Sichere Digitalisierung der Strafjustiz:

Cyberresilienz als gemeinsame Aufgabe von Polizei, Justiz und IT

SPIK

16.03.2026 / Jens Piesbergen und Melchior Dörflinger

WAVESTONE

HIS SCHWEIZ
HIJP SUISSE
AIGP SVIZZERA
Kompetenzzentrum digitale Transformation in der Strafjustiz

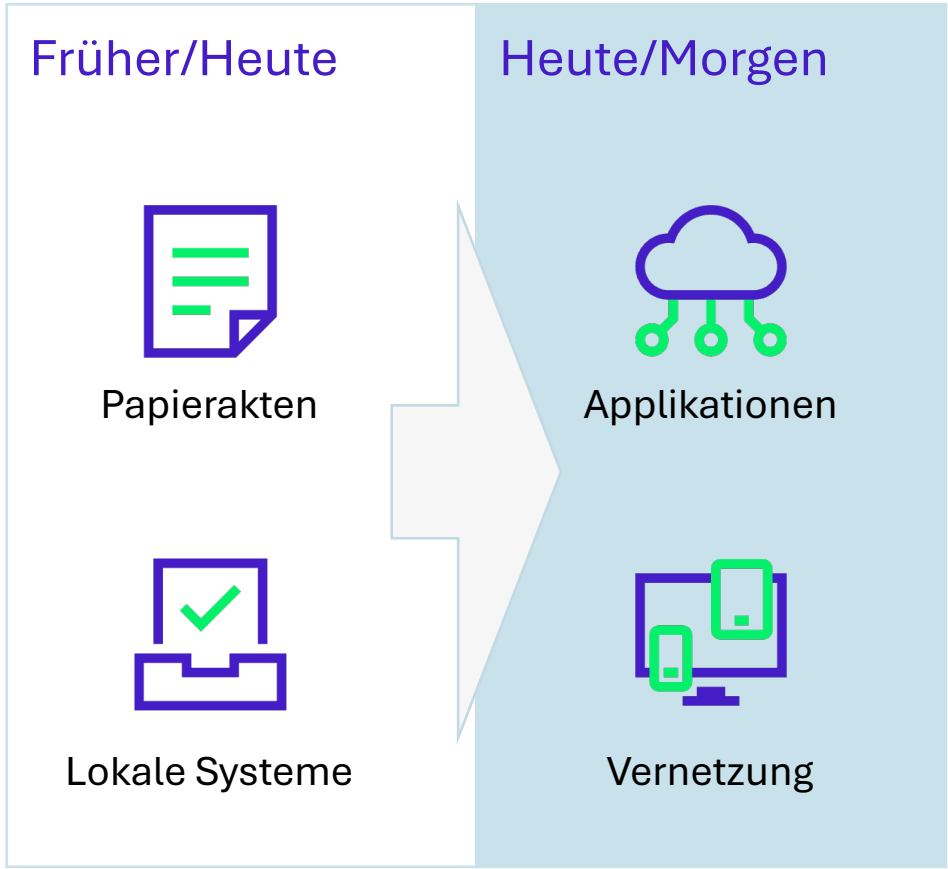
Ausgangslage – Digitale Transformation in der Strafjustiz

Akteure der Strafjustiz erleben eine strukturelle digitale Transformation (Effizienz, Datenqualität, Transparenz)

- **elektronische Akten** ersetzen Papierakten
- Fall- und Verfahrensführung durch **Fachanwendungen** und spezialisierten Analyse-Anwendungen
- **Austausch** von Daten, Dokumenten und Beweismittel **organisationsübergreifend**
- **standardisierte Schnittstellen** oder **Rechtsverkehrs-Plattformen** zwischen Polizei, Staatsanwaltschaften, Gerichten und Justizvollzugsorganen oder Registern

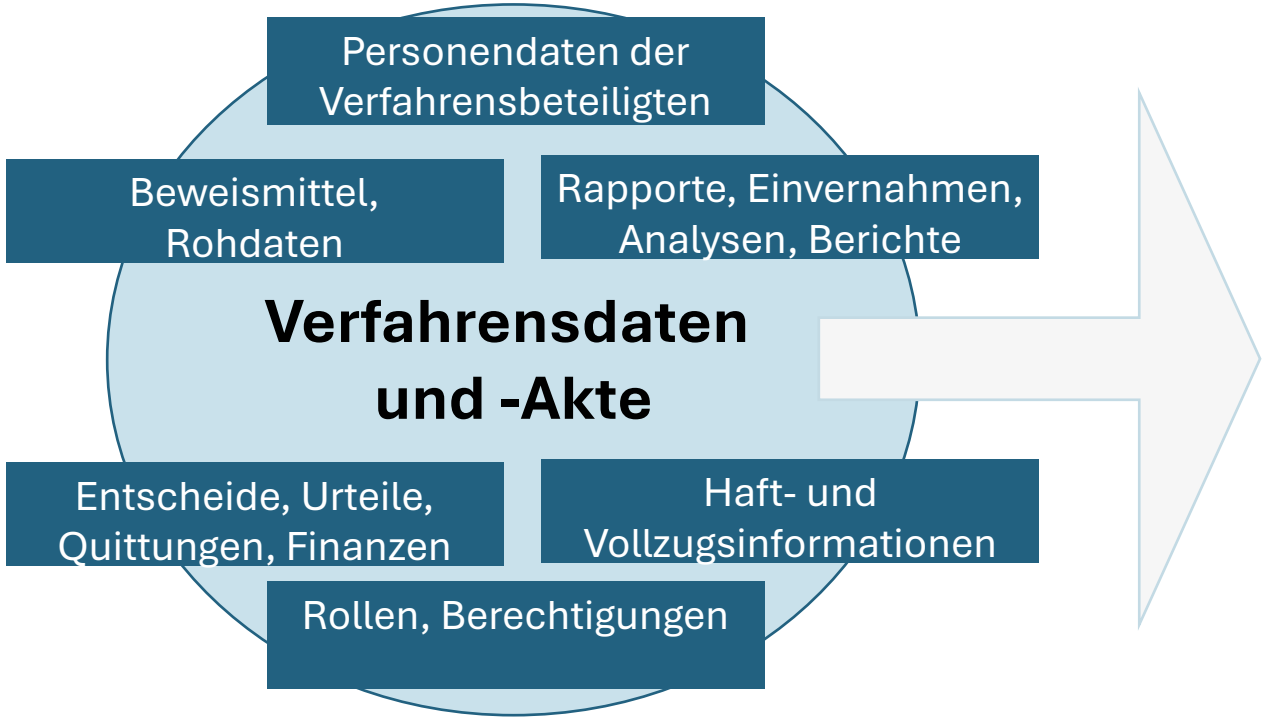
Vernetzung

- erweiterte, zentrale Abhängigkeit von **stabilen und vertrauenswürdigen** (Informatik-)Systemen



Schutzobjekte – Sensible Daten in der Strafjustiz

Welche Daten werden in Verfahren** digital verarbeitet?



- sensibel
- verfahrensrelevant
- potenziell manipulativ nutzbar
- attraktiv für Erpressung und Sabotage

**: Vorverfahren (Ermittlung/Untersuchung), Hauptverfahren, Vollzugsverfahren

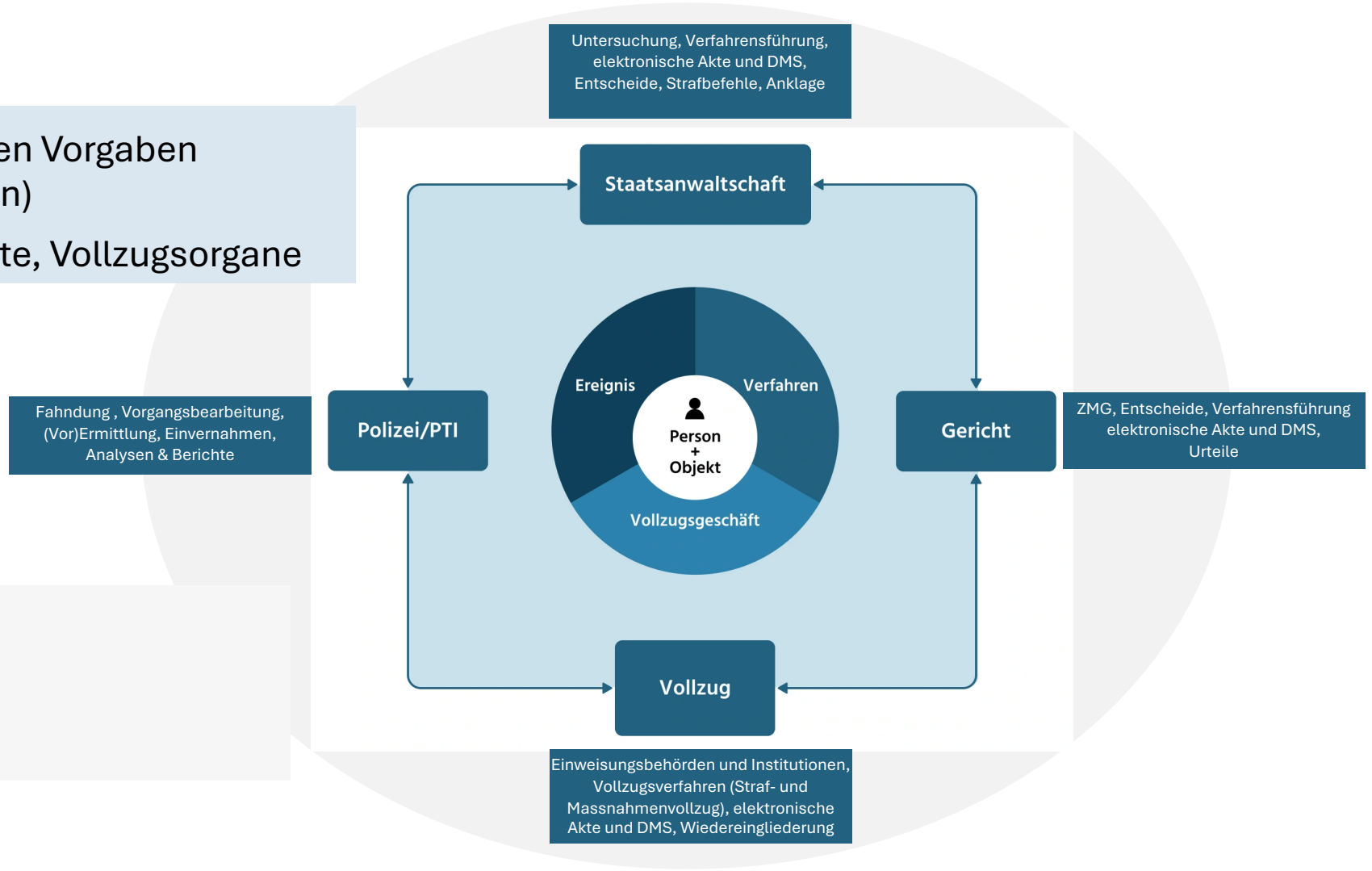
Strafjustizkette – Unterschiedliche Verantwortungsebenen

Fachverantwortung nach gesetzlichen Vorgaben (Verfahrensführung, Entscheide, Daten)

Polizei, Staatsanwaltschaften, Gerichte, Vollzugsorgane

Betriebsverantwortung
(Betrieb/Verfügbarkeit/Recovery)

IT-Provider (behörden-intern/extern)



Vernetzung – Veränderte Risikolage

Vernetzung schafft Effizienz – und neue systemische Risiken

Unterschiedliche Systeme

- diverse Fachanwendungen, Betriebsmodelle und Plattformen – heterogene IT-Landschaft

Operative Vernetzung

- systemübergreifende Datenflüsse erzeugen Abhängigkeiten und vergrössern Angriffsflächen

Gemeinsame Abhängigkeiten

- Ausfall eines Systems kann wichtige Teile der Strafjustizkette lahmlegen

Unterschiedliche Reifegrade

- kantonale Unterschiede in Sicherheitsstandards und IT-Ressourcen
- Bewusstsein auf Stufe Management

Lieferketten-Risiken

- externe Anbieter und Dienstleister als potenzielle Einfallstore (Supply Chain)
- eigener behördlicher Umgang mit Daten nicht konsequent

Datenschutz & Integrität

- sensible Daten über mehrere Systeme und Organisationen verteilt (Fachanwendungen)
- Meta- und Log-Daten

Bedrohungslage – Typische Angriffsformen

Ransomware

Verschlüsselung + Drohung zur Veröffentlichung (Doppelerpressung). Betriebsunterbrechung der gesamten Strafjustizkette möglich.

Phishing & Credential Theft

Gezielte Angriffe auf Mitarbeitende zur Übernahme privilegierter Zugänge. Häufigster Einstiegspunkt.

DDoS-Angriffe

Überlastung kritischer Dienste. Ziel: Störung staatlicher Institutionen, politische Wirkung.

Supply-Chain-Angriffe

Kompromittierung von Lieferanten oder Softwarekomponenten (vgl. Xplain 2023) – wirkt wie ein legitimer Zugang.

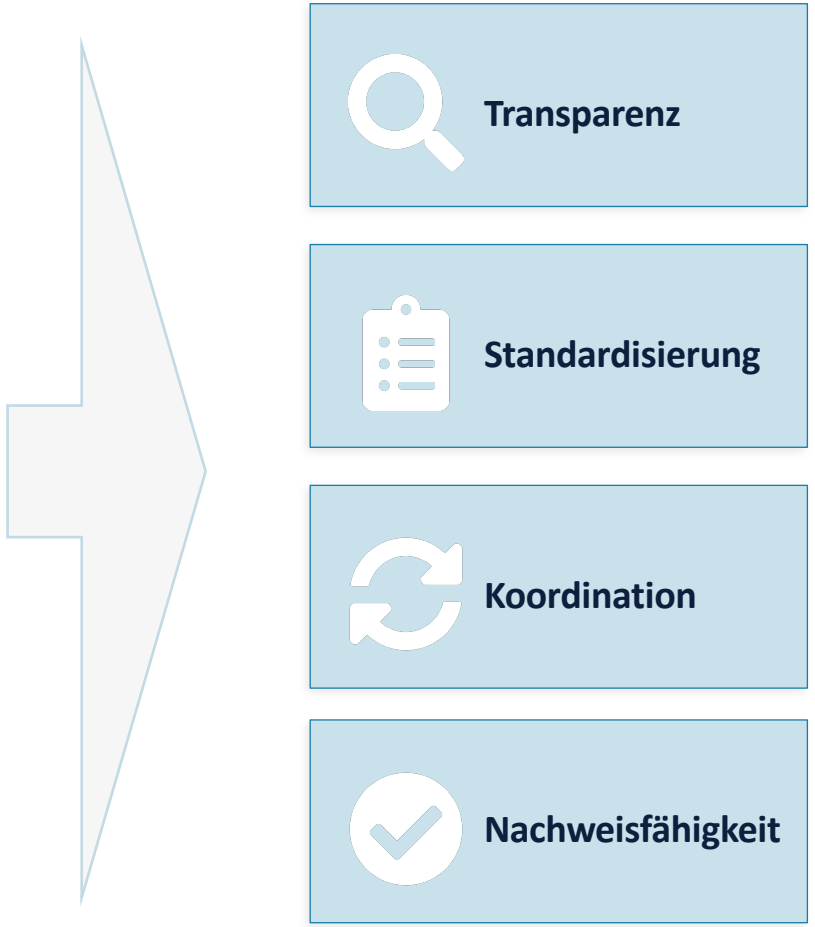
Schweizer Realität

Xplain (2023), Ransomware-Angriffe auf kantonale Verwaltungen (2023–2024), DDoS-Wellen gegen die Bundesverwaltung (2022–2024)

Sicherheitsmodell im Verbund mit verschiedenen Akteuren

Cybersecurity auf drei Ebenen

Wirkung: Reduktion der Risiken



Erlebter Cybervorfall 2025

ISJV: Eckwerte Informationssystem Justizvollzug

Zweck / Auftrag

Bereitstellung von Informationen und Dienstleistungen im Zusammenhang mit **Justizvollzugsdaten**

Ziele / Nutzen

- Vereinfachung von Prozessen
  - Datenlieferungen zu Statistikzwecken
  - Suche nach Personen
  - Suche nach Plätzen
- Erhöhung der Datenqualität durch Automatisierung
- Schaffung der rechtlichen Grundlage für den interkantonalen Umgang mit Personendaten

Dienstleistungen

- Tagesaktuelle Statistiken & Reports
- Suchservices

HIS HIJP AIGP

Erlebter Cybervorfall 2025 – Projektphase ISJV und Kanton GR

Datenlieferungen via Schnittstellen

- Fachanwendung im Kanton zu ISJV (@Bedag) und Bundesamt für Statistik
- eCH-0051 v2.11

Daten und UseCases

- statistische Daten: Zellenbelegung, Zellensuche
- schützenswerte Personendaten: Personensuche
- Produktiv- und anonymisierte Testdaten

Applikationen und IT-Infrastruktur

- Infrastruktur Fachanwendung in GR mit Produktiv- und Testsystem
- Ausfälle haben unmittelbare operative Auswirkungen auf UseCase-Ergebnisse

Integrations- und Testphase

- Mehrere Fachapplikationen verschiedener Anbieter müssen sicher integriert werden
- Kantonale Lieferseite: Unterscheidung Produktiv- vs. Testdaten
- Anwendung der vorhandenen Bordmittel (Lieferanten der Fachanwendungen)

Im Projekt berücksichtigt:

Schutzbedarfsanalyse
Systematische Bewertung des Schutzbedarfs aller verarbeiteten Informationen

ISDS-Konzept

Informationssicherheits- und Datenschutzkonzept als Pflichtbestandteil

Verantwortungszuordnung
Klare Regelung von Fach- und Betriebsverantwortung für jeden Teilbereich

Lieferantensicherheit
Vertragliche Sicherheitsanforderungen und wiederkehrende Überprüfung

Krisen- Notfallplanung

Notfall- und Wiederanlaufplanung und Krisen/-Notfallübungen

Kantonalen Datenschützer

Frühes Einbeziehen des kantonalen Datenschützers als Prüfinstanz

Schlussfolgerungen

01 Sichtbarkeit schaffen

Kennen Sie Ihre Systemlandschaft: Wer betreibt was, welche Daten fliessen wohin?

>>ohne Transparenz kein Schutz

02 Schutzbedarfsanalyse durchführen

Bewerten Sie systematisch, welche Daten und Systeme welchen Schutzbedarf haben

>>leiten Sie daraus Massnahmen ab

03 Verantwortlichkeiten klar regeln

Fach- und Betriebsverantwortung müssen eindeutig und vertraglich geregelt sein

>>auch mit externen Dienstleistern

04 Notfall gemeinsam planen

Entwickeln Sie Notfall- und Wiederanlaufpläne im Verbund. Ein Ausfall trifft alle

>>die Reaktion muss koordiniert sein

05 Sicherheit als Daueraufgabe

Cyber-Resilienz ist eine kontinuierliche organisatorische und technische Daueraufgabe

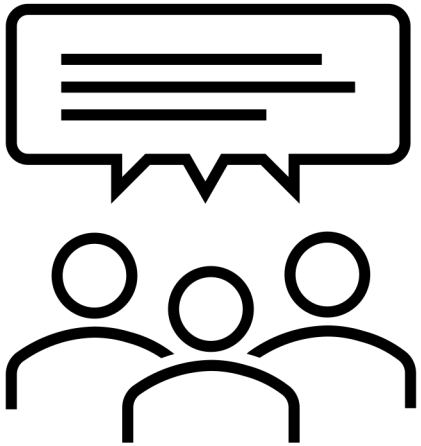
>> es ist kein Projekt, permanent

06 Standards nutzen & adaptieren

Orientieren Sie sich an Standards ISO-27001 oder NIST

>>passen Sie diese an Ihre föderale Realität an

Gerne beantworten wir Ihre Fragen...



Kontakte

Jens Piesbergen

Direktor HIS Schweiz

+41 79 473 87 56

jens.piesbergen@his-schweiz.ch

Melchior Dörflinger

Cyber Security Manager Wavestone & CISO HIS Schweiz

+41 76 467 22 41

melchior.doerflinger@his-schweiz.ch

melchior.doerflinger@wavestone.com

Newsletter

www.his-schweiz.ch

HIS Schweiz

Wavestone Kontakt

www.wavestone.com

WAVESTONE