Herzlich willkommen

TAROX ROAD'24 SHOW

Microsoft www.tarox.de intel

Cyber-Resilienz:

Cybersicherheit in Zeiten von KI

TAROX AG

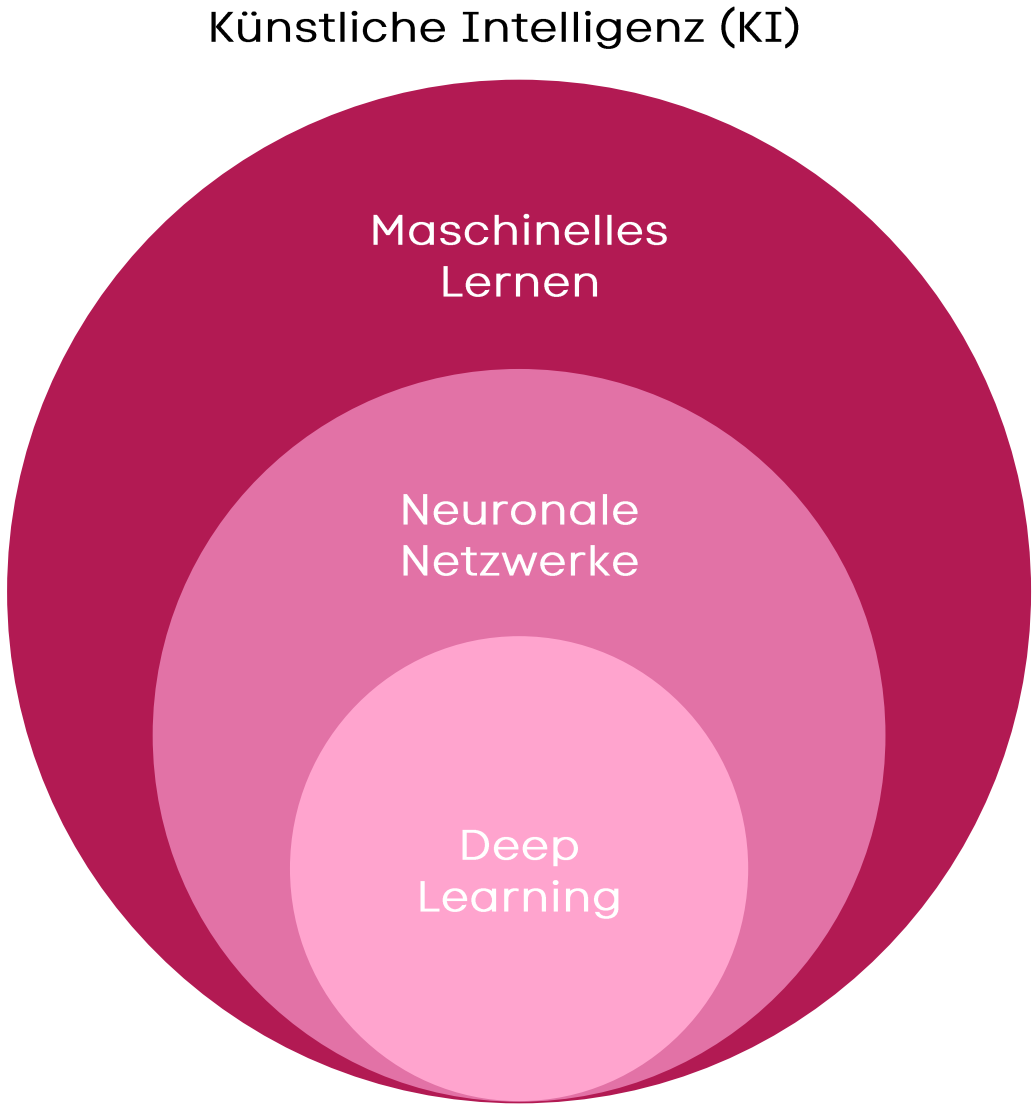
Was ist überhaupt KI?

Was ist AI, KI, was ist maschinelles Lernen, was sind neuronale Netze?

„**Künstliche Intelligenz (KI)** ist ein Teilgebiet der **Informatik**.

Sie imitiert menschliche kognitive Fähigkeiten, indem sie Informationen aus Eingabedaten erkennt und sortiert.

Diese Intelligenz kann auf programmierten Abläufen basieren oder durch **maschinelles Lernen** erzeugt werden."



Künstliche Intelligenz

Welche Arten von KI gibt es?

1. **Software**
   - z.B. Virtuelle Assistenten (ChatGPT)

2. **Eingebettete KI**
   - KI mit der nicht direkt interagiert wird

Für die Cybersicherheit ist vor allem die eingebettete KI interessant, aber auch die Software KI kann relevant sein, dazu aber später mehr.

Quelle: https://www.europarl.europa.eu/topics/de/article/20200827STO85804/was-ist-kunstliche-intelligenz-und-wie-wird-sie-genutzt

Künstliche Intelligenz

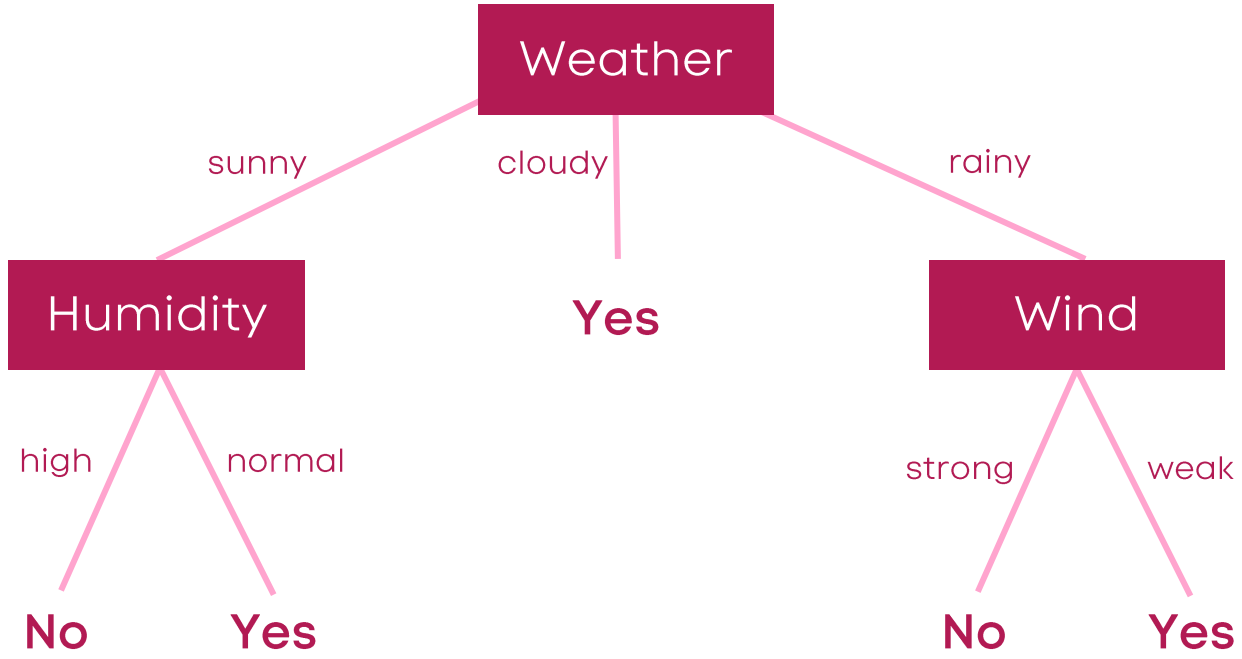
Wie funktioniert KI?

- KI basiert häufig auf Machine Learning
- Baut auf große Datenmengen und viel Rechenleistung
- Bigdata und Wachstum der Datenmengen fördern Relevanz von KI
- KI hilft Unternehmen riesige Datenmengen verarbeiten zu können
- Algorithmen zur Bewertung verschiedener Daten
- Trainiert werden diese mit bereits bekannten Daten
- Ziel ist, neue Daten einordnen zu können und ihre Bedeutung zu bestimmen

Künstliche Intelligenz

Wie funktioniert ein solcher Algorithmus?

- Nachvollziehbares Beispiel ist der Decision Tree (Entscheidungsbaum)
- Drei Komponenten sind die wichtigsten Bestandteile
- Der Knoten Weather ist die Wurzel, hier beginnt der Entscheidungsprozess
- Sunny, Cloudy und Rainy sind die Äste, an denen entlang eine Entscheidung getroffen werden kann.
- Humidity und Wind sind weitere Knoten, an denen sich für tieferliegende Äste entschieden werden muss.

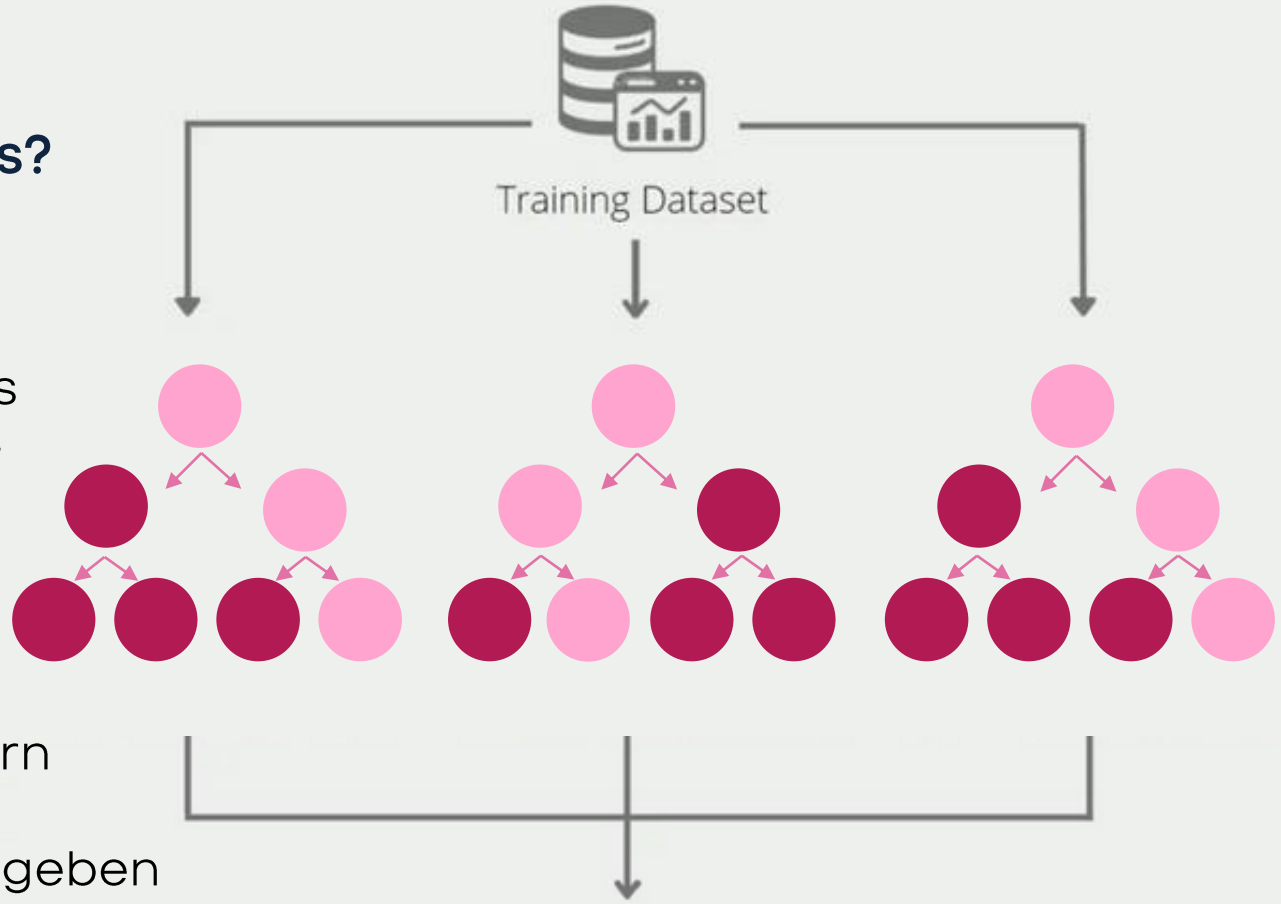


Quelle: https://databasecamp.de/ki/decision-tree

Künstliche Intelligenz

Wie funktioniert ein solcher Algorithmus?

- Entscheidungsbaum lässt sich auf Basis bekannter Daten aufbauen
- Das Aufbauen des Baums nennt man das Trainieren des Machine Learning Modells
- Nachteil: schnell sehr groß und komplex, deshalb gibt es weitere Verfahren zum vereinfachen
- Es gibt auch weitere Ansätze, um zum Beispiel auch die Ergebnisse zu verbessern
    - Mehrere solcher Bäume parallel ergeben ein Random Forrest Verfahren



Aufbau eines Random Forests

Quelle: https://databasecamp.de/ki/decision-tree

Künstliche Intelligenz

KI in der Cybersicherheit

Künstliche Intelligenz

KI in der Cybersicherheit

Künstliche Intelligenz

Wie wird KI in der Cybersicherheit heute bereits eingesetzt?

- Aktuell hauptsächlich als eingebettete KI
- Beispiel ist unser Distributionspartner Bitdefender

Machine Learning (HyperDetect)

- Entwickelt und verwendet seit 2009 Machine Learning Algorithmen und hält ca. 80 Patente
- Täglich tauchen mehr als 400.000 neue Schadsoftware Varianten auf
- Das Modul Hyper Detect nutzt diese Verfahren
- Bedrohungen können erkannt und Schäden verhindert werden
- Geschütz wird gegen dateilose Angriffe, gezielte Angriffe, verdächtige Dateien und Netzwerkverkehr, Exploits, Ransomware und Grayware
- KI wird vor allem für Verhaltensanalysen eingesetzt
- Scamio erkennt, ob Texte oder Mails Bedrohungen enthalten

Bitdefender

Quelle: https://www.bitdefender.de/business/gravityzone-platform/hyperdetect.html

Künstliche Intelligenz

Warum wird KI in der Cyber Sicherheit immer relevanter?

- Aktuell gibt es noch klare Grenzen zum Beispiel bei Genauigkeit und Komplexität
- KI wird laufend weiterentwickelt
- Datenmengen, die verarbeitet werden müssen und können, werden größer
- KI ist keine Komplettlösung, sondern eher ein mächtiges Werkzeug
- Kann IT-Teams in verschiedensten Bereichen der IT-Sicherheit unterstützen
- Sowohl als Software KI wie auch weiterhin als eingebettete KI
    - Entscheidungsfindung
    - Aufklärung
    - Abwehr

Quelle: https://www.europarl.europa.eu/topics/de/article/20200827STO85804/was-ist-kunstliche-intelligenz-und-wie-wird-sie-genutzt

Künstliche Intelligenz

Welche Risiken ergeben sich aus der KI für Cybersicherheit?

- Auch für Angreifer ist KI ein attraktives Werkzeug
- Es gibt hinreichend viele Möglichkeiten sowohl eingebettet als auch als Software
- Phishing Mails (ChatGPT)
- Programmierungsunterstützung (ChatGPT)
- Ransomware (ChatGPT)
- Finden neuer Ziele(ChatGPT)
- Angriffssteuerung (eingebettet)

Quelle: https://www.it-economics.de/software/die-welt-der-hacker/

Was sagen Sie?

Überwiegt das Risiko, oder ist KI ein nützlicher Verbündeter?

Unsere Partnerschaften

Unsere starken Partner, um Ihre und die Bedürfnisse Ihrer Kunden in der Cybersicherheit zu decken

Bitdefender

MADE IN GERMANY
ENGINSIGHT

MADE IN GERMANY
HORNETSECURITY
NEU - Demnächst erhältlich

KANGURU™
Secure. Anytime. Anywhere.

LastPass •••|

NETWORK BOX
NEXT GENERATION MANAGED SECURITY

MADE IN GERMANY
SECUREPOINT

RUCKUS
COMMSCOPE

SOPHOS

MADE IN GERMANY
SystoLOCK
Authentication Revolution!
NEU - Demnächst erhältlich

TAROX Roadshow 2024

Wir freuen uns auf Ihre Kontaktanfrage!

Alexander Wiediker

Leitung Cyber Security

T 0231 98980 312

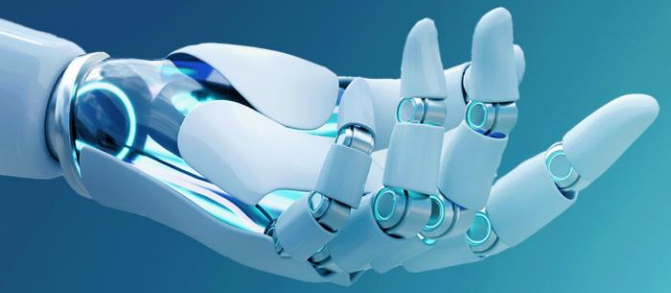
alexander.wiediker@tarox.de

Rouven Scobel

Sales Consultant Cyber Security

T 0231 98980 316

rouven.scobel@tarox.de



Vielen Dank für Ihre Aufmerksamkeit.

Haben Sie noch Fragen?

www.tarox.de

Cyber-Resilienz: Cybersicherheit in Zeiten von KI

Quellen

https://www.iks.fraunhofer.de/de/themen/kuenstliche-intelligenz.html

https://www.europarl.europa.eu/topics/de/article/20200827STO85804/was-ist-kunstliche-intelligenz-und-wie-wird-sie-genutzt

https://databasecamp.de/ki/decision-tree

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/kuenstliche-intelligenz_node.html

https://www.security-insider.de/bringt-ki-eine-revolution-fuer-die-it-sicherheit-a-2fb9cad315b1172243a55a84a5d75bad/

https://www.bitdefender.de/business/gravityzone-platform/hyperdetect.html

https://www.bitdefender.com/blog/hotforsecurity/artificial-intelligence-and-machine-learning/