Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Sichere generative KI in Organisationen und Unternehmen

Getting started: Secure AI Operations – generative KI für Unternehmen

Ausgangslage: *Die Menschen in Ihrer Organisation brennen darauf, KI (Künstliche Intelligenz) auszuprobieren und einzusetzen. Vielleicht geht es sogar darum, KI in bestehende Systeme und Prozesse einzubauen oder neue KI-basierte Systeme einzuführen. Diese Hilfe unterstützt Sie dabei, bei wenig bis gar keinen Erfahrungen mit KI-Systemen einen sicheren Start hinzulegen.*

KI-Schnittstellen nutzen

Sie möchten eine manuelle Schnittstelle zu einem KI-System nutzen. Beispielsweise für eine schnelle Übersetzung oder um Bilder für eine Präsentation zu generieren.

Was Sie beachten müssen:

- Führen Sie ein **Demand Management für KI** ein: Erfassen Sie den Ist-Stand Ihrer Organisation und erstellen Sie eine Übersicht der aktuell verwendeten KI-Systeme.
- Ermitteln Sie die für Sie geltenden **rechtlichen Bedingungen.**
- Entwickeln Sie Ihre Kriterien für mögliche KI-Anbieter: Achten Sie auf **Transparenz und den (Server-)Standort.**
- Legen Sie **Firmenaccounts** bei dem Anbieter an. Wählen Sie **datensparsame Konfigurations-möglichkeiten.** Verbieten Sie die Verwendung Ihrer Daten für Trainings. Setzen Sie **Löschfristen** für Chats und Dokumente.
- Erstellen Sie **KI-Leitlinien:** Wer darf welche KI-Systeme zu welchem Zweck einsetzen?
  - Verhindern Sie Schatten-IT: nur **genehmigte** KI-Systeme verwenden.
  - KI-Systeme nur für den definierten **Einsatzzweck** verwenden.
  - Geben Sie niemals personenbezogene Daten oder sensitive Geschäftsinformationen ohne **schützende Maßnahmen** weiter.
  - Übernehmen Sie KI-Ausgaben nie ungeprüft oder für kritische Geschäftsprozesse.
- Schaffen Sie Akzeptanz unter den Mitarbeitenden und Gremien und involvieren Sie Ihre Stakeholder frühzeitig.

KI-Schnittstellen integrieren

Sie möchten ein fremdes KI-System in eine eigene Anwendung per API integrieren. Beispiele hierfür sind ChatBots für Kunden oder das Durchsuchen von Daten im Rahmen eines Prozesses.

Beachten Sie zusätzlich:

- Weisen Sie **Rollen** und **Verantwortlichkeiten** für Ihre Anwendungen und die integrierten KI-Systeme eindeutig zu.
- Integrieren Sie die KI-Prozesse in Ihr **IT-Sicherheitsmanagement.**
- Sorgen Sie für Transparenz: **Kennzeichnen** Sie Systeme und Prozesse, die KI verwenden.
- Listen Sie die Systeme und Datenbanken auf, auf die das KI-System Zugriff hat. Schränken Sie den Zugriff des KI-Systems auf Ihre anderen Systeme ein. Validieren Sie KI-Ausgaben, bevor diese an Backendsysteme weitergegeben werden.
- Beschreiben Sie den **Verwendungszweck** Ihrer KI-Anwendung und legen Sie fest, welche Daten dafür **freigegeben** sind.
- Erstellen Sie ein **Berechtigungskonzept** für das KI-System, das auch berücksichtigt, welche Dokumente/Daten vorab hochgeladen wurden und damit dem Nutzer zur Verfügung stehen.
- Verwenden Sie Ihre Anwendung **nicht ungeprüft** in Geschäftsentscheidungen oder in kritischen Geschäftsprozessen.
- Binden Sie relevante interne Stakeholder ein. Beziehen Sie den Datenschutzbeauftragten von Beginn an ein.

KI-Systeme entwickeln

Sie möchten ein eigenes KI-System aufbauen und externe KI-Komponenten verwenden. Zum Beispiel ein eigens gebautes KI-gesteuertes Bildverarbeitungssystem zur automatisierten Qualitätskontrolle von Autoteilen.

Setzen Sie weitere Maßnahmen um:

- Bauen Sie zusätzlich zu Ihrem **IT-Sicherheitsmanagement** ein **AI-Expert-** und ein **AI-Security-Team** auf. Etablieren Sie AI-Security-Tests (z. B. AI Pen Testing).
- Dokumentieren Sie die **KI-Verantwortlichen** und die Integration in Ihre IT-Security.
- Erläutern Sie durchgeführte **Sicherheitsmaßnahmen** und definieren Sie Ihr **Risikomanagement.**
- Sorgen Sie auch hier für Transparenz:
  - Verfolgen Sie die **Supply Chain** der KI-Systeme und deren Komponenten.
  - Fordern Sie **Model Cards** für eingekaufte oder Open-Source-Modelle an.
  - Verwenden Sie nur vertrauenswürdige Komponenten.
- Führen Sie zusätzliche **Rollen und Verantwortlichkeiten** für den Entwicklungsprozess ein.

EU AI ACT

Mit dem am 12. Juli 2024 im Amtsblatt der EU veröffentlichten AI Act gibt es erstmals einen umfassenden und bindenden Rahmen für den Einsatz von KI. Der EU AI Act kategorisiert KI-Systeme mit verschiedenen Risikoklassen und daraus resultierenden Pflichten und trat am 1. August 2024 in Kraft. Dieser Guide bezieht sich auf KI-Systeme, welche in die Kategorie mit dem niedrigsten Risiko fallen.

Über den AI Act hinaus werden viele Fragestellungen im Zusammenhang mit KI (Urheberrecht, Datenschutz, Haftung, Ethik und Fairness etc.) in den kommenden Jahren in der Praxis z. B. durch Gerichtsentscheidungen ausdefiniert werden. Dabei wird es Unterschiede in verschiedenen Regionen der Welt geben. Für die Nutzung von KI-Systemen in Europa kann es daher rechtlich vereinfachend wirken, europäische KI-Systeme zu verwenden.

Generelles:

Das hier ist ein „Getting started"-Guide. Er ersetzt keine gründliche Auseinandersetzung mit dem Thema KI und erhebt keinen Anspruch auf Vollständigkeit, sondern stellt ein Mindestmaß an KI-spezifischen Überlegungen zur Verfügung, die sich eine Organisation machen sollte, bevor sie KI zum Einsatz bringt.

Weitere Informationen auf der BSI-Webseite

Impressum

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: 0800 274 1000
E-Mail: bsi@bsi.bund.de
www.bsi.bund.de

Bildnachweis Adobe Stock/ Sawitree88

Stand Juli 2024