

Dr. Detlef Houdeau, Infineon Technologies AG

Mit Sicherheit intelligent – KI in der IT-Sicherheit

5. April 2019, Hannover

Potentielle Verwundbarkeit durch Cyberangriffe

- Von Industrie 3.0 zu Industrie 4.0
Neue Angriffsflächen durch zunehmende Vernetzung
- 55 Mrd. Euro jährlicher Schaden in Deutschland
durch Wirtschaftsspionage, Sabotage und Datendiebstahl



Warum Cyberangriffe auf Industrie?

- Finanzielle Aspekte z.B. Erpressung
- Abfluss an Know-How und Daten
- Motivation durch Unruhestiftungen / Sabotage

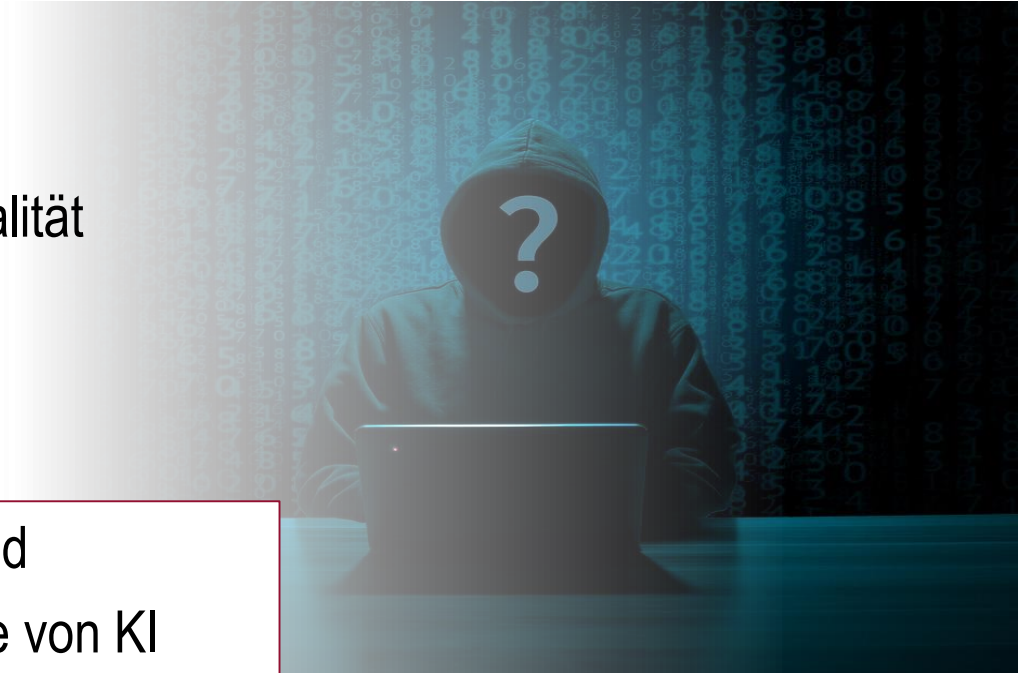


Wer sind die Angreifer?

- Innen vs. Außentäter
- Einzel vs. organisierte Kriminalität
- Black-Hat vs. White-Hat

Bisher Angriffe von Menschenhand

→ Neue Angriffsqualität mit Hilfe von KI



- Hohe Veränderungsgeschwindigkeit und Komplexität von IT-Systemen
- Fachkräftemangel in der IT-Sicherheit
- Besondere Bedürfnisse von KMU
- Internet of Thinking Things



- Verbesserte Angriffs- und Anomalieerkennung
- KI-unterstützte Authentisierungsverfahren
- Evaluierung von IT-Systemen mit kryptographischen Komponenten (Seitenkanalanalyse)



Herausforderung Dual-Use-Potenzial

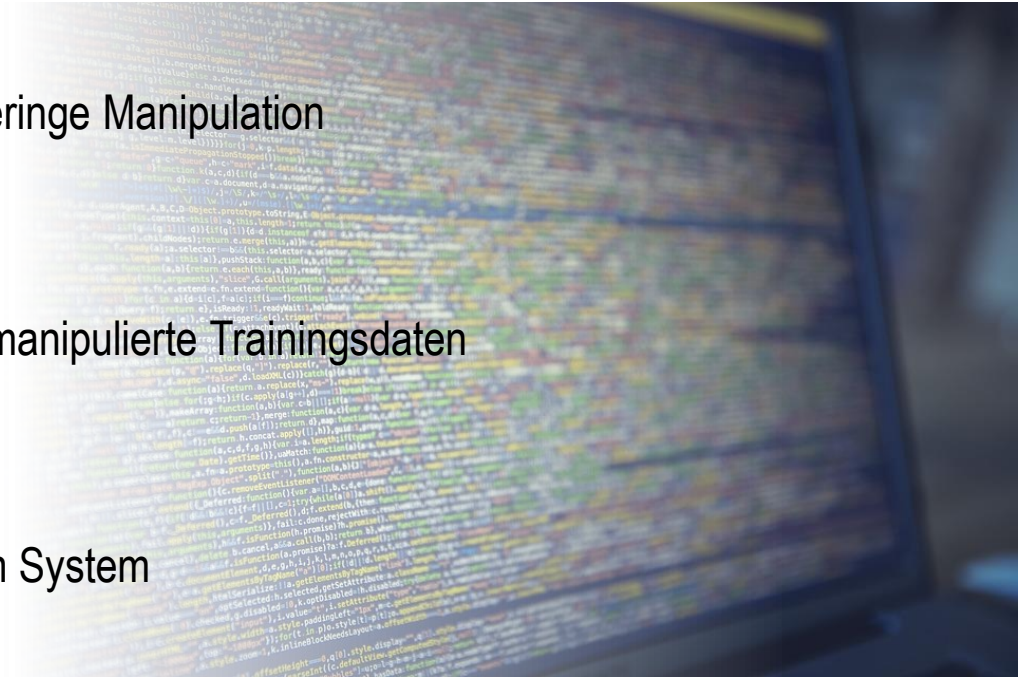
Zweckentfremdung von KI-Verfahren für böswillige oder kriminelle Zwecke

- Erweiterung und Optimierung bestehender Angriffsstrategien
z.B. Social Engineering
- Neue Bedrohungen
z.B. Angriffe auf spezifische Schwachstellen von KI-Systemen
- Veränderung grundlegender Eigenschaften der Attacken
Verringerung des Trade-offs zwischen Effizienz, Skalierbarkeit und Effektivität eines Angriffs



Angriff auf Schwachstellen der KI

- Angriffe auf die Vorhersage:
Falsche Vorhersagen bereits durch geringe Manipulation
- Angriffe während des Lernens:
Beeinträchtigung der Funktion durch manipulierte Trainingsdaten
- Angriffe auf den Datenschutz:
Extrahierung sensibler Daten aus dem System



- 
- Handlungsfelder für Politik und Behörden
 - Angebote für KMU schaffen / ausbauen
 - Anstrengungen im Bereich Aus- und Weiterbildung
 - Handlungsfelder für Unternehmen
 - Aufbau technischer Fähigkeiten und Kompetenzen
 - Revolvierende Überprüfung bereits eingesetzter intelligenter Abwehrmaßnahmen
 - Handlungsfelder im Bereich Forschung
 - Intensivierung von Forschung zur Resilienz
 - Forschung zu Verbesserung der Erklärbarkeit

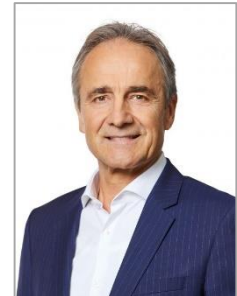
➔ Nächster Schritt: Sektoren- und architekturspezifische Vertiefung

Die Plattform Lernende Systeme

<https://www.plattform-lernende-systeme.de>

Ziele:

- Künstliche Intelligenz (KI) im Sinne der Menschen gestalten
- Wirtschaftliches Potenzial von KI ausschöpfen



Vorsitzende der Plattform:
Bildungsministerin Anja Karliczek,
acatech Präsident Karl-Heinz-Streibich

Arbeitsweise: Die Plattform Lernende Systeme

- vereint **Expertise** aus Wissenschaft, Wirtschaft und Gesellschaft
- ist ein Ort des **Austauschs** und der **vorwettbewerblichen Kooperation**
- will Deutschland als **Technologieführer** für Lernende Systeme positionieren

→ Sieben Arbeitsgruppen entwickeln **Handlungsempfehlungen** für Politik, Wirtschaft und Gesellschaft und **Anwendungsszenarien**

- Folie 2: <https://pixabay.com/de/photos/internet-cyber-netzwerk-finger-3592056/>
- Folie 3: Aus vorheriger Präsentation
- Folie 4: <https://pixabay.com/de/photos/hacker-silhouette-hacken-hack-3342696/>
- Folie 5: <https://pixabay.com/de/illustrations/internet-sicherheit-geschäft-3443625/>
- Folie 6: <https://pixabay.com/de/illustrations/binär-schloß-schutz-sicherheit-1538721/>
- Folie 7: <https://pixabay.com/de/illustrations/chatbot-chat-anwendung-künstliche-3589528/>
- Folie 8: <https://pixabay.com/de/photos/code-programmierung-computer-daten-1486361/>
- Folie 9: <https://pixabay.com/de/photos/mann-silhouette-schreibtischnetz-2692447/>