Deutsche Stiftung für Recht und Informatik

Künstliche Intelligenz in der Datensicherheit

Anforderungen und Maßnahmen

Dennis-Kenji Kipker/Sven Müller

Herbstakademie 2020

1. Rechtliche Rahmenbedingungen

- **Datensicherheit als Grundvoraussetzung für den Datenschutz:** informationelle Selbstbestimmung nur dann wirksam, wenn personenbezogene Daten Dritten nicht unbefugt zugänglich gemacht werden (können)
- Hoher Stellenwert von TOM deshalb im allgemeinen Datenschutzrecht an verschiedenen Stellen verankert:
  - **Grundsatz in Art. 5 Abs. 1 lit. f DSGVO:** Personenbezogene Daten sind in einer Weise zu verarbeiten, die ihre angemessene Sicherheit gewährleistet
  - **Weitergehend:** Art. 24 DSGVO (Verantwortung des für die Verarbeitung Verantwortlichen) und Art. 32 DSGVO (Sicherheit der Verarbeitung)

1. Rechtliche Rahmenbedingungen

- **Datensicherheit bedeutet konkret:**
  - Schutz vor unbefugter oder unrechtmäßiger Verarbeitung
  - Schutz vor unbeabsichtigtem Verlust
  - Schutz vor unbeabsichtigter Zerstörung
  - Schutz vor unbeabsichtigter Schädigung

- **Gem. Art. 24 DSGVO ist der Verantwortliche zuständig:** Dieser trifft unter Berücksichtigung der Umstände der Datenverarbeitung, der Eintrittswahrscheinlichkeit und der Schwere von Risiken geeignete TOM

1. Rechtliche Rahmenbedingungen

- **Art. 32 DSGVO – Sicherheit der Verarbeitung:**
  - **Ziel technisch-organisatorischer Datensicherheit:** Verhinderung einer Verletzung des Schutzes personenbezogener Daten gem. Art. 4 Nr. 12 DSGVO
  - **Legaldefinition:** Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung sowie zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet werden
  - **Absolute Sicherheit aber nicht erreichbar!** → Vielmehr nur Bestreben, Risiken und Sicherheit in angemessenen Ausgleich zu bringen

1. Rechtliche Rahmenbedingungen

- **Art. 32 DSGVO – Sicherheit der Verarbeitung:** Keine abschließende Regelung zur Datensicherheit, vom Verantwortlichen/Auftragsverarbeiter sind geeignete TOM zu treffen unter Berücksichtigung von:
  - Stand der Technik
  - Implementierungskosten
  - Art, Umfang, Umstände und Zwecke der Verarbeitung
  - Eintrittswahrscheinlichkeit und Schwere von Risiken
- **IT-Schutzziele:** Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit, Wiederherstellbarkeit von Systemen und Diensten

1. Rechtliche Rahmenbedingungen

- **Art. 32 DSGVO – Sicherheit der Verarbeitung:**
  - **Beispiele für TOM nicht abschließend:** „gegebenenfalls unter Umständen“ → Technikneutralität, durchzieht gesamte DSGVO
  - Begriff „KI“ findet sich aber in keiner Formulierung zur Datensicherheit gem. DSGVO wieder!
  - Damit aber nicht automatisch Aussage zur Nichtverwendung KI-gestützter TOM getroffen
  - → **Neue geeignete Datensicherheitsmaßnahmen, die vom Katalog gem. Art. 32 DSGVO nicht erfasst werden, sind ebenfalls zu berücksichtigen**
  - **KI:** bietet aufgrund ihrer Entwicklungsoffenheit die Möglichkeit, neue Bedrohungslagen zu erkennen und dadurch für die Zukunft ein angemessenes Schutzniveau gewährleisten zu können

1. Rechtliche Rahmenbedingungen

- **Technikoffenheit gesetzlich angeordneter Schutzmaßnahmen, z. B. § 8a BSIG für TOV von KRITIS:**
  - **„Stand der Technik“** als Generalklausel in der Anforderungstrias um „allgemein anerkannte Regeln der Technik“ und „Stand von Wissenschaft und Technik“
  - Stand der Technik als **„Mittelfeld“** erfordert regelmäßig gewissen Erprobungsgrad der Maßnahmen in der Praxis und den Nachweis zur Abwehr von Bedrohungen/Risikominimierung
  - → **Für KI zweifelsfrei gegeben?** Nicht für sämtliche Einsatzfelder, aber bereits etablierte Felder gegeben, z. B. KI-Erkennung von Angriffsmustern
  - **Überdies:** KI als entwicklungsoffene/iterative Maßnahme besonders zur Wiedergabe vom „Stand der Technik“ geeignet

1. Rechtliche Rahmenbedingungen

- **Ergebnis:**
  - Rechtlich betrachtet kann **KI als hilfreiche Ergänzung des ISMS oder DSMS** gesehen werden, um compliancekonform den „Stand der Technik“ abzubilden
  - **Darüber hinausgehend aber notwendig:** Daten- und IT-Sicherheitskonzept, Risikoanalyse und Dokumentation getroffener Maßnahmen
  - **Für konkrete Ausgestaltung gem. „Stand der Technik“ relevant:** technische Normen und Standards, z. B. IT-Grundschutz, ISO/IEC 2700X; und Standard-Datenschutzmodell
  - **Konkreter Anwendungsfall:** Intrusion Detection System **(IDS)**, das automatisiert Systemanomalien erkennt

2. Technisch-organisatorische Ausgestaltung

- **Grundlegende technische Normen für IT-Sicherheit und Datenschutz:**
  - ISO/IEC 27001 ff. bzw. BSI IT-Grundschutz
  - ISO/IEC 27701

- **Grundlegende technische Normen für KI:**
  - ISO/IEC CD 22989 AI - Concepts and terminology
  - ISO/IEC CD 38507 IT - Governance implications of the use of artificial intelligence by organizations
  - ISO/IEC AWI 24668 AI - Process management framework for Big data analytics

2. Technisch-organisatorische Ausgestaltung

- **KI als Umsetzungshilfe** der Anforderungen aus dem Anhang A der ISO/IEC 27001:
  - Security Information und Event-Management-Systeme (SIEM)-Lösung
  - Security-Operation-Center (SOC) bzw. Cyber-Defense Center (CDC)
  - Intrusion Detection System (IDS)/ Intrusion-Prevention-System (IPS)
    - Erkennung von Angriffsmustern
    - Anomalie-Erkennung
    - Korrelation von Ergebnisdaten

2. Technisch-organisatorische Ausgestaltung

1. Notwendige Rahmenbedingungen

a. Untrainiertes KI-System
b. Datensätze
c. Lernalgorithmus
d. Sichere Entwicklungsumgebung (ISO/IEC 27001)

2. Trainieren des untrainierten KI-Systems durch Lernalgorithmen
3. Test des trainiertes KI-System (Zertifizierung)
4. Selbstständige Entscheidungen durch das KI-System
5. Training neuer Anforderungen an das KI-System

2. Technisch-organisatorische Ausgestaltung

- **Praxisbeispiele:**
  - **Security-Operation-Center**
    - 20.000 Stunden jährlich, um IT-Sicherheitshinweise zu bearbeiten
    - Januar bis Mai 2019: insgesamt 94 Millionen Fälle Schadsoftware, davon wurde die Malware in rund 4,5 Millionen Fällen mittels ML-basierter Anomalie-Erkennung detektiert
  - **Filterung von Spam-Nachrichten**
    - Jeden Tag klassifizieren Lernalgorithmen über eine Milliarde E-Mails als Spam (Spam-Aufkommen bei normalen Nutzern liegt bei 80 bis 90% des Posteingangs)

Vielen Dank für Ihre Aufmerksamkeit!