Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 3. Übung im SoSe 2025:

KI und Datenschutz

3.1 Handlungsbedarf zu KI

Aufgabe:

- Leiten Sie aus den vier **ethischen Grundsätzen** aus der EU-Leitlinie für eine vertrauenswürdige KI als auch aus der KI-VO **handlungsrelevante Vorgaben** für die **Gestaltung eines** (Nicht-Hochrisiko-)**KI-Systems** ab!

3.1 Handlungsbedarf zu KI (1)

Handlungsbedarf aus ethischen Grundsätzen:

- Menschliche Autonomie: Durchsetzbarkeit Betroffenenrechte gewährleisten; Optionalität für Validierung mit Trainingsdaten
- Schadensverhütung: Vermeidung von Bias in Trainings- und Validierungsdaten; Haftung für Folgen KI-Einsatz auf Betroffene
- Fairness: Keine automatisierte Einzelfallentscheidung mit KI; Speicherung auf EU-Boden oder via Standardklauseln
- Erklärbarkeit: Pflicht zur unabhängigen Überprüfung KI-System; Informationspflicht über Zweckbestimmung & ordnungsgemäße Verwendung des KI-Systems

3.1 Handlungsbedarf zu KI (2)

Handlungsbedarf aus KI-VO:

- Art. 3 Nr. 15: Erstellung einer Betriebsanleitung mit Informationen zur Zweckbestimmung & ordnungsgemäßen Verwendung des KI-Systems
- Art. 3 Nr. 49: Bewertung, ob schwerwiegender Vorfall oder Fehlfunktion des KI-Systems vorliegt (z.B. durch schwere Störung des Betriebs kritischer Infrastrukturen oder der Verletzung des Schutzes der Grundrechte)
- Art. 5 Abs. 1 lit. a: KI-System darf keine Techniken aufweisen zur unterschwelligen Beeinflussung oder zur absichtlich manipulativen bzw. täuschenden Veränderung des Verhaltens
- Art. 5 Abs. 1 lit. c: KI-System nicht einsetzbar zur Bewertung oder Einstufung von Personen aufgrund sozialen Verhaltens oder Persönlichkeitsmerkmale, aus der deren Schlechterstellung bzw. Benachteiligung führen kann
- Art. 5 Abs. 1 lit. e: KI-System mit Datenbanken zur Gesichtserkennung durch ungezieltes Auslesen von Gesichtsbildern aus Internet oder Überwachung
- Art. 5 Abs. 1 lit. g: KI-System nicht zur biometrischen Kategorisierung anhand besonderer Kategorien personenbezogener Daten

3.1 Handlungsbedarf zu KI (3)

Handlungsbedarf aus KI-VO:

- Art. 50 Abs. 1: KI-System, das direkt mit natürlichen Personen interagieren soll, muss diese Personen darüber informieren, dass sie mit einem KI-System interagieren
- Art. 50 Abs. 2: KI-System, das synthetische Audio-, Bild-, Video- oder Textinhalte erzeugt, muss Ergebnisse als künstlich erzeugt bzw. manipuliert kennzeichnen
- Art. 50 Abs. 4: KI-System, das Deepfake mit Bild-, Ton- oder Videoinhalten erzeugt bzw. manipuliert, muss offenlegen, dass Inhalte künstlich erzeugt bzw. manipuliert worden sind
- Art. 50 Abs. 5: Informationspflichten sind bei der ersten Interaktion bereitzustellen

3.2 Zulässigkeit KI @ EU-DSGVO

Aufgabe:

- Welche Vorschriften aus der EU-DSGVO würden derzeit bei der **Zulässigkeitsprüfung von KI-Systemen** mit welchem Ergebnis herangezogen werden?

3.2 Zulässigkeit KI @ EU-DSGVO (1)

- Art. 5 Abs. 1 lit. a EU-DSGVO: Verarbeitung nach Treu und Glauben setzt voraus, dass der Betroffene abschätzen kann, was mit seinen Eingaben sowie Ergebnissen gemacht wird
  → setzt eine entsprechende Datenschutzerklärung (im Rahmen der Nutzungsregeln) voraus
- Art. 5 Abs. 1 lit. b EU-DSGVO: Zweckbindung setzt voraus, dass Weiterverarbeitung personenbezogener Daten (gemäß Art. 6 Abs. 4 EU-DSGVO) mit ursprünglichem Zweck vereinbar sein muss
  → Entweder Ausfilterung personenbezogener Daten aus Trainings-daten oder Nichteinspeisung eingegebener Daten mit Personenbezug in die Verarbeitungslogik (nach Art. 11 Abs. 2 EU-DSGVO)
- Art. 5 Abs. 1 lit. d EU-DSGVO: Richtigkeit der Daten setzt voraus, dass unrichtige Daten berichtigt werden (nach Art. 16 EU-DSGVO) bzw. keine Daten zur Person durch KI-System erfunden werden
  → Prüfen, ob Einsatzzweck des KI-Systems entsprechend beschränkt werden kann oder generell keine Daten über Personen vom KI-System ausgegeben werden

3.2 Zulässigkeit KI @ EU-DSGVO (2)

- Art. 5 Abs. 1 lit. e EU-DSGVO: Speicherbegrenzung personenbezogener Daten setzt voraus, dass Daten mit Personenbezug nicht dauerhaft als Trainings- bzw. Validierungsdaten gespeichert werden
  → Entweder Ausfilterung personenbezogener Daten aus Trainingsdaten oder Nichteinspeisung eingegebener Daten mit Personenbezug in die Verarbeitungslogik
- Art. 5 Abs. 2 EU-DSGVO: Rechenschaftspflicht setzt voraus, dass Rechtmäßigkeit der Verarbeitung durch KI-System nachgewiesen werden kann
  → Selbstverpflichtung des Anbieters des KI-Systems, flankiert durch entsprechend aussagekräftiger Datenschutzerklärung in Nutzungsbedingungen
- Art. 12 Abs. 1 EU-DSGVO: Transparenz über mit KI-System verbundene Verarbeitung durch Datenschutzerklärung
  → setzt eine entsprechende Datenschutzerklärung (im Rahmen der Nutzungsregeln) voraus

3.2 Zulässigkeit KI @ EU-DSGVO (3)

- Art. 15 Abs. 1 EU-DSGVO: Auskunftsrecht für personenbezogene Daten in Trainings- bzw. Validierungsdaten ggf. schwierig umsetzbar → Entweder Ausfilterung personenbezogener Daten aus Trainings-daten oder Nichteinspeisung eingegebener Daten mit Personenbezug in die Verarbeitungslogik (nach Art. 11 Abs. 2 EU-DSGVO)
- Art. 17 Abs. 1 EU-DSGVO: Löschungspflicht für personenbezogene Daten in Trainings- bzw. Validierungsdaten ggf. schwierig umsetzbar → Entweder Ausfilterung personenbezogener Daten aus Trainings-daten oder Nichteinspeisung eingegebener Daten mit Personenbezug in die Verarbeitungslogik (nach Art. 11 Abs. 2 EU-DSGVO)
- Art. 21 Abs. 1 EU-DSGVO: Widerspruchsrecht bezieht sich aktuell nur auf Verarbeitungen auf Basis von Art. 6 Abs. 1 lit. e oder f EU-DSGVO

3.2 Zulässigkeit KI @ EU-DSGVO (4)

- Art. 22 Abs. 1 EU-DSGVO: Ausschluss automatisierter Einzelentscheidung setzt Kenntnis über Einsatz von KI mit Personenbezug voraus, um überhaupt eigenen Standpunkt einbringen zu können
  → Prüfen, ob Einsatzzweck des KI-Systems entsprechend beschränkt werden kann oder generell keine Daten über Personen vom KI-System ausgegeben werden
- Art. 25 EU-DSGVO: Datenschutz durch Technikgestaltung als auch Datenschutzfreundliche Voreinstellung setzt voraus, dass KI-System zwischen personenbezogenen und anderen Daten überhaupt unterscheiden kann
  → Prüfen, ob Einsatzzweck des KI-Systems entsprechend beschränkt werden kann oder generell keine Daten über Personen vom KI-System ausgegeben werden
- Art. 32 EU-DSGVO: Sicherheit der Verarbeitung setzt umfassenden Schutz personenbezogener Daten voraus
  → Manipulationsschutz (insbesondere vor ungewolltem Bias) und Robustheit des KI-Systems nötig

3.2 Zulässigkeit KI @ EU-DSGVO (5)

- Art. 35 Abs. 1 EU-DSGVO: Datenschutz-Folgenabschätzung für Einsatz eines KI-Systems nötig, da zahlreiche Folgen für die Rechte und Freiheiten der Betroffenen möglich sind
  → Selbsterklärung des Herstellers und Durchführung der Folgenabschätzung durch Verantwortlichen, der das KI-System einsetzt mit entsprechender Ableitung benötigter technischer und organisatorischer Maßnahmen zum Schutz vor ungewollten Folgen
- Art. 44 EU-DSGVO: Datenübermittlung in Drittland nur, wenn geeignete Garantien vorliegen
  → KI-System entweder gezielt auf EU-Boden einsetzen, Speicherung personenbezogener Daten im KI-System vermeiden oder Betreiber für KI-System einsetzen, der sich gemäß Standardklauseln verpflichtet hat

Generelles Ergebnis: Einsatz KI-System an sich ist nach bestehenden Vorgaben aus EU-DSGVO möglich, jedoch gibt es einige Lücken, die durch Folgenabschätzung abzumildern sind!

3.3 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung I

Aufgabe:

- Für ein **KI-System** wurde Folgendes geplant:
  - Das KI-System speichert neben der Cookie-ID alle vom Nutzer eingegebenen personenbezogenen Daten zu den gestellten Aufgaben hinzu, um künftige Anfragen vom gleichen Nutzer personalisieren zu können (z.B. durch persönliche Ansprache).
  - Anhand der Themen gestellter Fragen, wird für den Nutzer eine geeignete Werbung auf der Webseite eingebunden, auf der das KI-System genutzt werden kann.
  - Als Trainingsdaten für das KI-System wurden Daten verwendet, die von den Systemerstellern anhand geplanter Einsatzzwecke im Hinblick auf Funktionalität erstellt worden sind.
  - Antworten des KI-Systems werden von dem Nutzer ob ihrer Nützlichkeit bewertet und diese Bewertung fließt als zusätzliche Trainingsdaten ein.
  - Das KI-System soll als Public Cloud implementiert werden, damit es weltweit und jederzeit genutzt werden kann.

3.3 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung II

Aufgabe: (Fortsetzung)

- Geben Sie an, welche potenziellen Datenschutzrisiken Sie im Rahmen einer **Datenschutz-Folgenabschätzung** (gem. Art. 35 EU-DSGVO) sehen (unter Berücksichtigung der Bußgeldbestimmungen und Meldepflichten bei Verletzungen des Schutzes personenbezogener Daten), schätzen Sie die Eintrittsstufe dieser Datenschutzrisiken ab und ermitteln Sie den Handlungsbedarf gemäß nächstehender 3x3-**Risk-Map**. Sofern Handlungsbedarf besteht, geben Sie eine passende, zu ergreifende Schutzmaßnahme an.

3.3 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (1)

1) Ermittlung potenzieller Datenschutzrisiken:

- Speicherung eingegebener personenbezogener Daten
  1. Verknüpfung der Daten mit nicht vereinbaren Zwecken → Gefahr: Verstoß gegen Art. 6 Abs. 4 EU-DSGVO möglich (→ Bußgeld nach Art. 83 Abs. 5 lit. a EU-DSGVO)
- Werbung abhängig von Eingabedaten
  2. Verwendung der Daten nicht transparent für Nutzer → Gefahr: Verstoß gegen Art. 5 Abs. 1 lit. a EU-DSGVO möglich, da unerwartet für Nutzer (→ Bußgeld nach Art. 83 Abs. 5 lit. a EU-DSGVO)
- Trainingsdaten nur rein funktional basiert
  3. Trainingsdaten können Bias aufweisen und infolge dessen Betroffene unerwartet benachteiligen → Gefahr: automatisierte Einzelentscheidung ohne Gewährleistung der Betroffenenrechte (→ Bußgeld nach Art. 83 Abs. 5 lit. b EU-DSGVO)
- Nutzer-Rückmeldung zur Ergebnisvalidierung
  4. Validierungsdaten können Bias aufweisen und damit analog 3. wirken → Gefahr: Intransparenz über Verarbeitung (→ analog Nr. 3)

3.3 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (2)

1) Ermittlung potenzieller Datenschutzrisiken: (Fortsetzung)

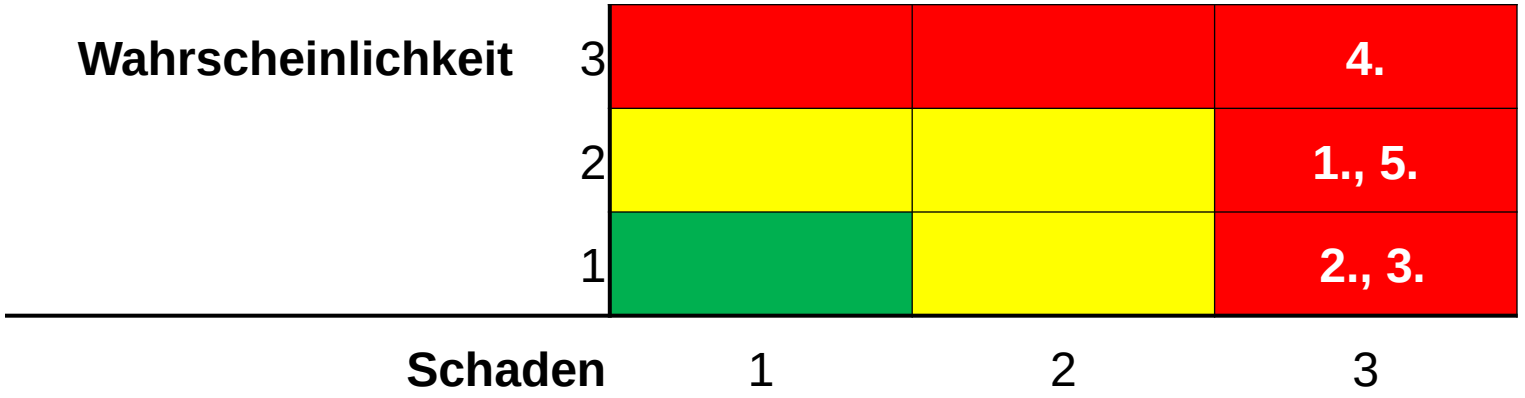
- KI-System als Public Cloud implementiert
  5. Daten und ggf. KI-Systemlogik ggf. unzureichend geschützt → Gefahr: Unbefugte Offenlegung ggf. möglich (Art. 32 Abs. 2 EU-DSGVO → Bußgeld nach Art. 83 Abs. 4 lit. a EU-DSGVO)

3.3 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (3)

2) Abschätzung der Eintrittsstufe:

1. Verknüpfung der Daten mit nicht vereinbaren Zwecken: Gefahreintritt wahrscheinlich, da Personalisierung laut Aufgabenstellung zu unspezifisch erfolgt
2. Verwendung der Daten nicht transparent für Nutzer: Gefahreintritt möglich, da zwar i.d.R. für Nutzer nicht störend, doch ist potenziell damit eine Weitergabe personenbezogener Daten an Werbetreibende verbunden
3. Trainingsdaten können Bias aufweisen und infolge dessen Betroffene unerwartet benachteiligen: Gefahreintritt möglich, da Funktionalität oftmals nicht alle relevanten potenziellen Folgen berücksichtigt
4. Validierungsdaten können Bias aufweisen: Gefahreintritt sicher, da Nützlichkeit der Antwort i.d.R. nicht frei von Interessen bzw. Benachteiligung begünstigende Umstände ist (z.B. infolge Spieltrieb der Nutzer, Aktivitäten von „Trollen“ und durch Crime as a Service…)
5. Daten und ggf. KI-Systemlogik ggf. unzureichend geschützt: Gefahreintritt wahrscheinlich, da i.d.R. preisgünstig aufgrund geringerer Schutzvorkehrungen

3.3 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (4)



Rot = Aktivität nötig; **Gelb** = Aktivität prüfen; **Grün** = Akzeptabel

Wahrscheinlichkeit: **Eintritt einer Verletzung des Schutzes personenbezogener Daten**	**Schaden:** **Grad der Verletzung des Schutzes personenbezogener Daten**
1 = möglich	1 = niedrig (ohne unmittelbare Wirkung)
2 = wahrscheinlich	2 = mittel (formaler Verstoß)
3 = sicher	3 = hoch (Bußgeld/Meldepflicht)

3.3 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (5)

3) Handlungsempfehlung:

1. Bereitstellung einer entsprechend erläuternden Datenschutzerklärung und Einrichtung einer optionalen Funktion, ob Verknüpfung gewünscht wird
2. Bereitstellung einer entsprechend erläuternden Datenschutzerklärung
3. Aussagekräftige Beschreibung der geplanten Einsatzzwecke in Nutzungsbedingungen und Selbsterklärung des Herstellers über durchgeführte Folgenabschätzung
4. Temporäre Speicherung von Validierungsdaten mit Option, ob diese eingespeist werden sollen und unabhängige Überprüfung, ob KI-System menschenwürde-beeinträchtigenden Bias aufweist
5. Ausreichend sichere Cloud verwenden mit ausreichenden Nachweisen oder On-Premise-Lösung anbieten

3.3 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (6)

Anmerkung:

- *Die Angabe der Punkte aus Art. 35 Abs. 7 EU-DSGVO ist bei der Durchführung von Datenschutz-Folgenabschätzungen verpflichtend*
  ° auf systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, ggf. einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen
  in der Aufgabe jedoch verzichtet, da nach Aufgabenstellung nicht zwingend verlangt

3.4 Technischer Schutz KI-System

Aufgabe:

- Welche **technischen Maßnahmen** sollten für ein **KI-System** zum maschinellen Lernen implementiert werden (sowohl bei dessen Entwicklung als auch beim Betrieb), damit es widerstandsfähig gegenüber Fehlern, Störungen oder Unstimmigkeiten (inkl. aus Rückkopplungsschleifen) ist?

3.4 Technischer Schutz KI-System (1)

Vorbemerkung:

- *Hilfreiche Quellen zur Bestimmung technischer Schutzvorkehrungen sind:*
  BSI: Große KI-Sprachmodelle – Chancen und Risiken für Industrie und Behörden (Stand 03.05.2023), abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Grosse_KI_Sprachmodelle.pdf?__blob=publicationFile&v=2
  NSA/FBI/ACSC/NCSC-UK/CCCS/BSI/NCSC-NL/CERT NZ/NCSC-NZ: Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and –Default (Stand 13.04.2023), abrufbar unter https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf
- *In der KI-Verordnung der EU werden sog. „Hochrisiko-KI-Systeme" mit besonderen Schutzvorkehrungen bedacht: u.a. wird dort ein Risikomanagement hinsichtlich Folgen auf Gesundheit, Sicherheit und Grundrechte vorgeschrieben, eine Beaufsichtigung durch natürliche Personen sowie Maßnahmen zur Genauigkeit, Robustheit und Cybersicherheit und für Rückkopplungsschleifen im Betrieb Risikominderungsmaßnahmen eingefordert, die Festlegung einer Gebrauchsanweisung und die Einholung einer unabhängigen Konformitätsbewertung vorgeschrieben*

3.4 Technischer Schutz KI-System (2)

- Für „böswillige“ Zwecke vordefinierte Ausgabe generieren (Problem: Lässt sich bisher recht leicht umgehen, wenn der „bösartige“ Zweck durch „freundlichen“ Zweck über sog. „Prompt Injection“ maskiert wird – z.B. Kampagne zur Warnung vor bösartiger Handlung unter Berücksichtigung der bösartigen Handlung)
- Trainingsdaten aus vertrauenswürdigen Quellen verwenden
- Bei Trainingsdaten insbesondere auch auf potenziellen Missbrauch achten (inkl. einer gezielten „Vergiftung“ des Modells) und bei der Validierung entsprechend bewerten („Adversarial Training“)
- Keine Verwendung sensibler Daten zum Training des KI-Systems, da Original-Daten u.U. rekonstruierbar sind – bezieht sich nicht nur auf personenbezogene Daten, sondern auch auf Geschäftsgeheimnisse
- Entwicklung des KI-Systems unter Einhaltung einschlägiger Frameworks für sichere Software-Entwicklung, z.B. „Secure Software Development Framework“ des NIST (SP 800-218; Version 1.1 aus 02/2022), abrufbar unter https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf
- Implementierung einer abgesicherten Protokollierung, um potenzielle Angriffe auf KI-System möglichst identifizieren zu können
- Härtung eingesetzter Komponenten des KI-Systems

3.5 Datenschutz Protokolldaten

Aufgabe:

- Eine **kritische Infrastruktur** muss **Protokolldaten** in sein **System zur Angriffserkennung** einspeisen. Skizzieren Sie hierzu Beachtenswertes aus dem Datenschutz unter Berücksichtigung der Vorschriften aus dem BSIG für kritische Infrastrukturen!
  Hinweis:
  Von den Vorschriften aus dem BSIG sind aufgabenrelevant:
  § 2 Abs. 8 & 9b
  § 5 Abs. 2
  § 8a Abs. 1a

3.5 Datenschutz Protokolldaten (1)

- Protokolldaten, bestehend aus Verkehrsdaten sowie Nutzungsdaten, sind faktisch personenbezogen, da für den Betreiber i.d.R. mit vertretbarem Aufwand repersonalisierbar
- **Verkehrsdaten** nach § 3 Nr. 70 TKG = Daten, deren Erhebung, Verarbeitung oder Nutzung bei der Erbringung eines Telekommunikationsdienstes erforderlich sind
- **Nutzungsdaten** nach § 2 Abs. 2 Nr. 3 TDDDG = personenbezogene Daten eines Nutzers von digitalen Diensten, deren Verarbeitung erforderlich ist, um die Inanspruchnahme von digitalen Diensten zu ermöglichen und abzurechnen; dazu gehören insbesondere
  a) Merkmale zur Identifikation des Nutzers,
  b) Angaben über Beginn und Ende sowie über den Umfang der jeweiligen Nutzung und
  c) Angaben über die vom Nutzer in Anspruch genommenen digitalen Dienste
- Nach Art. 6 Abs. 1 lit. c EU-DSGVO ist bei kritischen Infrastrukturen die Aufzeichnung von Protokolldaten erforderlich zur Erfüllung einer rechtlichen Verpflichtung aus § 8a Abs. 1a BSIG für den Betrieb des vorgeschriebenen Systems zur Angriffserkennung zum Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern (aufgrund Vergleichbarkeit technischer Events), die auf Angriffe hindeuten (Hauptzweck)

3.5 Datenschutz Protokolldaten (2)

- Zum Nebenzweck der Auskunftserteilung [gegenüber dem BSI bzw. BKA] nach § 22 Abs. 3 TDDDG (hier: Abwehr von Gefahren für die öffentliche Sicherheit oder zur Ermittlung des Aufenthaltsorts eines Beschuldigten oder Betroffenen im Rahmen der Verfolgung von Straftaten bzw. Ordnungswidrigkeiten) i.V.m. § 24 Abs. 2 TDDDG dürfen nach § 22 Abs. 1 TDDDG Nutzungsdaten automatisiert ausgewertet werden, um insbesondere zugewiesene IP-Adressen zu bestimmen
- Der Betroffene hat nach Art. 17 Abs. 3 lit. b EU-DSGVO kein (!) Löschungsrecht
- Protokolldaten dürfen nach § 5 Abs. 2 BSIG längstens 18 Monate gespeichert werden, wobei eine Auswertung der gespeicherten Daten nur automatisiert (mittels Event-Korrelation im SIEM-Anteil des Systems zur Angriffserkennung) erfolgen darf und ein Zugriff auf Daten, die länger als drei Monate gespeichert sind, nur bei Vorliegen tatsächlicher Erkenntnisse […] erfolgt; folglich ist die Verarbeitung von Protokolldaten ab dem 3. Monat faktisch im Sinne von Art. 4 Nr. 3 EU-DSGVO einzuschränken (unabhängig von Art. 18 EU-DSGVO, da diese Einschränkung ja nicht durch die betroffene Person erwirkt werden kann, da durch Art. 23 Abs. 1 EU-DSGVO beschränkt).
- Nach § 8a Abs. 1a BSIG müssen geeignete Parameter und Merkmale, technisch als Event protokolliert, aus dem laufenden Betrieb kontinuierlich und automatisch erfasst und ausgewertet werden, um fortwährend Bedrohungen identifizieren und vermeiden zu können (bewertet durch & mit Reaktion von Experten eines SOC).

3.5 Datenschutz Protokolldaten (3)

- Die ins System zur Angriffserkennung eingespeisten Protokolldaten wiederum sind nach Art. 32 EU-DSGVO wiederum angemessen zu schützen; dabei sind insbesondere Risiken zu berücksichtigen, die aus Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von bzw. unbefugten Zugang zu den Protokolldaten resultieren; die Integrität des Systems zur Angriffserkennung setzt dabei die Integrität der Protokolldaten voraus, da sonst der nach § 2 Abs. 9b BSIG vorgesehene Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten, nicht zuverlässig erfolgen kann
- Getroffene Maßnahmen sind nach § 24 Abs. 1 EU-DSGVO erforderlichenfalls zu überprüfen und zu aktualisieren *(ergänzender Hinweis: Nach § 8a Abs. 1 BSIG muss der Betreiber der kritischen Infrastruktur angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind in diesem Zusammenhang angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.)*