Intrusion Detection mit Honeypots

Pascal Brückner

T-SYSTEMS MULTIMEDIA SOLUTIONS

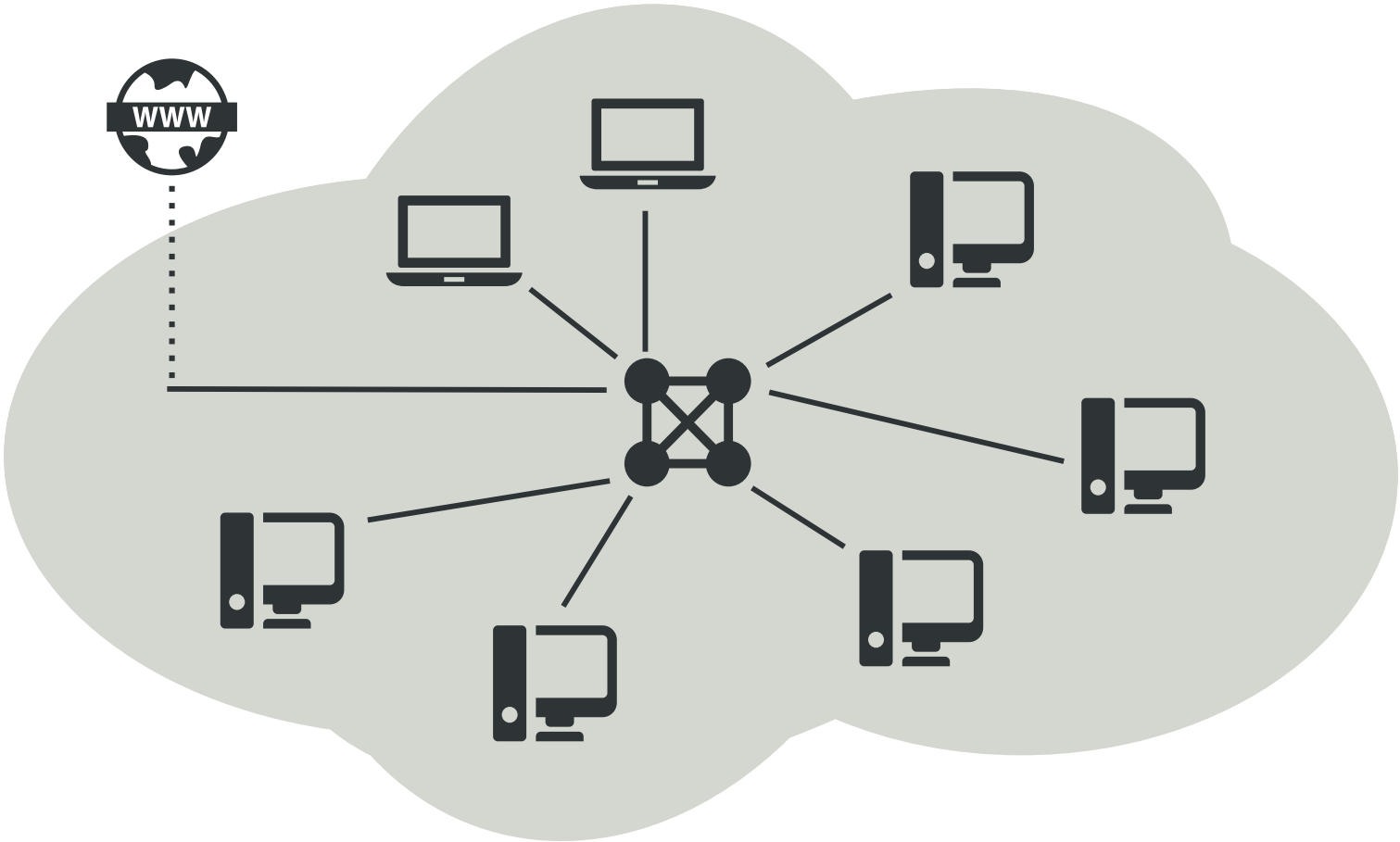
TECHNISCHE UNIVERSITÄT DRESDEN

SAX.CERT

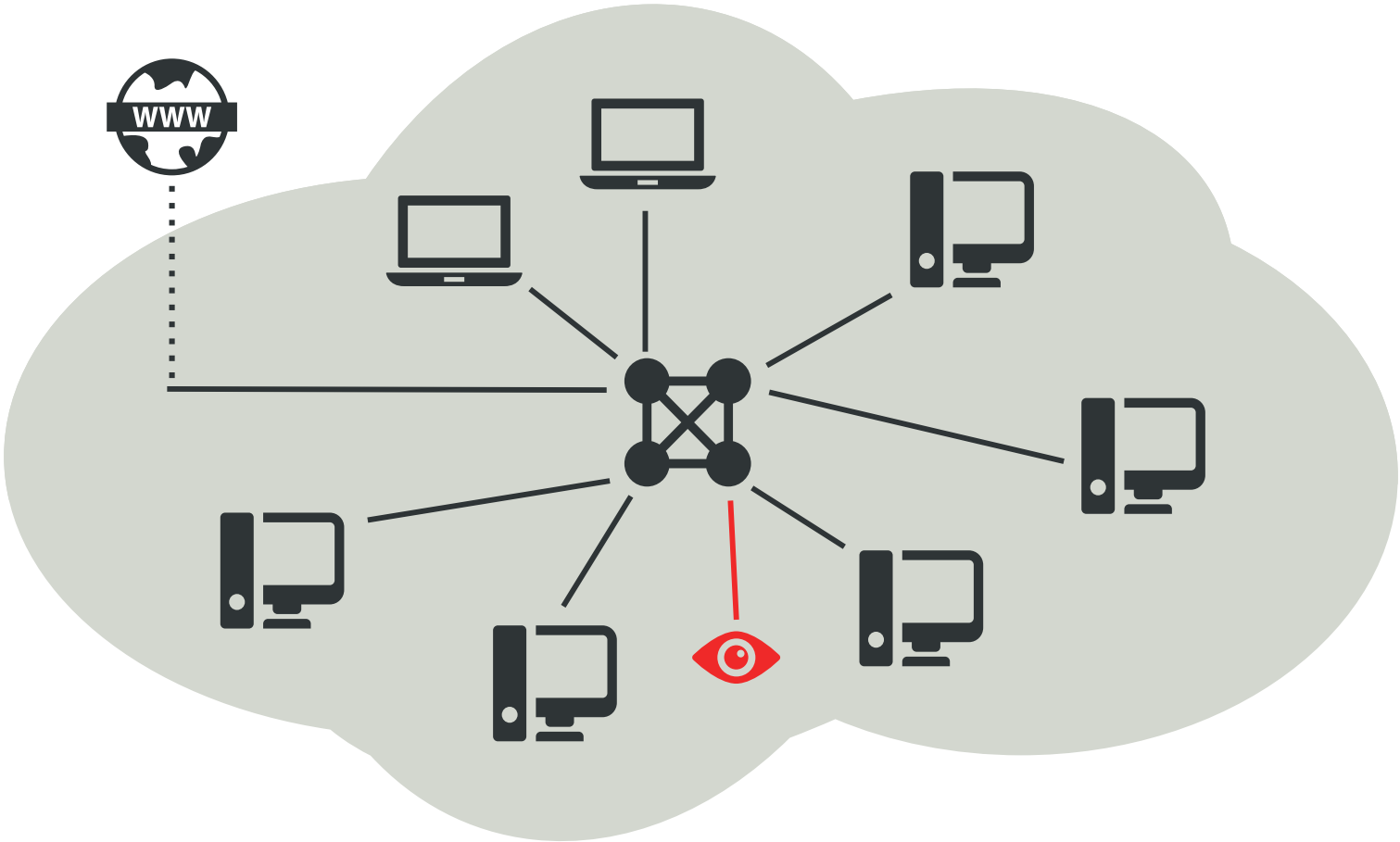
STAATSMINISTERIUM DES INNERN

Freistaat SACHSEN

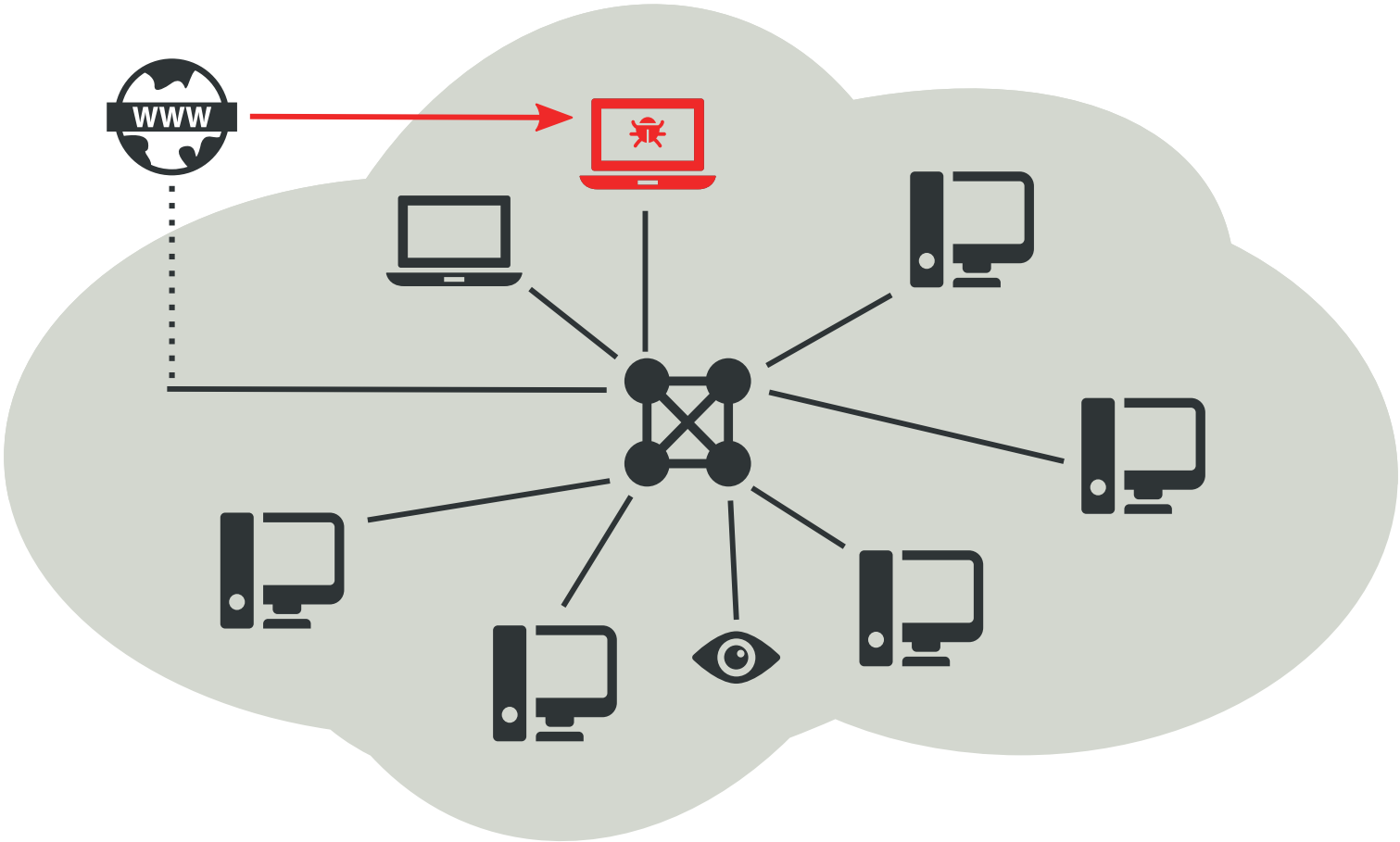
Was ist ein Honeypot?



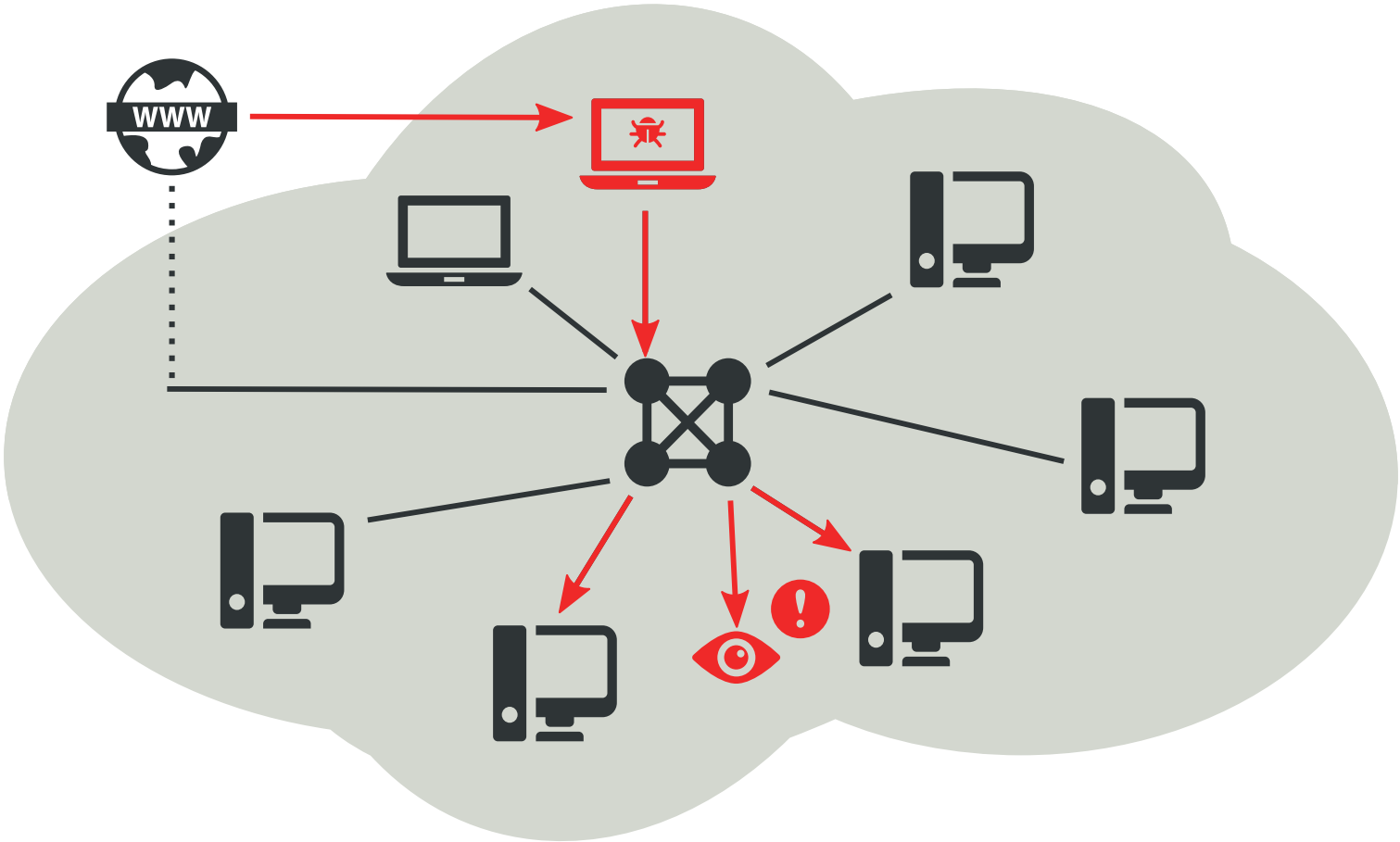
Was ist ein Honeypot?



Was ist ein Honeypot?



Was ist ein Honeypot?



Honeypot: Grundlagen

Definition **nach Lance Spitzner**

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

Honeypot: Grundlagen

Definition **nach Lance Spitzner**

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

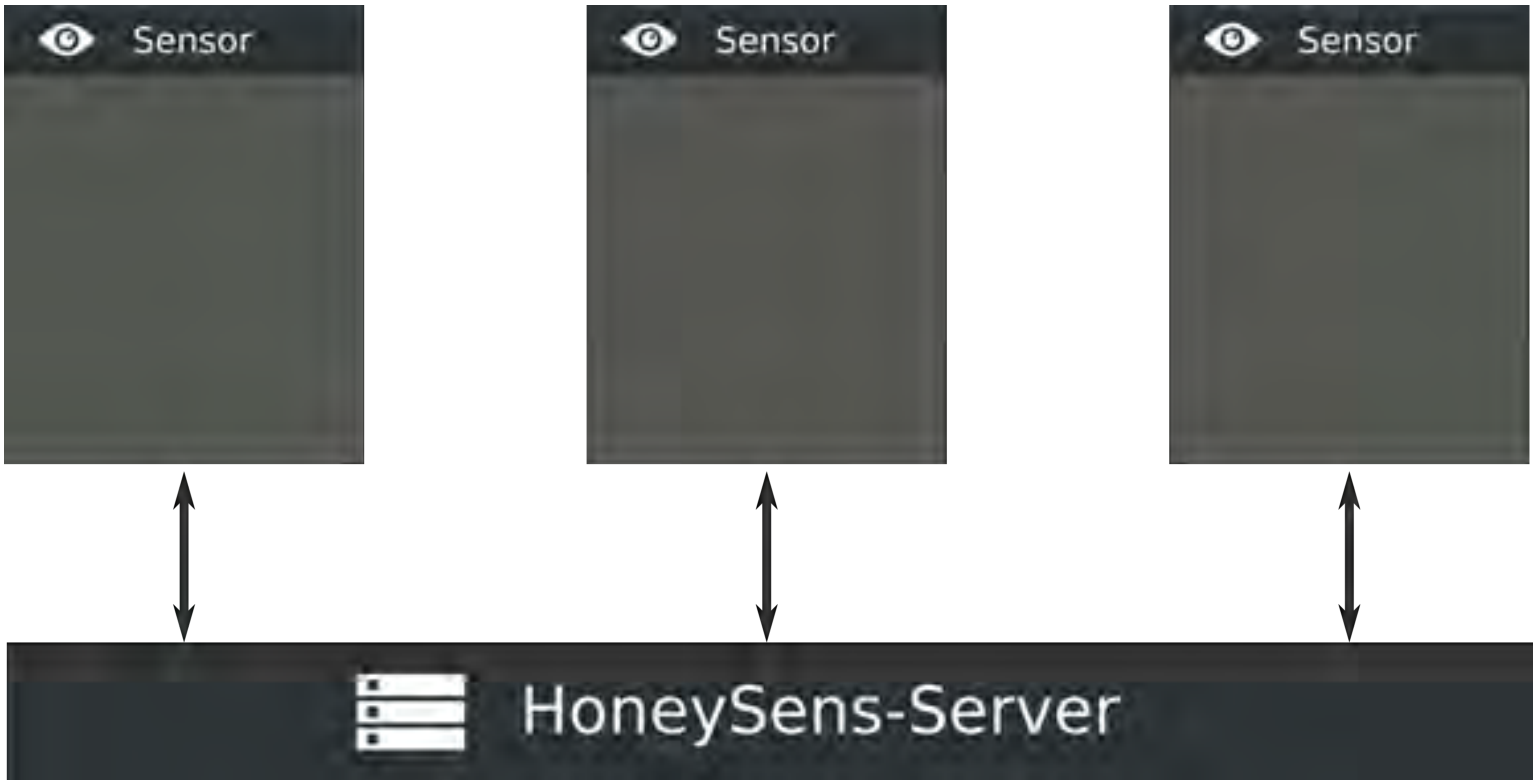
Ziele

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

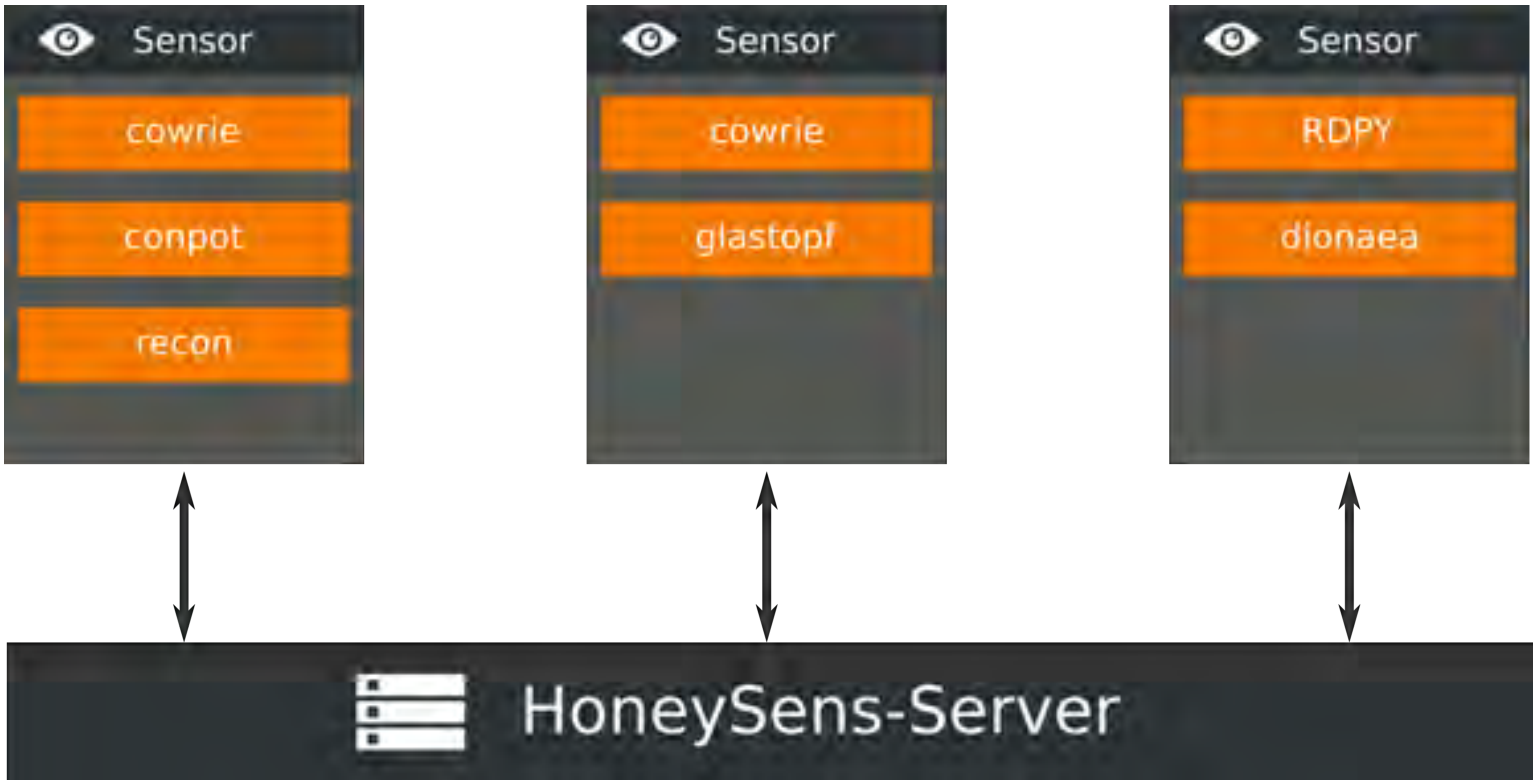
Honeypots gibt es bereits...

- 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.
  - Delilah - 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.
  - EcHoneypotBundle - Honeypot type for Symfony2 forms.
  - shockpot - WebApp Honeypot for detecting Shell Shock exploit attempts.

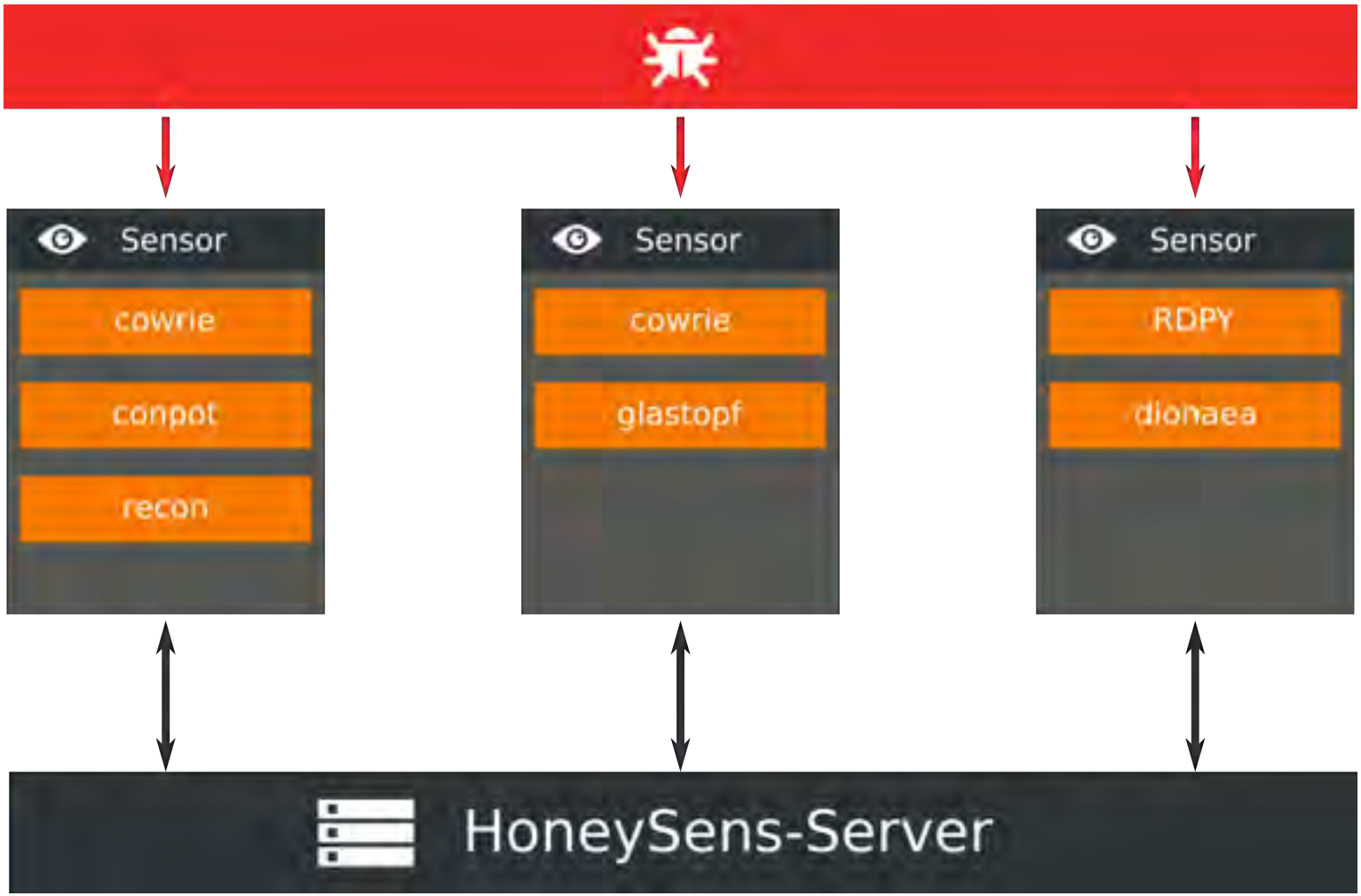
. . . , wir machen sie bequem nutzbar



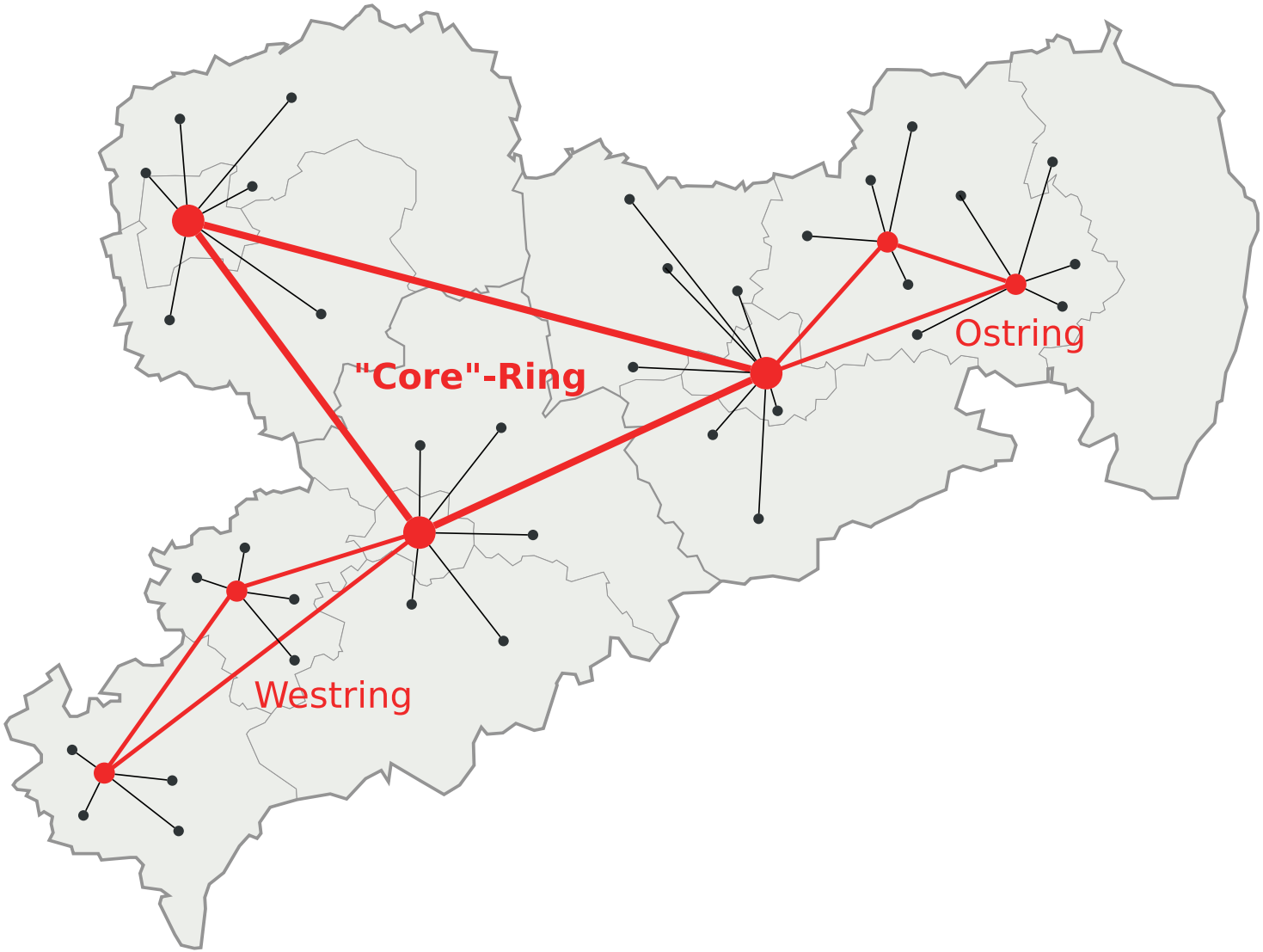
. . . , wir machen sie bequem nutzbar



. . . , wir machen sie bequem nutzbar



Motivation



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

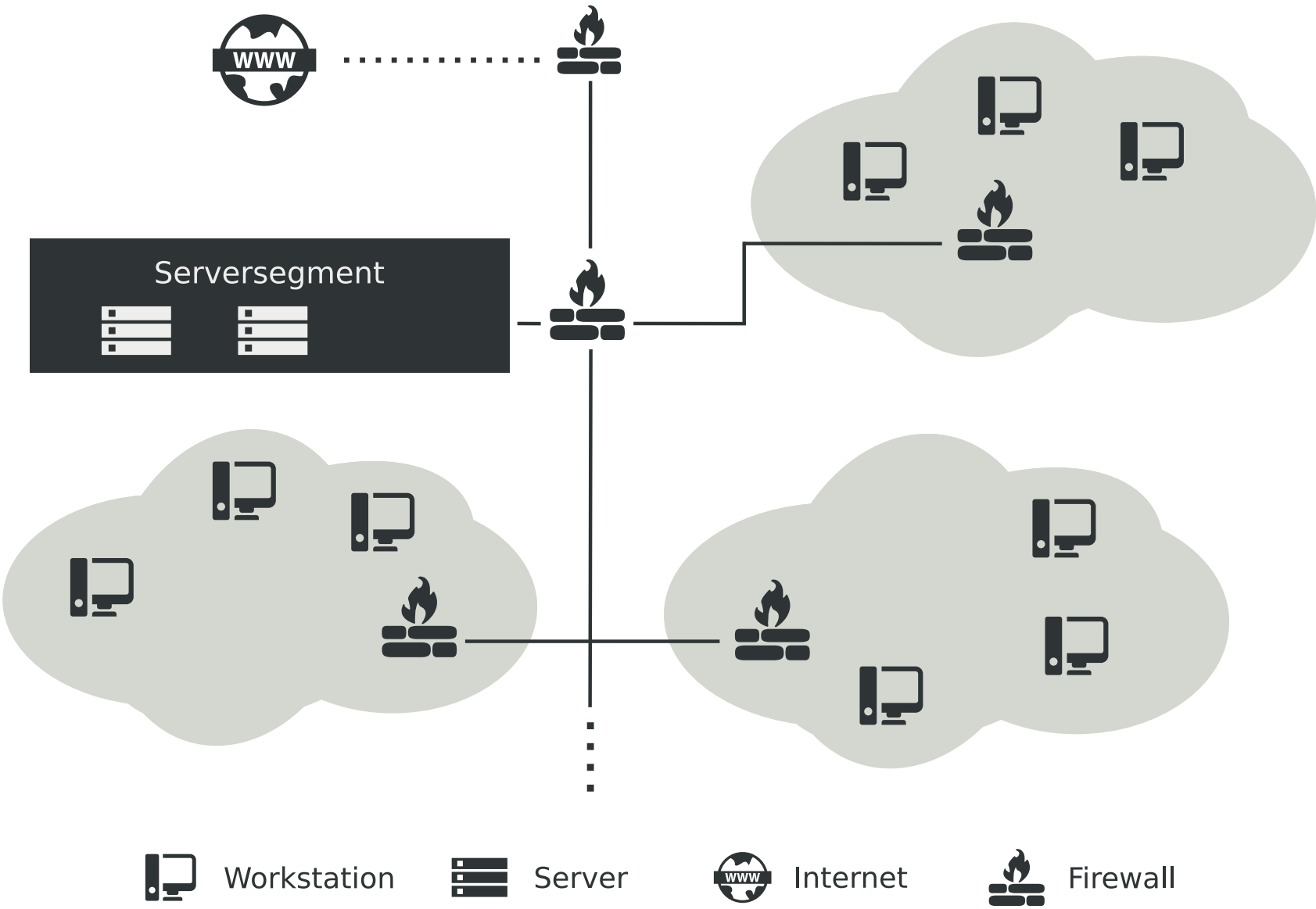
Motivation

Zielstellung Konzeption eines Frühwarnsystems für Angriffe *aus dem Inneren* eines Netzwerks (z.B. Malware oder Innentäter)

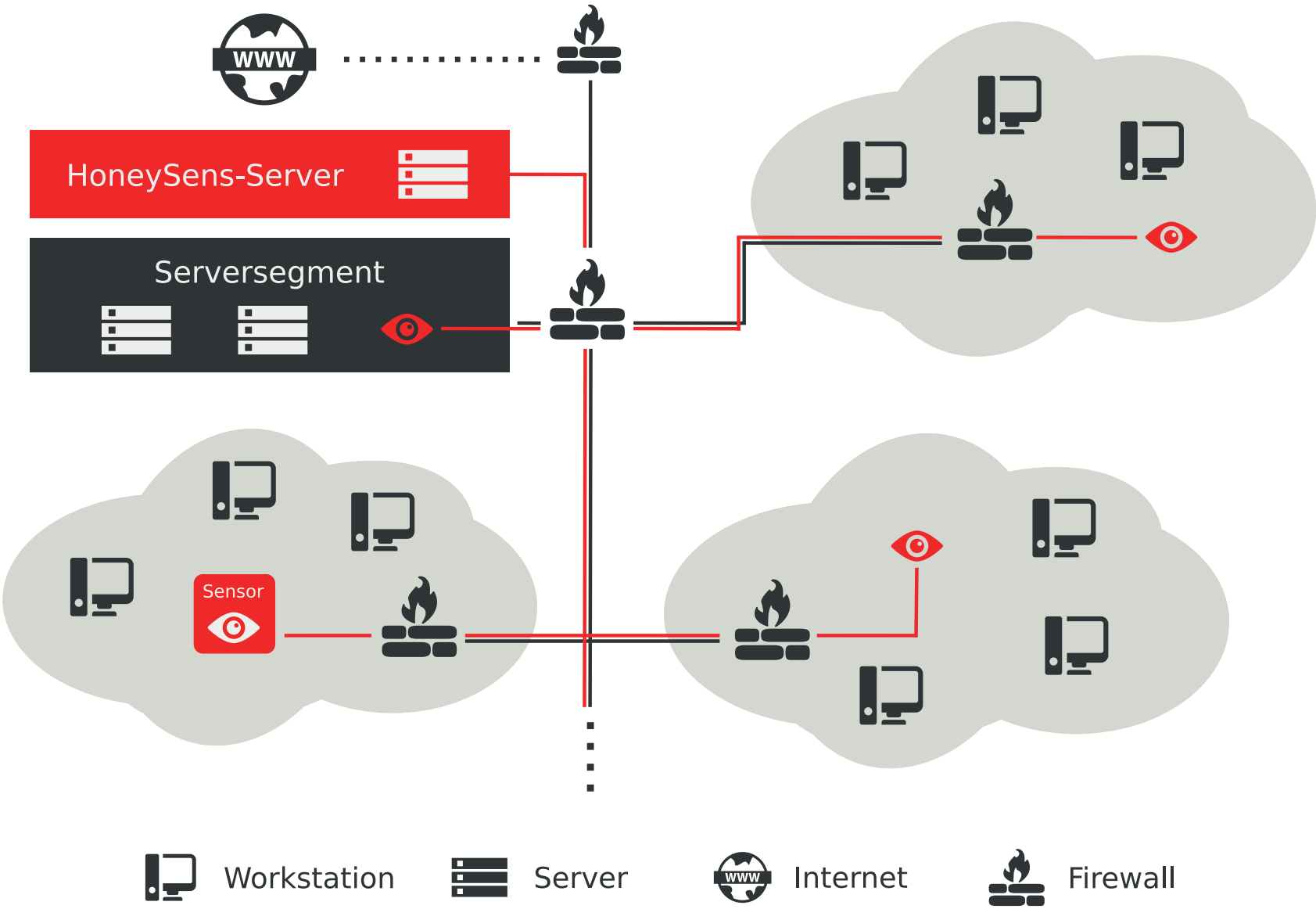
- . . . mit Hilfe von Honeypots
- . . . kostengünstig
- . . . transparent in ein bestehendes Netzwerk integrierbar
- . . . nutzerfreundlich
- . . . mit möglichst großer Netzabdeckung

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

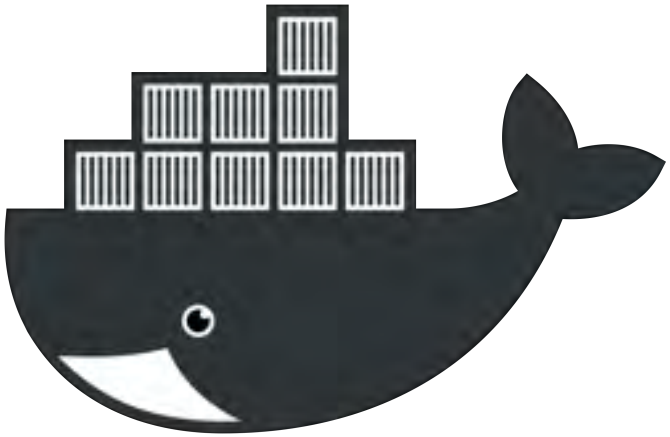
Integration ins Unternehmensnetz



Integration ins Unternehmensnetz



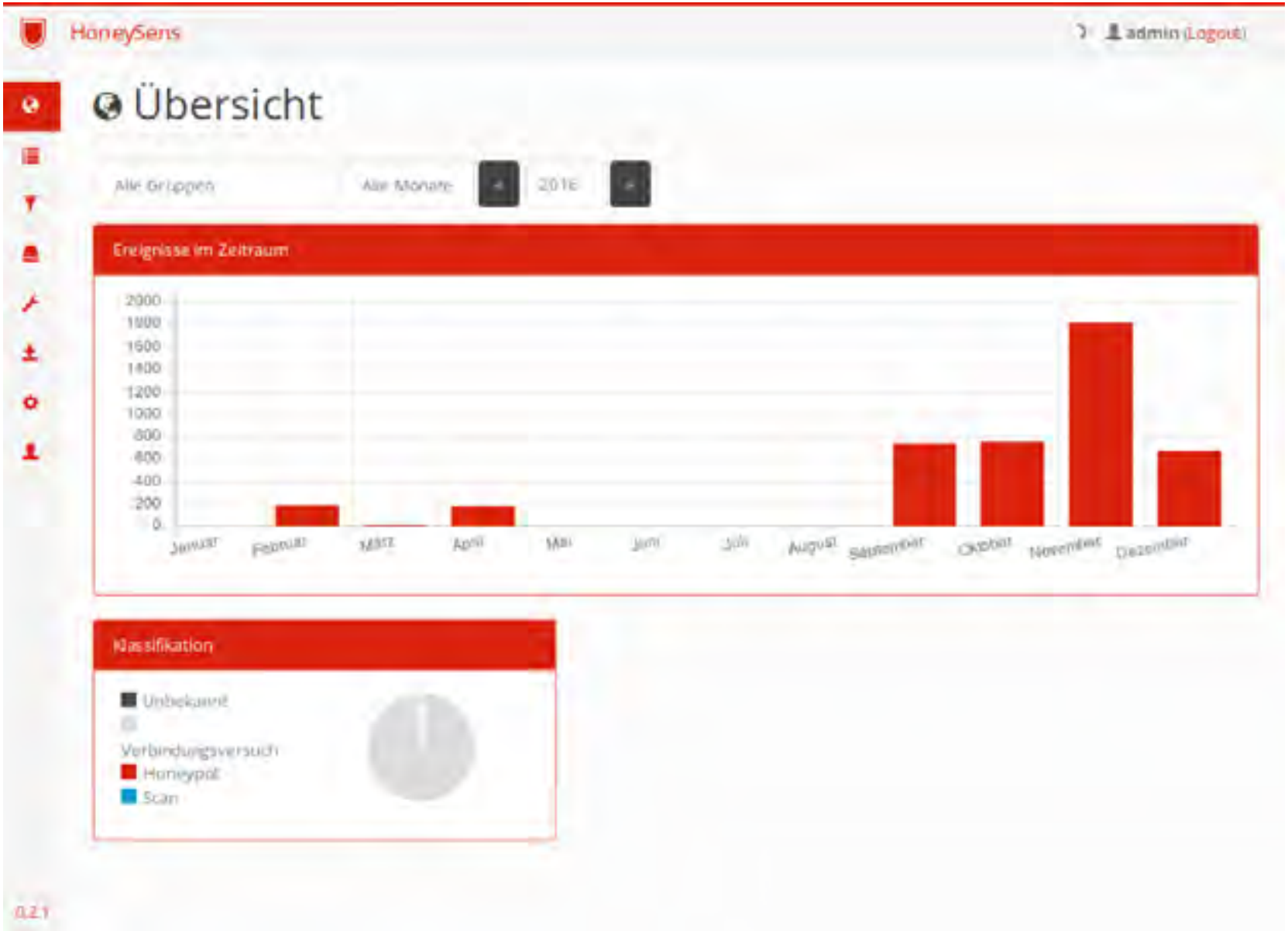
Sensoren



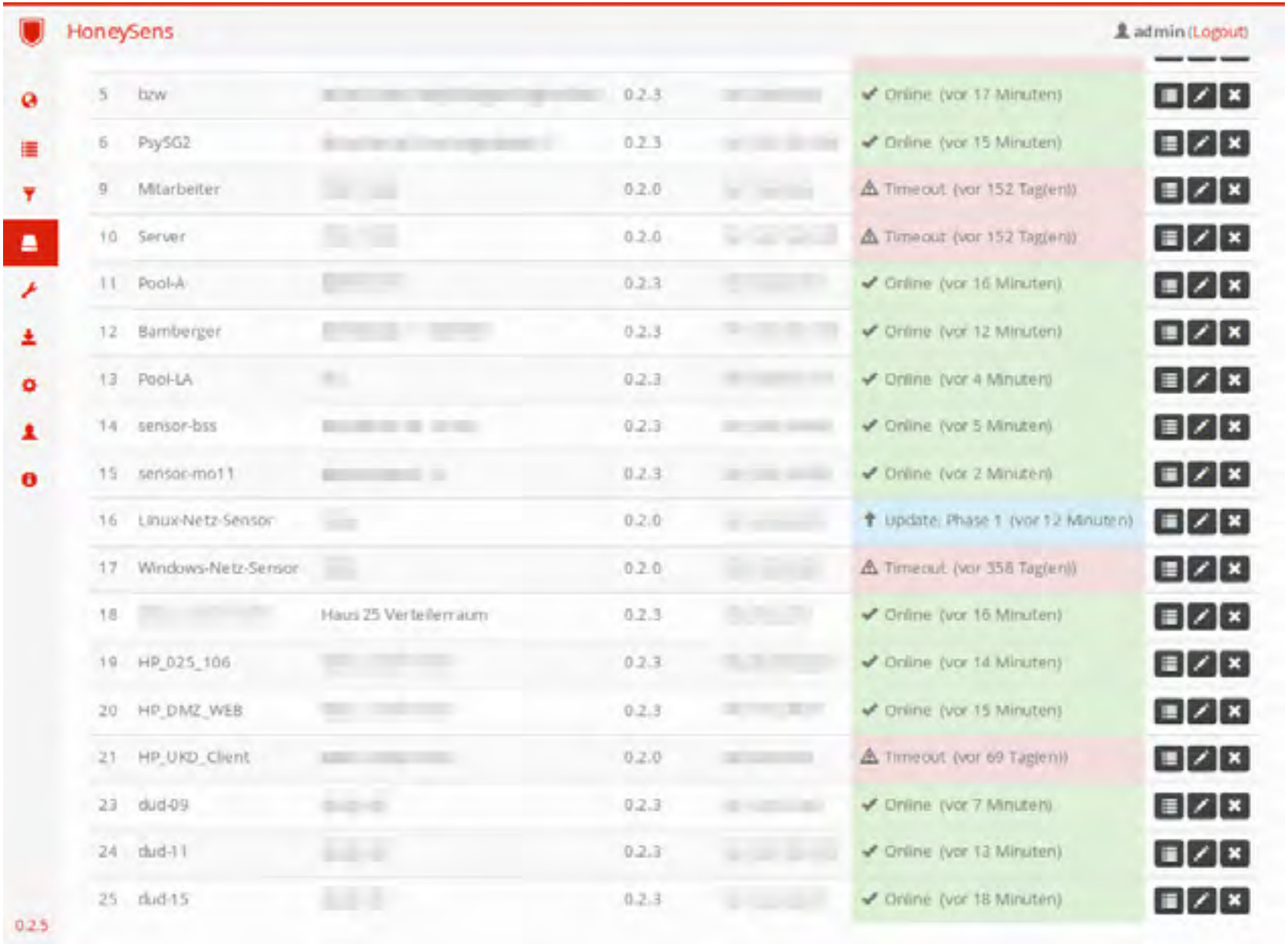
Funktion Simulation von Netzwerkdiensten,
Täuschung von Angreifern,
Datenlieferant zum Server

Plattform BeagleBone Black,
Virtualisiert (als Docker-Container)

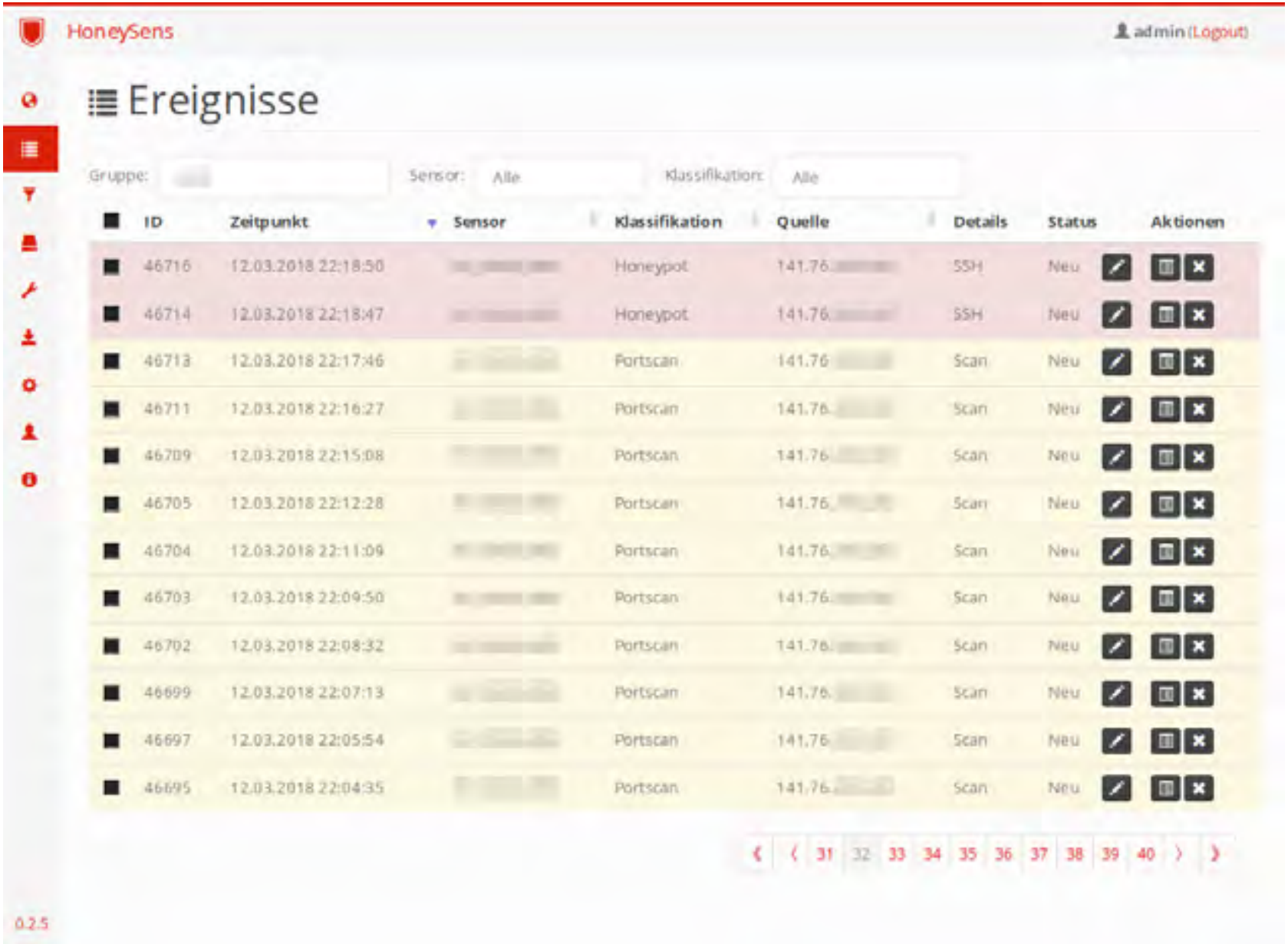
Server: Dashboard



Server: Sensorliste

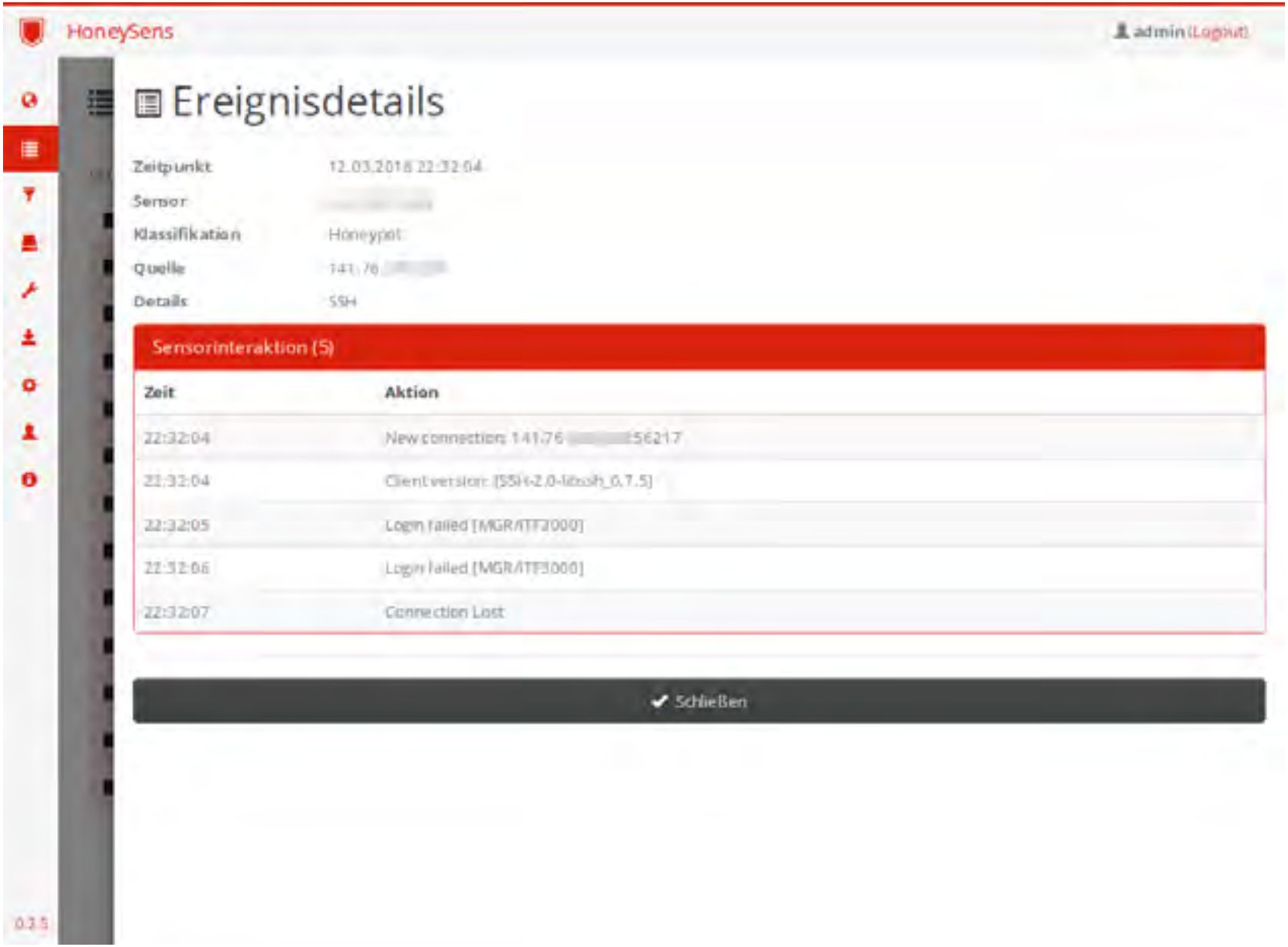


Server: Ereignisse

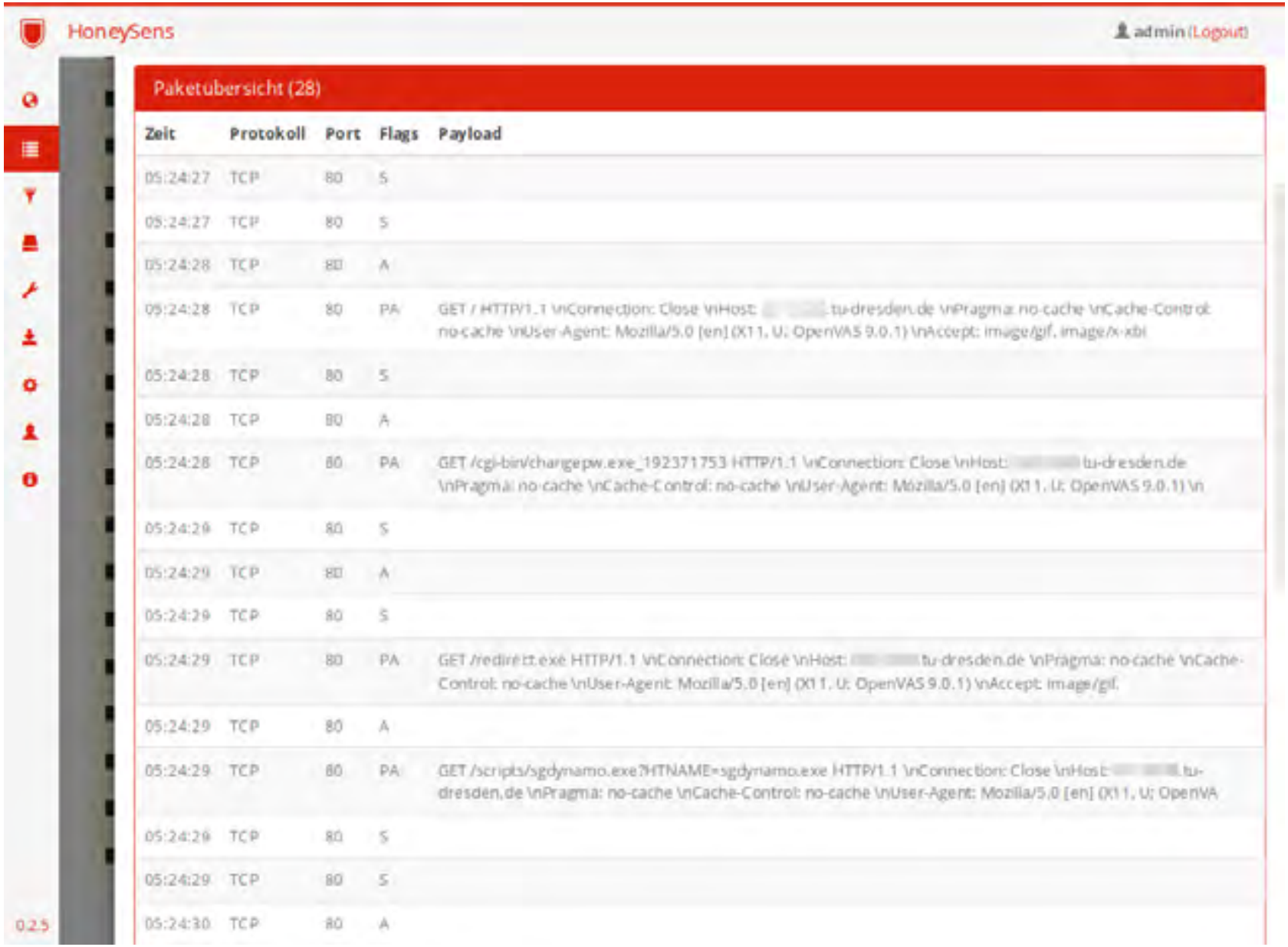


Beispiel: Portscan

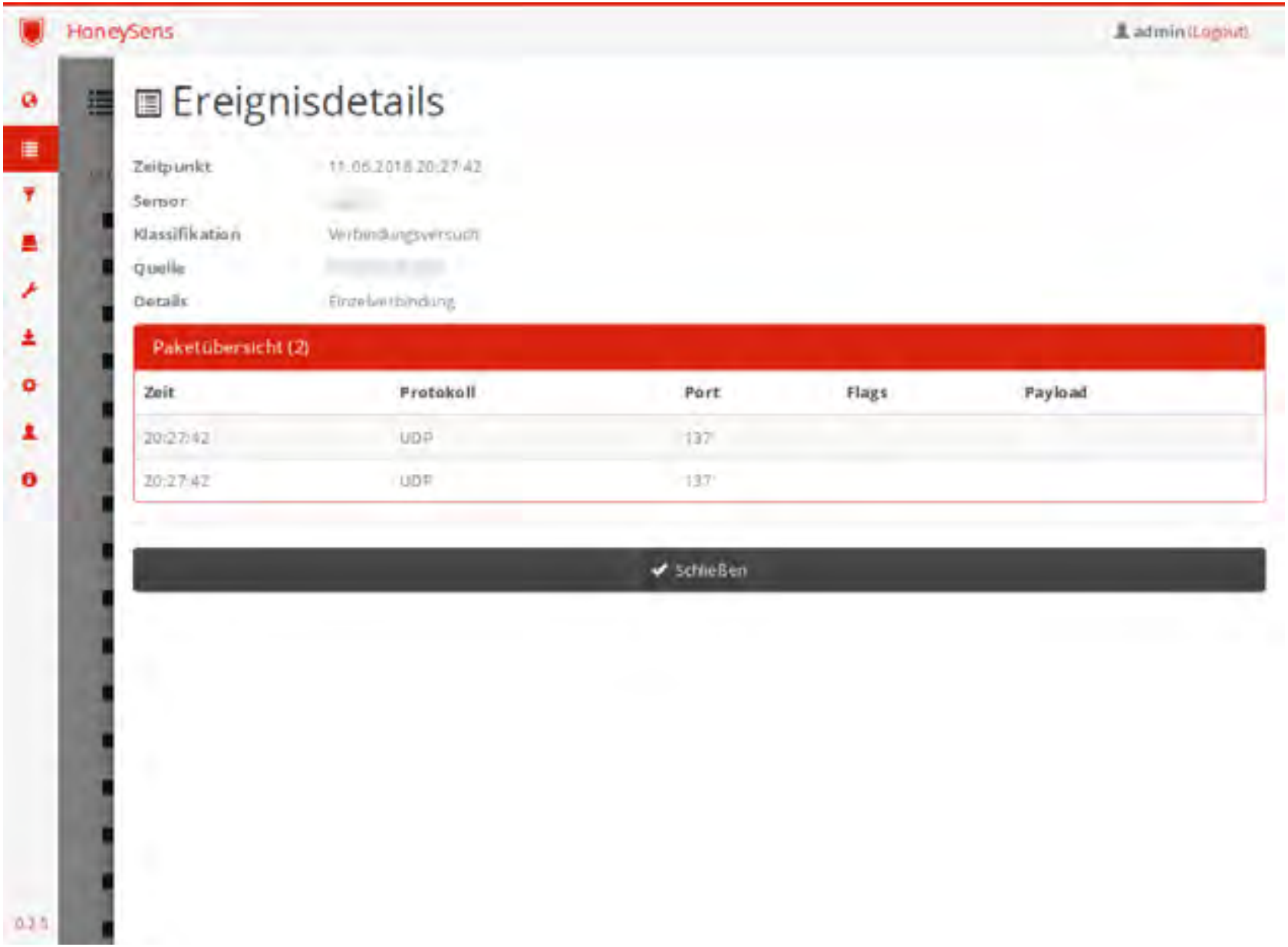
Beispiel: SSH-Zugriff



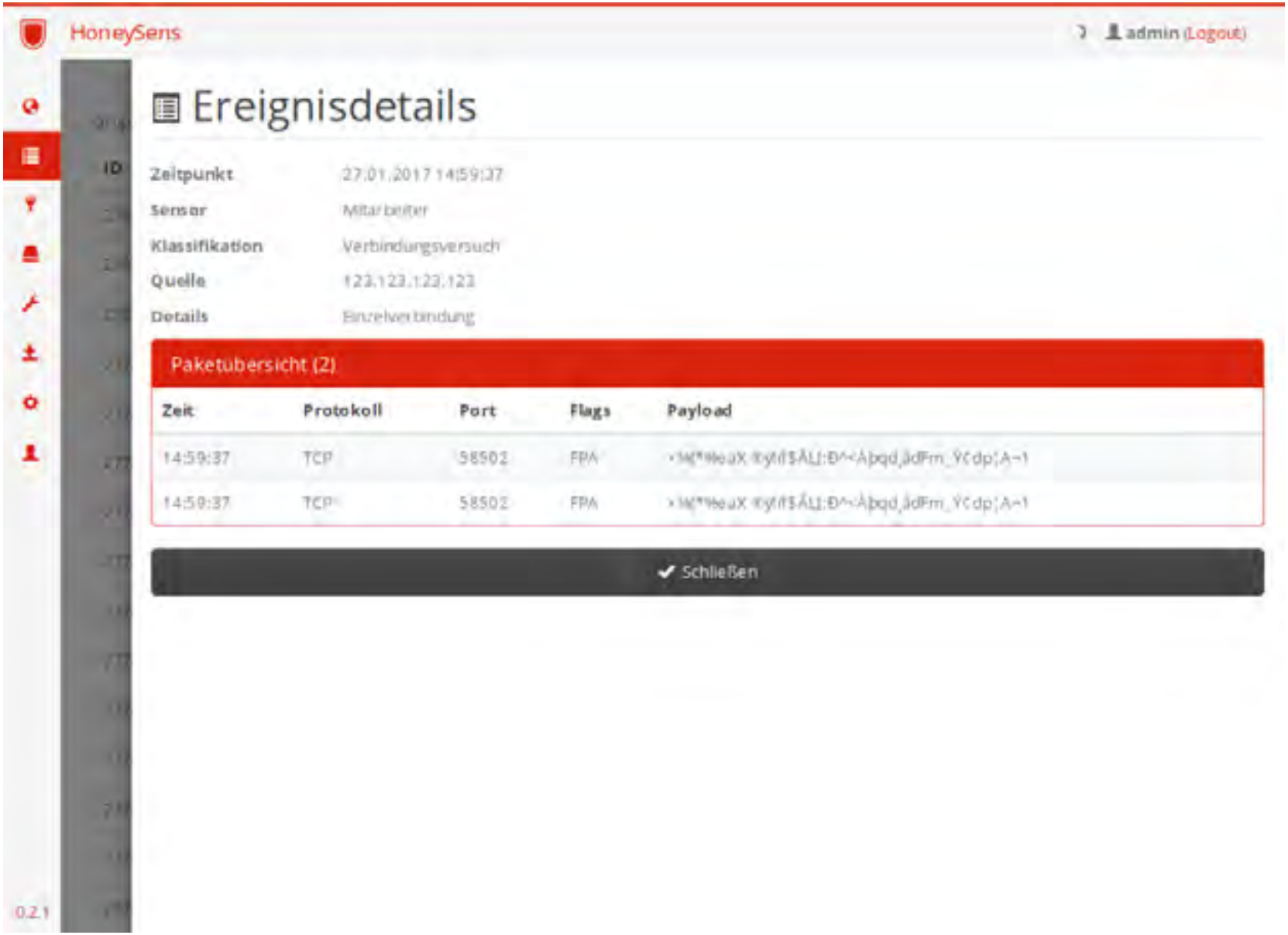
Beispiel: HTTP/CGI-Angriff



Beispiel: NetBIOS



Beispiel: ???


HoneySens
admin (Logout)
Ereignisdetails
ID
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
14:59:37 TCP 58502 FPA
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

Bestandsaufnahme & Ausblick

Honeypots

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

Bestandsaufnahme & Ausblick

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

Bestandsaufnahme & Ausblick

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

Bestandsaufnahme & Ausblick

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