**
4. **Auf Systeme zugreifen**
5. Privilegien ausbauen
6. Suche nach Vertrauensbeziehungen
7. Hintertüren einbauen
8. Spuren verwischen

Ablauf eines typischen Cyber-Angriffes

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 DMZ 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.

Christian Scheucher (Geschäftsführer secXtreme) im Interview mit Behörden Spiegel:

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

C. 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 nach einem Update der Datenverkehr, welcher vorher noch einwandfrei übertragen wurde, gestört ist.

Das Interview wurde geführt von: Guido Gehrt, Redakteur „Behörden Spiegel“

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

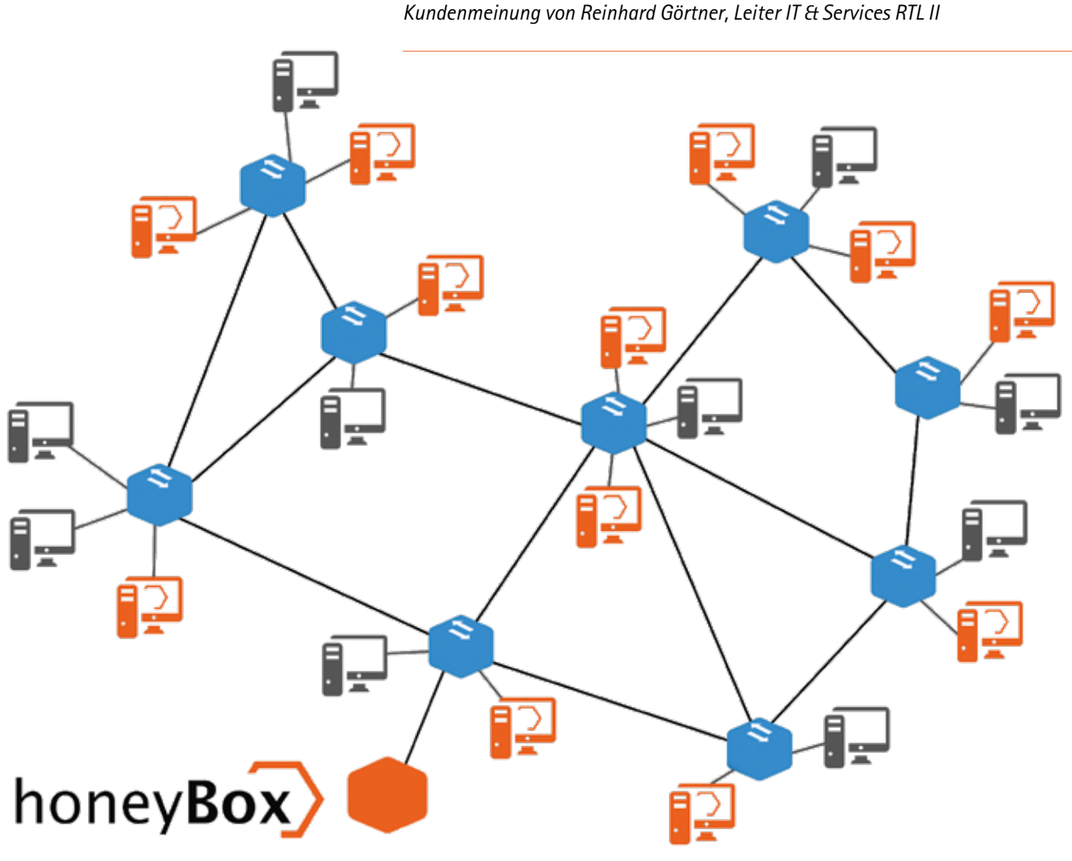
constant network control

Technische Informationen

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

Designed by Freepik and distributed by Flaticon

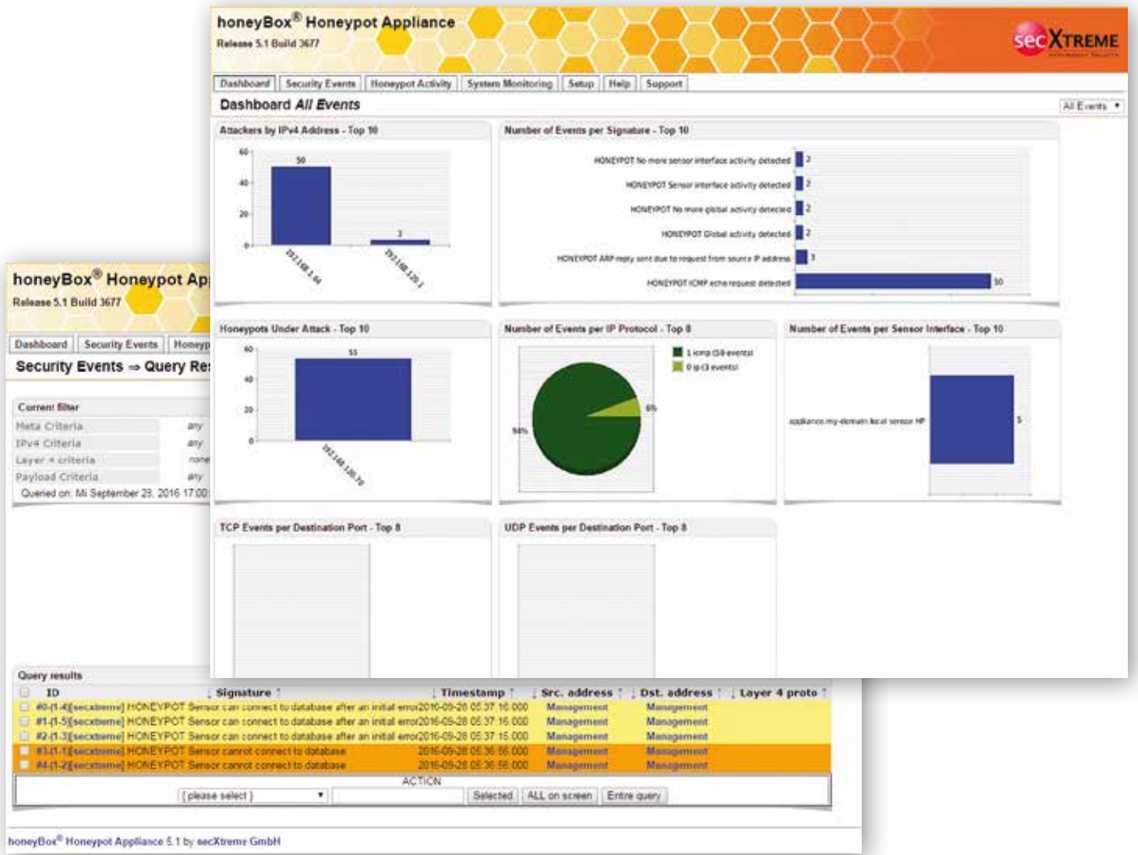
Hardware	honeyBox® industrial Generation 2	honeyBox® micro Generation 2	honeyBox® universal Generation 3	honeyBox® enterprise Generation 4
				
CPU	Intel Atom N2600, 1,6 GHz, 2 Kerne, Hyperthreading	Intel® Celeron® Processor N3010, 2-Core, 1.04 GHz	Intel 64 Bit	Intel Xeon
Arbeitsspeicher	2 GB DDR3 SoDIMM	4 GB DDR3L, 1600 MHz SO-DIMM	8 GB DDR4	16 GB Registered DIMMs
Netzwerk	2 x 10/100/1000 Kupfer (1-Port Lizenz oder 2-Port Lizenz)	3 x 10/100/1000 Kupfer	8 x 10/100/1000 Kupfer Erweiterung optional möglich	4 x 10/100/1000 Kupfer Erweiterung optional möglich
USB (extern)	4 x USB 2.0	1 x USB 3.0 1 x USB 2.0	2 x USB 3.0	5 x USB 3.0 1 x optional USB 2.0
Speichermedium	4 GB C-Fast-Karte (1-Netzsegement) 60 GB 2,5 Zoll S-ATA MLC SSD (2-Port Lizenz)	32 GB, SSD mSATA mini	240 GB, 2,5“ SATA SSD	2 x 300 GB, 12 GB SAS
RS232	2 x DB9	1 x RJ-45	1 x RJ-45	1 x DB9
Spannungsversorgung	DC 9 – 32 Volt	100 – 240 VAC, 50 – 60 Hz	100 – 240 VAC, 50 – 60 Hz	2 x 200 – 240 VAC, 50 – 60 Hz
Leistungsaufnahme	min. 17 Watt, typ. 25 Watt	36 Watt	30 Watt typ. 150 Watt max.	105 Watt typ. 800 Watt max.
Betriebstemperatur	0 bis +50 °C	0 bis 40°C	0 bis +40 °C	+10 bis +35 °C
Luftfeuchte	5 % – 95 % nicht kondensierend	5% – 90% nicht kondensierend	10 % – 90 % nicht kondensierend	5 % - 95 % nicht kondensierend
Abmessungen	50 x 145 x 115 mm (B x H x T)	137 x 22 x 120 mm (B x H x T)	438 x 44 x 344,4 mm (B x H x T)	435 x 34 x 707 mm (B x H x T)
Zertifizierungen	CE, RoHS	CISPR 22, EN55022, CE EN55024, FCC, RoHS u. a.	CE, FCC	CISPR 32, EN6100-6-1, EN62368-1, u a.

honeyBox

constant network control

Technische Informationen

honeyBox® – mit Sicherheit mehr Kontrolle über Ihr Netzwerk.



Funktionen	Funktionsdetails	honeyBox® industrial Generation 2 (1 Layer-3 Netzsegment)	honeyBox® industrial Generation 2 (2 Layer-3 Netzsegmente)	honeyBox® micro Generation 2	honeyBox® universal Generation 3 (1 Layer-3 Netzsegment)	honeyBox® universal Generation 3 (4 Layer-3 Netzsegmente)	honeyBox® universal Generation 3 (8 Layer-3 Netzsegmente)	honeyBox® enterprise Generation 4	Management
Honeypot Sensor	max. Anzahl der Honeypots je Appliance	250	500	250	1.000	4.000	8.000	40.000	▨
	max. Anzahl der Honeypots je Layer-3 Netzsegment	250	250	250	1.000	1.000	1.000	500	▨
	max. Anzahl überwachbarer Layer-3 Netzsegmente	1	2	1	1	4	8	80	▨
	Anzahl der nutzbaren Netzwerkschnittstellen	2 Kupfer	2 Kupfer	1 Kupfer	8 Kupfer	8 Kupfer	8 Kupfer	4 Kupfer	1 virt.
	Anzahl spezielle Services	28+	28+	28+	28+	28+	28+	28+	▨
	Anzahl Honeypot Templates	79+	79+	79+	79+	79+	79+	79+	▨
	Netzwerk-Daten-Recorder	●	○	●	●	●	●	●	▨
Honeypot Management	Monitoring Web-GUI	●	●	●	●	●	●	●	●
	Alarmauswertung auf zentralem Management	●	●	●	●	●	●	●	●
	Management-Komponente enthalten	○	●	○	●	●	●	●	●
	Setup über SSHv2 und seriell	●	●	●	●	●	●	●	●
	Alert-System (E-Mail, Syslog, Datenbank, Logfiles)	●	●	●	●	●	●	●	●
	Meldung über digitale Ausgänge	Ja	Ja	Ja*	Ja*	Ja*	Ja*	Ja*	Ja*
	Backup/Restore/Recovery	●	●	●	●	●	●	●	●
	Watchdog	●	●	●	●	●	●	●	●
	Hardware-Monitoring	●	●	●	●	●	●	●	○
	Meldung an Syslog-Server/SIEM	●	●	●	●	●	●	●	●
Installation	ISO-Image	●	●	●	●	●	●	●	●
	USB-Stick	●	●	●	●	●	●	●	○
Integration	digital signierte Updates über Internet	●	●	●	●	●	●	●	●
	NTPv3 Zeitsynchronisation	●	●	●	●	●	●	●	●
	Meldungen an Syslog-Server/SIEM	●	●	●	●	●	●	●	
Sicherheit	gehärtetes Debian Linux	●	●	●	●	●	●	●	●
	SSHv2	●	●	●	●	●	●	●	●
	HTTPS (lokale CA)	●	●	●	●	●	●	●	●
	Filesystem-Integrity-Checks	●	●	●	●	●	●	●	●
	Security-Baselining	●	●	●	●	●	●	●	●
	lokale Firewall	●	●	●	●	●	●	●	●
Support	Support 5x8 per Telefon oder E-Mail	●	●	●	●	●	●	●	●
	Managed Security Services (SOC, on-site)	opt.	opt.	opt.	opt.	opt.	opt.	opt.	opt.
Hardwaretausch	Standardgewährleistung Hardwaretausch	3 Jahre	3 Jahre	3 Jahre	3 Jahre	3 Jahre	3 Jahre	3 Jahre	▨
	verlängerbar bis	5 Jahre	5 Jahre	5 Jahre	5 Jahre	5 Jahre	5 Jahre	5 Jahre	▨
	Keep-Your-Hard/Flash-Disk-Option	●	●	●	●	●	●	●	▨
Neutrales Gehäuse	„Stealth Option"	●	●	●	●	●	●	●	▨

*○ nicht unterstützt ● unterstützt ▨ nicht relevant *(mit opt. USB-Schnittstellenmodul)*

honeyBox

constant network control

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

Die honeyBox® bietet Ihnen:

- 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

Auszeichnung mit dem Bayerischen Sicherheitspreis 2009.

Die honeyBox® wurde mit dem Bayerischen Sicherheitspreis 2009 ausgezeichnet. Im Innovationspreis der Initiative Mittelstand errang sie 2009 und 2010 vordere Plätze und wurde 2013 sowie 2014 mit dem BEST-OF-Zertifikat ausgezeichnet. Sie errang ebenfalls die BEST-OF-Auszeichnung des Industriepreises 2016.

honeyBox®-Modelle

honeyBox® industrial Generation 2

honeyBox®-Management

honeyBox® universal Generation 3

honeyBox® enterprise Generation 4

honeyBox® micro Generation 2

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 bietet Managed Security Services an und unterstützt seine Kunden bei Incident-Management- und Forensik-Aufgaben.

secXtreme Information Security

secXtreme GmbH
Alte Landstraße 21
D-85521 Ottobrunn
Telefon: +49 89 18 90 80 68-0
Telefax: +49 89 18 90 80 68-77
E-Mail: info@sec-xtreme.com
www.honeybox.com

Überreicht durch secXtreme Partner: