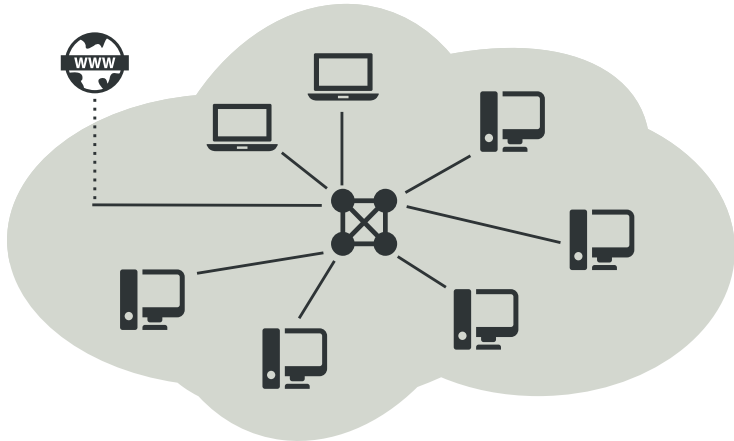


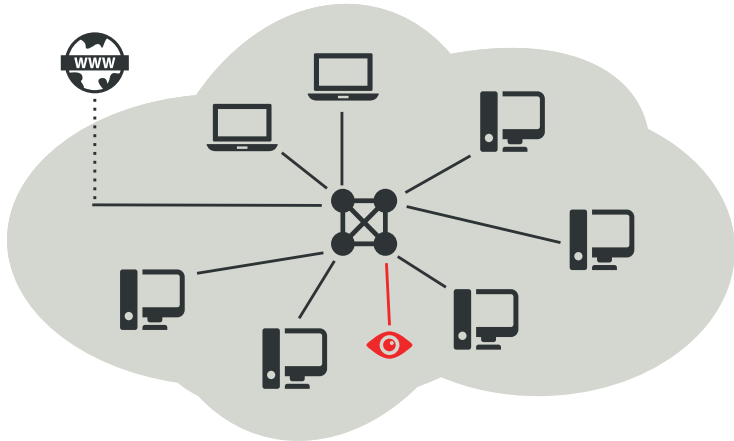
## Intrusion Detection mit Honeypots

Pascal Brückner

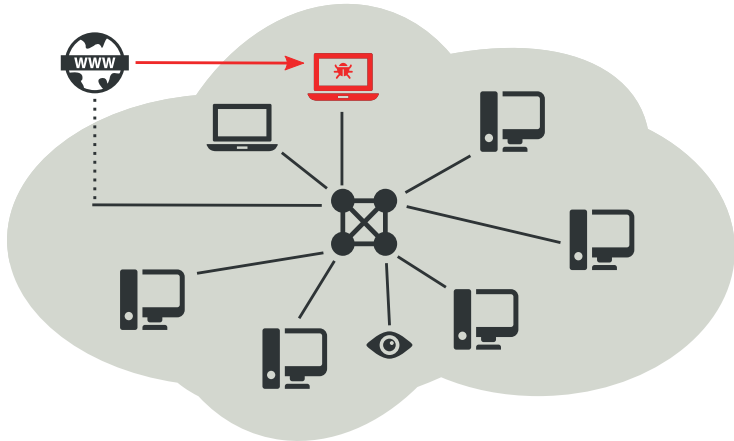
# Was ist ein Honeytrap?



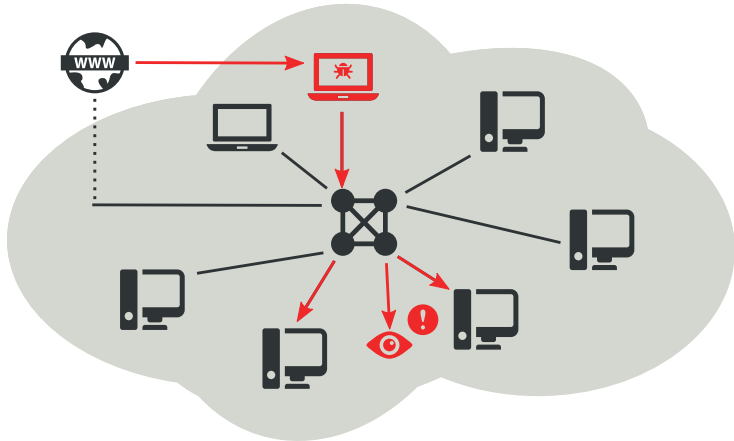
# Was ist ein Honeytrap?



# Was ist ein Honeytrap?



# Was ist ein Honeytrap?



## Definition nach Lance Spitzner

*„A honeypot is a closely monitored computing resource that we want to be probed, attacked or compromised.“*

## Definition nach Lance Spitzner

*„A honeypot is a closely monitored computing resource that we want to be probed, attacked or compromised.“*

- Ziele**
- Gewinn von Daten über Angreifer und deren Methoden
  - Ablenkung
  - Erkennung von Zero-Day-Angriffen
  - (Automatische Mitigation)

# Honeypots gibt es bereits. . .

## ■ Database Honeypots

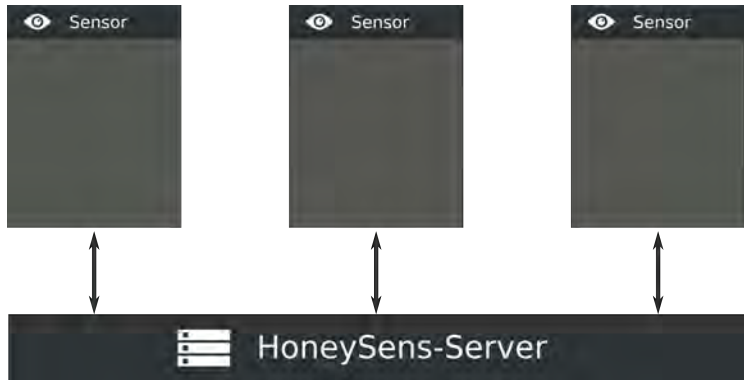
- [MongoDB-HoneyProxy](#) - A MongoDB honeypot proxy.
- [Elastic honey](#) - A Simple Elasticsearch Honeypot.
- [mysql](#) - A mysql honeypot, still very very early stage.
- [NoSQLpot](#) - The NoSQL Honeypot Framework.
- [ESPot](#) - An Elasticsearch honeypot written in NodeJS, to capture every attempts to exploit CVE-2014-3120.
- [Deilalah](#) - An Elasticsearch Honeypot written in Python.
- [mysql-honeypotd](#) - Low interaction MySQL honeypot written in C.

## ■ Web honeypots

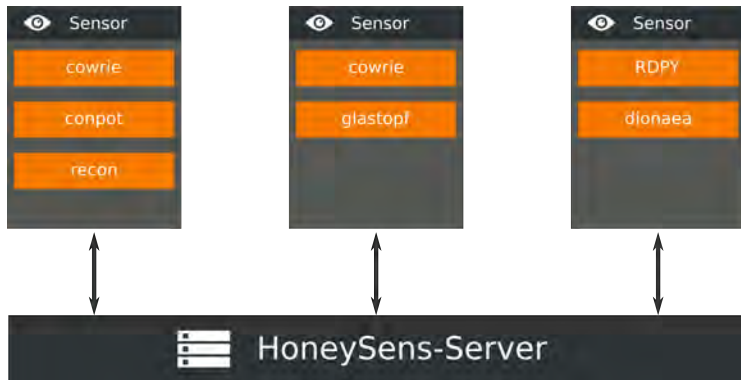
- [Glastopf](#) - Web Application Honeypot.
- [Snare/Tanner](#) - successors to Glastopf
  - [Snare](#) - Super Next generation Advanced Reactive honEypot
  - [Tanner](#) - Evaluating SNARE events
- [phpmyadmin\\_honeypot](#) - - A simple and effective phpMyAdmin honeypot.
- [Nodepot](#) - A nodejs web application honeypot.
- [basic-auth-pot](#) [bap](#) - http Basic Authentication honeyPot.
- [Shadow Daemon](#) - A modular Web Application Firewall / High-Interaction Honeypot for PHP, Perl & Python apps.
- [Servletpot](#) - Web application Honeypot.
- [Google Hack Honeypot](#) - designed to provide reconnaissance against attackers that use search engines as a hacking tool against your resources.
- [smart-honeypot](#) - PHP Script demonstrating a smart honey pot.
- [Bukkit Honeypot Honeypot](#) - A honeypot plugin for Bukkit.
- [Laravel Application Honeypot](#) - Honeypot - Simple spam prevention package for Laravel applications.
- [stack-honeypot](#) - Inserts a trap for spam bots into responses.
- [EoHoneypotBundle](#) - Honeypot type for Symfony2 forms.
- [shockpot](#) - WebApp Honeypot for detecting Shell Shock exploit attempts.



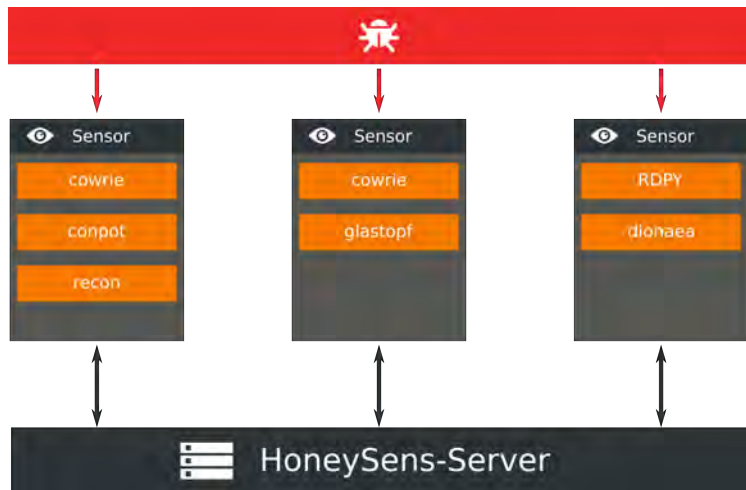
..., wir machen sie bequem nutzbar



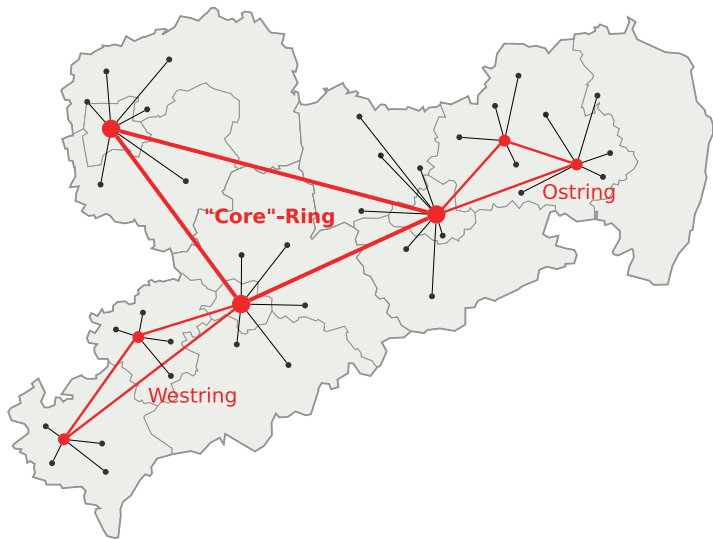
..., wir machen sie bequem nutzbar



..., wir machen sie bequem nutzbar



# Motivation

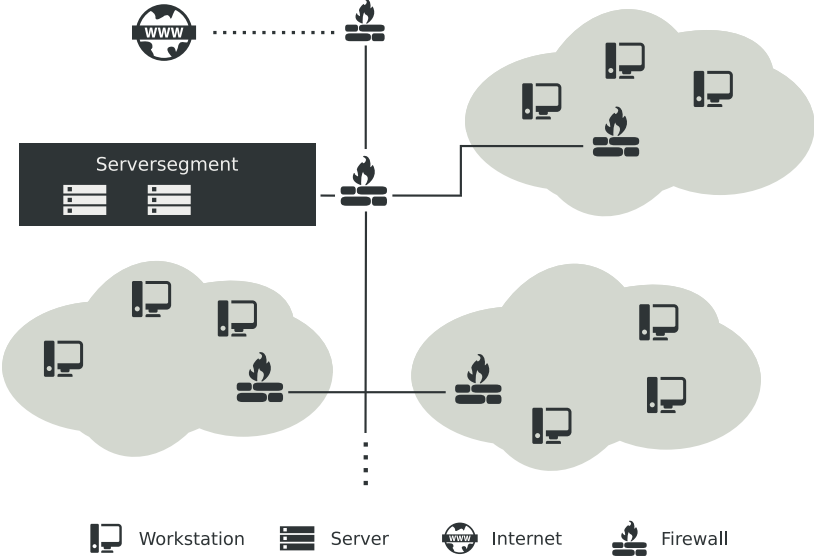


- Zielstellung** Konzeption eines Frühwarnsystems für Angriffe *aus dem Inneren* eines Netzwerks (z.B. Malware oder Innentäter)
- ... mit Hilfe von Honeypots
  - ... kostengünstig
  - ... transparent in ein bestehendes Netzwerk integrierbar
  - ... nutzerfreundlich
  - ... mit möglichst großer Netzabdeckung

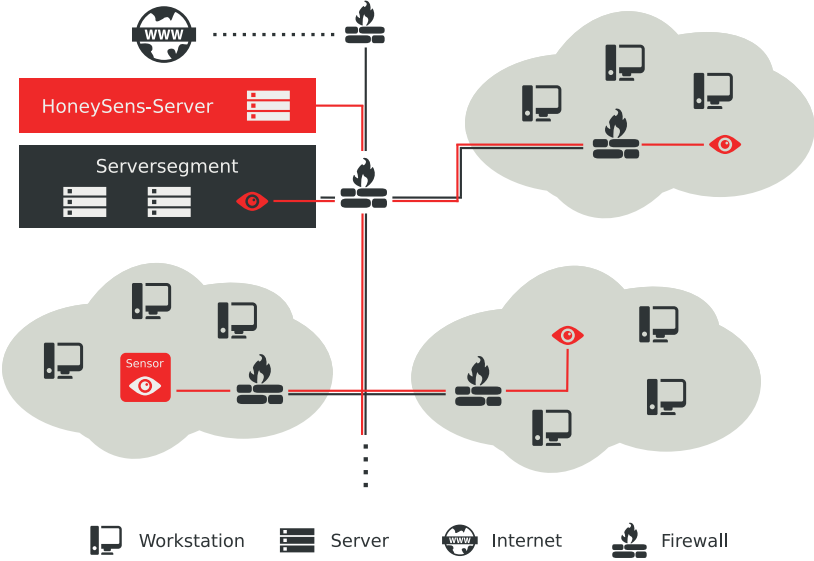
- Zielstellung** Konzeption eines Frühwarnsystems für Angriffe *aus dem Inneren* eines Netzwerks (z.B. Malware oder Innentäter)
- ... mit Hilfe von Honeypots
  - ... kostengünstig
  - ... transparent in ein bestehendes Netzwerk integrierbar
  - ... nutzerfreundlich
  - ... mit möglichst großer Netzabdeckung

**Werdegang** **2014:** Konzeption als Diplomarbeit  
**seit 2015:** Forschungsprojekt, finanziert und unterstützt vom Sächsischen Innenministerium  
**seit 2017:** Veröffentlichung als OpenSource, sowie kommerziell vertrieben durch die T-Systems MMS,  
**seit 2018:** verfügbar als Cloud-Lösung

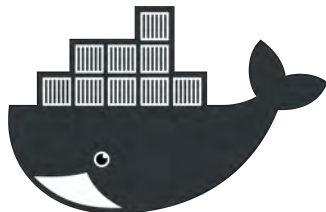
# Integration ins Unternehmensnetz



# Integration ins Unternehmensnetz







**Funktion** Simulation von Netzwerkdiensten,  
Täuschung von Angreifern,  
Datenlieferant zum Server

**Plattform** BeagleBone Black,  
Virtualisiert (als Docker-Container)



# Server: Sensorliste

HoneySens admin (Logout)

5	lzw		0.2.3	Online (vor 17 Minuten)	
6	PySG2		0.2.3	Online (vor 15 Minuten)	
9	Mitarbeiter		0.2.0	Timeout (vor 152 Tag(en))	
10	Server		0.2.0	Timeout (vor 152 Tag(en))	
11	Pool-A		0.2.3	Online (vor 16 Minuten)	
12	Bamberger		0.2.3	Online (vor 12 Minuten)	
13	Pool-LA		0.2.3	Online (vor 4 Minuten)	
14	sensor-bss		0.2.3	Online (vor 5 Minuten)	
15	sensor-mo11		0.2.3	Online (vor 2 Minuten)	
16	Linux-Netz-Sensor		0.2.0	Update: Phase 1 (vor 12 Minuten)	
17	Windows-Netz-Sensor		0.2.0	Timeout (vor 358 Tag(en))	
18		Haus 25 Verteilerraum	0.2.3	Online (vor 16 Minuten)	
19	HP_025_106		0.2.3	Online (vor 14 Minuten)	
20	HP_DMZ_WEB		0.2.3	Online (vor 15 Minuten)	
21	HP_UKD_Client		0.2.0	Timeout (vor 69 Tag(en))	
23	dud-09		0.2.3	Online (vor 7 Minuten)	
24	dud-11		0.2.3	Online (vor 13 Minuten)	
25	dud-15		0.2.3	Online (vor 18 Minuten)	

0.2.5

# Server: Ereignisse

HoneySens admin (Logout)

## Ereignisse

Gruppe:  Sensor: Alle Klassifikation: Alle

ID	Zeitpunkt	Sensor	Klassifikation	Quelle	Details	Status	Aktionen
46716	12.03.2018 22:18:50	...	Honeypot	141.76....	SSH	Neu	
46714	12.03.2018 22:18:47	...	Honeypot	141.76....	SSH	Neu	
46713	12.03.2018 22:17:46	...	Portscan	141.76....	Scan	Neu	
46711	12.03.2018 22:16:27	...	Portscan	141.76....	Scan	Neu	
46709	12.03.2018 22:15:08	...	Portscan	141.76....	Scan	Neu	
46705	12.03.2018 22:12:28	...	Portscan	141.76....	Scan	Neu	
46704	12.03.2018 22:11:09	...	Portscan	141.76....	Scan	Neu	
46703	12.03.2018 22:09:50	...	Portscan	141.76....	Scan	Neu	
46702	12.03.2018 22:08:32	...	Portscan	141.76....	Scan	Neu	
46699	12.03.2018 22:07:13	...	Portscan	141.76....	Scan	Neu	
46697	12.03.2018 22:05:54	...	Portscan	141.76....	Scan	Neu	
46695	12.03.2018 22:04:35	...	Portscan	141.76....	Scan	Neu	

0.2.5

31 32 33 34 35 36 37 38 39 40

# Beispiel: Portscan

The screenshot shows the HoneySens web interface. At the top left is the HoneySens logo. At the top right, the user 'admin' is logged in. The main heading is 'Ereignisdetails'. Below this, the event details are listed: Zeitpunkt: 12.03.2018 22:18:53, Sensor: [redacted], Klassifikation: Portscan, Quelle: 141.76.[redacted], and Details: Scan. Below the details is a red header for 'Paketübersicht (26)'. A table follows with columns for Zeit, Protokoll, Port, Flags, and Payload. The table contains 12 rows of scan results.

Zeit	Protokoll	Port	Flags	Payload
22:18:47	TCP	256	S	
22:18:47	TCP	256	S	
22:18:47	TCP	993	S	
22:18:48	TCP	199	S	
22:18:50	TCP	113	S	
22:18:50	TCP	25	S	
22:18:51	TCP	110	S	
22:18:51	TCP	195	S	
22:18:51	TCP	80	S	
22:18:51	TCP	587	S	
22:18:51	TCP	256	S	
22:18:51	TCP	993	S	

# Beispiel: SSH-Zugriff

The screenshot shows the HoneySens web interface. At the top left is the HoneySens logo. At the top right, the user 'admin' is logged in, with a 'Logout' link. The main heading is 'Ereignisdetails'. Below this, the event details are listed:

- Zeitpunkt: 12.03.2018 22:32:04
- Sensor: [redacted]
- Klassifikation: Honeypot
- Quelle: 141.76.[redacted]
- Details: SSH

A red header bar indicates 'Sensorinteraktion (5)'. Below it is a table with two columns: 'Zeit' and 'Aktion'.

Zeit	Aktion
22:32:04	New connection: 141.76.[redacted]:56217
22:32:04	Client version: [SSH-2.0-libssh_0.7.5]
22:32:05	Login failed [MGRATTS000]
22:32:06	Login failed [MGRATTS000]
22:32:07	Connection Lost

At the bottom of the table area, there is a dark grey button with a checkmark icon and the text 'Schließen'. In the bottom left corner of the interface, the version number '0.2.5' is displayed.

# Beispiel: HTTP/CGI-Angriff

HoneySens admin (Logout)

Paketübersicht (28)

Zeit	Protokoll	Port	Flags	Payload
05:24:27	TCP	80	S	
05:24:27	TCP	80	S	
05:24:28	TCP	80	A	
05:24:28	TCP	80	PA	GET / HTTP/1.1 \nConnection: Close \nHost: [REDACTED] tu-dresden.de \nPragma: no-cache \nCache-Control: no-cache \nUser-Agent: Mozilla/5.0 [en] (X11; U; OpenVAS 9.0.1) \nAccept: image/gif, image/x-x
05:24:28	TCP	80	S	
05:24:28	TCP	80	A	
05:24:28	TCP	80	PA	GET /cgi-bin/chargepw.exe_192371753 HTTP/1.1 \nConnection: Close \nHost: [REDACTED] tu-dresden.de \nPragma: no-cache \nCache-Control: no-cache \nUser-Agent: Mozilla/5.0 [en] (X11; U; OpenVAS 9.0.1) \n
05:24:29	TCP	80	S	
05:24:29	TCP	80	A	
05:24:29	TCP	80	S	
05:24:29	TCP	80	PA	GET /redirect.exe HTTP/1.1 \nConnection: Close \nHost: [REDACTED] tu-dresden.de \nPragma: no-cache \nCache-Control: no-cache \nUser-Agent: Mozilla/5.0 [en] (X11; U; OpenVAS 9.0.1) \nAccept: image/gif,
05:24:29	TCP	80	A	
05:24:29	TCP	80	PA	GET /scripts/sgdynamo.exe?HTNAME=sgdynamo.exe HTTP/1.1 \nConnection: Close \nHost: [REDACTED] tu-dresden.de \nPragma: no-cache \nCache-Control: no-cache \nUser-Agent: Mozilla/5.0 [en] (X11; U; OpenVA
05:24:29	TCP	80	S	
05:24:29	TCP	80	S	
05:24:30	TCP	80	A	

0.25

The screenshot shows the HoneySens web interface. The top left corner displays the HoneySens logo and name. The top right corner shows the user 'admin' with a 'Logout' link. The main heading is 'Ereignisdetails'. Below this, the event details are listed:

- Zeitpunkt: 11.06.2018 20:27:42
- Sensor: [redacted]
- Klassifikation: Verbindungsversuch
- Quelle: [redacted]
- Details: Einzelverbindung

Below the details is a section titled 'Paketübersicht (2)' which contains a table of network packets:

Zeit	Protokoll	Port	Flags	Payload
20:27:42	UDP	137		
20:27:42	UDP	137		

At the bottom of the table area, there is a dark grey bar with a checkmark and the text 'Schließen'.



# Beispiel: ???

The screenshot shows the HoneySens web interface. At the top left is the HoneySens logo. At the top right, there is a user profile for 'admin' with a 'Logout' link. A vertical sidebar on the left contains various navigation icons. The main content area is titled 'Ereignisdetails' (Event Details). Below the title, several key-value pairs are listed: 'Zeitpunkt' (Timestamp) is 27.01.2017 14:59:37, 'Sensor' is Mitarbeiter, 'Klassifikation' (Classification) is Verbindungsversuch (Connection Attempt), 'Quelle' (Source) is 123.123.123.123, and 'Details' is Einzelverbindung (Single Connection). Below this is a section titled 'Paketübersicht (2)' (Packet Overview (2)), which contains a table with two rows of packet data. The table has columns for 'Zeit' (Time), 'Protokoll' (Protocol), 'Port', 'Flags', and 'Payload'. Both rows show a timestamp of 14:59:37, protocol TCP, port 58502, and flags FPA. The payload for both is 'x\x\*\xexax \ixyif\$ÄÜ;D^~Äpqj,äDfm\_YCdp}A~1'. At the bottom of the packet overview section is a dark button with a checkmark and the text 'Schließen' (Close).

HoneySens admin (Logout)

## Ereignisdetails

ID: [redacted]

Zeitpunkt: 27.01.2017 14:59:37

Sensor: Mitarbeiter

Klassifikation: Verbindungsversuch

Quelle: 123.123.123.123

Details: Einzelverbindung

### Paketübersicht (2)

Zeit	Protokoll	Port	Flags	Payload
14:59:37	TCP	58502	FPA	x\x*\xexax \ixyif\$ÄÜ;D^~Äpqj,äDfm_YCdp}A~1
14:59:37	TCP	58502	FPA	x\x*\xexax \ixyif\$ÄÜ;D^~Äpqj,äDfm_YCdp}A~1

✓ Schließen

0.2.1

# Testbetrieb: Behördennetz (SVN)

- Auswertung von Ereignissen durch das **CERT**

# Testbetrieb: Behördennetz (SVN)

- Auswertung von Ereignissen durch das **CERT**
- Misstrauen einiger Teilnetzbetreiber ggü. der Lösung



# Testbetrieb: Behördennetz (SVN)

- Auswertung von Ereignissen durch das **CERT**
- Misstrauen einiger Teilnetzbetreiber ggü. der Lösung



- **Erkenntnis:** Netz-Fehlkonfigurationen können sichtbar werden

- Honeypots**
- simulieren Webanwendungen, Remote-Wartungstools (SSH/RDP), Industriesteuerungen usw.

## Honeypots

- simulieren Webanwendungen, Remote-Wartungstools (SSH/RDP), Industriesteuerungen usw.

## Betrieb

- Im **SVN** mit 15 Teilnehmern aus Ländern & Kommunen, im Aufbau
- An der **Technischen Universität Dresden**
- Testinstallationen **in Unternehmen** in Dresden und Umgebung

- Honeypots**
  - simulieren Webanwendungen, Remote-Wartungstools (SSH/RDP), Industriesteuerungen usw.
- Betrieb**
  - Im **SVN** mit 15 Teilnehmern aus Ländern & Kommunen, im Aufbau
  - An der **Technischen Universität Dresden**
  - Testinstallationen **in Unternehmen** in Dresden und Umgebung
- Vertrieb**
  - kommerziell durch die T-Systems Multimedia Solutions
  - Als **On-Premise-Lösung** oder **cloudbasierter Dienst**
  - **OpenSource**-Variante auf GitHub verfügbar

- Honeypots**
  - simulieren Webanwendungen, Remote-Wartungstools (SSH/RDP), Industriesteuerungen usw.
- Betrieb**
  - Im **SVN** mit 15 Teilnehmern aus Ländern & Kommunen, im Aufbau
  - An der **Technischen Universität Dresden**
  - Testinstallationen **in Unternehmen** in Dresden und Umgebung
- Vertrieb**
  - kommerziell durch die T-Systems Multimedia Solutions
  - Als **On-Premise-Lösung** oder **cloudbasierter Dienst**
  - **OpenSource**-Variante auf GitHub verfügbar
- Roadmap**
  - Ab Herbst Einbindung der Sächsischen Wirtschaft
  - Weiterentwicklung parallel über MMS und TUD



Vielen Dank für Ihre Aufmerksamkeit!



**Kontakt** **SAX.CERT**

sax.cert@cert.sachsen.de

**T-Systems MMS**

marcel.wallbaum@t-systems.com

**Pascal Brückner** (für Forschungsfragen)

pascal.brueckner@tu-dresden.de