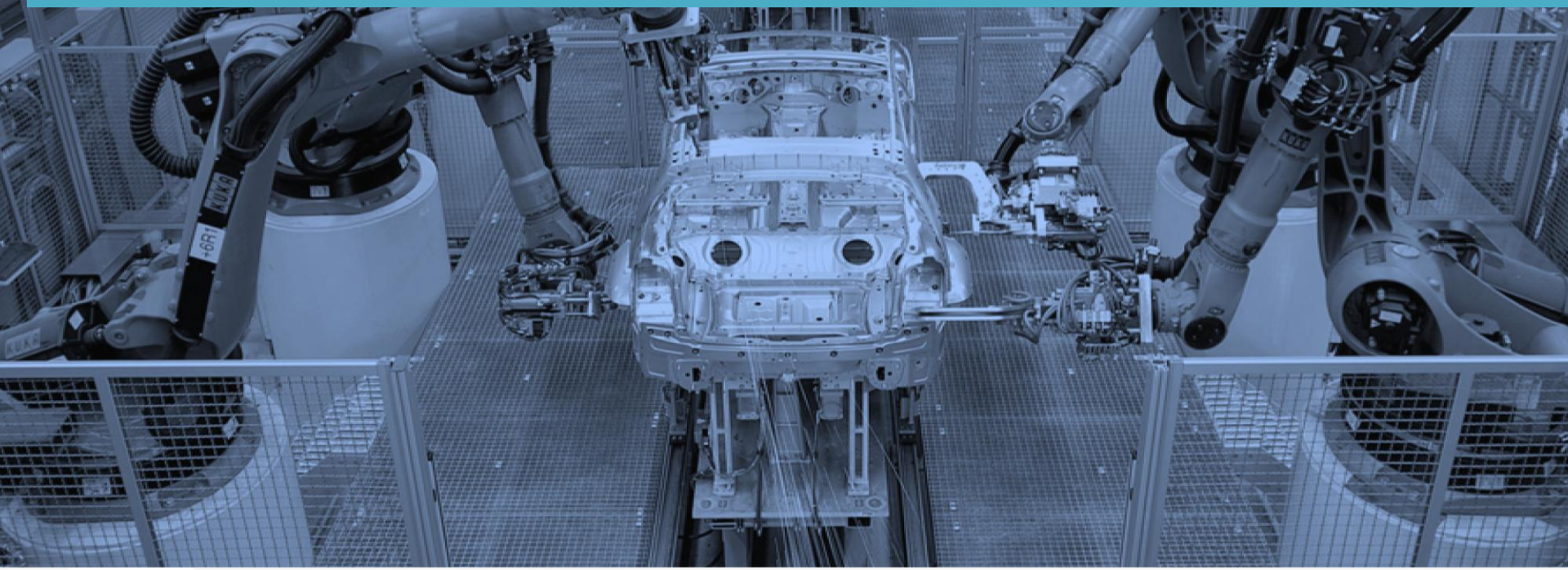
Stuxnet zum Frühstück
Industrielle Netzwerksicherheit 2.0

Stuttgart und München



TÜV SÜD

HIRSCHMANN
A BELDEN BRAND

secXTREME
Information Security

YELLO NETCOM

Angriffe und Schadsoftware zuverlässig erkennen

Christian Scheucher
secXtreme GmbH
Kiefernstraße 38, D-85649 Brunnthal-Hofolding
Tel: +49 (0)89-18 90 80 68-11
Fax: +49 (0)89-18 90 80 68-77
E-Mail: christian.scheucher@sec-xtreme.com
www.sec-xtreme.com

Über secXtreme

- Penetrationstests und Security-Audits auf Netzwerk- und Anwendungsebene
- Angriffe erkennen und darauf reagieren
- Angriffserkennung mit Honeypots, IPS und Netflow
- Log-Management und SIEM
- Verfolgung und Analyse von Angriffen (Incident Response, CERT und Forensics)
- Linux-Entwicklungen im Security-Umfeld

Aktuelle Situation

- Industrielle Systeme und Embedded Systeme nutzen immer mehr TCP/IP
- Feldbusse nutzen immer mehr Ethernet und TCP/IP
- Es werden dort immer mehr Windows und *NIX-Systeme verwendet
- Verwundbarkeiten aus Office-Umgebungen haben damit die industriellen Netzwerke erreicht
- Stuxnet hat viele Verwundbarkeiten davon ausgenutzt.

Aktuelle Schutz-maßnahmen

- Manchmal Firewalls
- Sehr oft ungepatchte Betriebssysteme und Anwendungen
- Anti-Virus selten genutzt und nur unregelmäßig oder nie aktualisiert
- Ungehärtete Betriebssysteme
- Systeme für einen Betriebszeitraum von 10 und mehr Jahren ausgelegt
- IT-Sicherheit 10 Jahre im Vergleich zur Office-IT zurück

Offensichtliche, aber nicht funktionierende Lösungen

- Nutzung von bekannten Technologien aus dem Office-Umfeld
  - Patch-Management
  - Anti-Virus
  - Intrusion Detection und Intrusion Prevention
  - Firewalls
  - ...

Problem Anti-Virus und Patchen

- Anti-Virus verändert das Systemverhalten (wird langsamer, schlechtere Verfügbarkeit, …)
- Signaturen müssen mindestens einmal täglich aktualisiert werden
- Patche müssen mindestens alle 4-8 Wochen eingespielt werden
- Manchmal sind Systeme nicht patchbar (es gibt keine Patche mehr, Gewährleistungsverlust, …)

Herausforderung Firewalls

- In den Firewalls müssen die benötigten Ports geöffnet werden.
- Schadsoftware nutzt dieselben Ports für die Verbreitung (z. B. TCP/445)
- Firewalls verringern die Verfügbarkeit. Sie müssen daher redundant ausgelegt werden (höhere Komplexität und trotzdem geringerer Verfügbarkeit).
- Firewalls werden mit der Zeit immer „offener“ (Regeln werden eingetragen aber selten wieder entfernt).

Probleme mit IDS und IPS

- Erkennt nur bekannte Angriffe
- Unterwanderung ist möglich
- Sehr hoher Aufwand für den Betrieb
- Viel zu teuer, um im gesamten Netzwerk installiert zu werden
- Brauchen regelmäßige Updates der Signaturen
- IPS muss meist hochverfügbar ausgelegt werden (Bandbreite, niedrigere Verfügbarkeit)
- False positives haben direkte Auswirkungen auf die Produktion
- Im Auslieferungszustand sind nur 30%-50% der Signaturen aktiv

Innovative Lösung mit der honeyBox®

- Ein Honeypot ist ein System, dessen Wert darin besteht, von Angreifern attackiert zu werden. Angreifer sollen sich mit ihnen beschäftigen.
- Die Honeypot-Technologie wird seit vielen Jahren im Internet von IT-Sicherheitsforschern erfolgreich genutzt.
- secXtreme treibt die Nutzung von Honeypots in internen Netzwerken seit 5 Jahren voran und bietet die Technologie „out of the box" als Appliances an.

Angriffe mit der honeyBox® erkennen: Wie es funktioniert

1. Informationsrecherche (im Internet)

2. Scannen (Ping Ports, Betriebssysteme)
3. Erkunden (Dienste, Benutzer, Software)
4. Auf Systeme zugreifen

honeyBox®

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

honeyBox®

- Hardware- oder Software-Appliance
- 1, 4 oder 8 Ports
- Stellt virtuelle Honeypots zur Verfügung
- Bis zu 1.000 virtuelle Honeypots je Port möglich
- Einfache Inbetriebnahme
- Zuverlässige Erkennung
- Geringe Betriebsaufwände

honeyBox®

secXTREME Information Security

honeyBox® industrial

honeyBox® micro

honeyBox® Software

honeyBox® 4-Port

TÜV SÜD

HIRSCHMANN
A BELDEN BRAND

secXTREME Information Security

YELLO NETCOM

Ausgezeichnete Sicherheit

- Bayerischer Sicherheitspreis 2009
- Innovationspreis Mittelstand 2009 – Top 20 Kategorie IT-Security
- Innovationspreis Mittelstand 2010 – Bestenliste IT-Sicherheit

Funktionsweise

- Rauchmelder/Minenfeld
- Emulation einer großen Anzahl von Systemen
- Gleiche Betriebssysteme, nur schlechterer Patchstand oder ältere Versionen
- Für den Angreifer interessante Systeme

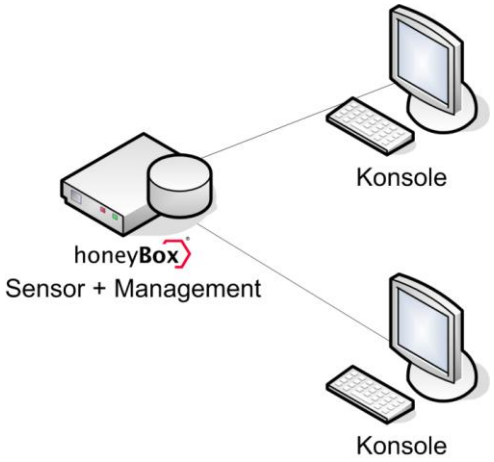
Zeit sparen mit der honeyBox®

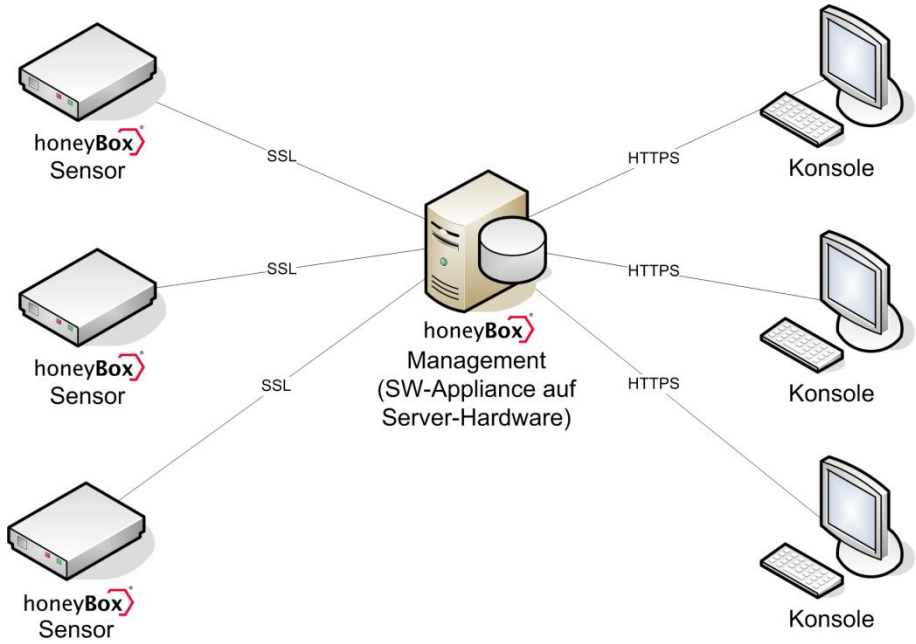
- Der Rollout ist sehr einfach, es sind keine Infrastrukturänderungen im Netzwerk notwendig
- Die Konfiguration ist schnell und einfach (kein langwieriges Tuning von Regeln)
- Sie benötigen wenig Betriebsaufwand
- Es gibt sehr wenig Fehlalarme

Geld sparen mit der honeyBox®

- Die Honeypots müssen nicht mit der Bandbreite der Netze, die sie überwachen, skalieren
- Sie sind deutlich billiger als IDS/IPS Systeme
- Auf einer Appliance lassen sich mehrere hundert virtuelle Honeypots je Port emulieren, daher ist kein eigenes System je Honeypot notwendig
- Wo bisher IDS Systeme im Einsatz waren, kann deren Erkennungspotential u. U. auf Honeypots verlagert werden

Mögliche Architekturen





Event-Management

secXTREME Information Security

Queried on : Tue June 02, 2009 20:38:38

Meta Criteria	*any*
IP Criteria	*any*
Layer 4 Criteria	*any*
Payload Criteria	*any*

Summary Statistics

- Sensors
- Unique Alerts
- (classifications)
- Unique addresses: Source | D
- Unique IP links
- Source Port: TCP | UDP

	ID	< Si
☐	#0-(8-3) [secxtreme] HONEYPOT IDENT conn	
☐	#1-(8-2) [secxtreme] HONEYPOT IDENT conn	
☐	#2-(8-1) [secxtreme] HONEYPOT IDENT conn	

{ action }

Meta

ID #	Time	Triggered Signature
8 - 3	2009-06-01 00:42:13	[secxtreme] HONEYPOT IDENT connection established (mod_ident.sh)

Sensor	Sensor Address	Interface	Filter
	server5.scheucher.de	eth0	*none*

Alert Group: *none*

Source Address	Dest. Address
192.168.100.1	192.168.100.89

Options: *none*

TCP

Source Port	Dest Port	R 1	R 0	URG	ACK	PSH	RST	SYN	FIN	seq #	ack	offset	res	window	urp	chksum
37124 [sans] [tantalo] [sstats]	113 [sans] [tantalo] [sstats]											0				= 0x0

Options: *none*

Payload

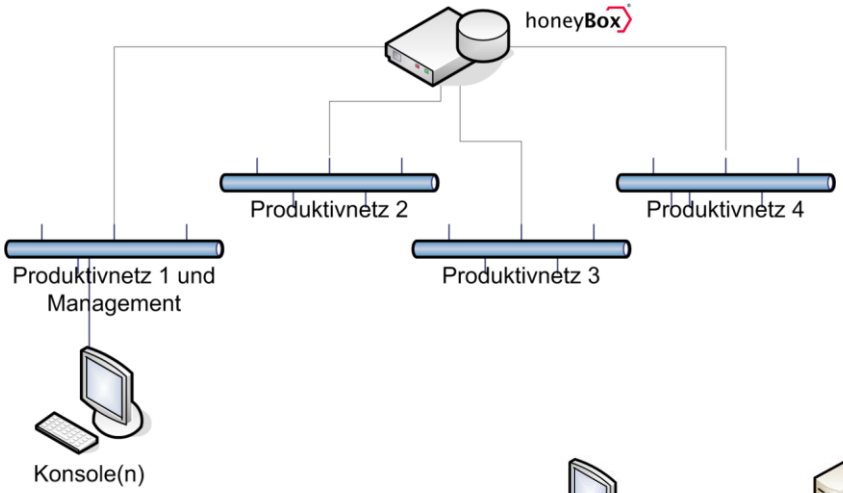
TÜV SÜD

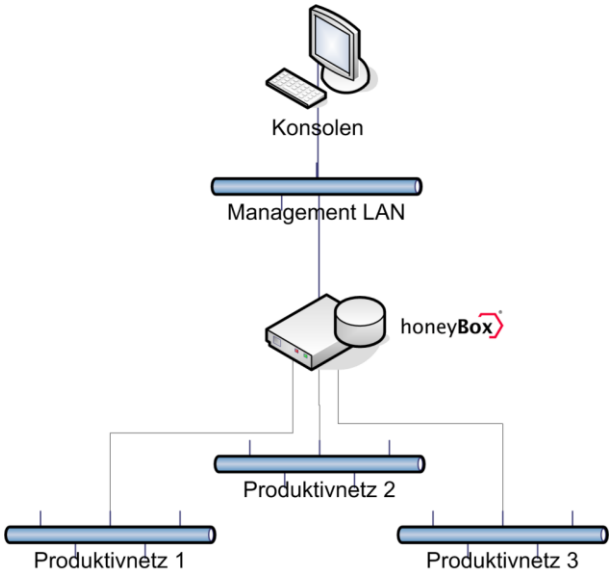
HIRSCHMANN A BELDEN BRAND

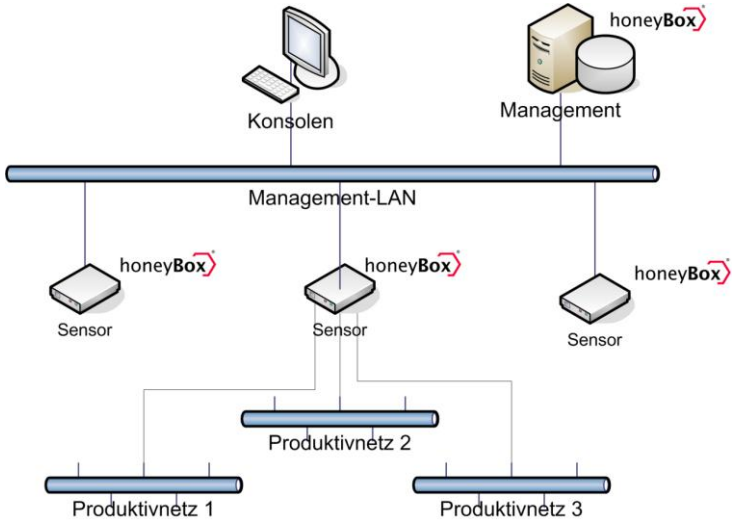
secXTREME Information Security

YELLO NETCOM

Integration ins Netzwerk







Was können Sie mit der honeyBox® erreichen?

- Angriffe einfach und zuverlässig erkennen
- Endlich das interne Netzwerk flächendeckend überwachen
- Erkennung ohne Verringerung der Verfügbarkeit
- Angreifer von produktiven Systemen auf Honeypots ziehen
- Zeit für Gegenmaßnahmen gewinnen
- Erhöhung der Sicherheit
- Dem Angreifer einen Schritt voraus sein

Vielen Dank für Ihre Aufmerksamkeit

Christian Scheucher
secXtreme GmbH
Kiefernstraße 38, D-85649 Brunnthal-Hofolding
Tel: +49 (0)89-18 90 80 68-11
Fax: +49 (0)89-18 90 80 68-77
E-Mail: christian.scheucher@sec-xtreme.com
www.sec-xtreme.com