
# CyberSecurity - wirksamer, effizienter, souveräner gestalten – Innovationen und Chancen aus F&E-Projekten

CyberSecurity-Verbund LSA

Prof. Dr. Hermann Strack,
Dr. Sandro Wefel,
Dr. Robert Altschaffel

SACHSEN-ANHALT
EUROPÄISCHE UNION
EFRE
Europäischer Fonds für regionale Entwicklung

# CyberSecurity-Verbund LSA

## Bündelung von wiss. Security-Kräften LSA (EFRE, Digitale Agenda LSA):

**netlab (Hochschule Harz, FB Automatisierung und Informatik)**

- CyberSec-LSA-HS-Harz: Komponenten-basierte Security-Integrationen per Security-By-Design/Management für Wirtschaft und Verwaltung
- Prof. Dr. Strack & Team

**ITSecLab (Institut für Informatik der Universität Halle-Wittenberg)**

- CyberSec-LSA-MLU: Embedded-System-Security und Kryptographie
- Prof. Dr. Molitor,  Dr. Wefel  & Team

**Arbeitsgruppe Multimedia and Security (Otto-von-Guericke-Universität Magdeburg)**

- CyberSec-LSA-OVGU-AMSL: Security-by-Design-Orchestrierung
- Prof. Dr. Dittmann, Dr. Altschaffel & Team

# Strategische Impulse – CSI-Liste

„Gib mir einen Punkt, wo ich hintreten kann, und ich bewege die Erde“
*Archimedes, 3. Jh. v. Chr.*

**01** **Sicherheitsniveau erhöhen –**
**in (IT-)Strukturen und Bewusstsein**

**02** **Sicherheitseffizienz++**
**– Nutzer/Admin entlasten statt belasten**

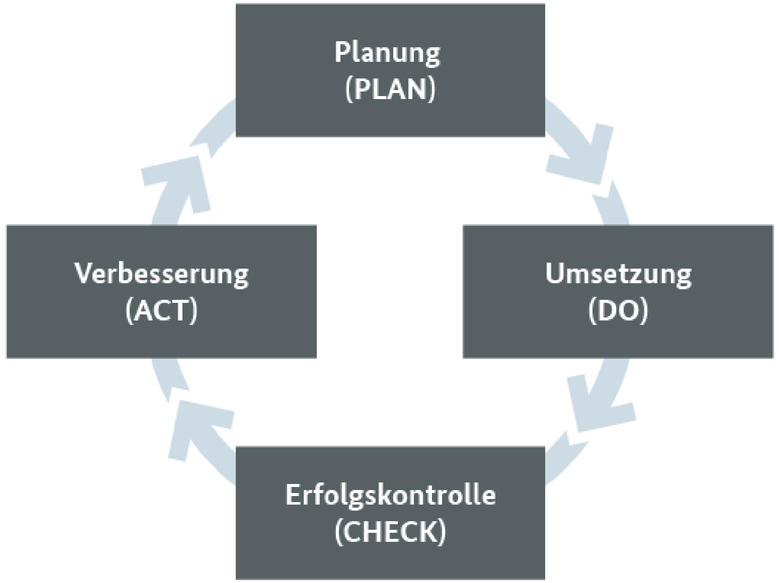
**03** **Härtung ²: Applikationen & Infrastrukturen**
**gemeinsam, mit Standards DE/EU**

**04** **Souveränität und Transparenz stärken**

*… nachfolgend Beispiele - innovative Technik bis zu F&E*

# Security by Design & Management – mit CyberSecurity-Verbund LSA


Quelle: ENISA 2019, Security by Design




Quelle: BSI IT-Grundschutz, Security by Management

**Umsetzung CSI-Liste u.a.: NBP, Ransomware, Trustsistor, …**

# Gesicherte Digitalisierungen/Infrastrukturen - Projektinnovationen – zum Transfer

Tagung CyberSecurity-Verbund Sachsen-Anhalt 11/2022
– Innovationen, Schutz und Chancen im CyberSpace

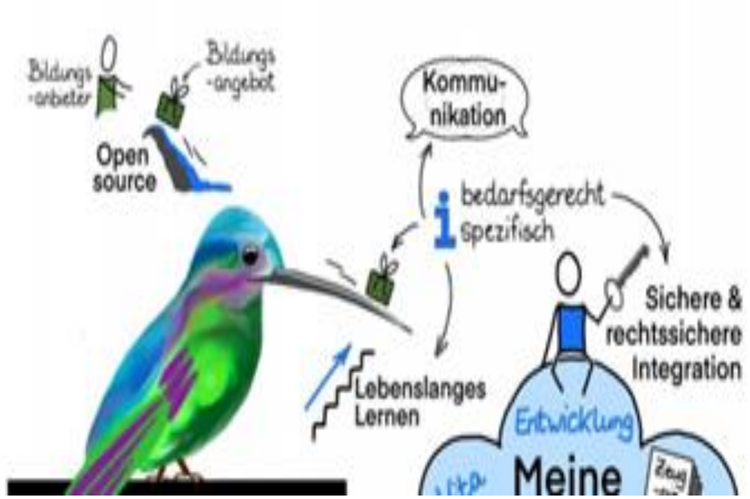
**eNotar**

**Zeugniskopie-Beglaubigung 2022, ABI LSA**
Innovation Netzwerksicherheit

eID Schaufenster 2020 BMWI/Mf LSA
https://www.shield24.de/

[Hühn et. al. 20]

SACHSEN-ANHALT
Ransomware-Workshop mit Kommunen 2021




Wirtschaftsschutztag/Workshop

Onlinezugangsgesetz
Bildung
Hochschule
XHigherEducationInstitutionExchange (XHEIE)

Nationale Bildungsplattform Infrastruktur:
BMBF: Bechtle, Dataport, Univention, HS-Harz;
assoz.: MLU, OVGU, HIS

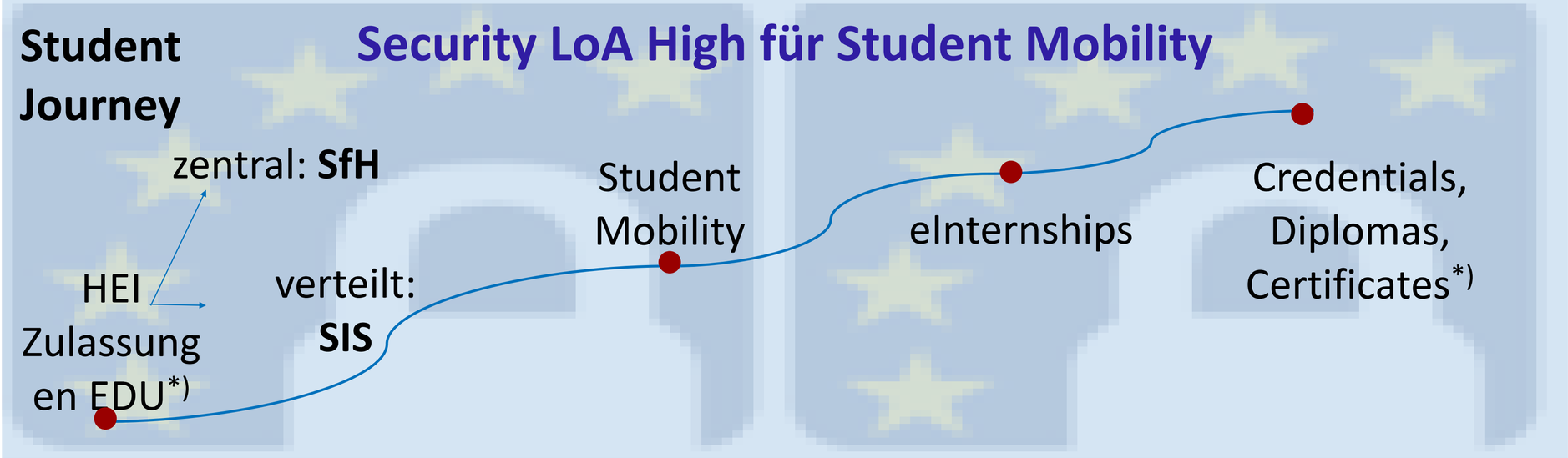
PKI-Workshop

HRK Modus

# Kontexte, Ziele und Fragestellungen

## Student Journey

### Security LoA High für Student Mobility




**eID-Projekte (ab 2012, HS Harz)**

**Projekte mit eIDAS (ab 2017):**

- TREATS (EU CEF, LSA)
- StudIES+ (EU CEF, LSA)
- SHIELD (BMWi, LSA)
- NBP Infra. KOLIBRI (BMBF)
- CyberSec-LSA/Booster (EFRE, LSA)

Co-financed by the European Union
Connecting Europe Facility

## Infrastruktur (Auswahl)

- eIDAS
- eID TS (sign,seal...)
- OZG-Konten
- EDCI
- XHEIE
- EMREX
- Verifiable Credentials, W3C
- **Nationale Bildungsplattform NBP**
- **eNotar**
- **(Your)Credentials**

## Legal Requirements & Standards

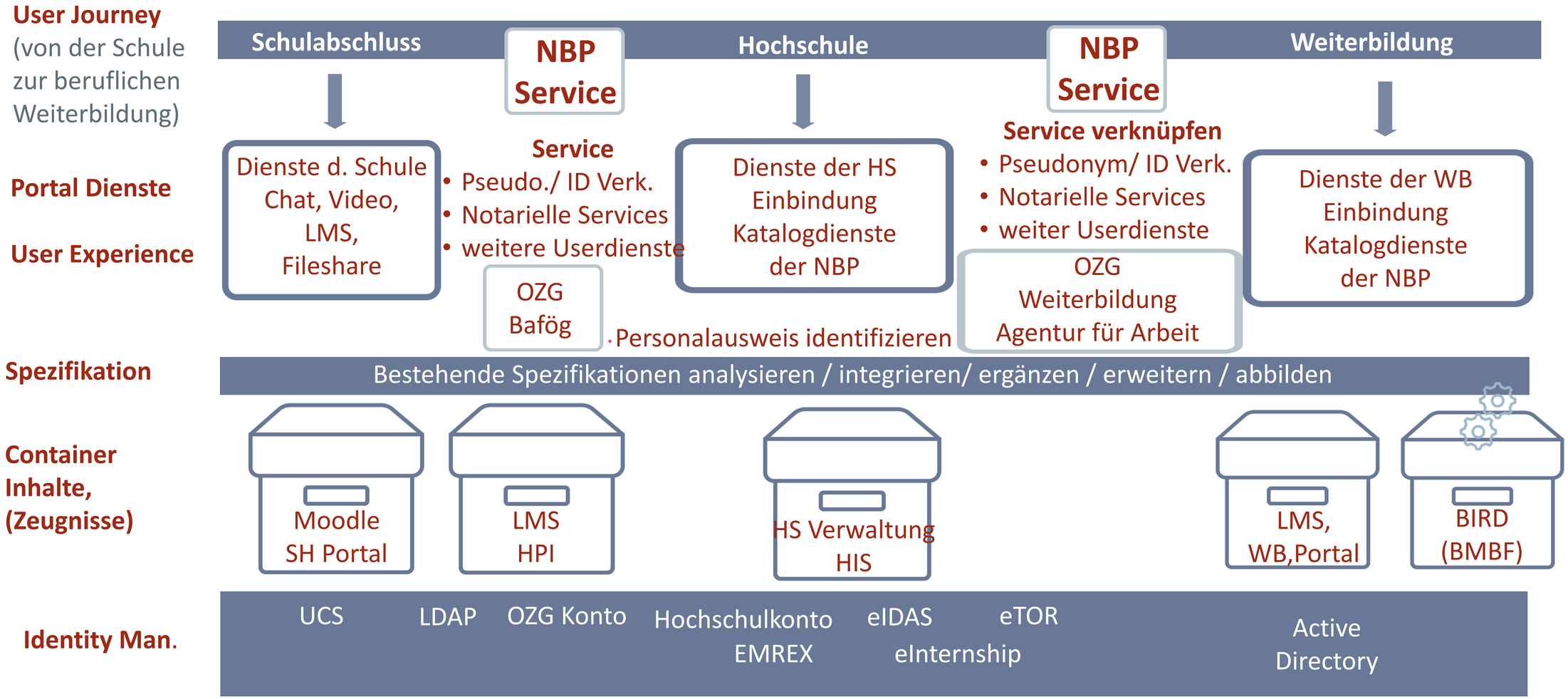
OZG Online Access Law

eIDAS

ETSI

SDG Single Digital Gateway

# Nationale Bildungsplattform (NBP) KOLIBRI - Big Picture: User Journey




- Crossover/Konnektion, Zugang und Austausch für Bildungsträgersysteme
- Sicherheit, Datenschutz und Standards (anpassungsfähig, interoperabel)

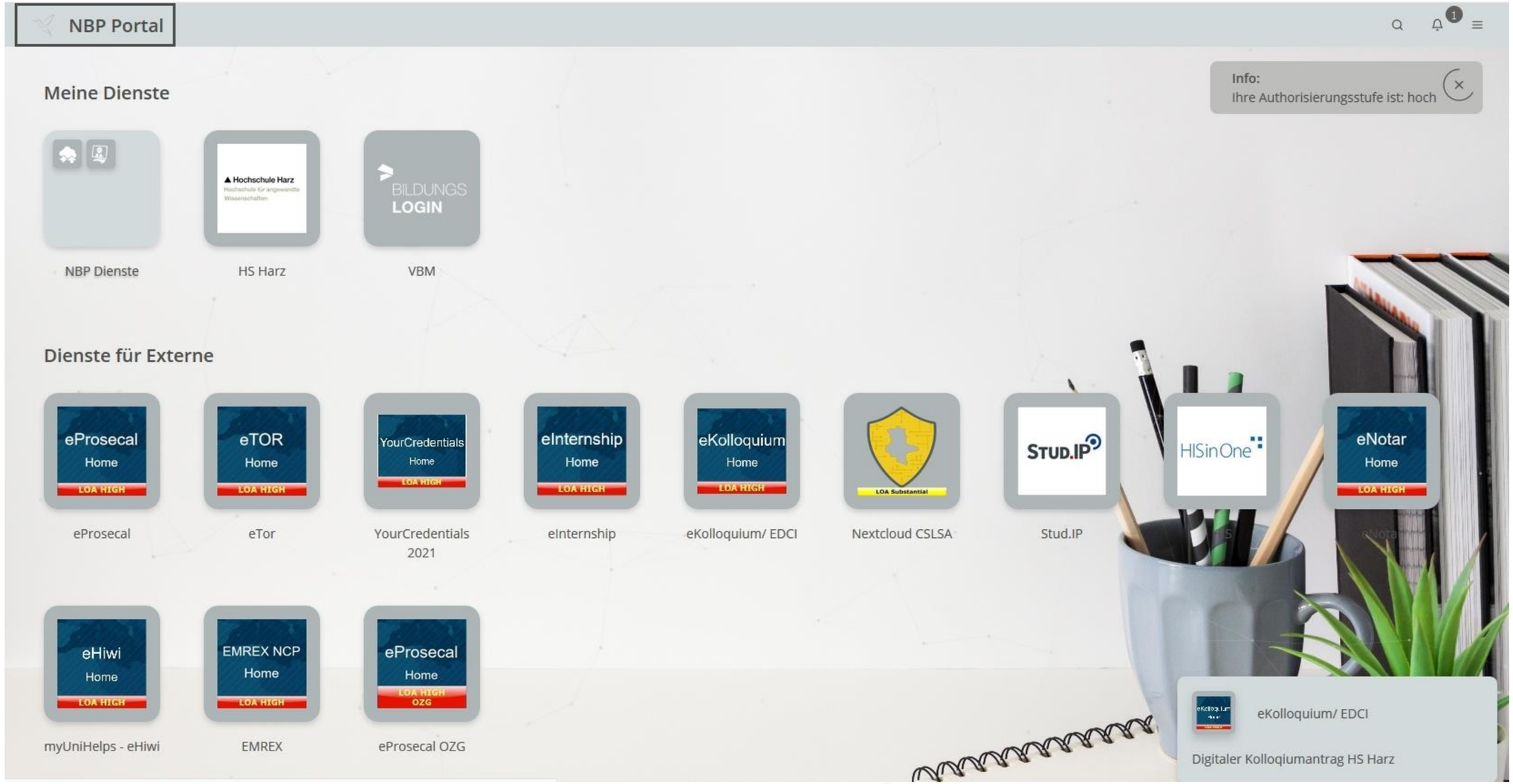
[BSI19b], [BSI21], [Stra22a], [Stra22b]

# Nationale Bildungsplattform (NBP) KOLIBRI - Screenshot

**LoA High** – Level of Assurance High: Sicherheitsstufen Authentisierungen

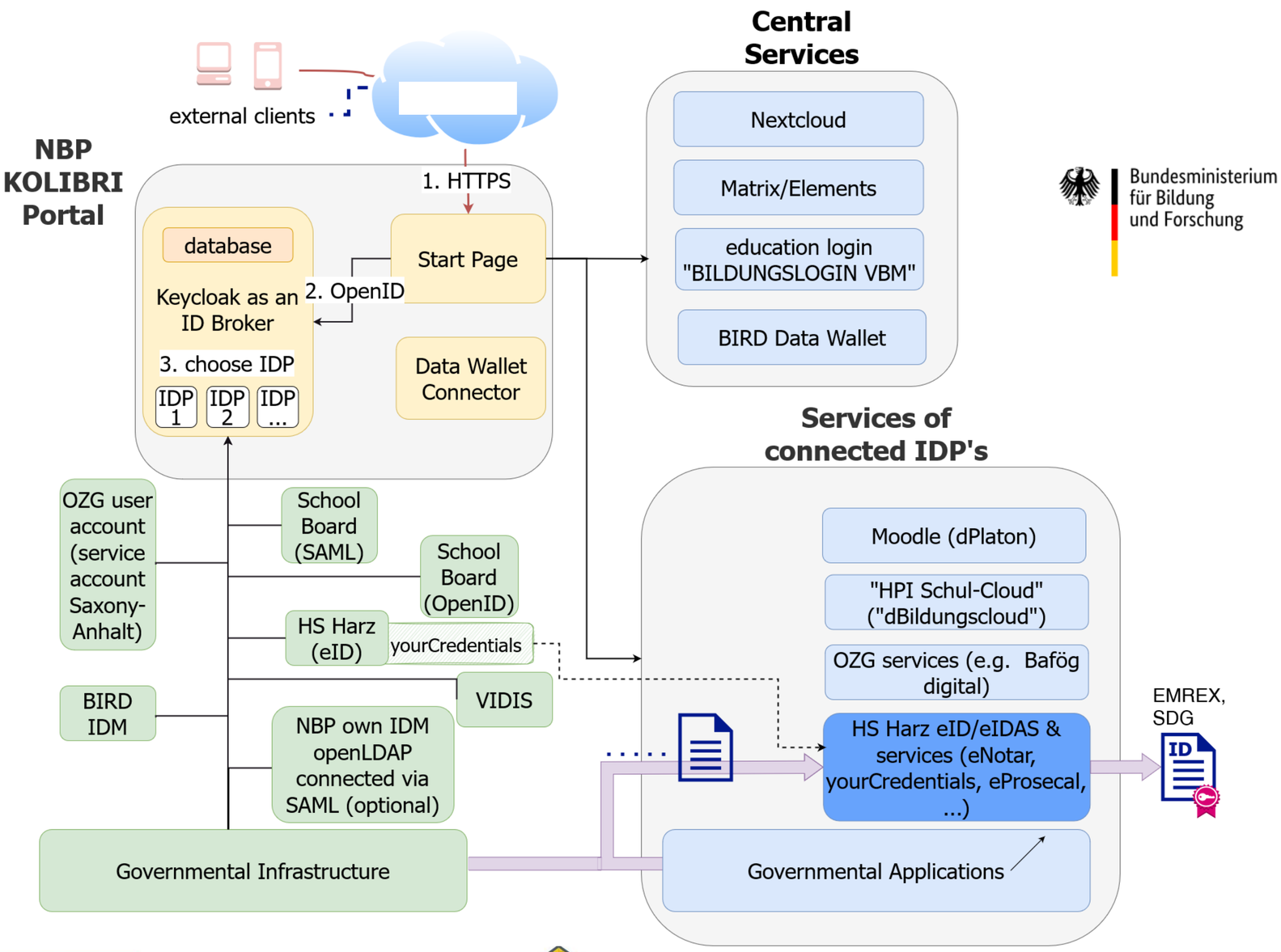
Anbindung von OZG-Nutzerkonten mit LoA-Stufung (High, Substantial, Low)

Erhaltung und Markierung von LoA bei Zugang und Workflow

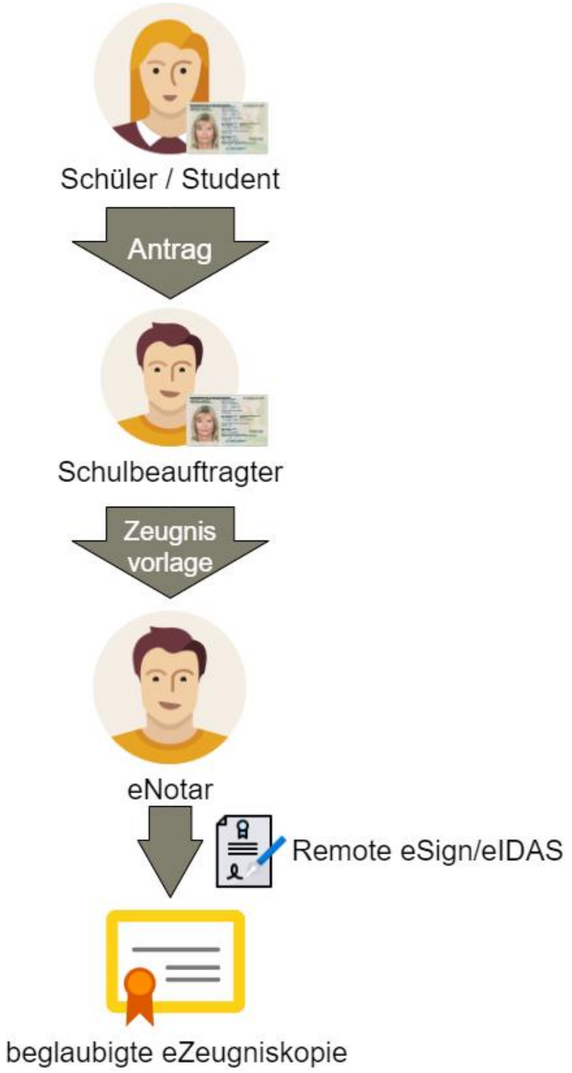


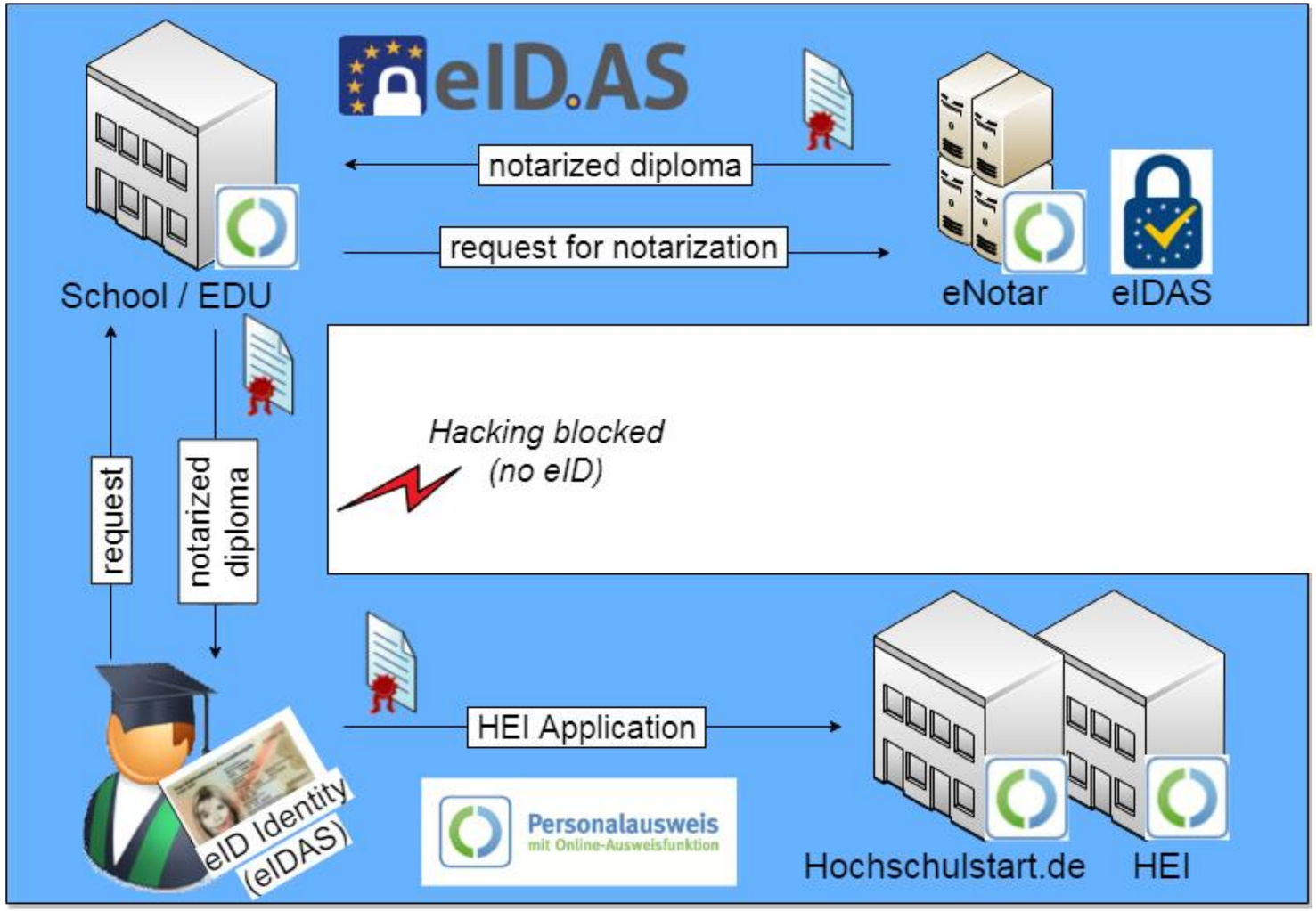
# NBP KOLIBRI – Architektur-Überblick

- Security & Privacy by Design
- ID-Broker innen, IDPs extern
- LoA „High“ für eID/OZG-Login
- SSO zu externen  HEI/EDU Anbietern
- (Metadata-) Konnektor, BIRD (BMBF)
- eIDAS Wallet eProsecal
- eNotar-Extensions

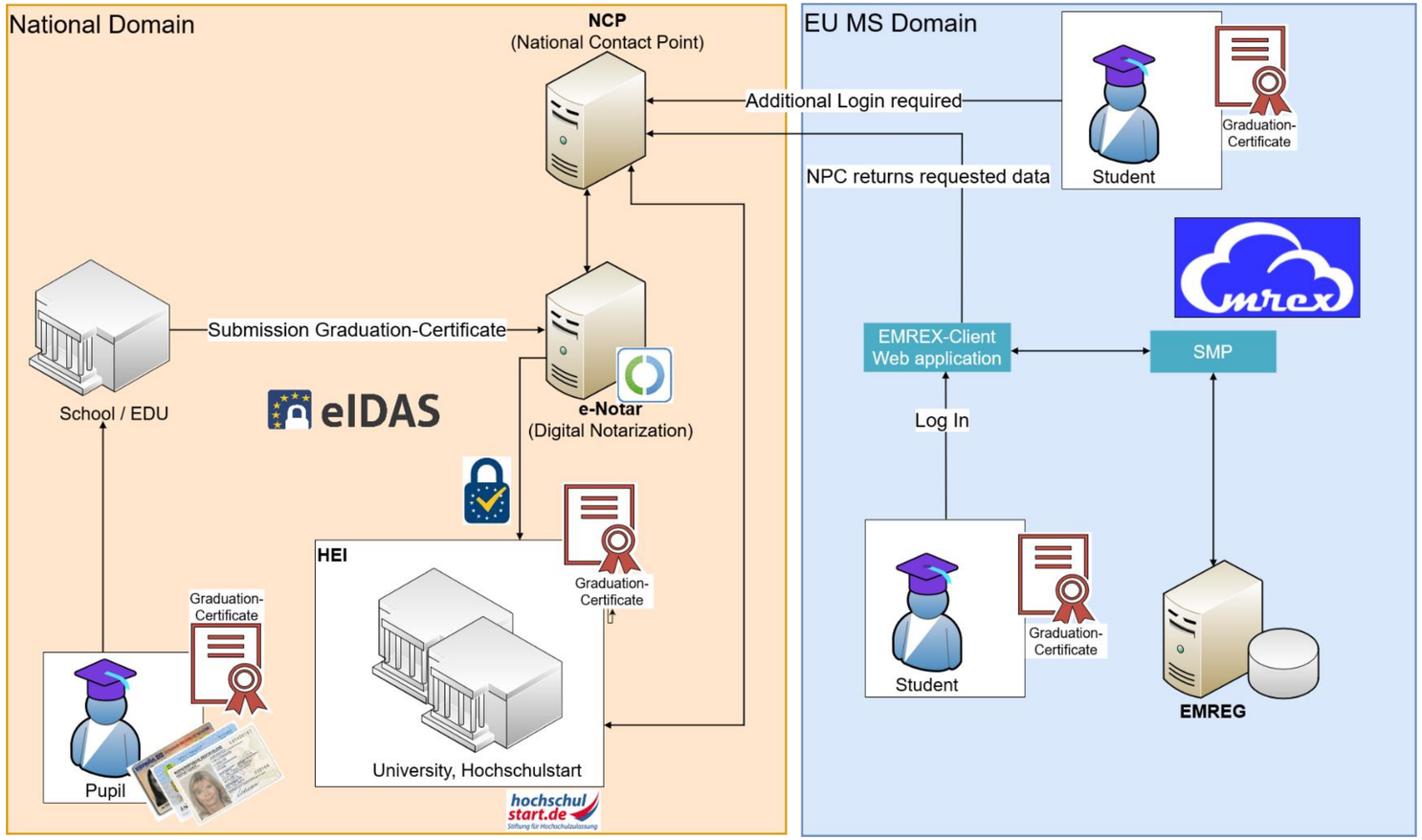


# eNotar: Beglaubigung & Work/Dok.-Flow mit eID/QeS/TS



# EMREX, eIDAS and eNotar – Security for Student Mobility – Zeugniskopie-Beglaubigung Martineum Halberstadt

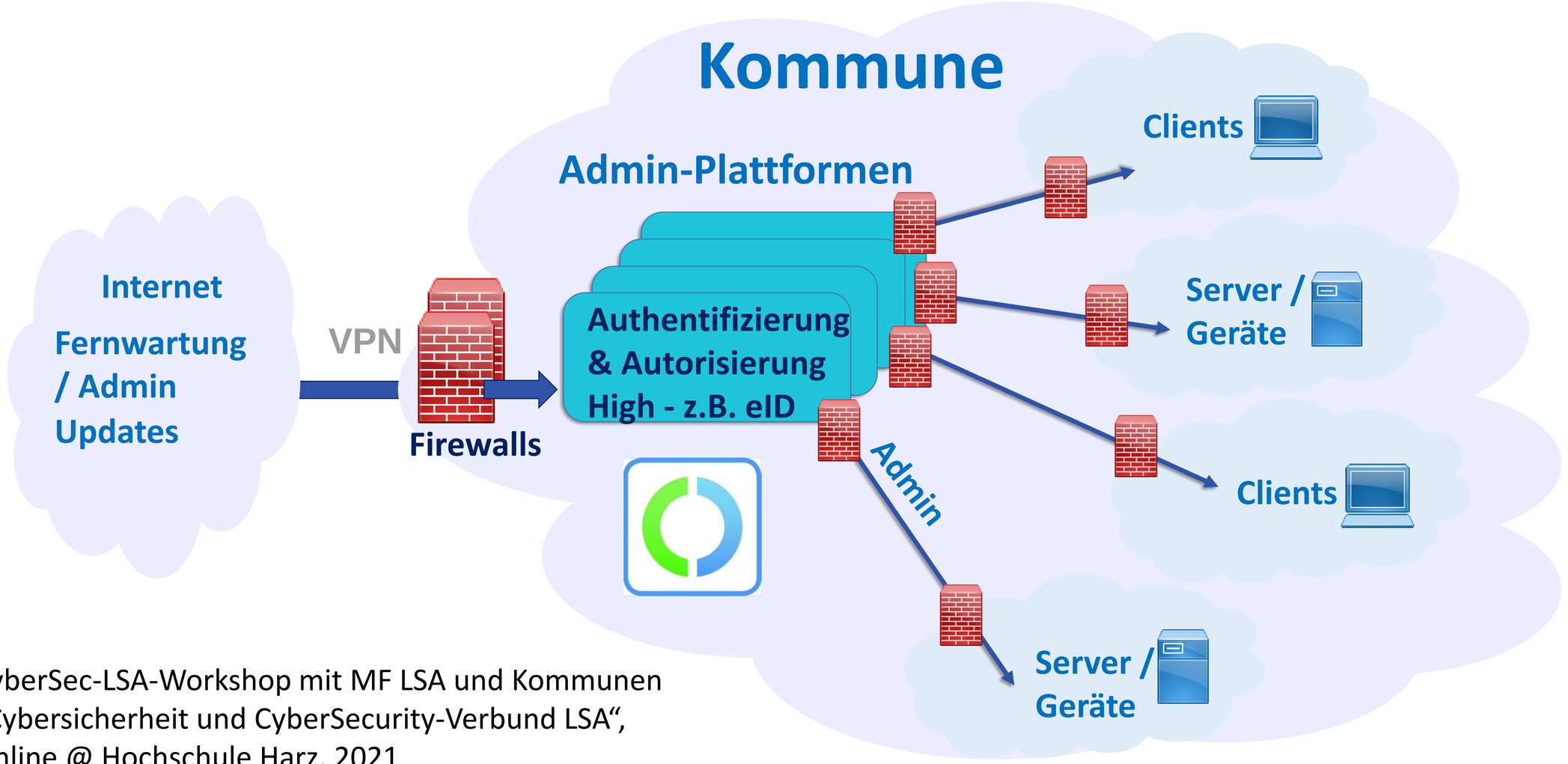



**Erfolgreiche EMREX-Tests mit UNIT/SIKT Norwegen und UNI Warschau, Polen**

**Sicherheitsmanagement++**

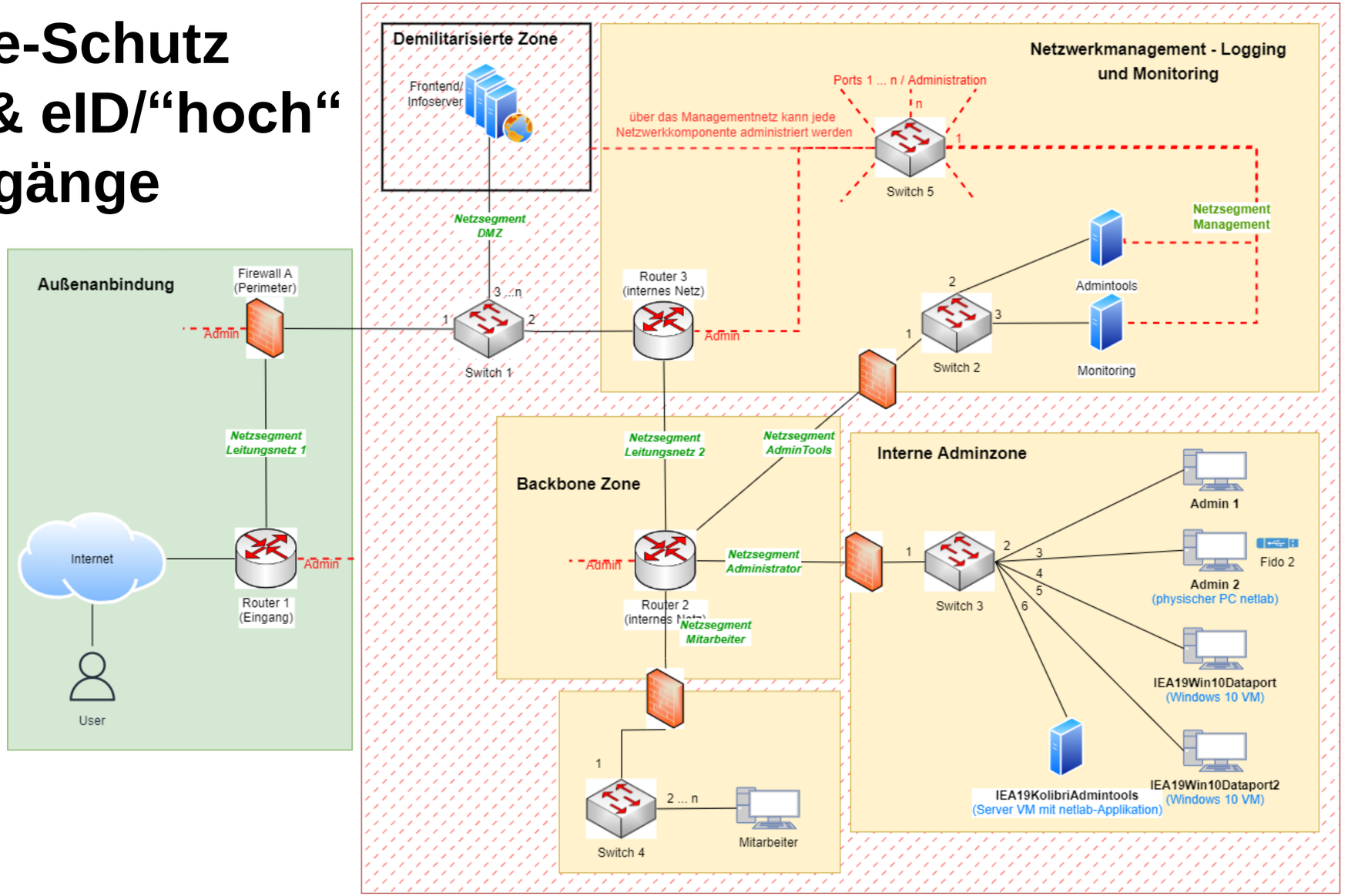
- EMREX/ELMO Security – Plan zu Security AddOns [Stra22]

# Ransomware-Schutz: Admin-Zugang eID/“hoch“




CyberSec-LSA-Workshop mit MF LSA und Kommunen
„Cybersicherheit und CyberSecurity-Verbund LSA“,
Online @ Hochschule Harz, 2021

# Ransomeware-Schutz Separierung & eID/“hoch“ für Admin-Zugänge



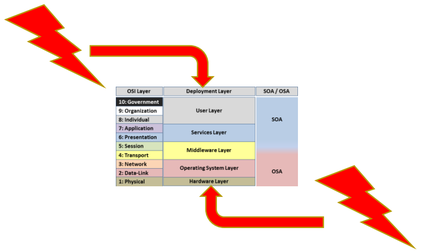
# F&E: von Zero Trust zum – „Trustsistor“-Konzept

**Anforderungen und Beschränkungen:**

- bisher: “statischer” Domain-Schutz durch Datendioden und Firewalls
- Nachteil: nur "geografische" Domains (classified), keine Appl.-Domains, keine vertrauenswürdigen Handshakes/MLS-Ebenen
- Anforderung: mehrschichtiger Schutz gegen multiple Angriffs-Layer, Appl.-orientierte Trust-Domains anbieten
- Idee: Durchflussteuerung anhand Vertrauensattributen an den Protokoll-Flüssen/Layer

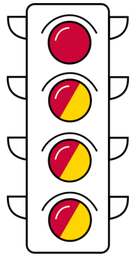
**“Trustsistor” Grundkonzept**

- “Trustsistor” Konzept: Durchflusssteuerung anhand dynamisch als vertrauenswürdig “gefärbter” IP-Flüsse, basierend auf kryptografischen (notariell beglaubigten) Vertrauensattributen
- Vertrauensattribute für verpflichtende Identifikation- und Zugriffs-verwaltung (IAM) von Stakeholder-Domains, Externalisierung von Trust-Relationen
- Erweiterungen der Projekte StudIES+/NBP KOLIBRI: eIDAS & IAM basierter Schutz auf Prozess- und Dokumentfluss-Ebene, LoA “high”

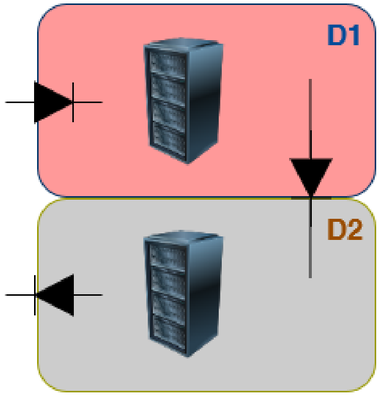



Multi Layer Angriffe

CSI Ampel



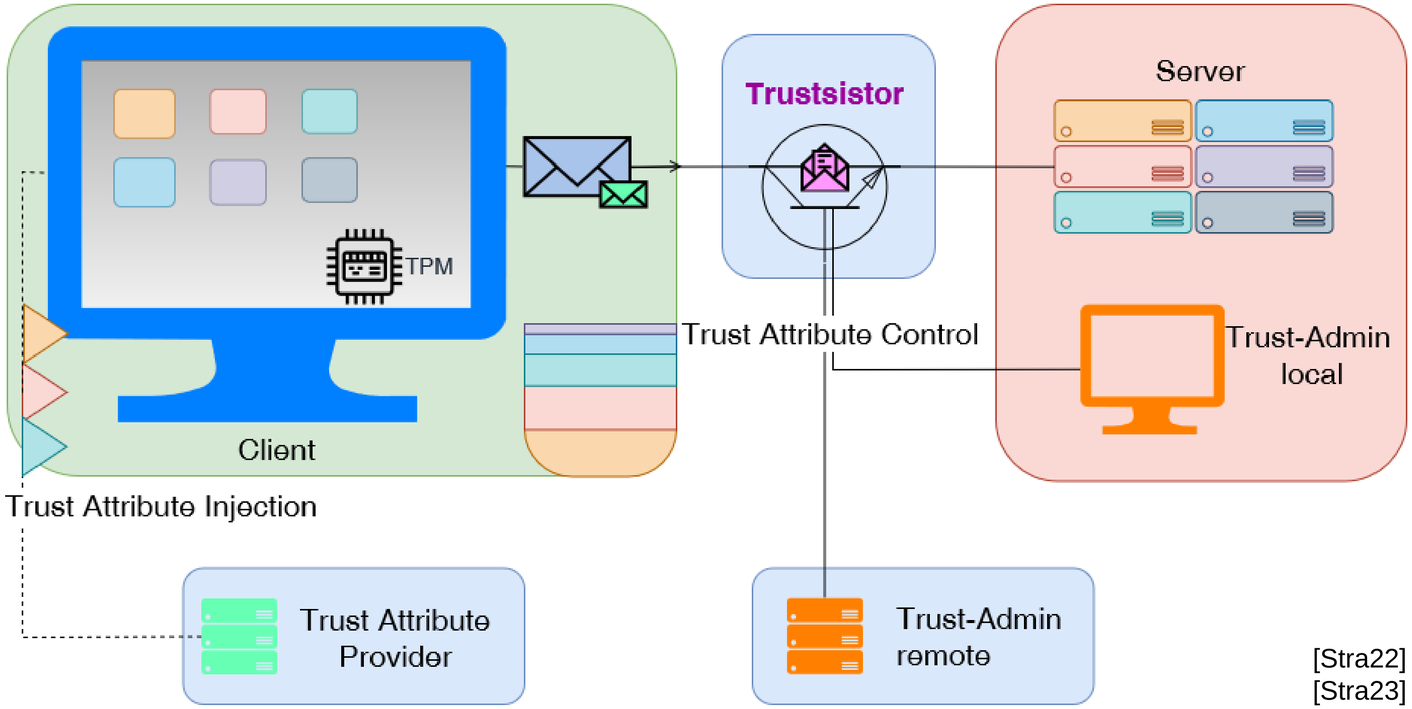
Niveau
Effizienz
Härtung
Souveränität




Datendiode

# F&E: Trustsistor-Konzept – Details

- Trust Attribute Injection ermöglicht die Einfärbung und Kennzeichnung von vertrauenswürdigen IP-Flows durch Attribute (TSP) (statt nur "klassifizierter" Domains)
- Mandatory Policies / Trust Attribute Bindings durch TPM, Protokoll-Umsetzung z. B. IPv6
- Kontrolle der Vertrauensattribute: innerhalb/außerhalb der Zieldomäne, multi level/lateral extensions
- Vertrauensverstärkung durch Kombination verschiedener Anbieter von Vertrauens-attributen (unterschiedliche Zwecke)
- Next Level: Trustsistoren-Netzwerke, Integration Supply-Chain




[Stra22]
[Stra23]

# Vortrag BSI LSA Roadshow Kommunen 23.08.2022

IT-Planungsrat
Digitale Zukunft gestalten

SACHSEN-ANHALT #moderndenken

SACHSEN-ANHALT

EUROPÄISCHE UNION
EFRE
Europäischer Fonds für regionale Entwicklung

SACHSEN-ANHALT

#moderndenken

IT-Planungsrat
Digitale Zukunft gestalten

# Verwaltung digital

# Mensch macht´s!

11. Fachkongress des IT-Planungsrats

MARTIN-LUTHER-UNIVERSITÄT
HALLE-WITTENBERG

OTTO VON GUERICKE
UNIVERSITÄT
MAGDEBURG

Hochschule Harz
Hochschule für angewandte Wissenschaften

CYBER | SEC
VERBUND SACHSEN-ANHALT

# Härtung von Applikationen und Infrastrukturen

# Innovationen für Angriffsdetektion/-response mit Machine Learning

# Unser Ziel

**Allgemein: Verbesserung der Datensicherheit**

- Unterstützung von Bedarfsträgern bei der Verbesserung der „Datensicherheit“ auf Ebene der IT-Infrastruktur und durch organisatorische Maßnahmen (Hilfe zur Selbsthilfe)
- Eindämmung der Gefährdung vernetzter Systeme: Embedded Devices, IoT, I(I)ot, **Firmen-/Verwaltungsnetze** *durch zielorientierte Auswertung von Netzwerkverkehr hinsichtlich Schadprogrammen*
- Praktikable Werkzeuge für IT-Administration
- Sensibilisierung und Weiterbildung der Belegschaft

MARTIN-LUTHER-UNIVERSITÄT HALLE-WITTENBERG

GitLab

element

BigBlueButton

Nextcloud

# Vernetzte IT-Infrastruktur - Rückgrat der Digitalisierung

**und Bedrohung für die Sicherheit?**

- zunehmender Einsatz vernetzter Systeme

  *Intelligente Beleuchtungssysteme, Sicherheitssysteme, Klimatisierung, Smartmeter, WallBoxen, SmartTV*
- Geräte unterliegen im Schnitt 5.200 Angriffen jeden Monat, 2017 Anstieg an IoT-Angriffen 600%

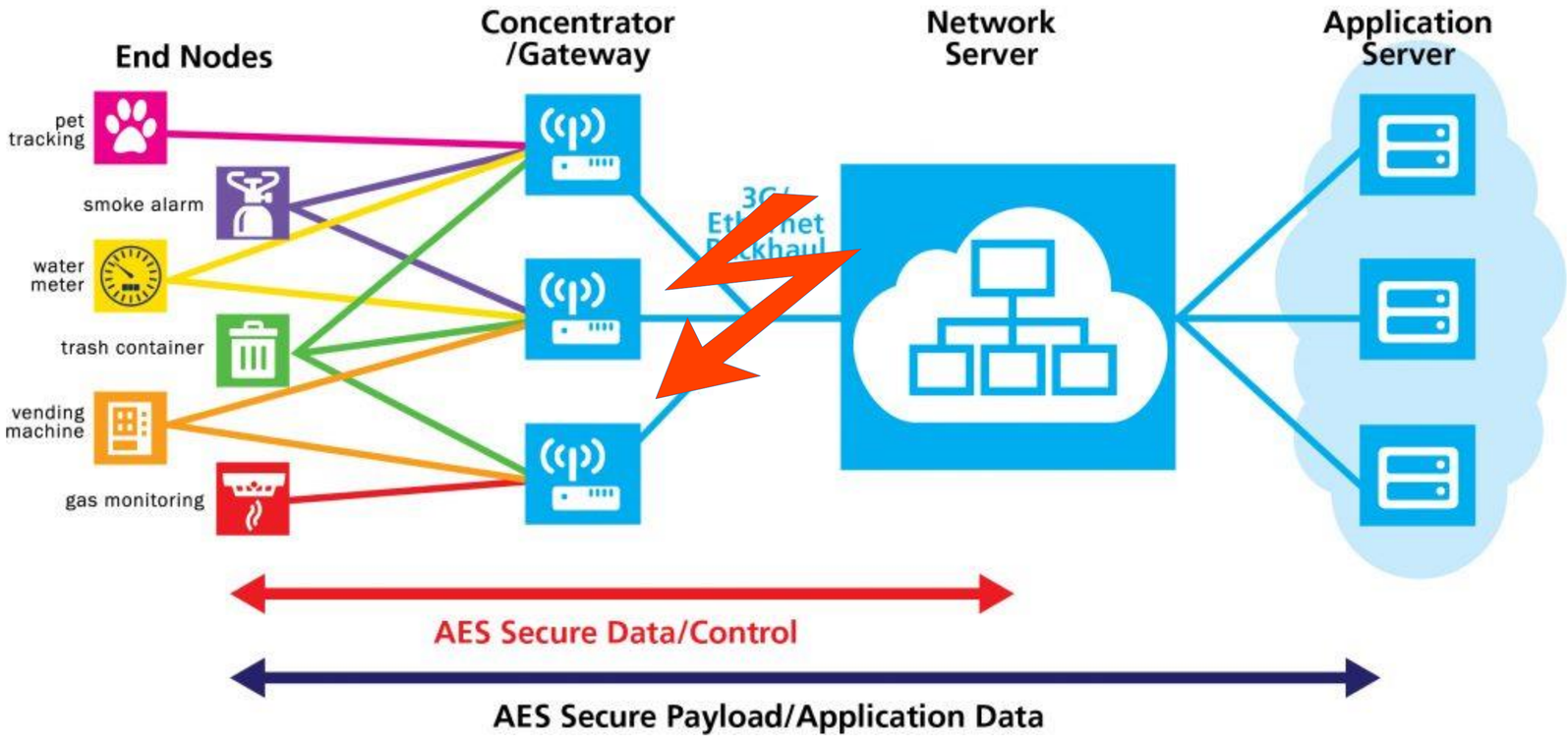
Quelle: Symantec Internet Security Threat Report Volume 24

**Größte Gefahrenquellen**

- Schadsoftware:
  - BYOD - Bring Your Own Devices
  - Email-Anhänge oder Datenträger (USB-Sticks)
- IoT-Geräte etc. - Kommunikation mit Herstellercloud

# Rechnernetze

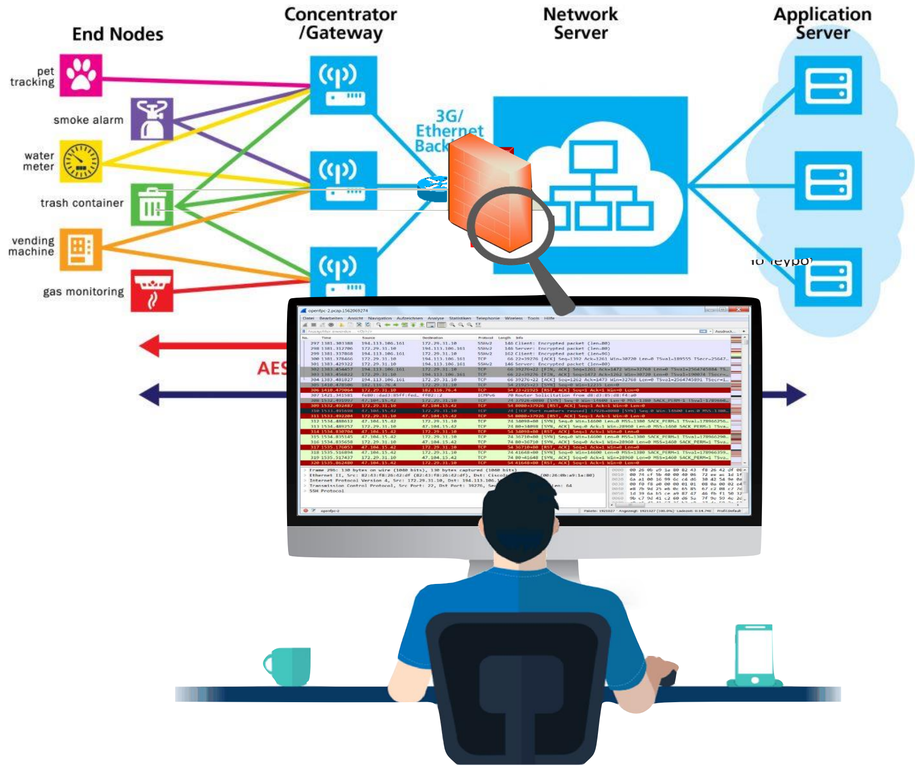
**zunehmend Ausgangspunkt für Angriffe auf IT-Infrastruktur und -Dienste**

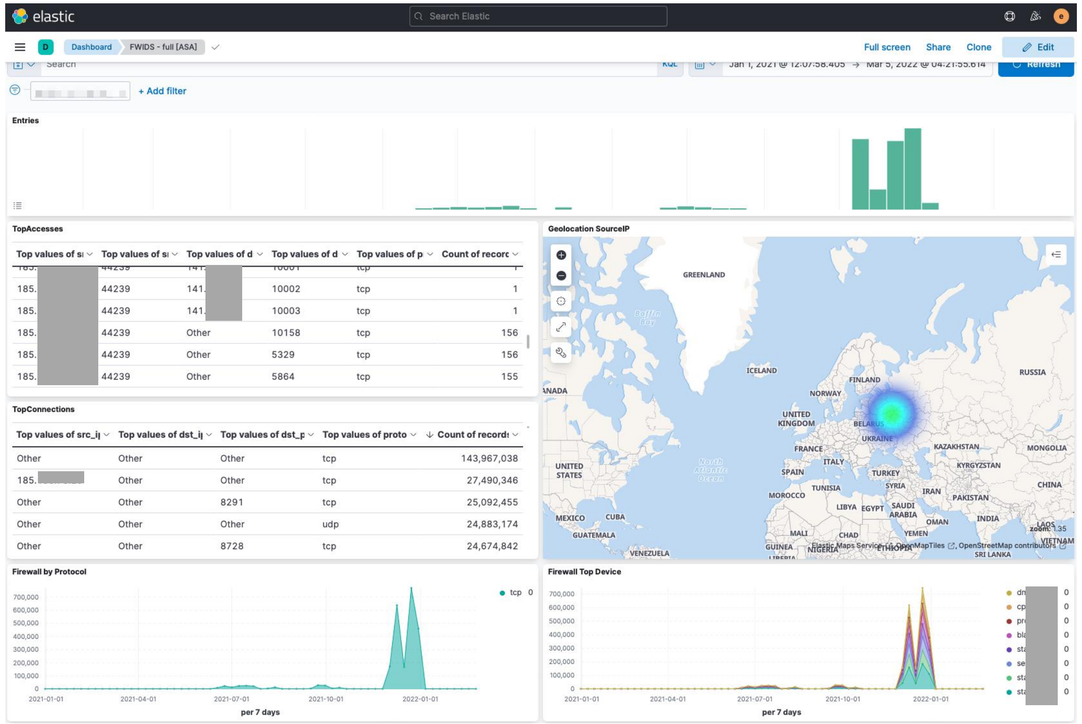



Quelle: LoRa WAN: Protokoll-Sicherheit-Anwendung - iot-design.de + Semtech GmbH

# Rechnernetze – Trafficanalyse per Hand

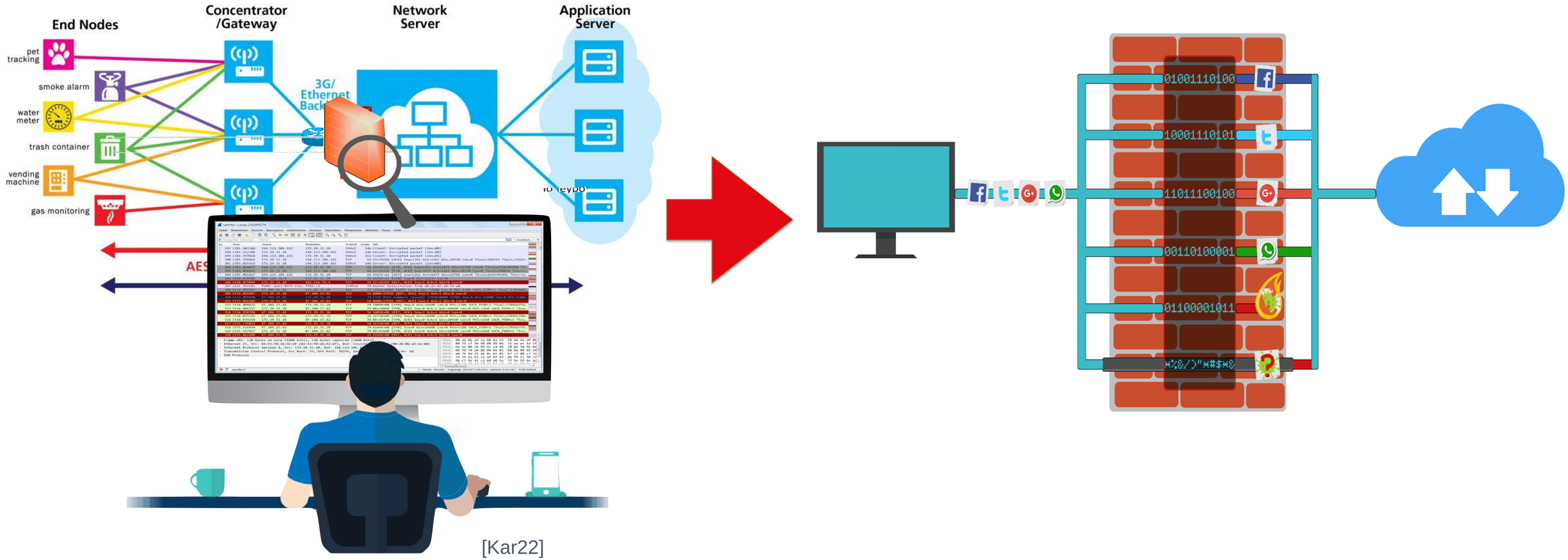
## Auswertung des Datenverkehrs: Suche nach bösartigen oder versteckten Inhalten



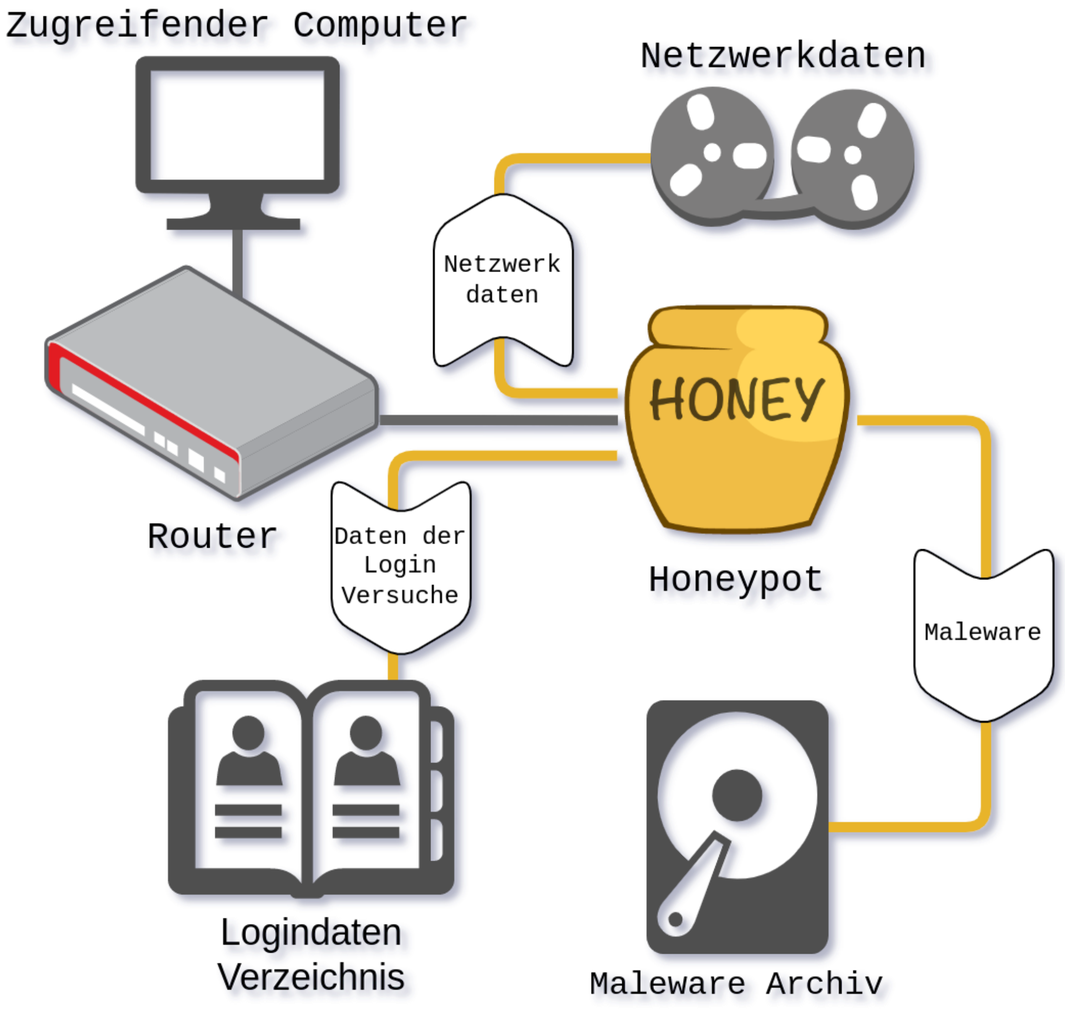



# Rechnernetze – Trafficanalyse - Maßnahmen

## Auswertung des Datenverkehrs: Suche nach bösartigen oder versteckten Inhalten – Unterscheidung der Inhalte - Filterung




[Kar22]
[Knö22]

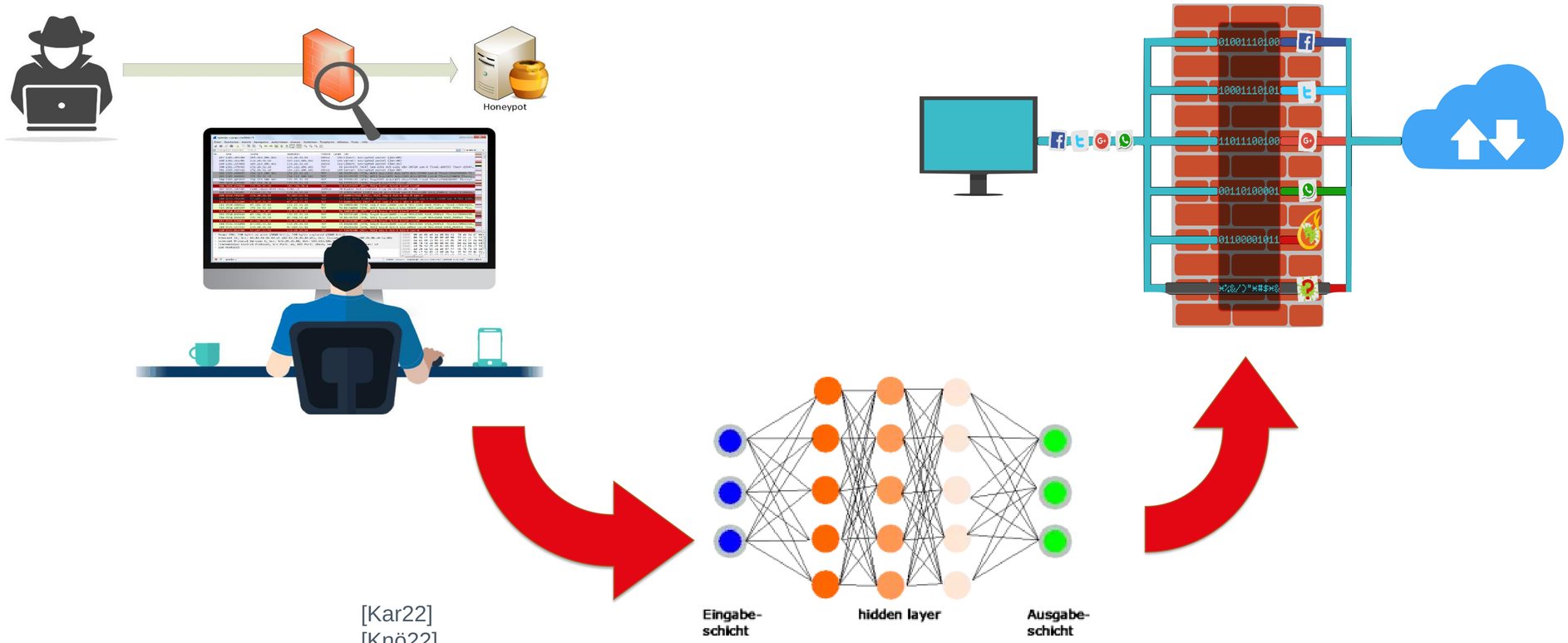



# Honeypot

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

# Rechnernetze – Trafficanalyse mit KI-Methoden - Maßnahmen

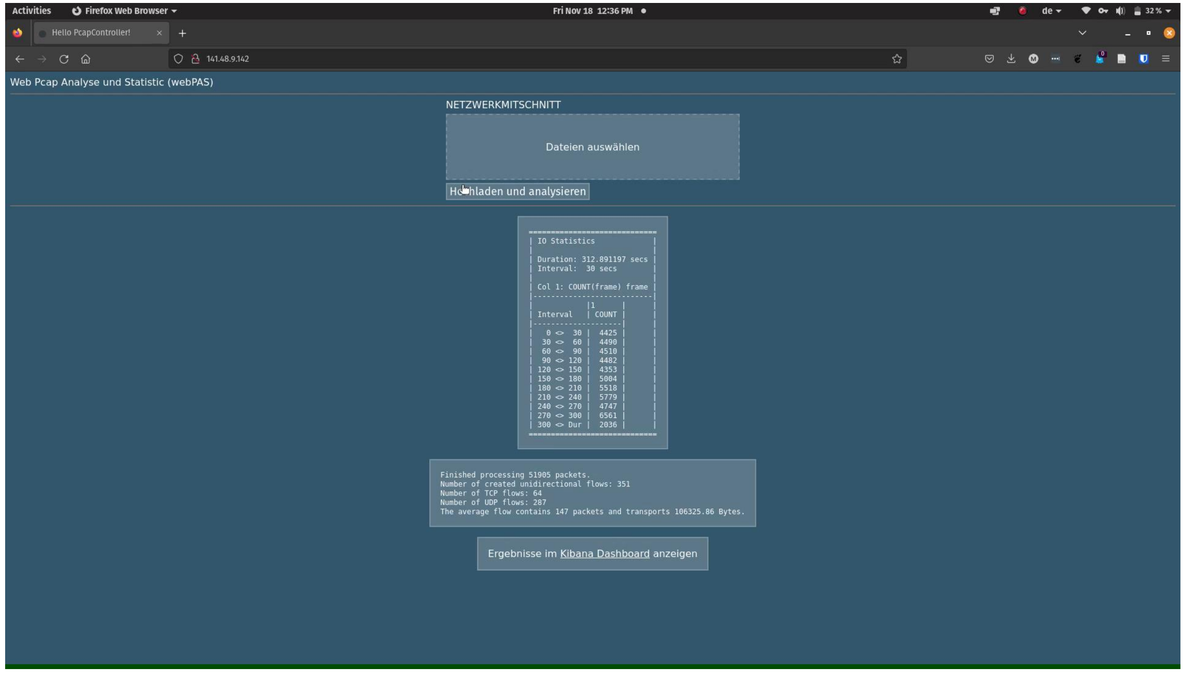
**Auswertung des Datenverkehrs: Erlernen des normalen Verkehrs, Auswertung ungewöhnlichen Verhaltens**

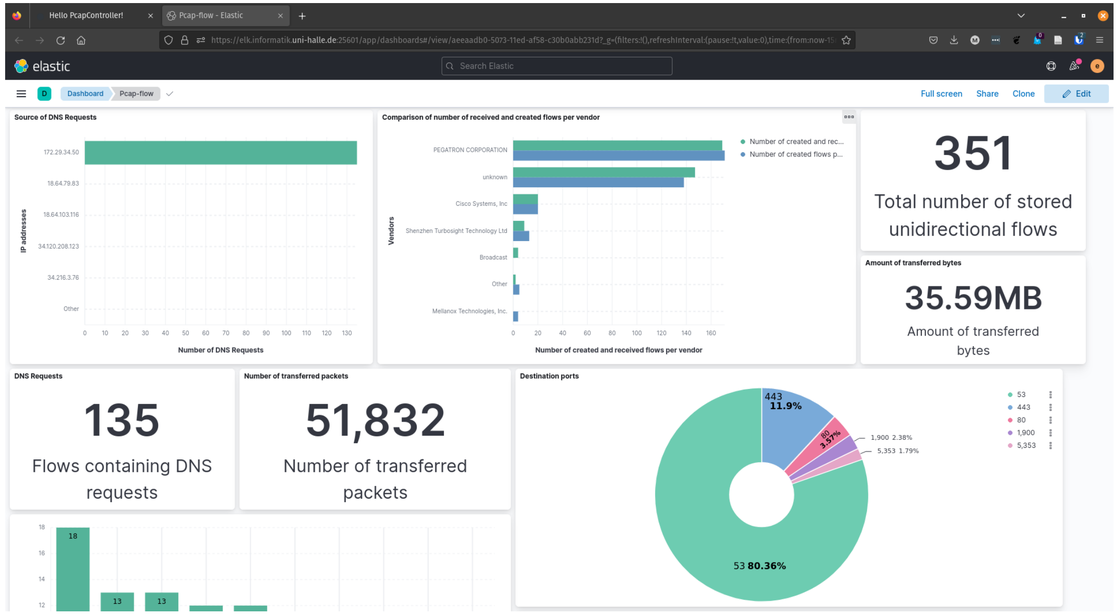



[Kar22]
[Knö22]

# Mitschnittanalyse

## Auswertung des Datenverkehrs: Suche nach bösartigen oder versteckten Inhalten – Unterscheidung der Inhalte



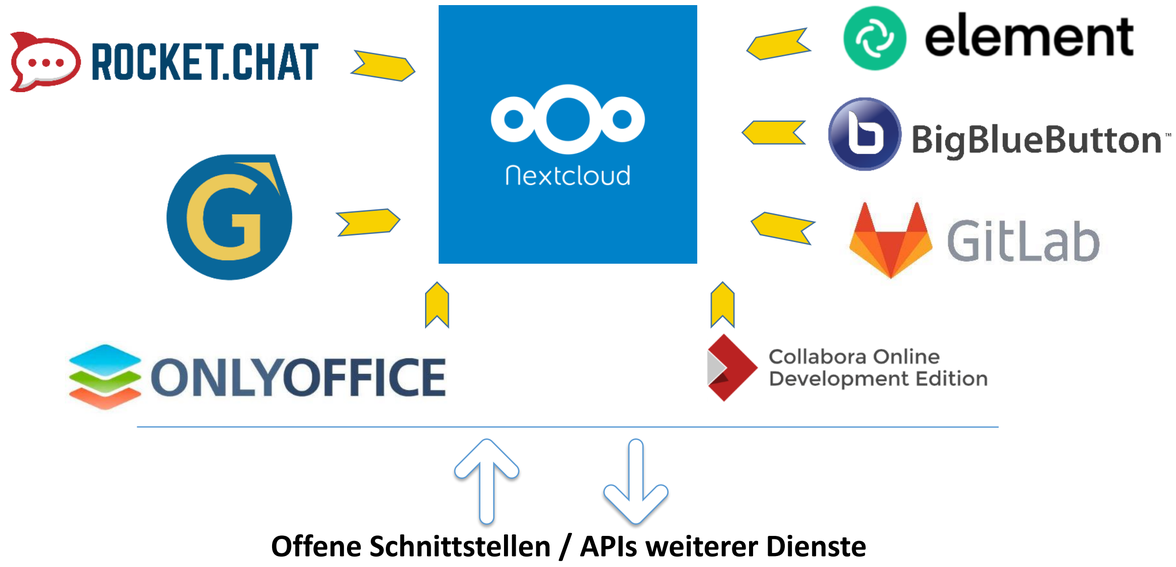

https://cloud.cslsa.de/index.php/f/273576

# Souveränität und Transparenz stärken

# Mehr Unabhängigkeit von Herstellerlösungen

**Allgemein: Verbesserung der Datensicherheit**

- Schaffung von alternativen Angeboten auf Basis von FOSS
- Verwendung von ausgesuchter Software hinsichtlich Datensparsamkeit, Datensicherheit, On-Premise Einsatz



IT-Planungsrat
Digitale Zukunft gestalten

SACHSEN-ANHALT #moderndenken

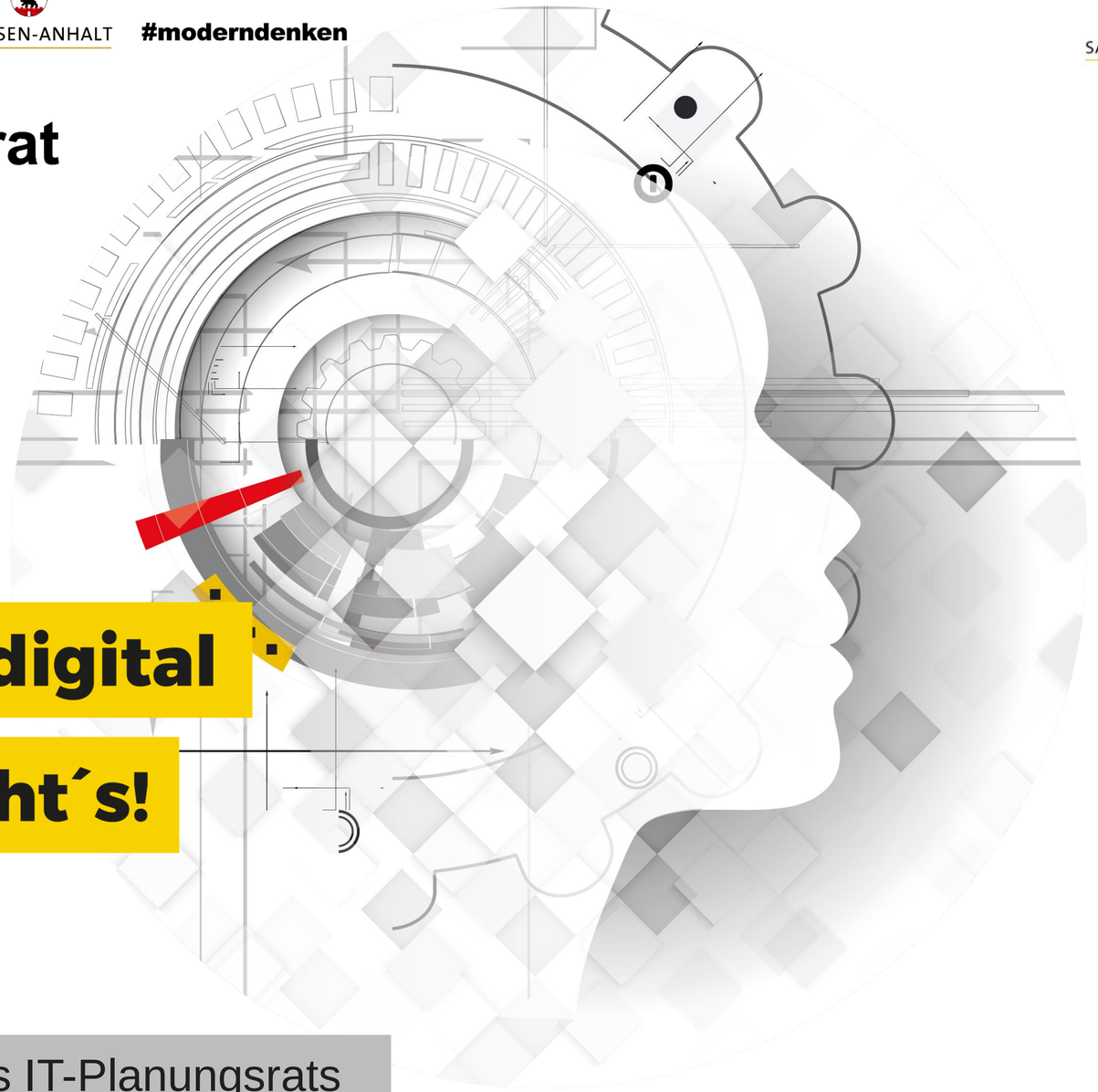
SACHSEN-ANHALT

EUROPÄISCHE UNION
EFRE
Europäischer Fonds für regionale Entwicklung

SACHSEN-ANHALT

#moderndenken

IT-Planungsrat
Digitale Zukunft gestalten



# Verwaltung digital

# Mensch macht´s!

11. Fachkongress des IT-Planungsrats

MARTIN-LUTHER-UNIVERSITÄT
HALLE-WITTENBERG

OTTO VON GUERICKE
UNIVERSITÄT
MAGDEBURG

Hochschule Harz
Hochschule für angewandte Wissenschaften

CYBER | SEC
VERBUND SACHSEN-ANHALT

# Situation

**Gesteigerte Sensibilität für Relevanz verschiedener Querschnittsziele**

- Datensicherheit
- Technischer Datenschutz
- Datensparsamkeit
- Digitale Souveränität
- Nachhaltigkeit
- Betreffen verschiedene Akteure: Verwaltungen, Kommunen, Behörden, aber auch Privatpersonen ...

# Kompetenzvermittlung und Kompetenzaufbau

**Wie können wir Kompetenzen vermitteln?**

- **Demonstratoren & Evaluationsinstanzen**: Sichere und ressourcensparsame OS zum Anfassen
- Erforschung und Erarbeitungen von Möglichkeiten für **Fort- und Weiterbildungen** sowie **Vorträge** für Bedarfsträger
- Souveräne und nachhaltige **Digitalisierungsprojekte** für Bedarfsträger mit **wissenschaftlicher Begleitung**

# Demonstratoren/Evaluationsinstanzen

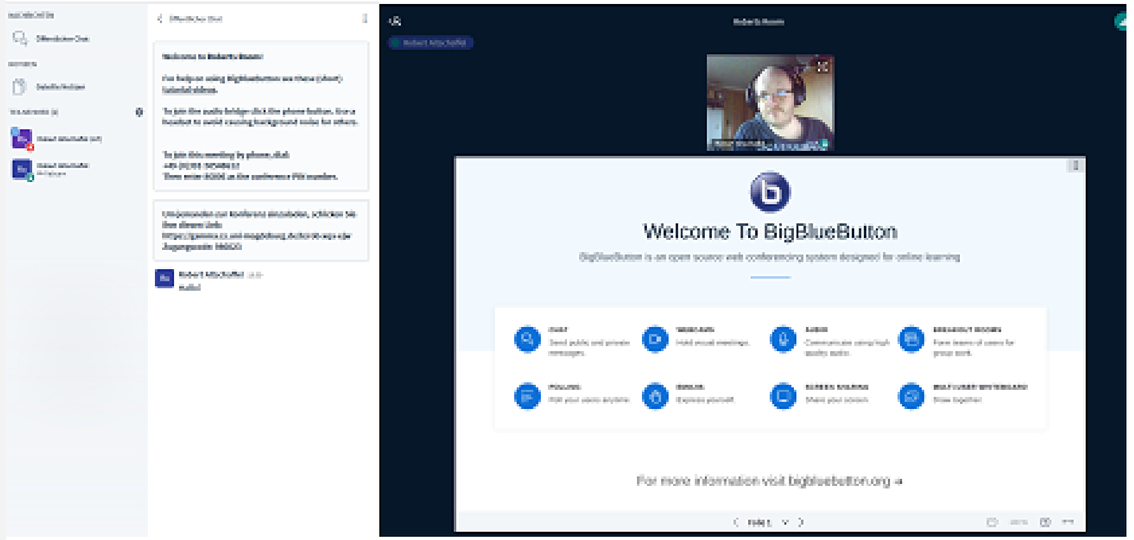
**Wie können wir Kompetenzen vermitteln? Demonstratoren für verschiedene Systeme**

- Digital souverän (lokal betrieben – keine Abflüsse an Dritte!)
- Datenschutzfreundlich / Datensparsam
- IT-Sicher
- Open Source
- Als Technologiedemonstratoren - Zum Ausprobieren und Anfassen

# BigBlueButton

**Videokonferenzsoftware**

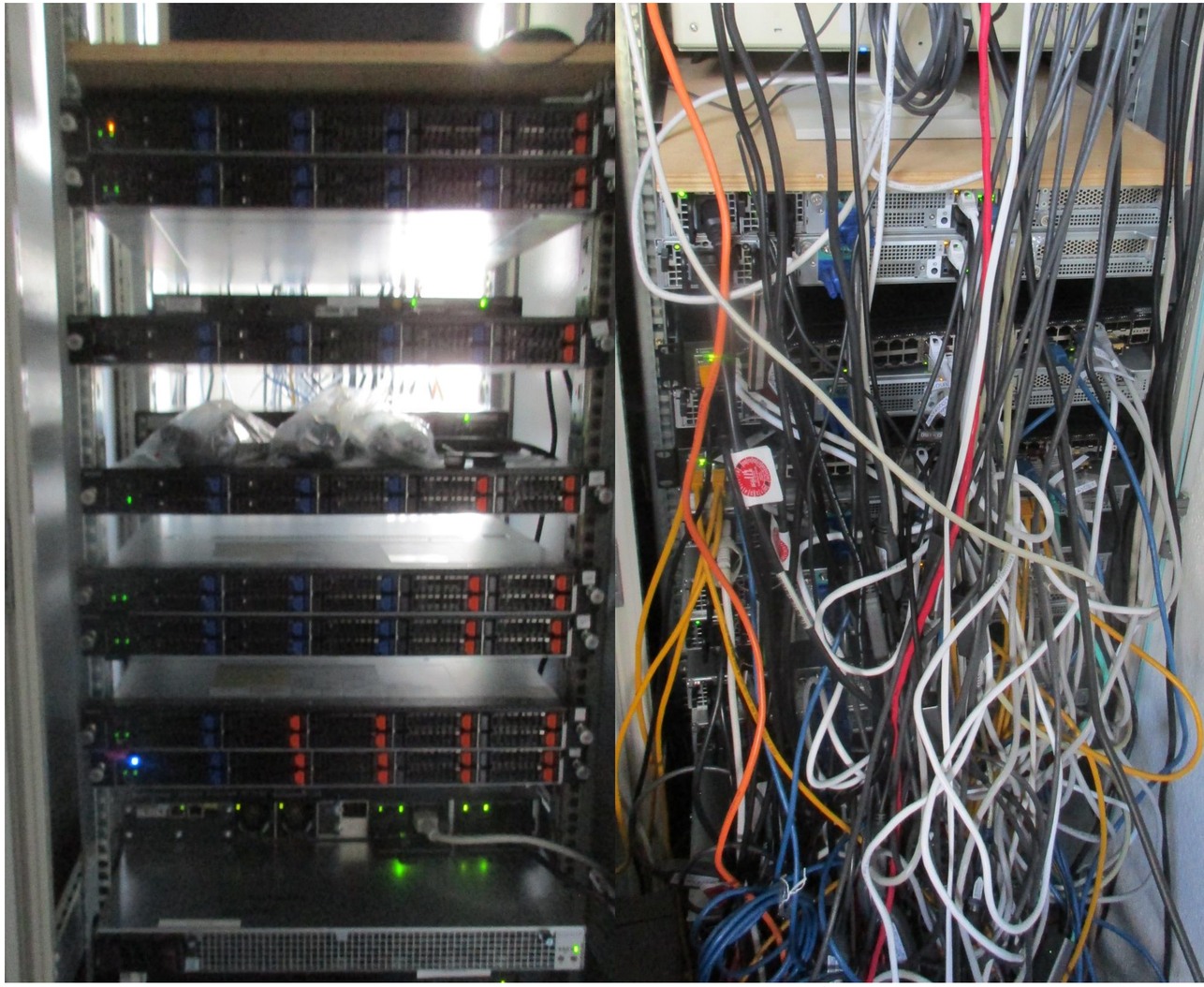
- Open Source
- Auf Bildung ausgerichtet
- Lokal gehostet
- Datensparsam/Datenschutzfreundlich
- Wird innerhalb der Lehre verwendet
- Diversen Interessenten für Evaluation zur Verfügung gestellt



# OpenSourceCloud

**Demonstrator für eine souveräne, privatssphären-schützende, IT-sichere, forensisch vorbereitete Cloud-Umgebung**

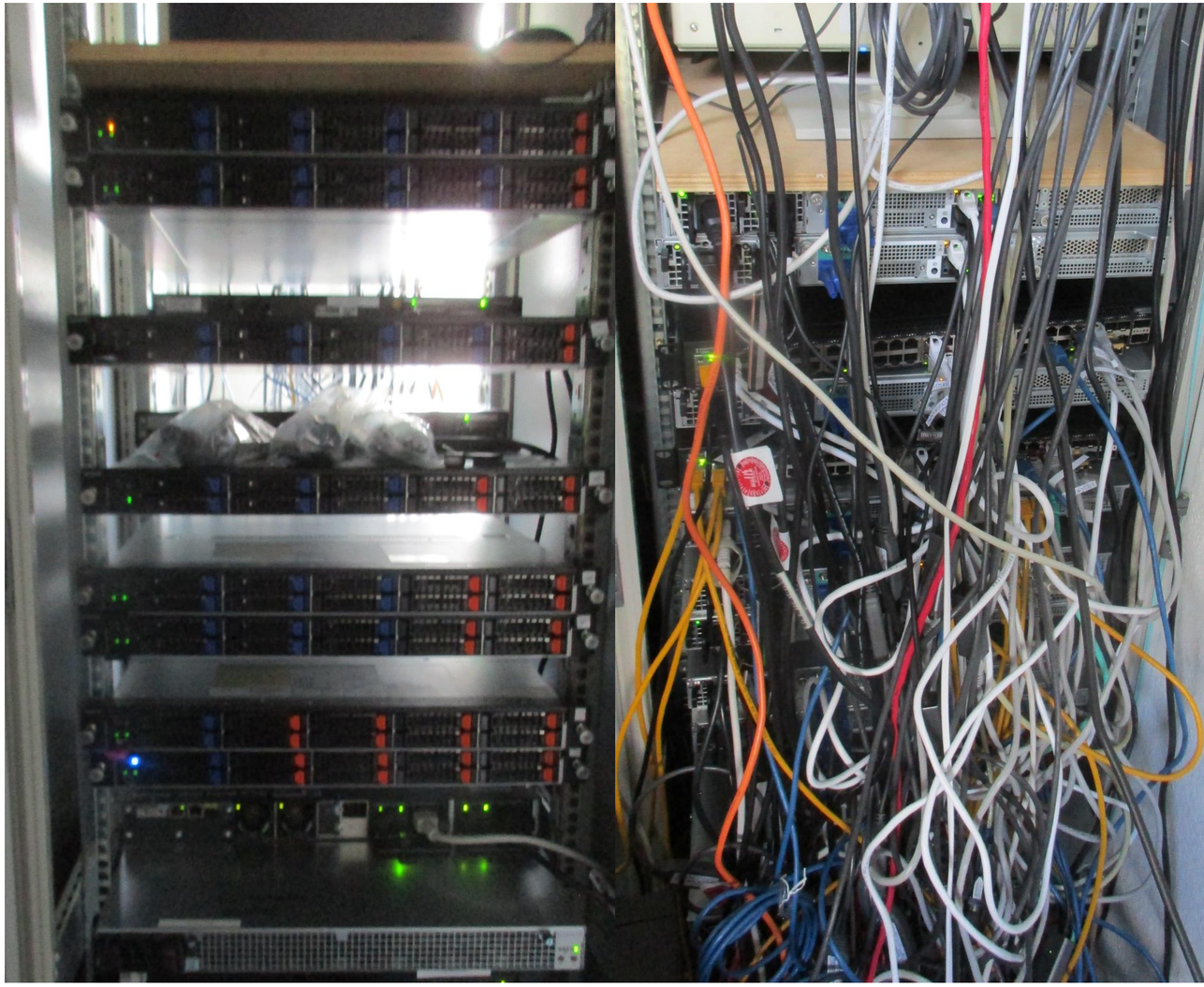
- Verschiedene Use-Cases:
  - Cloud-basierter Speicher für Dateien/Daten
  - Hosting für Webseiten mit Backend
  - Web/Server-Anwendungen (zum Beispiel Audio/Videokonferenz)
  - Datenbankspeicher
- Wichtigste Aspekte:
  - Sammeln und Weitergabe von Erfahrungen
  - Kontakt mit der Community
  - Erforschen von Ansätzen zur Bewertung der gewünschten Querschnittsziele
  - OpenBSD, FreeBSD, BISDN Linux, Debian Linux



# OpenSourceCloud

**Demonstrator für eine souveräne, privatssphären-schützende, IT-sichere, forensisch vorbereitete Cloud-Umgebung**

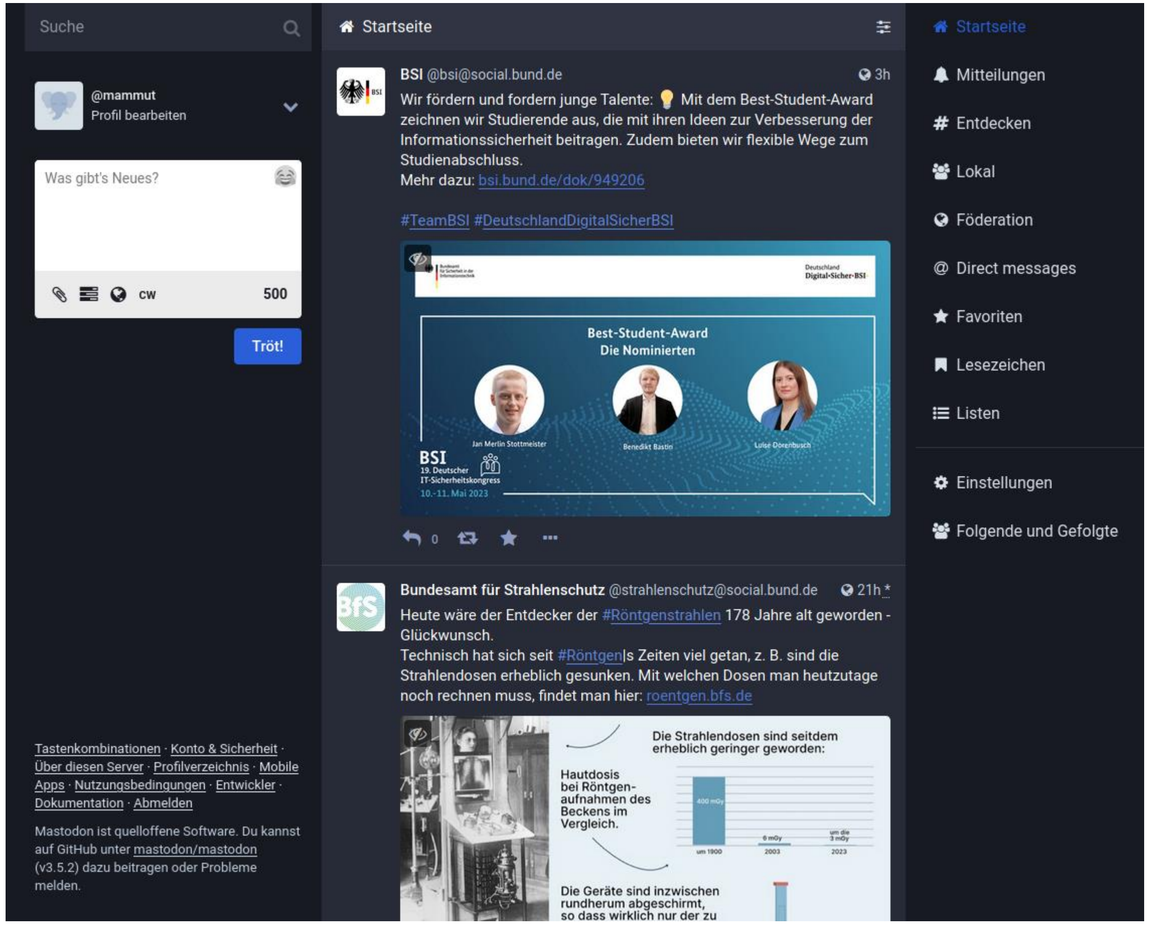
- Hardware:
  - 3 Cloud Nodes (ARM64)
  - 1 Storage Node (ARM64)
  - 1 Syslog Node (ARM64)
  - 3 Firewalls (ARM64)
  - 3 Switches
- Software:
  - OpenBSD, FreeBSD, BISDN Linux, Debian Linux
- Wissenschaftlicher Artikel: *Get it running - A sovereign Open Source and server environment in hard and software as a basic setup to enhance IT security, privacy and sustainability"- Stefan Kiltz, Robert Altschaffel, Jana Dittmann Otto-von-Guericke University Magdeburg, Magdeburg, Germany https://mediatum.ub.tum.de/1685828*



# Weitere Beispiele

**Demonstrator für eine souveräne, privatssphären-schützende, IT-sichere, forensisch vorbereitete Cloud-Umgebung**

- Kommunikationsplattformen (Matrix, Mastodon)
- Betriebssysteme und Systemumgebungen
- Integration und Anbindung verschiedener Dienste und Demonstratoren



# Fort-/Weiterbildungen und Vorträge

**Zu verschiedenen Querschnittszielen der digitalen Agenda**

- Sensibilisierung technischer Datenschutz/Datensicherheit
- Datensparsamkeit
- Digitale Souveränität
- Nachhaltigkeit
- Digitale Inklusion
- Unterschiedliche Formate: Vorträge, Workshops (mit praktischen Anteil)

# Digitalisierungsprojekte

**Wissenschaftliche Begleitung für die Sicherheit, Datensparsamkeit und Nachhaltigkeit von Digitalisierungsprojekten**

- Unterstützung bei Konzeption und Umsetzung
- Betrachtung des technischen Datenschutzes, Datensparsamkeit, der Datensicherheit und der Nachhaltigkeit
- Dafür wenn nötig auch forensische Untersuchung von Software und Hardware
- Stetiger Austausch mit verschiedenen Akteuren zur Stärkung der Community
- Auch Kontakt mit Softwareherstellern zur Klärung von Detailfragen oder für Verbesserungsvorschläge

**Open Source und Open Data Ansprechpartner**

- Open Source- und Open Data-Kooperationsraum in Kooperation mit MID Sachsen-Anhalt

Adresse: LSA-OpenSource-OpenData-Contact {at} iti.cs.uni-magdeburg.de

Betreff: [LSA-OpenSource-Contact]

# Fragen, Kontakte, F&E-Kooperationen, Fort-/Weiterbildung

CYBER | SEC
VERBUND LAND SACHSEN-ANHALT

www.cslsa.de

**Prof. Dr. H. Strack**

Hochschule Harz, FB AI, netlab
Tel: +49 3943 659 307
Mail: hstrack@hs-harz.de

http://netlab.hs-harz.de/research/

**Dr. S. Wefel**

Martin-Luther-Universität, Halle-Wittenberg
Institut für Informatik
Tel: +49 345 5524725
Mail: sandro.wefel@informatik.uni-halle.de

https://www.informatik.uni-halle.de/ti/

**Dr. R. Altschaffel**

Otto-von-Guericke-Universität
Fakultät für Informatik
Tel: +49 391 5756048
Mail: robert.altschaffel@iti.cs.uni-magdeburg.de

https://omen.cs.uni-magdeburg.de/itiamsl/home/index.html

# Literatur

[BSI19a] BSI (2019),Blockchain sicher gestalten - Konzepte, Anforderungen, Bewertungen, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf

[BSI19b] BSI (2019), Abschlussbericht Projekt 374 - Sicherheitsuntersuchung ausgewählter Blockchain-Anwendungen, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Studie-374.pdf

[BSI21] BSI (2021), Eckpunktepapier für Self-sovereign Identities (SSI) - unter besonderer Berücksichtigung der Distributed-Ledger-Technologie (DLT), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Eckpunkte_SSI_DLT.pdf

[ENISA19] ENISA (2019), Good Practices for Security of IoT - Secure Software Development Lifecycle, https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1/

[Hühn20], Hühnlein, Detlef; Hühnlein, Tina; Hornung, Gerrit; Strack, Hermann (2020): Towards Universal Login. In: Lecture Notes in Informatics (LNI) (Open Identity Summit 2020), S. 193–200. DOI: 10.18420/ois2020_18.

[Kar22], Karius, S., Knöchel, M. & Wefel, S., (2022). Datasets for Training and Validating Advanced Flow-Based Network Traffic Classifiers under Real-World Conditions. To be published in APCC 2022.

[Knö22], Knöchel, M., Karius, S. & Wefel, S., (2022). Analysing Attackers and Intrusions on a High-Interaction Honeypot System. To be published in APCC 2022.

[Knö21], Knöchel, M., Karius, S. & Wefel, S., (2021). Developing a Web-based Training Platform for IT Security Education. In: Kienle, A., Harrer, A., Haake, J. M. & Lingnau, A. (Hrsg.), DELFI 2021. Bonn: Gesellschaft für Informatik e.V.. (S. 223-228).

[Kusb21] Kusber, T.; Schwalm, S.; Korte, U.; Shamburger, K, (2021). Records Management and Long-Term Preservation of Evidence in DLT. In Roßnagel, H., Schunck, C. H. & Mödersheim, S. (Hrsg.), Open Identity Summit 2021. Bonn: Gesellschaft für Informatik e.V..

[PM Kol 22], Pressemitteilung Kolibri 2022, https://www.bechtle.com/ch/ueber-bechtle/news/unternehmensmeldungen/pressemeldungen/2022/konsortium-um-bechtle-praesentiert-prototyp-fuer-nationale-bildungsplattform

[Stra19a], Strack, Hermann (2019): eID/eIDAS-Anwendungen – grenzüberschreitende Sicherheit und Interoperabilität für Bürger, Hochschulen, Verwaltungen und Wirtschaft (EU). In: Jorge Marx Gómez, Andreas Solsbach, Thomas Klenke und Volker Wohlgemuth (Hg.): Smart Cities/Smart Regions – Technische, wirtschaftliche und gesellschaftliche Innovationen, Bd. 32. Wiesbaden: Springer Fachmedien Wiesbaden, S. 391–401.

[Stra19b], Strack, Hermann; Otto, Oliver; Klinner, Sebastian; Schmidt, André (2019): eIDAS eID & eSignature based Service Accounts at University environments for cross boarder/domain access. In: H. Roßnagel, S. Wagner und D. Hühnlein (Hg.): Proceedings of the Open Identity Summit 2019. Bonn, S. 171–176. Online verfügbar unter https://dl.gi.de/handle/20.500.12116/20986.

[Stra18], Strack, Hermann; Schmidt, André; Schmidsberger, Falk; Wefel, Sandro (2018): eIDAS based Applications at University Management. In: EUNIS 2018 Congress - Proceedings. Paris.

[Stra17], Strack, Hermann; Wefel, Sandro; Molitor, P.; Räckers, M.; Becker, J.; Dittmann, J. et al. (2017): eID & eIDAS at University Management - Chances and Changes for Security & legally Binding in cross boarder Digitalization. In: EUNIS 2017 – Shaping the Digital Future of Universities: European University Information Systems Organization (EUNIS), S. 133–141.

[Stra22a], Strack, H., Karius, S., Gollnick, M., Lips, M., Wefel, S. & Altschaffel, R., (2022). Preservation of (higher) Trustworthiness in IAM for distributed workflows and systems based on eIDAS. In: Roßnagel, H., Schunck, C. H. & Mödersheim, S. (Hrsg.), Open Identity Summit 2022. Bonn: Gesellschaft für Informatik e.V.. (S. 125-130).

[Stra22b], H. Strack, M. Gollnick, S. Karius, M. Lips, S. Wefel,R. Altschaffel, G. Bacharach, M. Gottlieb, H. Pongratz, W. Radenbach and A. Waßmann, (2022).Digitization of (Higher) Education Processes: Innovations, Security and Standards. In proceedings of EUNIS 2022 and EasyChair.

[Stra22c] Strack, H. (2022): Kontext Cybersecurity und Standards (wie eIDAS) im Bildungswesen. In: Herausforderungen und Lösungsansätze im Umgang mit elektronischen Identitätsnachweisen im Hochschulumfeld. Whitepaper. BigPicture-Initiative OZG Bildungswesen (NRW/ bundesweit), S. 28–51. Online verfügbar unter https://hss-opus.ub.ruhr-uni-bochum.de/opus4/frontdoor/index/index/docId/9318.

[Stra23] Strack, H.; Gollnick, M.; Karius, S.; Kopitz, R.; Wefel, S. (to be published in 2023): Multilevel Trustworthiness for improved Process and Network Security in Critical Infrastructures and Domains. In: proceedings of ICTA-EMoS, Springer Nature.