SACHSEN-ANHALT

EUROPÄISCHE UNION
EFRE
Europäischer Fonds für regionale Entwicklung

Künstliche Intelligenz zur Erkennung von Sicherheitsvorfällen in Netzwerken

Vorstellung des IT-Sec-Labors

Mandy Knöchel, Sebastian Karius, Sascha Heße,

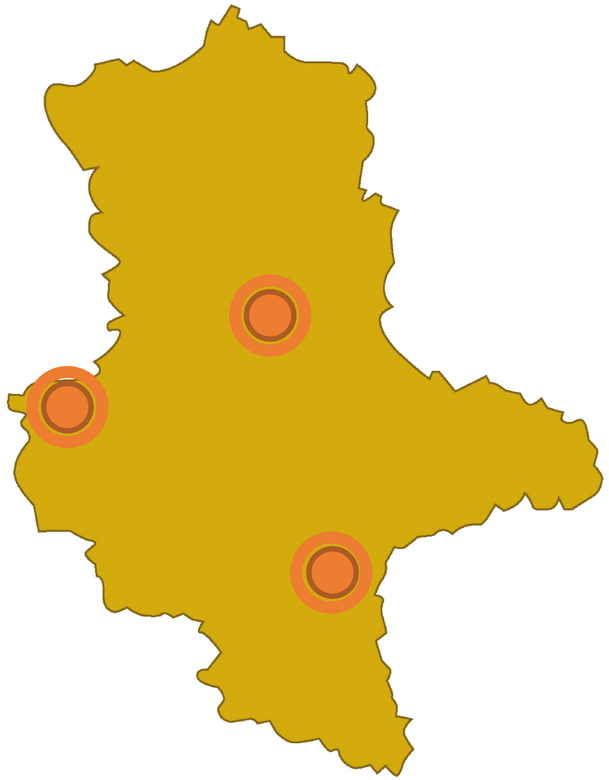
Tim Reiprich, Dr. Sandro Wefel,

Martin-Luther-Universität Halle-Wittenberg (MLU)

04/2024

CyberSecurity-Verbund Sachsen-Anhalt

- Otto-von-Guericke Universität (OvGU)
- Hochschule Harz (HS Harz)
- Martin-Luther-Univ. Halle/Wittenberg (MLU)



gefördert durch:

04/2024

Zielstellung und Zielgruppe

- Unterstützung von Bedarfsträgern bei der Verbesserung der „Datensicherheit“ auf Ebene der IT-Infrastruktur und durch organisatorische Maßnahmen
- Bedarfsträger auf verschiedenen Ebenen
  - kommunale Einrichtungen, Verwaltung
  - KMUs (ohne eigene IT-Abteilung)
  - Bildungseinrichtungen
  - Endanwender

Projekt CyberSec-I 2020-2024

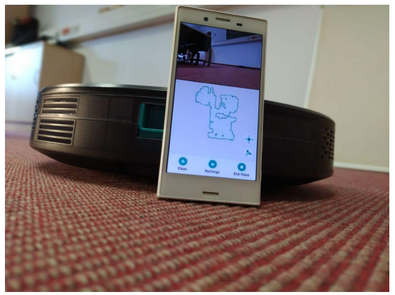
- Unterstützung der Bedarfsträger auf verschiedenen Ebenen Hilfe zur Selbsthilfe
  - Eindämmung der Gefährdung vernetzter Systeme, u.a. durch Embedded Devices, IoT, I(I)ot
  - zielorientierte Auswertung von Netzwerkverkehr hinsichtlich Schadprogrammen (Forschungstransfer)
  - Praktikable Werkzeuge für IT-Administration
  - Sensibilisierung und Weiterbildung

Projekt CyberSec-II 2024-2028

- Unterstützung der Bedarfsträger auf verschiedenen Ebenen
  - Eindämmung der Gefährdung vernetzter Systeme durch Anwendung von KI-Mechanismen
  - zielorientierte Auswertung von Netzwerkverkehr hinsichtlich Schadprogrammen
  - Praktikable Werkzeuge für IT-Administration
  - Sensibilisierung und Weiterbildung
  - Erweiterung der KI-Kompetenz

1. Eingebettete Systeme und Kryptographie

- zunehmender Einsatz vernetzter Geräte in allen Bereichen:
  Intelligente Beleuchtungssysteme, Klimatisierung, Sicherheitssysteme, Smartmeter, WallBoxen, SmartTV
- aber: IoT-Geräte unterliegen im Schnitt, 2017: 5.200 Angriffen jeden Monat; Anstieg an IoT-Angriffen jährlich ca. 600%



Quelle: Symantec Internet Security Threat Report Volume 24

Bedrohung durch IoT-Geräte bleibt bestehen

Adversary	Date in 2023	Activity
SPECTRAL KITTEN	OCTOBER 9	*MALEKTEAM* PERSONA LEAKED PII, CCTV FOOTAGE AND OTHER DATA ALLEGEDLY SOURCED FROM INTRUSIONS TARGETING ISRAELI ENTITIES
HAYWIRE KITTEN	OCTOBER–NOVEMBER	HAYWIRE KITTEN, ASSOCIATED WITH IRGC CONTRACTOR EMENNET PASARGAD, OPERATED PERSONAS *YARE GOMNAN CYBER TEAM* AND *AL-TOUFAN TEAM* TO CLAIM CCTV SYSTEM TARGETING AT U.S. AIRPORTS, THREATEN CYBER-ENABLED KINETIC ATTACKS AGAINST ISRAEL, AND CARRY OUT HACK-AND-LEAK AND DDOS OPERATIONS
BANISHED KITTEN	OCTOBER	MOIS-LINKED BANISHED KITTEN DEPLOYED THE *BIBIWIPER* MALWARE FAMILY AGAINST COMPANIES IN ISRAEL; A *KARMA POWER* ANTI-ISRAELI MESSAGING CAMPAIGN OCCURRED ALONGSIDE THE REPORTED WIPER OPERATIONS
VENGEFUL KITTEN	OCTOBER 26–28	*MOSES STAFF* CLAIMED DATA-WIPING ACTIVITY AGAINST MORE THAN 20 COMPANIES' INDUSTRIAL CONTROL SYSTEMS (ICS) IN ISRAEL AND INDICATED INTEREST IN SMS, BASE-TRANSCEIVER STATIONS AND PUBLIC ALERT SYSTEMS
UNATTRIBUTED IRGC-NEXUS PERSONAS	OCTOBER–NOVEMBER	IRGC-LINKED *SOLDIERSOFSOLOMON* USED DESTRUCTIVE RANSOMWARE VARIANT *CRUCIO* AGAINST INTERNET OF THINGS (IoT) DEVICES IN ISRAEL; IRGC-AFFILIATED *CYBER AV3NGERS* COMPROMISED AND DEFACED PROGRAMMABLE LOGIC CONTROLLERS (PLCs) IN ISRAEL AND THE U.S. AT CRITICAL INFRASTRUCTURE ENTITIES SUCH AS WATER TREATMENT FACILITIES‘
UNKNOWN IRAN-NEXUS ACTOR	DECEMBER 19	UNKNOWN IRAN-NEXUS ACTOR DEPLOYED WIPERS AGAINST ISRAELI ORGANIZATIONS
HAYWIRE KITTEN	DECEMBER 25	*YARE GOMNAM CYBER TEAM* CLAIMED RESPONSIBILITY FOR POWER OUTAGES IN ISRAEL

Figure 5. Iran-nexus cyber activity during the conflict

Quelle: Crowdstrike Global Threat Report 2024

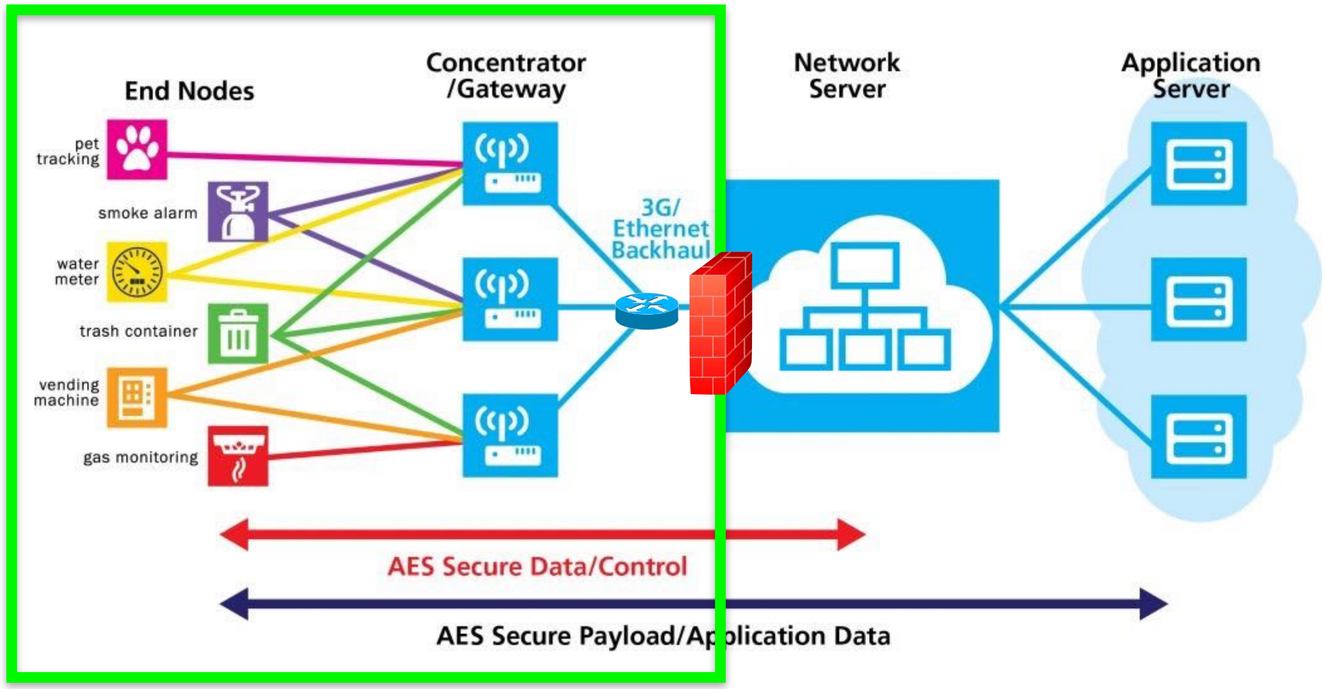
Gefahrenquellen

- IoT-Geräte - Kommunikation mit Herstellercloud und Nutzung von Ende-zu-Ende Verschlüsselung !?
  - (I)IoT Geräte als Relay für Schadsoftware
- andere Infektionswege für Schadsoftware:
  - BYOD - Bring Your Own Devices
  - Email-Anhänge oder Datenträger (USB-Sticks)
- *unterschiedliche Infektionswege, aber*

  Schadsoftware kommuniziert im Netz !

Rechnernetze

- Rückgrat der Digitalisierung
- zunehmend Ausgangspunkt für Angriffe auf IT-Infrastruktur und -Dienste

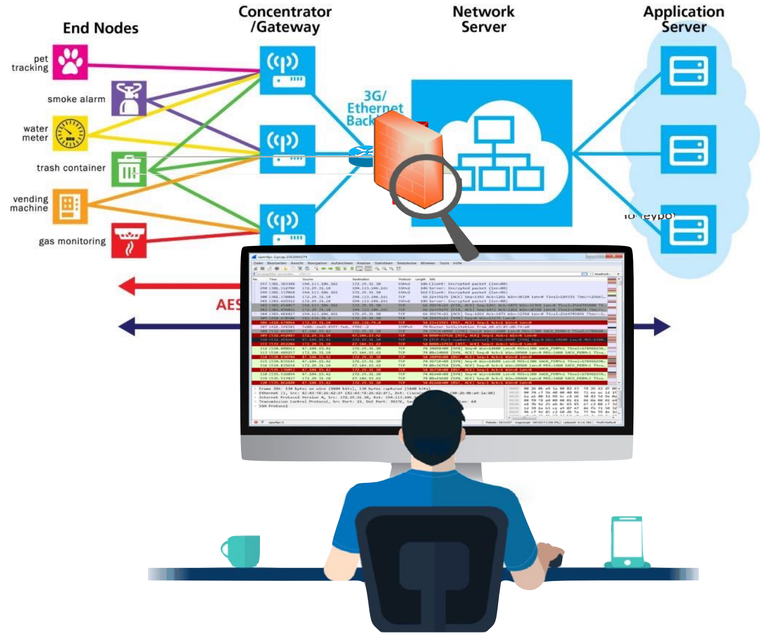


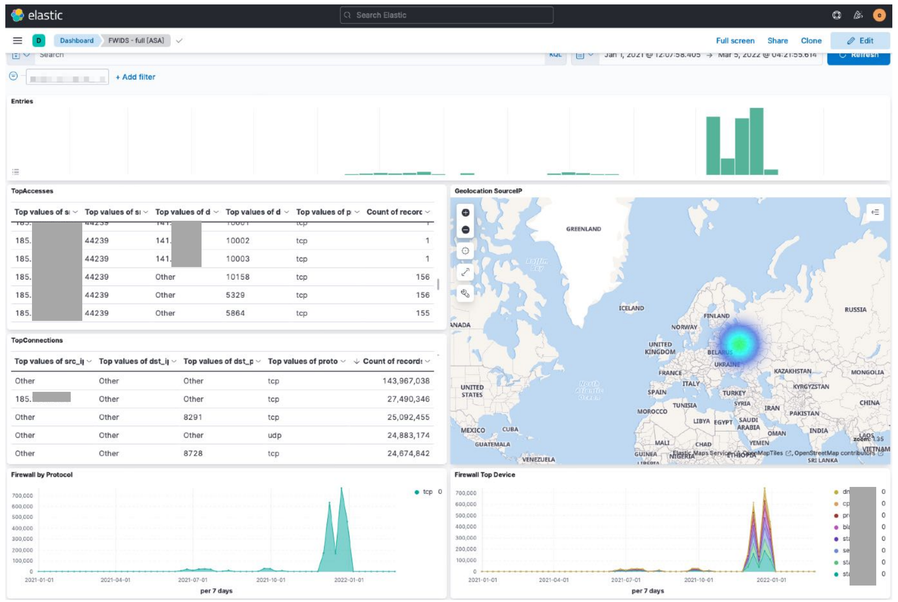
Bildquelle: LoRa WAN Protokoll-Sicherheit-Anwendung iot-design.de + Semtech GmbH

Ansätze für Schutzmaßnahmen auf Netzwerkebene

Trafficanalyse

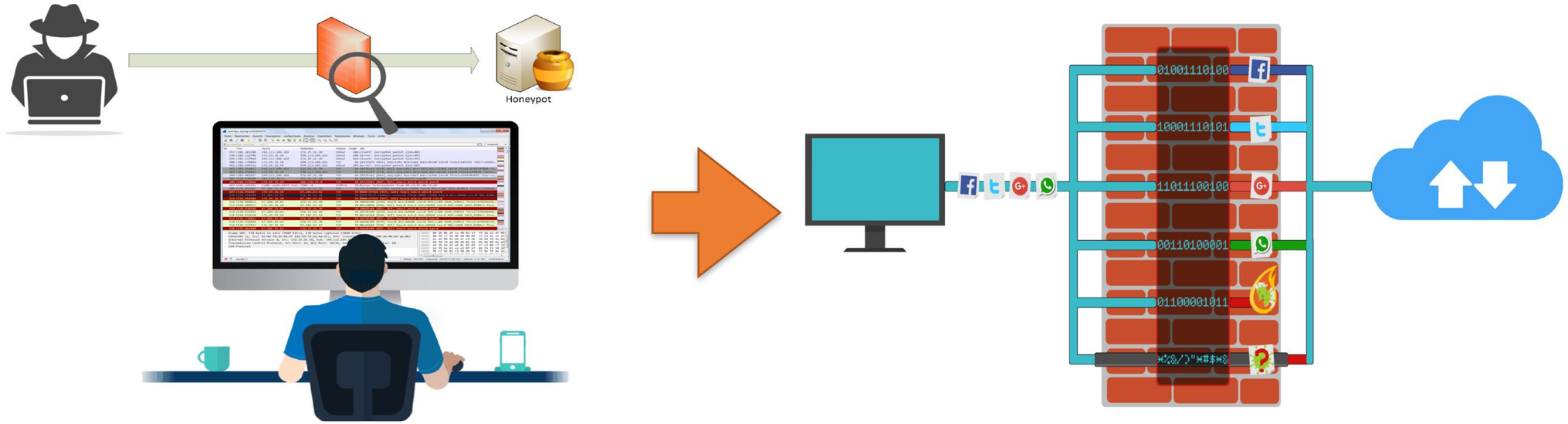
- Auswertung des Datenverkehrs
- Suche nach bösartigen oder versteckten Inhalten





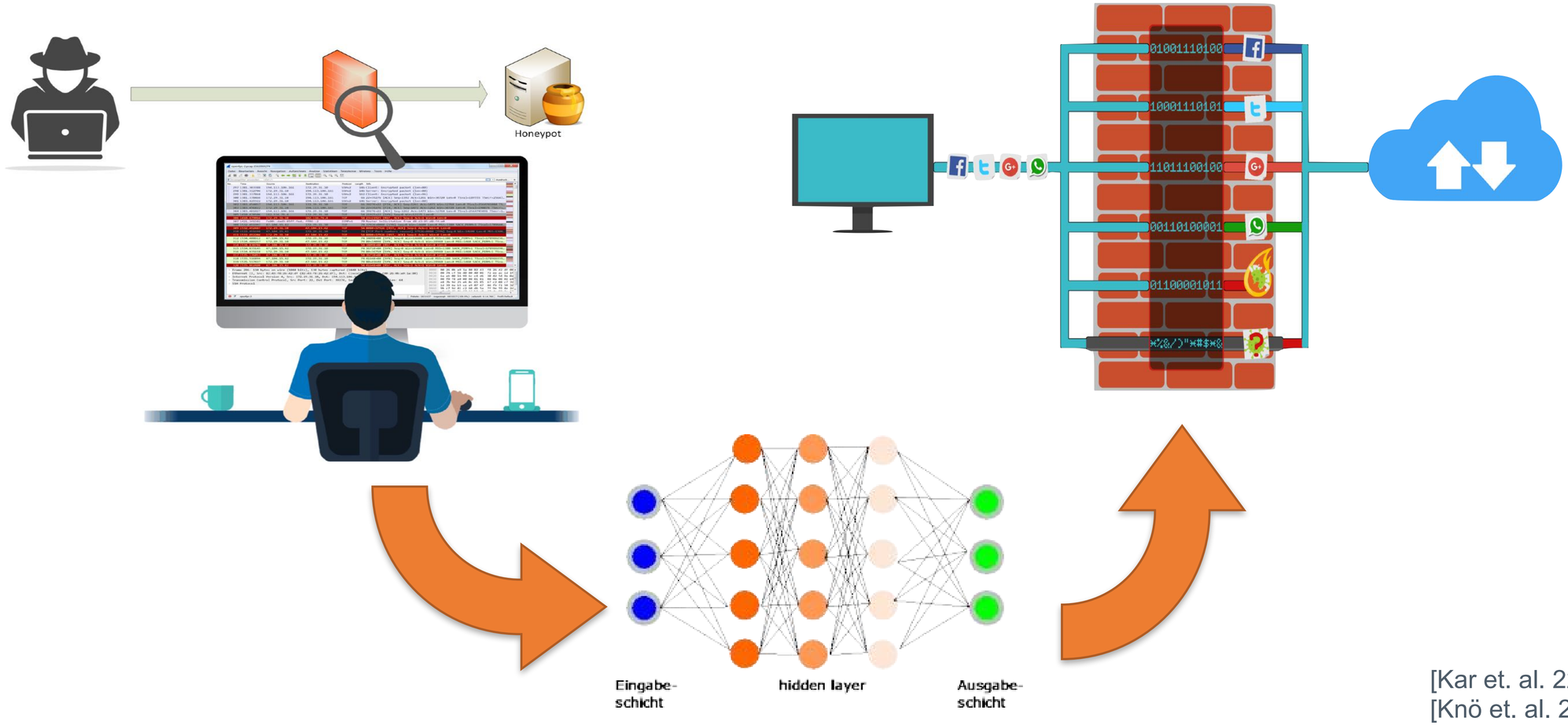
Trafficanalyse führt zur Klassifikation

- Unterscheidung übertragener Inhalts, manuelle Filtererstellung
- Filterung unerwünschter Datenströme



[Kar et. al. 22]
[Knö et. al. 22]

Rechnernetze Klassifikation:
Einführung von Methoden des maschinellen Lernens

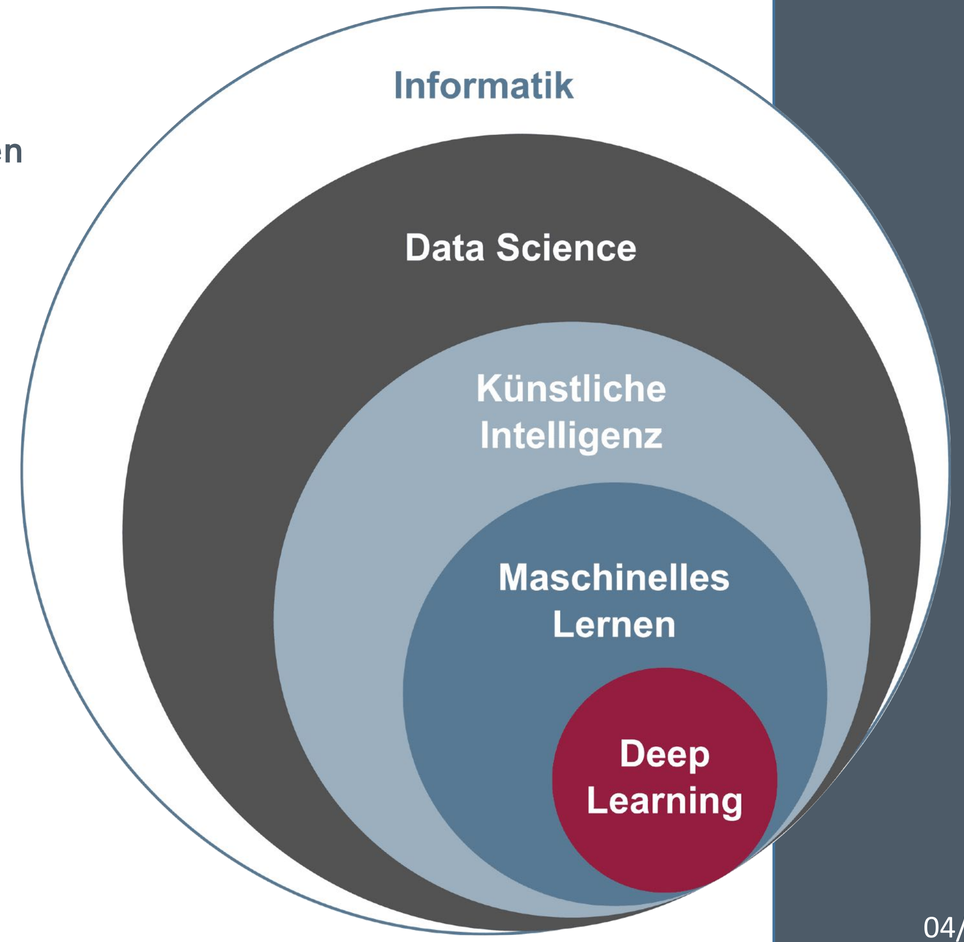


[Kar et. al. 22]
[Knö et. al. 22]

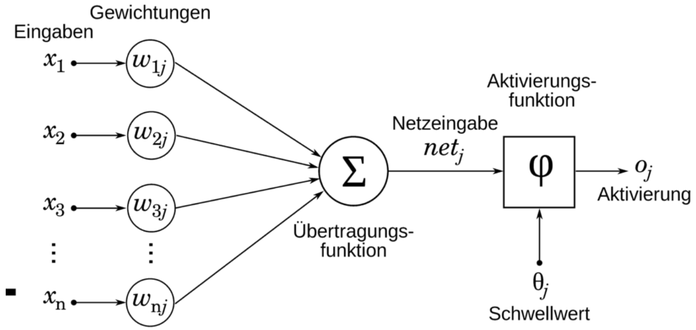
Maschinelles Lernen ?

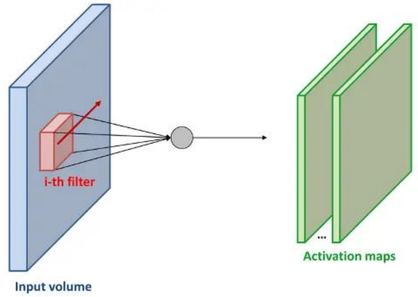
Teilgebiet der KI

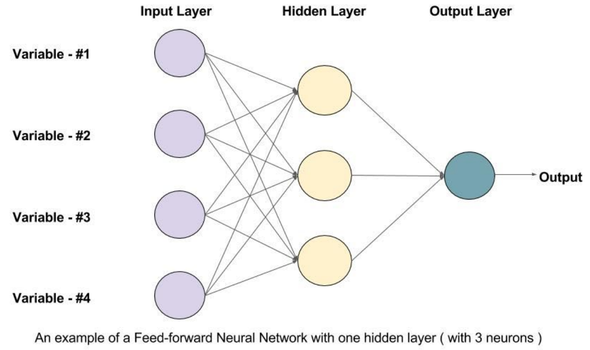
- **Expertensysteme**: Computerprogramme, die menschliches Wissen in einem spezifischen Bereich nachahmen, um komplexe Aufgaben oder Probleme zu lösen
- **Maschinelles Lernen**: Algorithmen, die es Computern ermöglichen, aus Daten zu lernen und Vorhersagen oder Entscheidungen zu treffen, ohne explizite Programmierung
- Ziel ist **Mustererkennung:** auf großen Datensätzen Zusammenhänge erkennen
- Werkzeug: **Neuronale Netze** sind nach dem menschlichen Gehirn aus miteinander verbundenen Knoten („Neuronen“) modelliert
  - für komplexe Aufgaben wie Spracherkennung, natürliche Sprachverarbeitung (menschliche Sprache verstehen und generieren), Übersetzungsdienste, Sprachmodelle (Chatbots), Bildgeneratoren, Deep-Fake-Anwendungen



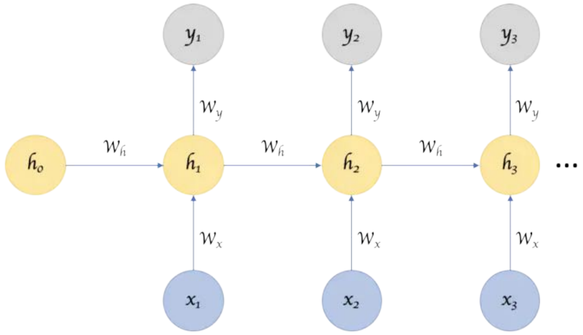
Maschinelles Lernen („KI“) nutzt häufig Neuronale Netze

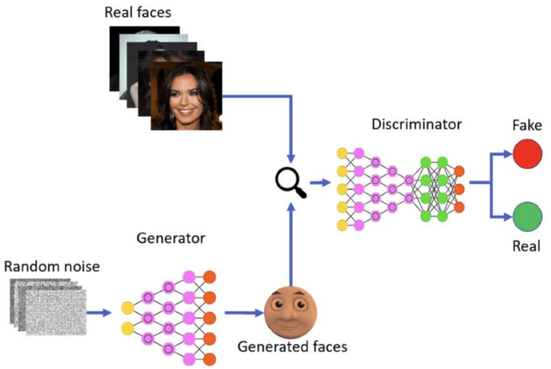






An example of a Feed-forward Neural Network with one hidden layer (with 3 neurons)





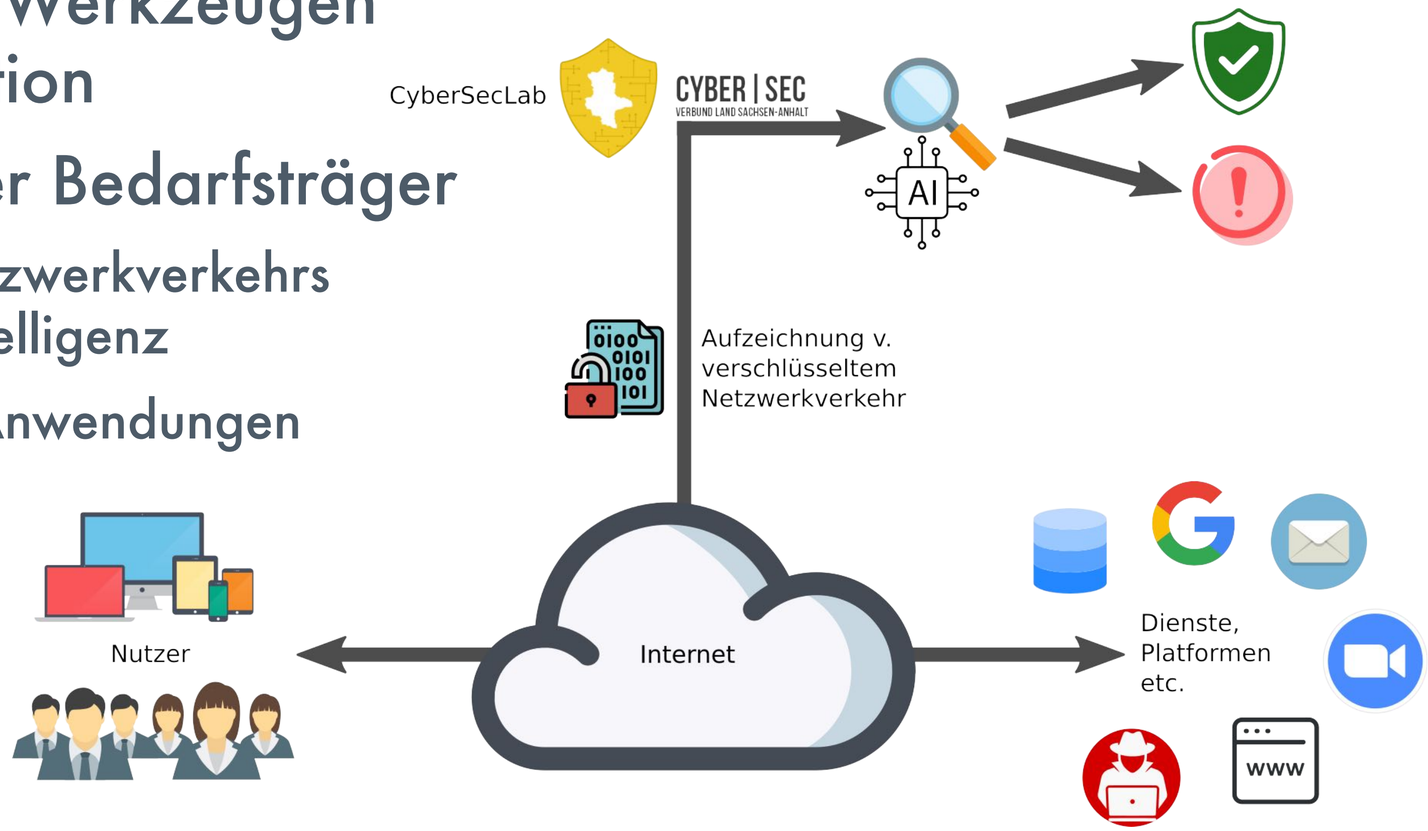
- Perceptron
- Feed forward neural networks
- Convolutional Neural Networks (CNN)
- Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM)
- Generative Adversarial Networks (GAN)

Bildquellen:
- https://learnopencv.com
- https://datasolut.com

04/2024

2. IT-Sec Labor

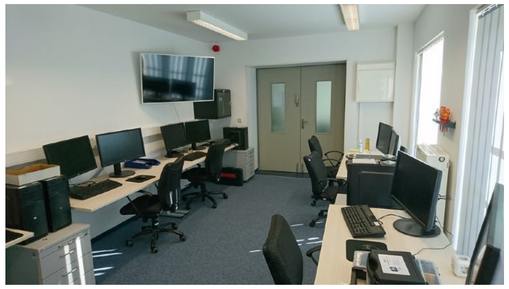
- Entwicklung von Werkzeugen für IT-Administration
- Unterstützung der Bedarfsträger
- z.B. Analyse des Netzwerkverkehrs mittels Künstlicher Intelligenz
- Sicherheitstests von Anwendungen
- Weiterbildung



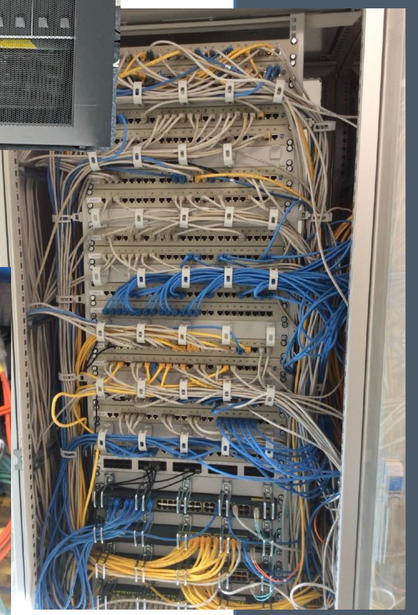
Bestandteile IT-Sec Labor

Sammlung von Testobjekten (u.a. IoT-Geräte)

GPU-Compute-Server

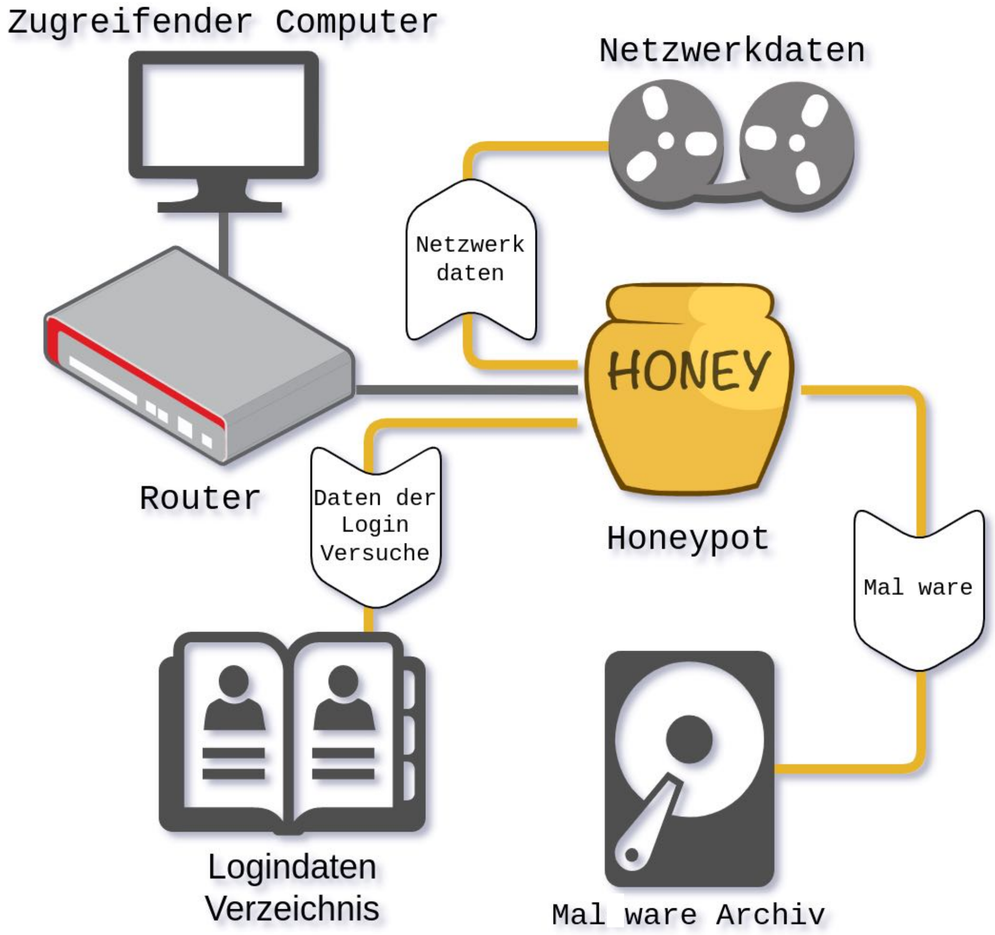


Raum für Untersuchung , Entwicklung und Erprobung von Konzepten



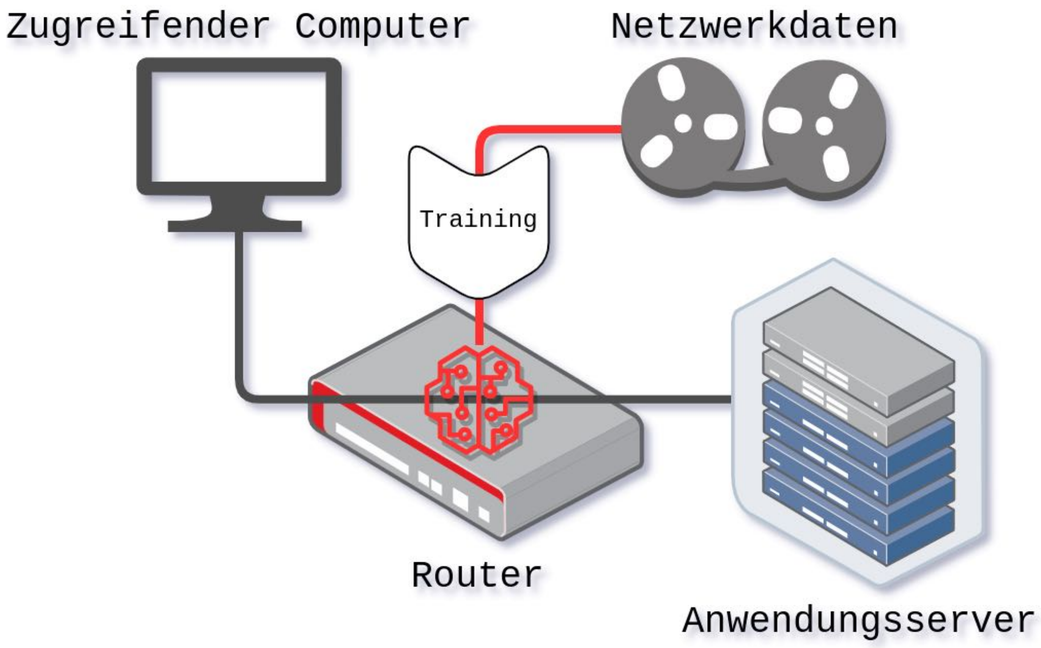
Abgeschottete Netzwerkinfrastruktur

Honeypot



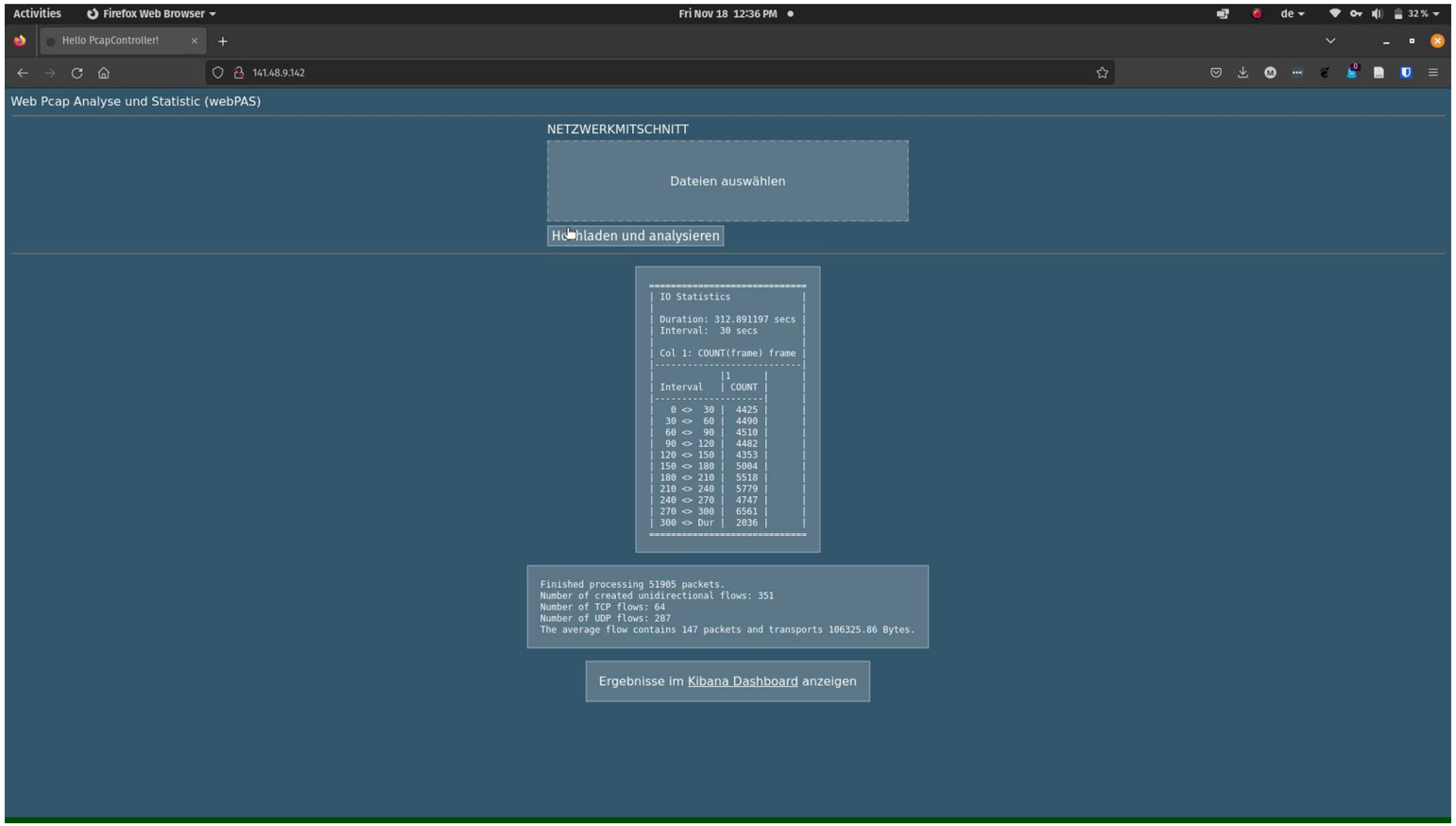
- Honeypot ist „Falle“ für Angreifer
- Honeypot zeichnet alle Interaktionen mit dem System auf
  - Netzwerkdaten
  - eingeschleuste Malware
  - eingegebene Logindaten
- Archive zur späteren Auswertung
- Vorteil: Die Daten können unverschlüsselt aufgezeichnet werden
- Vorteil: Es fallen ausschließlich Angriffsdaten an

Netzwerkklassifikation + KI-Methoden



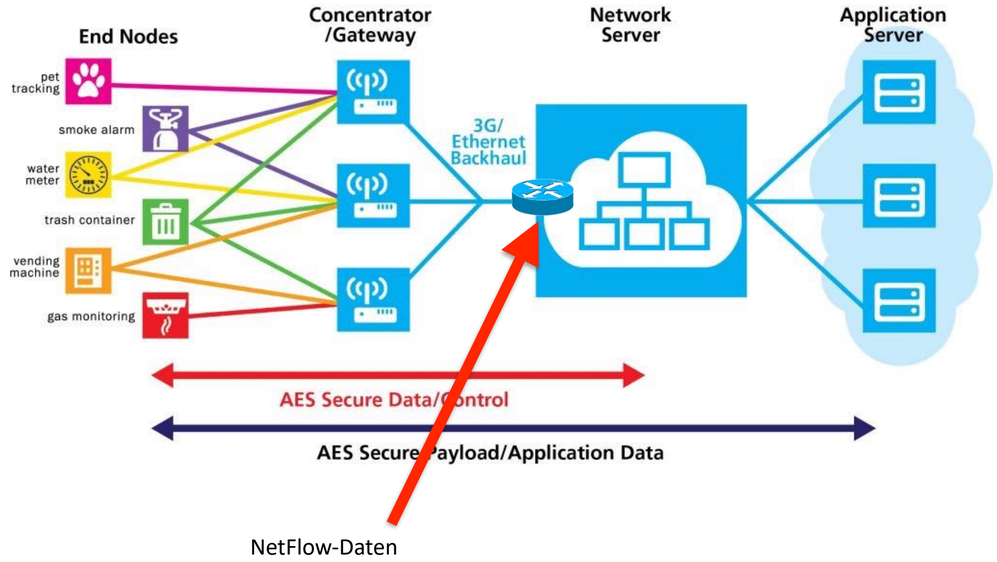
- aufgezeichnete Honeypot Daten werden zum Training eines Netzwerkklassifikators verwendet
- Netzwerkverkehr kann nun auf Angriffe geprüft werden
  - beschränkt auf Angriffe die vom Honeypot erfasst wurden
- Versuche mit verschlüsselten Netzwerkverkehr (SSH) zeigen Erkennungsquote von ca. 80%

Netzwerkklassifikation: Mitschnittanalyse



Freischaltung auf Anfrage

3. Erkennung von Anomalien in Netzen



- Aufzeichnung von NetzFlow-Daten
- 1. klassische Analyse
  z.B. Holt-Winter-Prognose zur Berechnung von Hüllkurven
- Alarmierung bei Abweichung

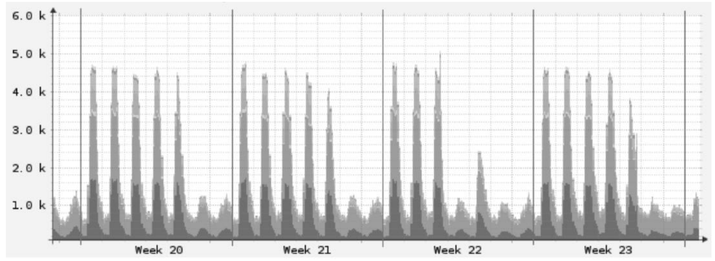
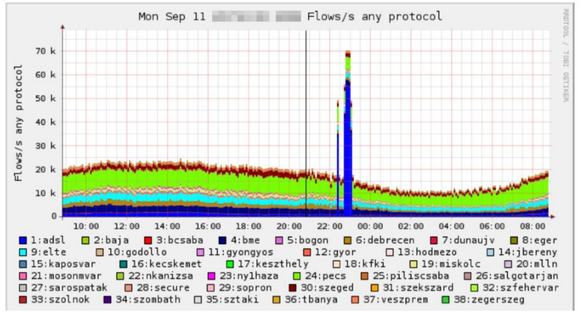


Abbildung 28: MLU Flows Monatsübersicht



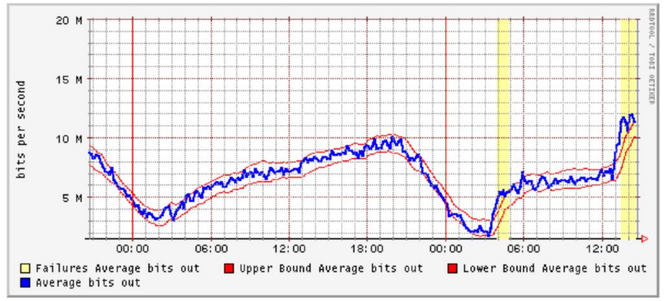
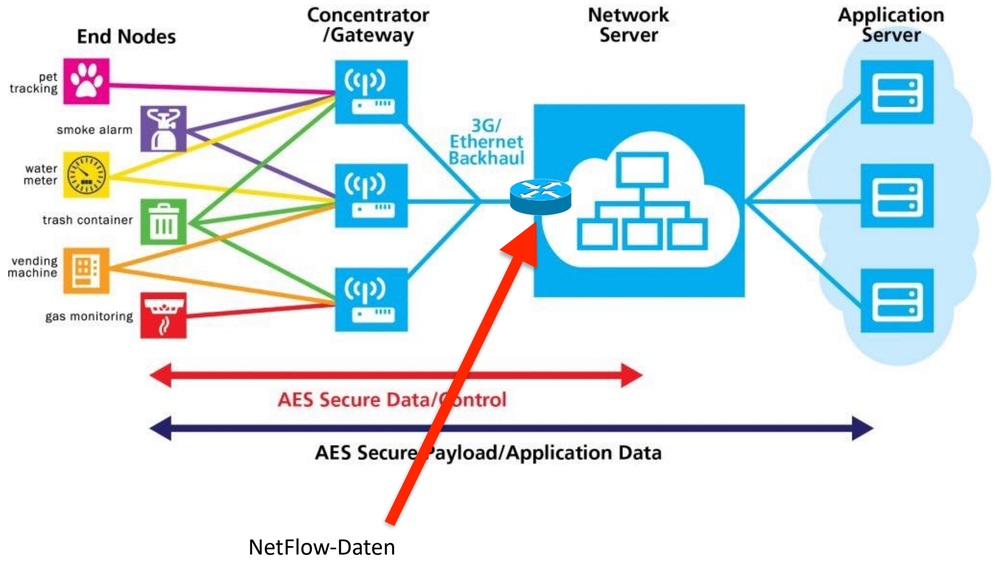


Abbildung 17: RRDTool Abweichungserkennung [7]

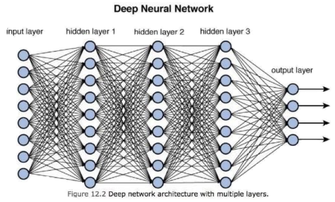
Quelle: Sascha Wiegleb 2014/15

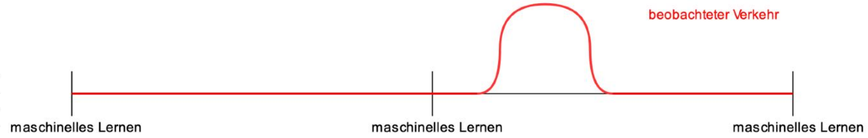
Mit KI zur Erkennung von Sicherheitsvorfällen

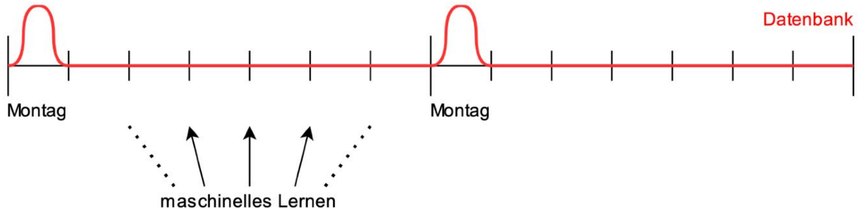


- Aufzeichnung von NetzFlow-Daten
- 2. Einsatz von Machine-Learning Methoden
- Datenauswertung mit Zeitbezug
- Klassifizierung von Netzwerkverkehr

Quelle: Till B. Nowakowski 2020







Mit KI zur Erkennung von Sicherheitsvorfällen

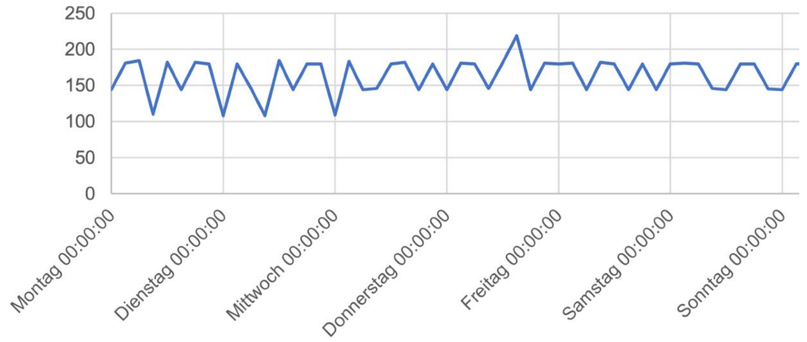


Abbildung 5 Flows ohne Korrelation zu Arbeitszeiten

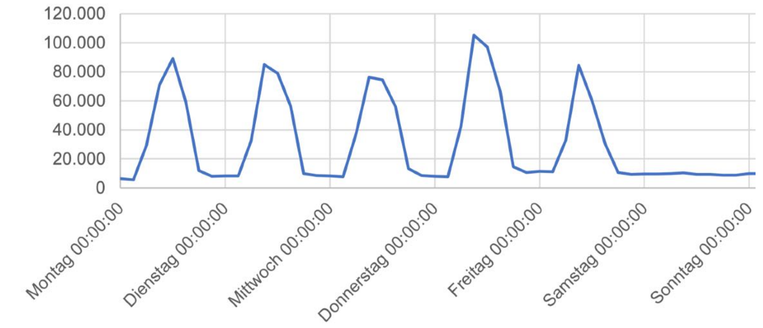


Abbildung 4 Flows in Korrelation zu Arbeitszeiten

- Prognose mittels „Prophet“ (Facebook OpenSource-Projekt zur Eventvorhersage auf Basis historischer Daten)
- Alarmierung bei Abweichung

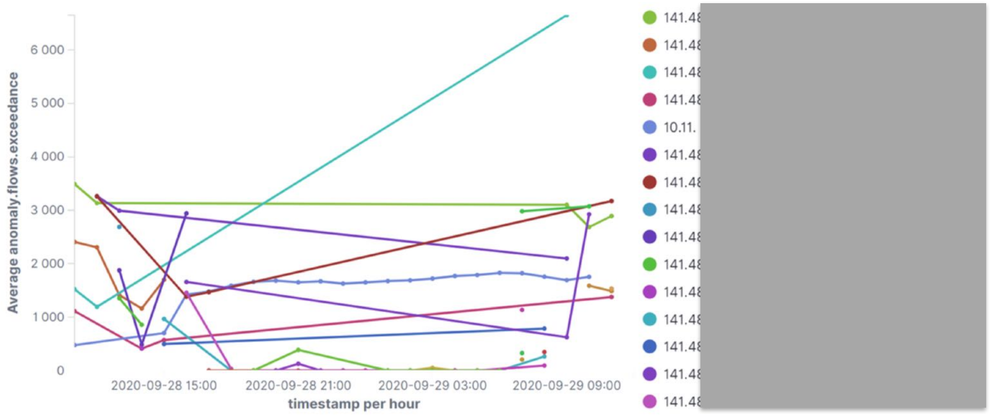
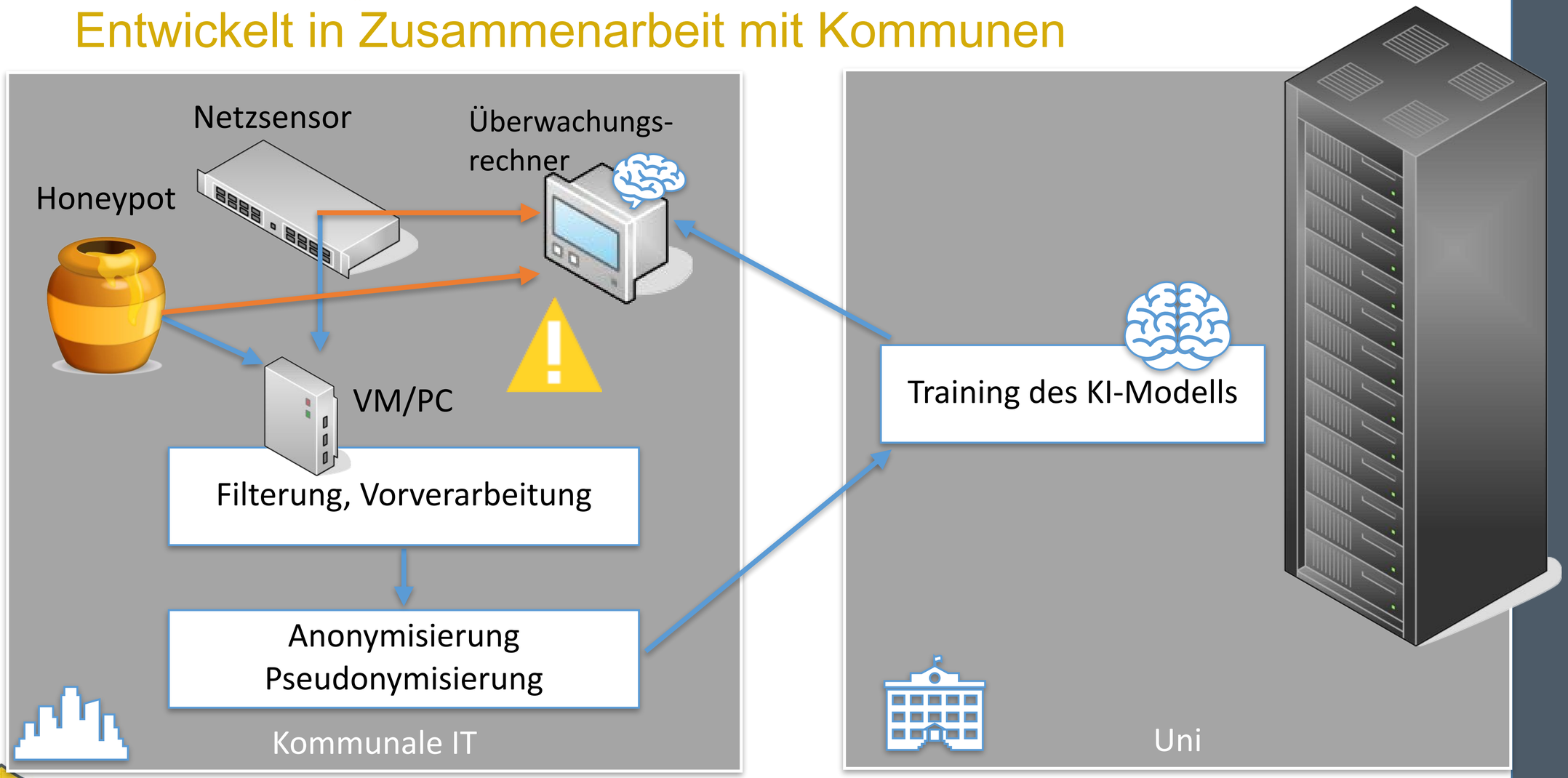


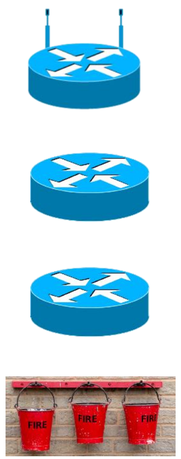
Abbildung 10 Darstellung der anomalen Flows für jeden Verursacher

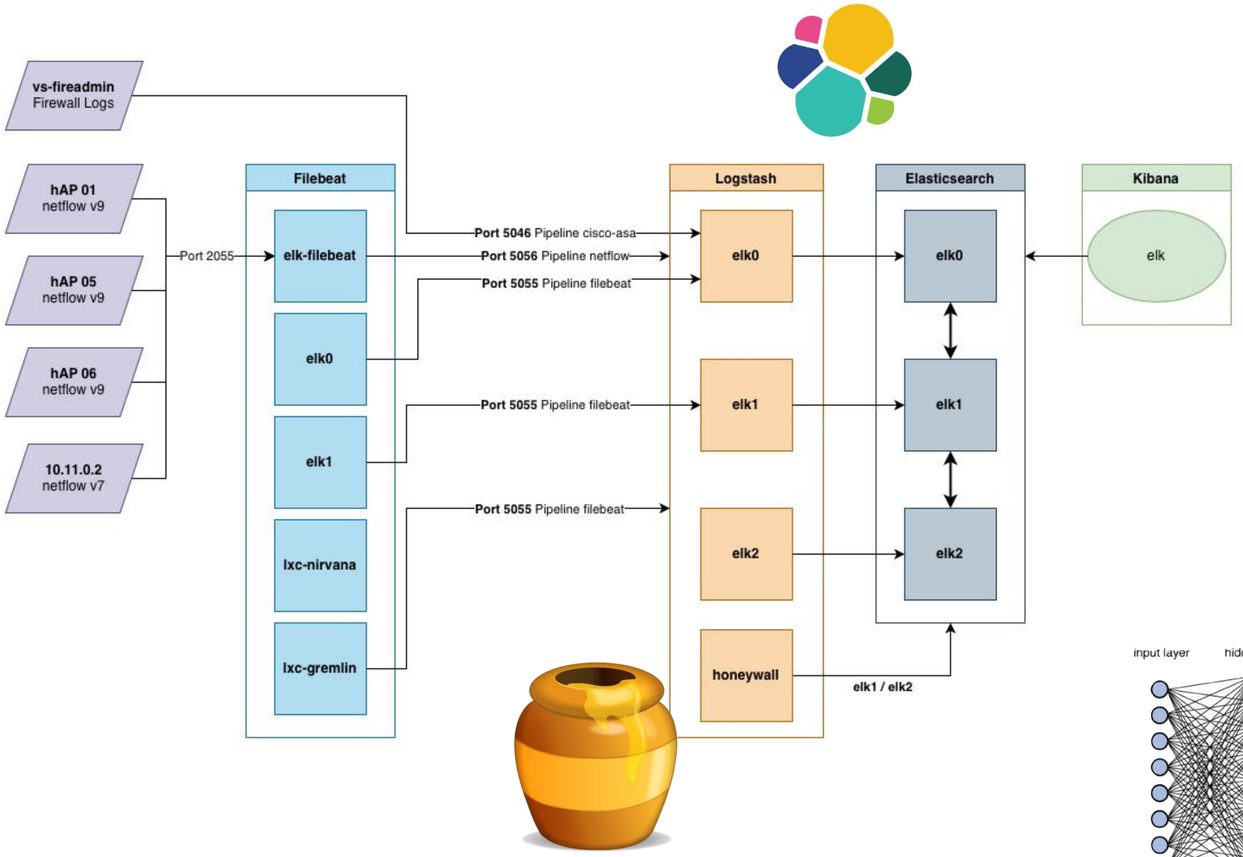
Quelle: Till B. Nowakowski 2020

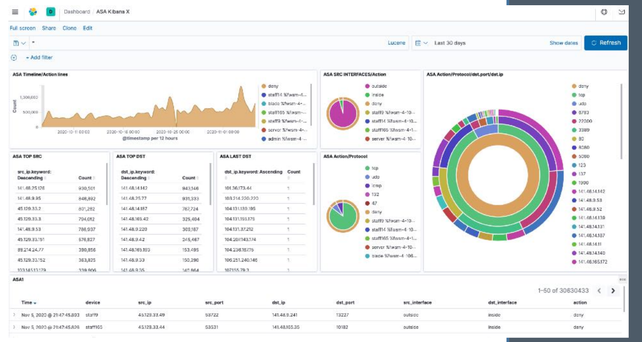
Frühwarnsystem
Entwickelt in Zusammenarbeit mit Kommunen



IT-Sec Labor - Erprobung der Frühwarn-Infrastruktur







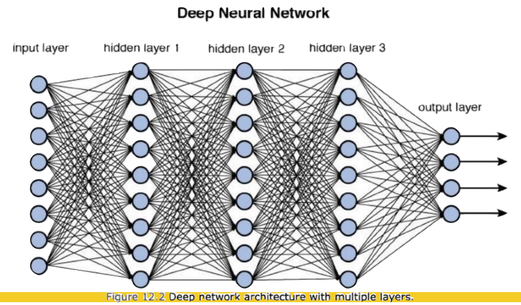
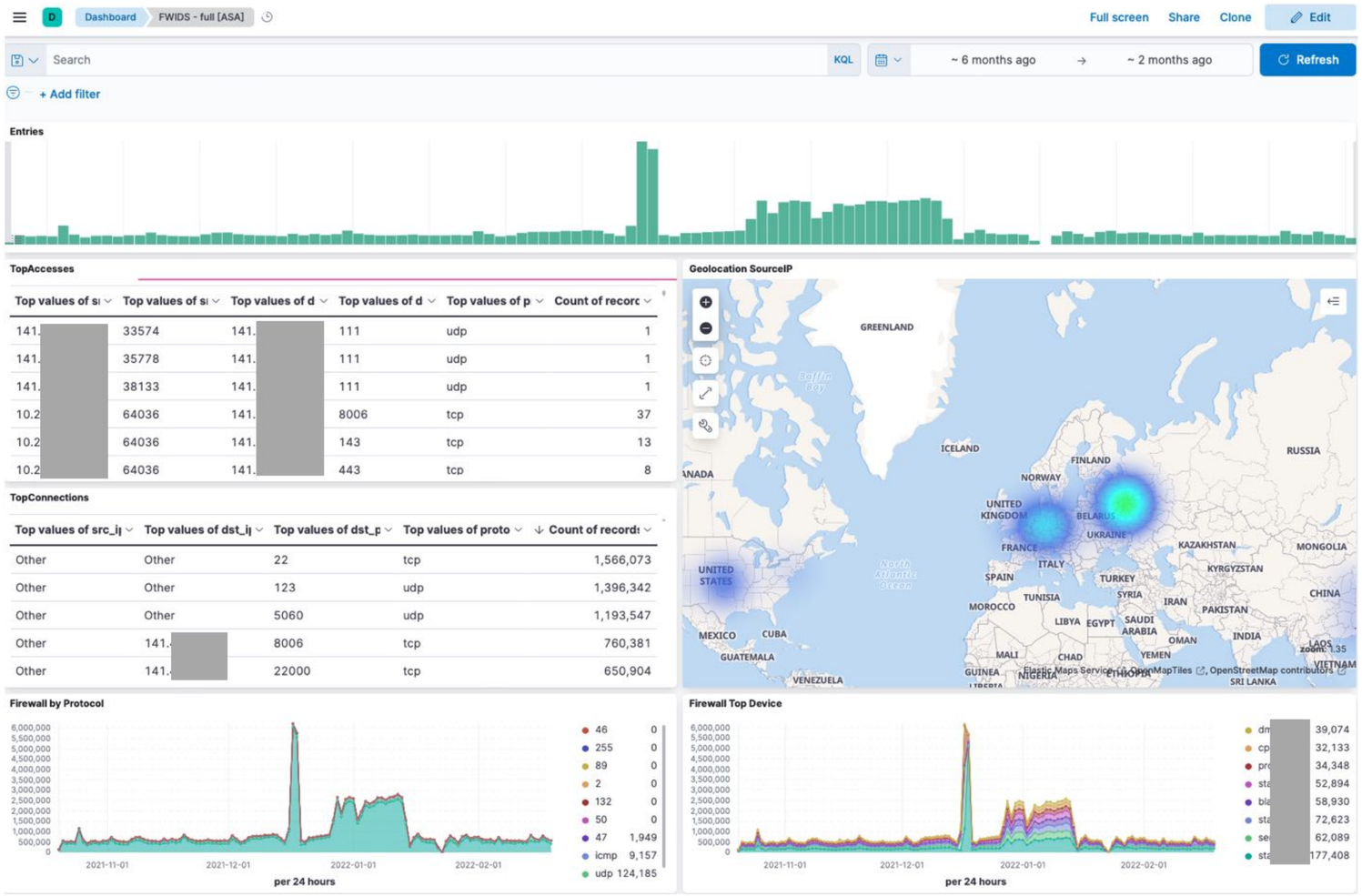
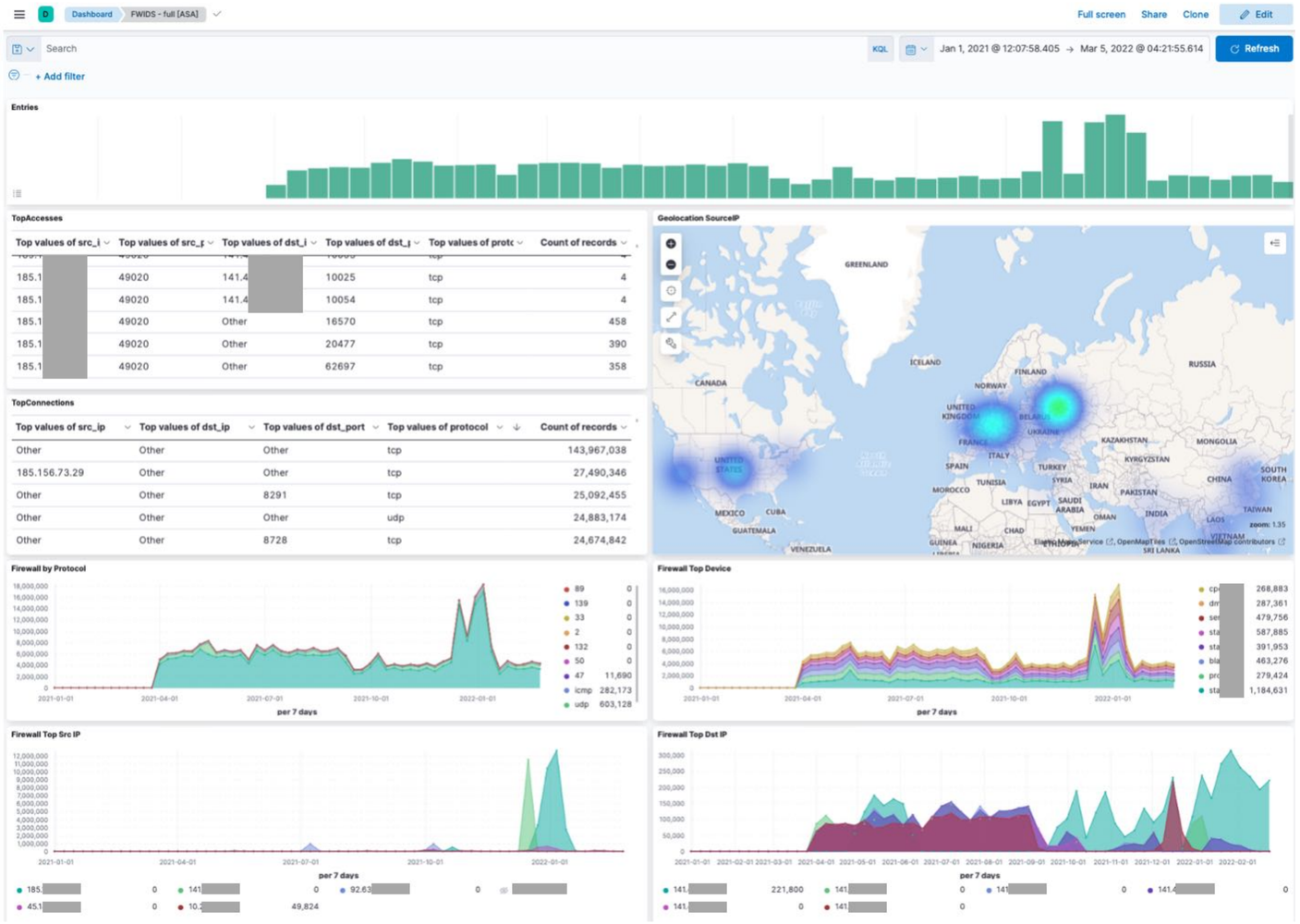


Figure 12.2 Deep network architecture with multiple layers.

IT-Sec Labor - Netzwerktraffic (11/21 - 3/22)



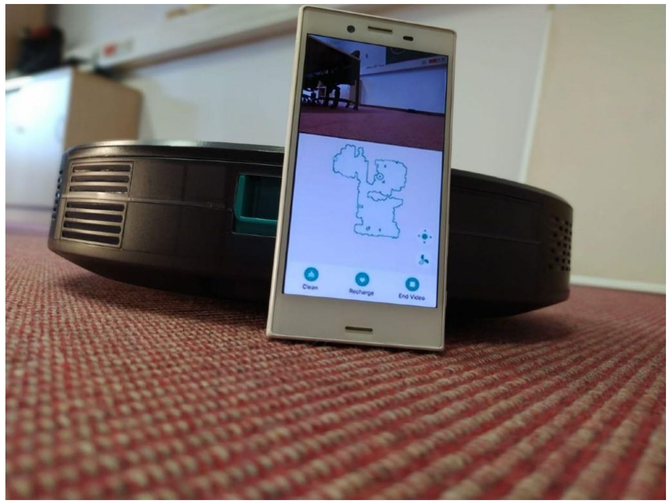
IT-Sec Labor - Netzwerktraffic (1/22 - 3/22)

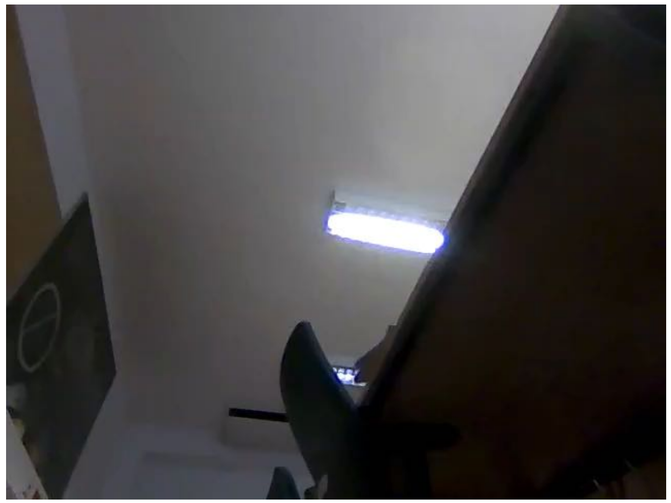


Untersuchung an IoT-Geräte

Staubsauger

normale Übertragung





versteckte Übertragung

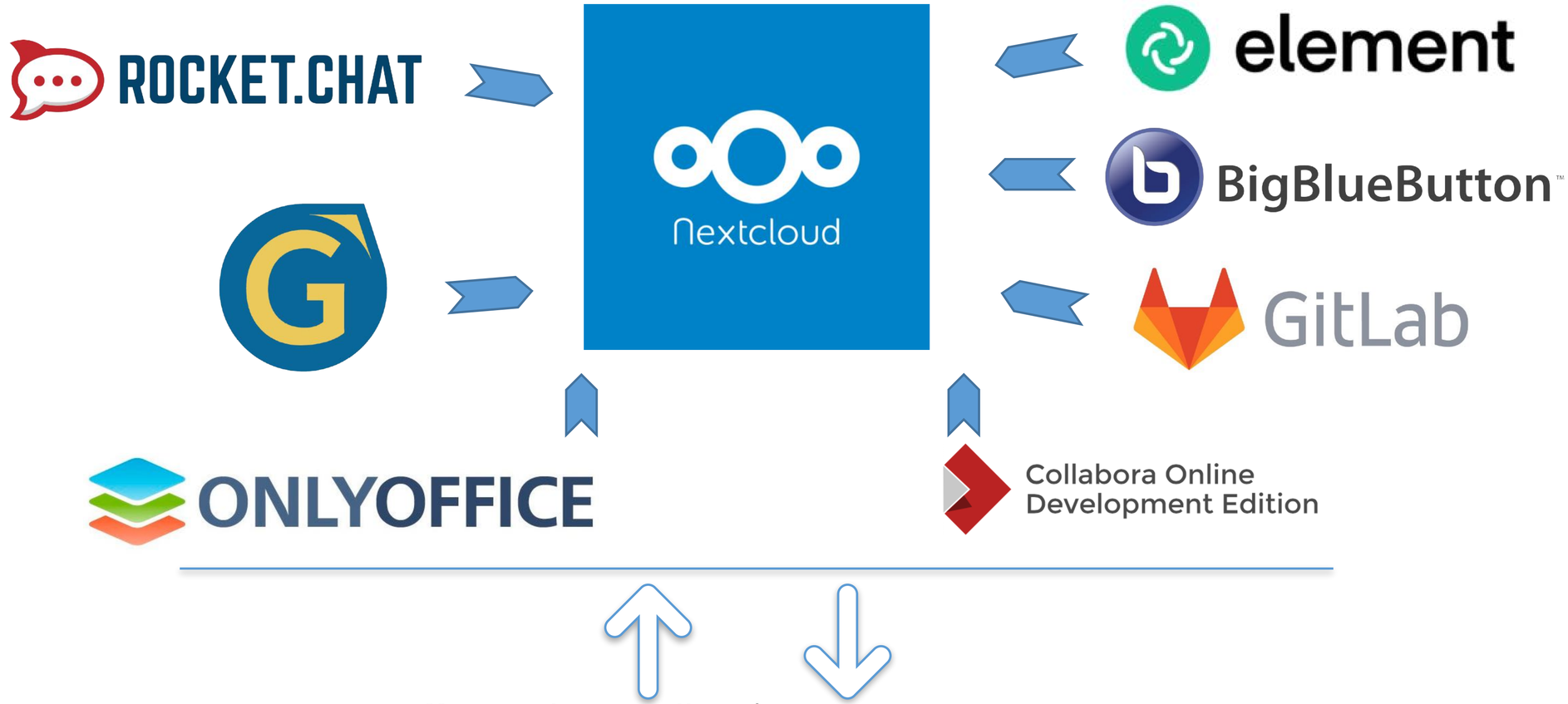
4. Demonstratoren / Evaluationsinstanzen

- wir bieten Demonstratoren zu folgenden Themen
  - Netzwerksicherheit, Aufspüren versteckter Schädlinge
  - Einbruchserkennung und -prävention
  - On-Premise-Lösungen (Videokonferenz, Private Cloud)
  - Verwendung von OpenSource / FOSS
- Formate
  - Demonstratoren als VM, Kubernetes/Container, Appliance
  - Vorstellungen vor Bedarfsträgern / Workshops

Demonstratoren: u.a. für OpenSource Applikation

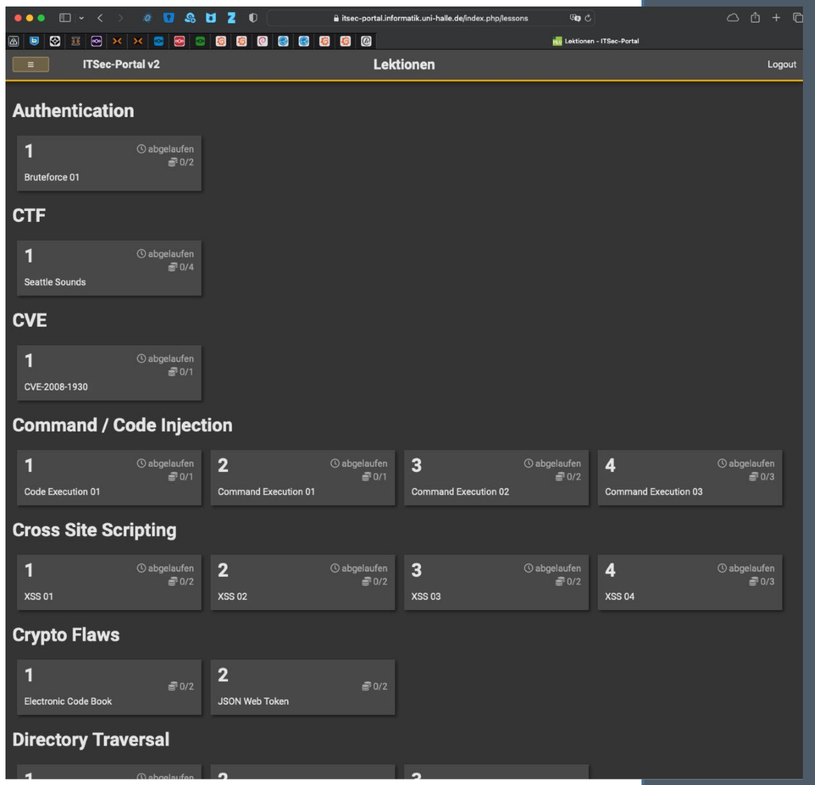
- Beispiel: On-Premise Cloud / Cloud Federation
- Ziel: Digitale und technologische Souveränität
  - kein Vendor-Lock / herstellerübergreifende Standards
  - „Self-Hosting“
  - Datensparsamkeit / Nachvollziehbarkeit
  - Einbindung adäquater kryptographischer Schutzmaßnahmen, wie Ende-zu-Ende-Verschlüsselung

Demonstratoren: Integration FOSS Cloud-Dienste



5. Fort- und Weiterbildungen für kommunale Einrichtungen, KMUs und die allg. Öffentlichkeit

- Verschiedene Formate
  - Online-Tools für Selbsttests (werden auch in der Lehre der MLU verwendet)
  - individuelle Systemanalyse, Beratung und Konzeption
  - Vorträge und Workshops



Fragen, Kontakte

CYBER | SEC
VERBUND LAND SACHSEN-ANHALT

- **Dr. Sandro Wefel**
- **Mandy Knöchel**
- **Sebastian Karius**
- **Tim Reiprich**
- **Sascha Heße**

- Martin-Luther-Universität
  Halle-Wittenberg
  Institut für Informatik
- Mail: <firstname>.<surname>@informatik.uni-halle.de
- Tel: +49 345 5524725

www.cslsa.de