Deutsche Stiftung für Recht und Informatik

KI-GETRIEBENE IT-SICHERHEITSLÖSUNGEN UND (DATENSCHUTZ-) RECHTLICHE HERAUSFORDERUNGEN

Florian Groothuis
ByteLaw Rechtsanwälte

Herbstakademie 2024

Übersicht

1. Hintergründe und Ablauf von Cyberangriffen

2. Systeme zur Angriffserkennung (SzA)
   a) Security Information and Event Management (SIEM)
   b) Endpoint Detection and Response (EDR)

3. SzA – Rechtsgrundlagen im Datenschutz
   a) Berechtigtes Interesse (lit. f)
   b) Erfüllung einer rechtlichen Verpflichtung - Art. 6 Abs. 1 S. 1 lit. c DSGVO i.V.m. (…)
   c) Exkurs: Risikomanagementmaßnahme

4. Regulierung von SzA in der KI-Verordnung

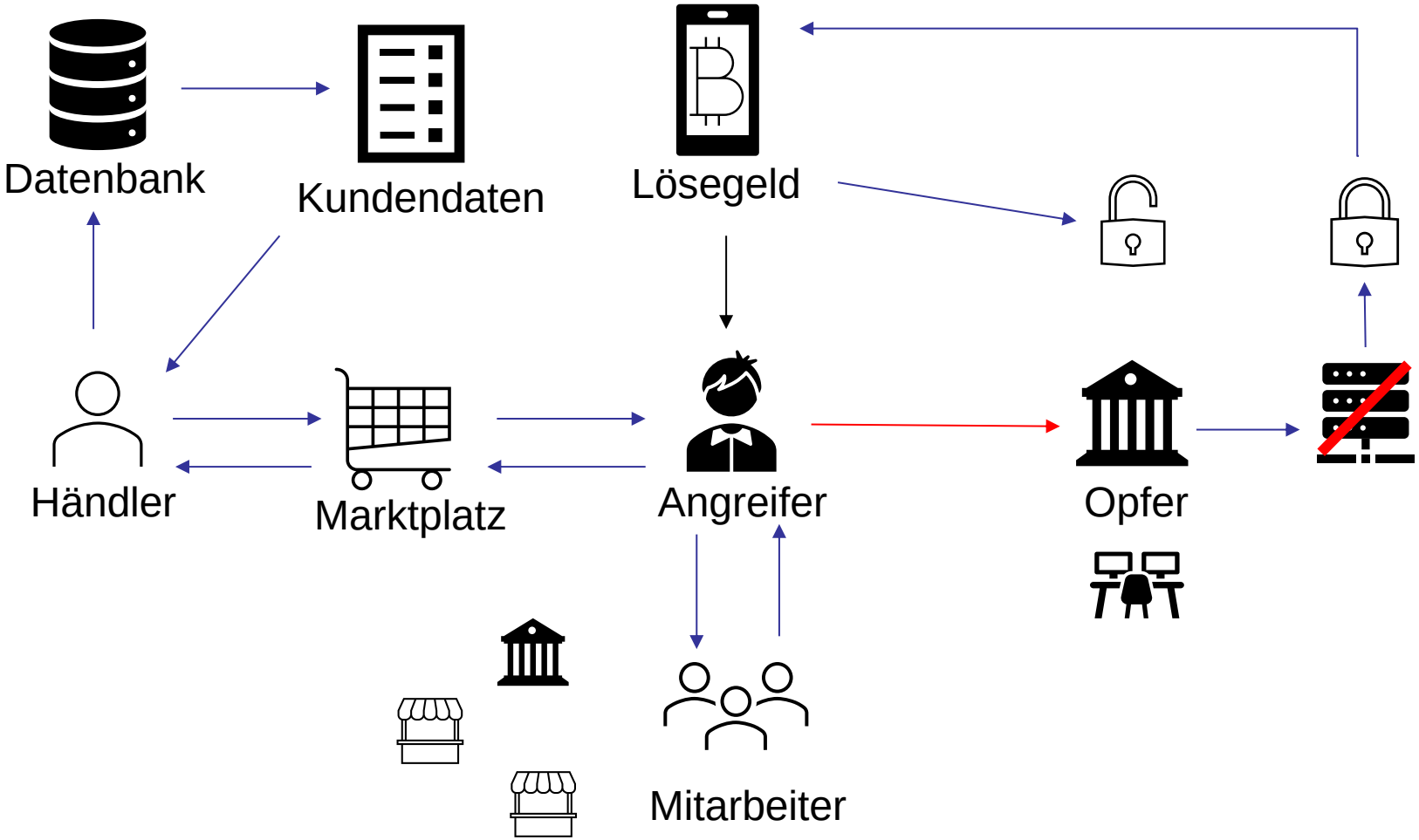
1. Hintergründe und Ablauf von Cyberangriffen

- Irrglaube: „*Mein Unternehmen ist nicht attraktiv genug für Cyberangriffe*!“
  - Keine oder wenig Ausgaben für IT-Sicherheit

- Realität: Zufällige Angriffe sind die Regel und gezielte die Ausnahme

- Kosteneffizienter Einsatz von Mitteln bei Cyberkriminellen
  - Auswurf digitales Fischernetz zur Schwachstellensuche
  - Künftiges Angriffsobjekt (z.B. Krankenhaus, Restaurant, Konzernunternehmen) zunächst unbekannt

1. Hintergründe und Ablauf von Cyberangriffen

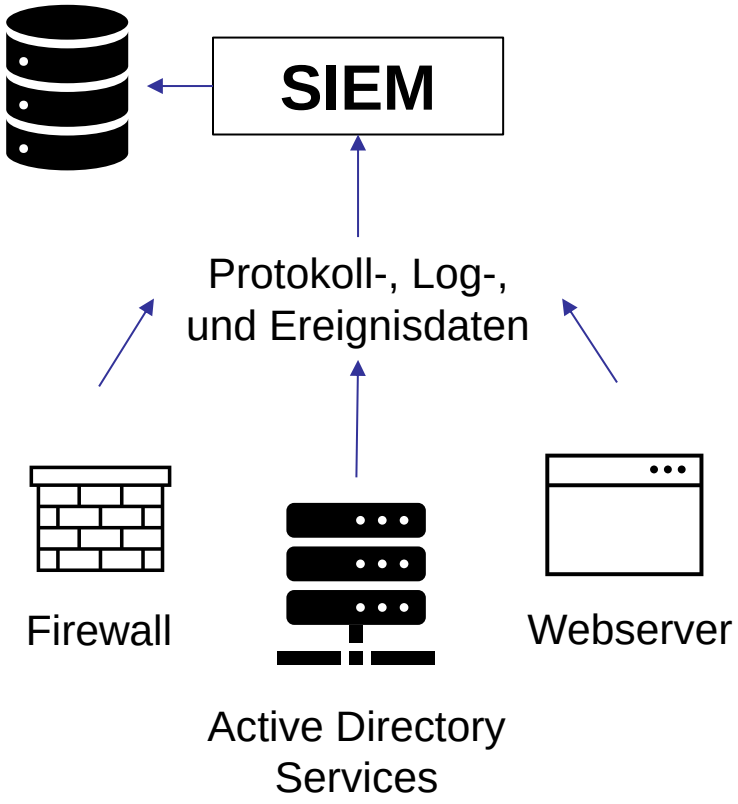


2. Systeme zur Angriffserkennung (SzA)

- SzA
  - SIEM
  - EDR
- Funktionen
  - Protokollierung
  - Detektion
  - Reaktion

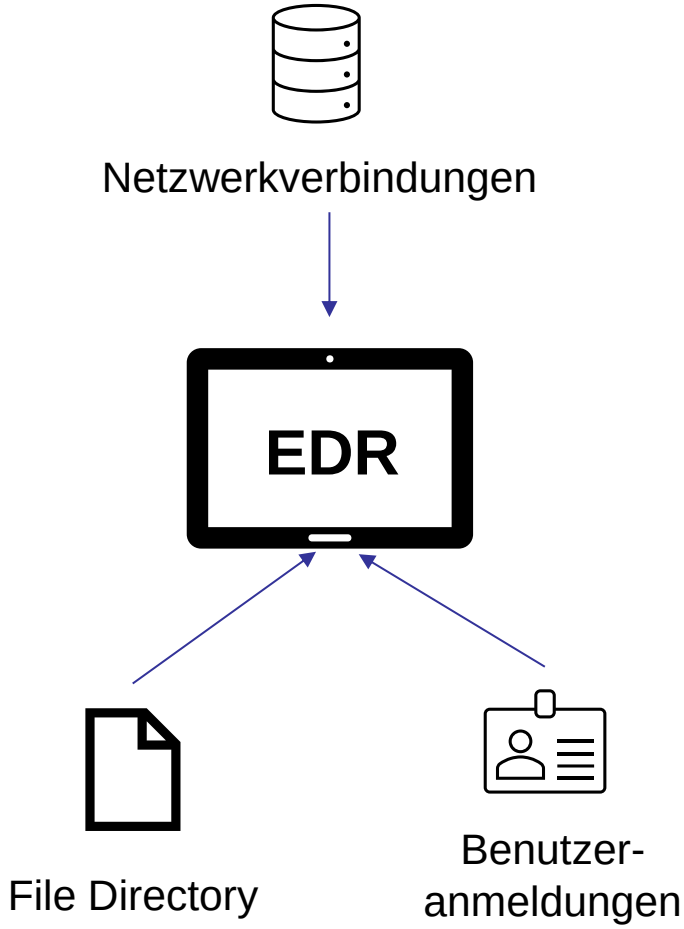
a) Security Information and Event Management (SIEM)

- Sammlung von Daten aus verschiedenen Quellen
- Nominalisierung und Aggregation der Daten
- Analyse von Korrelationen und Erkennung von Bedrohungen
- Versenden eines Alarms und Erstellen von Berichten
- **Vordefinierte Regeln und Muster**



b) Endpont Detection and Response (EDR)

- Sammlung endpunktspezifischer Telemetriedaten
- KI-basierte Erkennung atypischen Verhaltens
- Automatisiertes Ergreifen von Gegenmaßnahmen
- Versenden eines Alarms und Erstellen von Berichten



3. SzA - Rechtsgrundlagen im Datenschutz

- Personenbezug von Protokoll-, Ereignis- und Logdaten

- Rechtsgrundlagen – Art. 6 Abs. 1 S. 1 DSGVO
  - Einwilligung
  - Vertragsdurchführung
  - Erfüllung einer rechtlichen Verpflichtung
  - Schutz lebenswichtiger Interessen
  - Wahrnehmung einer öffentlichen Aufgabe
  - Interessenabwägung

a) Berechtigtes Interesse (lit. f)

- Drei-Stufen-Prüfung
  - Berechtigtes Interesse
  - Erforderlichkeit
  - Kein überwiegendes Interesse des Betroffenen

- **P:** Widerspruchsmöglichkeit
  - Praktikabilität von SIEM und EDR?
  - Grenzen des Widerspruchs

b) Erfüllung einer rechtlichen Verpflichtung - Art. 6 Abs. 1 S. 1 lit. c DSGVO i.V.m. (…)

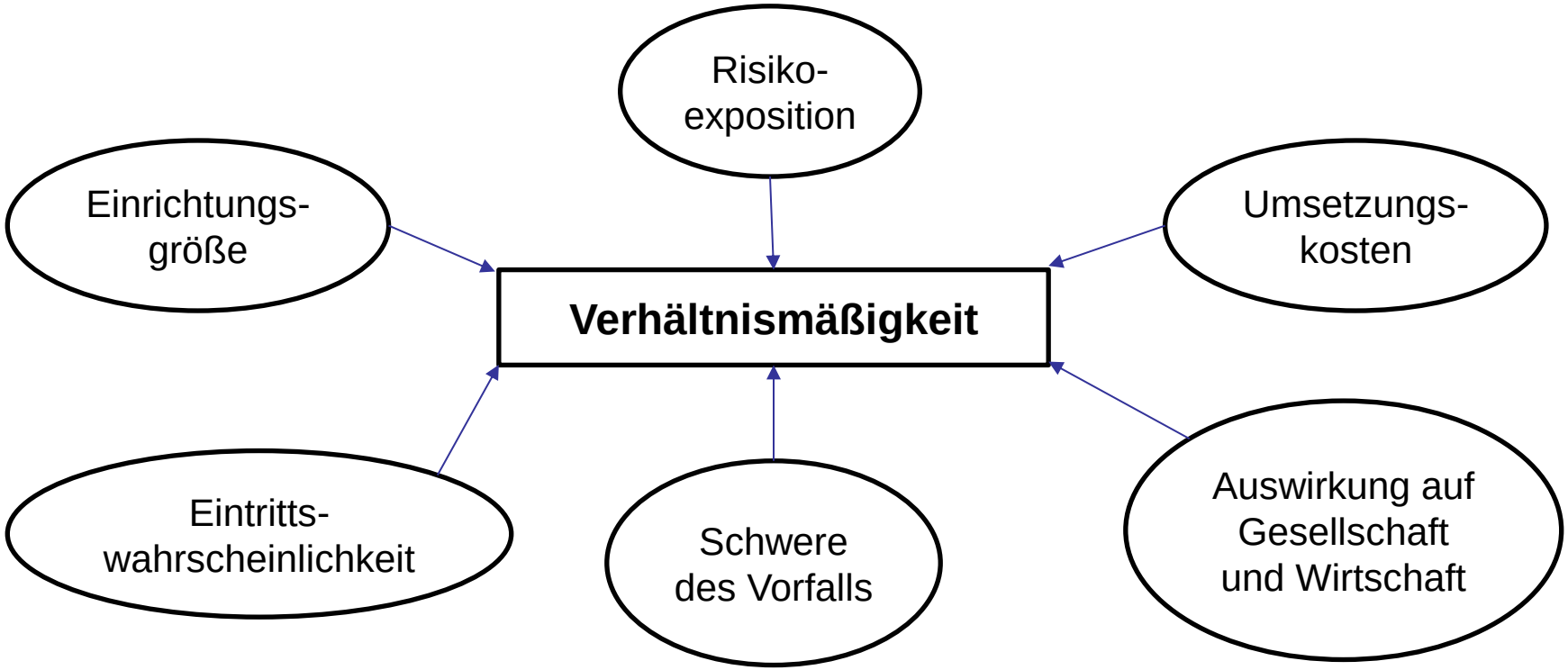
- § 8a Abs. 1a BSIG bzw. § 31 Abs. 2 S. 1 BSIG(E)
  - Einsatz von SzA für Betreiber kritischer Anlagen
  - Pflicht zur Erfassung und Auswertung der "*in einem informationstechnischen System verarbeiteten Daten*"

- Art. 4 Abs. 1 DORA
  - Finanzunternehmen
  - IKT-Risikomanagementmaßnahmen

- § 30 Abs. 1 BSIG(E)
  - Wichtige und besonders wichtige Einrichtungen
  - Risikomanagementmaßnahmen

c) Exkurs: Risikomanagementmaßnahme

- Vermeidung von Störungen der IT-Systeme und Minimierung von Auswirkungen von Sicherheitsvorfällen



4. Regulierung von SzA in der KI-Verordnung

- SzA als KI-System
  - Maschinengestütztes System und autonomer Betrieb
  - Anpassungsfähigkeit
  - Ableitung von Zielen
  - Beeinflussung der Umgebung

- Hochrisiko-KI
  - Störung oder Ausfall führt zu erheblicher Beeinträchtigung von Gesundheit und Sicherheit
  - Betreiber kritischer Anlagen

- Pflichten, u.a.
  - Informationspflicht ggü. Mitarbeitern
  - Bereitstellung menschlicher Aufsicht

KI und Daten: Digitalregulierung auf dem Höhepunkt?

Vielen Dank für Ihre Aufmerksamkeit!