Künstliche Intelligenz

Fluch oder Segen der Cybersicherheit?

Inhalt

- Künstliche Intelligenz – Überblick
- Europäische KI-Verordnung (und Cybersicherheit)
- NIS2-Verordnung (und Künstliche Intelligenz)
- Einsatz von Künstlicher Intelligenz – Fluch oder Segen für die Cybersicherheit?

Künstliche Intelligenz - Überblick

- Es gibt eine Vielzahl unterschiedlicher Definitionen zur „Künstlichen Intelligenz"
- Im Wesentlichen
  - Software
  - die Ergebnisse liefert, für die man bisher menschliche kognitive Leistungen benötigt hat.
- Darunter fällt jedenfalls Software, die mittels **Machine Learning** (insb **Deep Learning**) entwickelt wurde
  - Vielzahl an Daten
  - Statistik (zB „dieses Foto bildet mit hoher Wahrscheinlichkeit einen Menschen ab")
  - Mustererkennung (zB Sprache, Gesichter, Verhaltensmuster,...)

EU KI-Verordnung („AI-Act") und Cybersicherheit

- Erwägungsgrund 51 KI-Verordnung (Entwurf)

  *„Die **Cybersicherheit** spielt eine entscheidende Rolle, wenn es darum geht sicherzustellen, dass KI-Systeme widerstandsfähig gegenüber Versuchen böswilliger Dritter sind. […]*

  *Um ein den Risiken angemessenes Cybersicherheitsniveau zu gewährleisten, sollten die Anbieter von Hochrisiko-KI-Systemen daher **geeignete Maßnahmen** ergreifen, wobei gegebenenfalls auch die zugrunde liegende IKT-Infrastruktur zu berücksichtigen ist."*
- Generell gilt: Anforderungen aus der KI-Verordnung treffen vor allem „Hochrisiko KI-Systeme" (Kapitel 2 und 3 der KI-Verordnung)
- KI-Systeme sollen im gesamten Lebenszyklus sicher sein

EU KI-Verordnung („AI-Act") und Cybersicherheit

- Cybersicherheitsanforderungen an (Hochrisiko) KI-Systeme (Achtung: KI-Verordnung derzeit noch Entwurf, nicht geltendes Recht!)
  - Insbesondere Art 15 KI-Verordnung („Genauigkeit, Robustheit und Cybersicherheit")
    - *„Hochrisiko-KI-Systeme werden so konzipiert und entwickelt, dass sie **im Hinblick auf ihre Zweckbestimmung** ein **angemessenes Maß** an Genauigkeit, Robustheit und **Cybersicherheit** erreichen und in dieser Hinsicht während ihres gesamten Lebenszyklus beständig funktionieren."*
    - müssen widerstandfähig gegen Ausnutzung von Systemschwachstellen sein
    - müssen den jeweiligen Umständen und Risiken angemessen sein (abhängig vom Einsatzbereich)
    - Einsatzbereich muss klar definiert sein (Gebrauchsanweisung; Art 13 KI-Verordnung)
    - Maßnahmen müssen auch Angriffe auf Datensätze adressieren: Datenvergiftung („*data poisoning*"), feindliche Beispiele („*adversarial examples*"), Modellmängel.

Künstliche Intelligenz in der NIS2-Richtlinie

- Erw 51 NIS2-RL
  - *„Die **Mitgliedstaaten** sollten den Einsatz innovativer Technologien, einschließlich **künstlicher Intelligenz, fördern**, deren Einsatz die **Aufdeckung und Verhütung von Cyberangriffen** verbessern könnte, sodass Ressourcen wirksamer gegen Cyberangriffe genutzt werden können. Die Mitgliedstaaten sollten daher **im Rahmen ihrer nationalen Cybersicherheitsstrategie** Tätigkeiten im Bereich Forschung und Entwicklung fördern, um die Nutzung derartiger Technologien, insbesondere solcher, die sich auf automatisierte oder halbautomatisierte Instrumente für die Cybersicherheit beziehen, und gegebenenfalls den Austausch von Daten zu erleichtern, die für die Schulung und Verbesserung dieser Technologien erforderlich sind.* […]"
- Erw 89 NIS2-RL (iVm Art 21)
  - *„Außerdem sollten diese [Anm: **wesentlichen und wichtigen] Einrichtungen** ihre eigenen Cybersicherheitskapazitäten bewerten und gegebenenfalls die **Integration von Technologien zur Verbesserung der Cybersicherheit anstreben**, **etwa künstliche Intelligenz** oder Systeme des maschinellen Lernens, um ihre Kapazitäten und die Sicherheit von Netz- und Informationssystemen zu erhöhen*"

Einsatzgebiete von KI

Zukünftige Anwendungen werden mit KI schneller, genauer und weniger fehleranfällig.

Gefahren können damit nicht nur diagnostizieren, sondern auch zuverlässig vorausgesagt werden.

Künstliche Intelligenz bereits allgegenwärtig!

- System- und Umgebungsmonitoring (zB Log Analyse)
- Sprachassistenzsysteme und Chatbots (zB ChatGPT, ua.)
- Suchmaschinen
- Gesichtserkennung
- Mobilität (zB autonomes Fahren)
- Software-Development (zB Programmiercode wird vorgeschlagen; Fehlersuche)
- Drohnentechnologie und Robotik
- Medizinische Befunde (zB Diagnosen von Röntgenbildern),...

Vorteile von KI in der Cybersicherheit

KI kann zukünftig helfen, Angriffe von Hackern deutlich schneller und präzise zu erkennen, Schäden zu vermeiden und Auswirkungen von Cyberangriffen zu minimieren.

- Erhöhung der Erkennungsrate von Angriffen in Netzwerken und IT-Endgeräten
- Log-Analyse und Korrelation über Systeme hinweg
- Quellcode-Analyse in bestehender Software aber auch beim Entwickeln neuer Software („Security by design")

Beispiele: KI-basierte Analysen auf Netzwerkebene (Analyse großer Datenmengen auf potentielle Bedrohungen, Deep Learning zur Malware-Erkennung)

Herausforderungen von KI in der Cybersicherheit

- Hacker werden künftig vermehrt KI-Tools verwenden, um raffinierter anzugreifen (z.B. automatisierte Angriffe, realistische Phishing Mails, Einsatz von KI in Malware)
- Systeme ohne KI-gestützte Verteidigung können somit zur leichten Beute von Angreifern werden
- Einsatz für Massenüberwachung („Sharp Eyes"-Projekt in China)
- Transparenz von Algorithmen (Nachvollziehbarkeit)

KI - Fluch oder Segen der Cybersicherheit?

Entwicklungen rund um KI müssen im Auge behalten werden,
um sich sowohl auf **Marktchancen** als auch auf **Risiken** vorzubereiten.

Cybersicherheit ohne KI wird in Zukunft nicht mehr machbar sein.

Transparenz wird immer wichtiger!

Ob KI zum Fluch oder Segen wird, hängt davon ab, wie wir damit umgehen.