

TeleTrust-Mitgliederkonferenz

TeleTrust – Bundesverband IT-Sicherheit e.V.

Berlin, 29.11.2018

KI in der IT Security

Ben Kröger, Leitung Professional Services
Axians IT Security GmbH

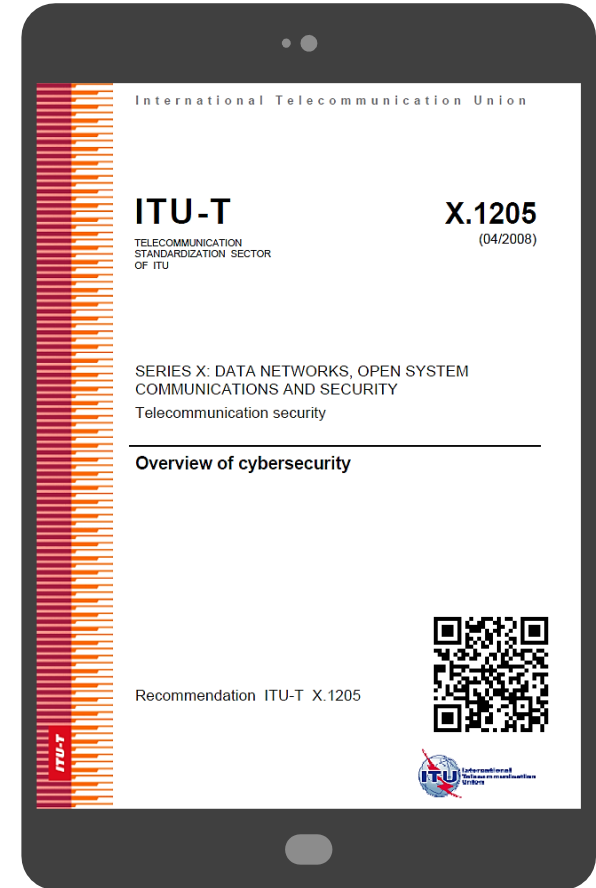
IT Security

- ▶ Vertraulichkeit
- ▶ Integrität
- ▶ Verfügbarkeit



“IT Security vs. Cyber Security”

- ▶ ITU definiert CS schon 2008
- ▶ TL;DR: CS: “IT Security”
und “organisatorische Security”





Elon Musk

@elonmusk

Folgen



Well, at least the pieces were bigger this time!



: SpaceX, Screenshot: Golfn.de

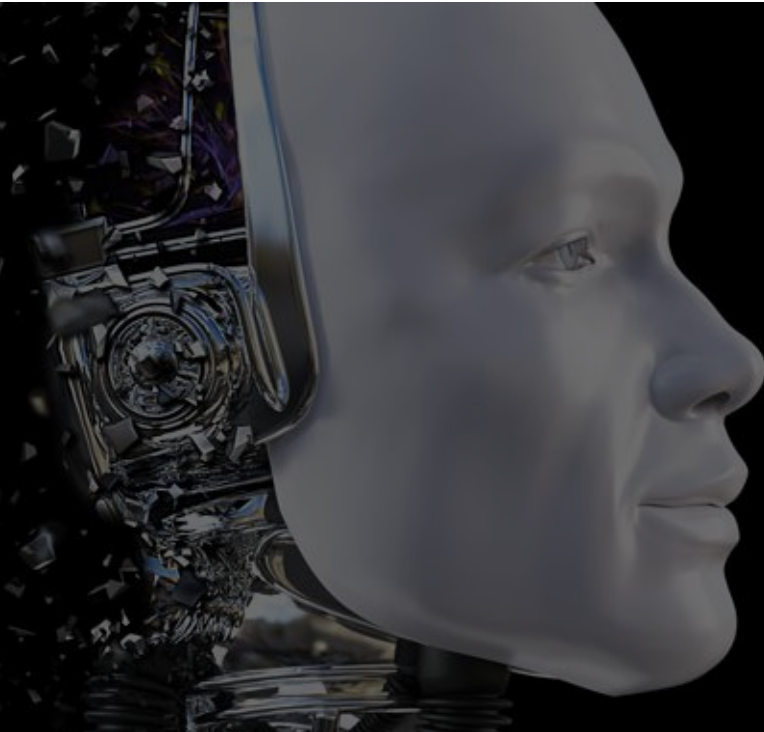


KASPANOV

Künstliche Intelligenz (KI), auch Artifizielle Intelligenz (AI bzw. A. I.)

Im Allgemeinen bezeichnet künstliche Intelligenz den Versuch, menschenähnliche Entscheidungsstrukturen in einem nichteindeutigen Umfeld nachzubilden, d. h., einen Computer so zu bauen oder zu programmieren, dass er eigenständig Probleme bearbeiten kann. Oftmals wird damit aber auch eine nachgeahmte Intelligenz bezeichnet, wobei durch meist einfache Algorithmen ein „intelligentes Verhalten“ simuliert werden soll, etwa bei Computerspielen. [...]

Quelle: Wikipedia, künstliche Intelligenz



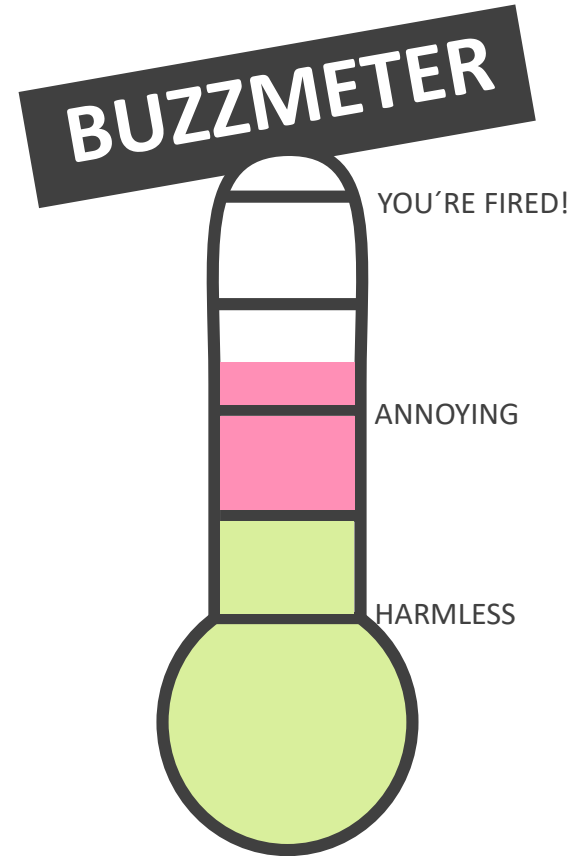
Das Buzzword Bingo ist eröffnet

“Starke” KI

- ▶ Intelligente
- ▶ Kreative
- ▶ Problemlösende Maschine

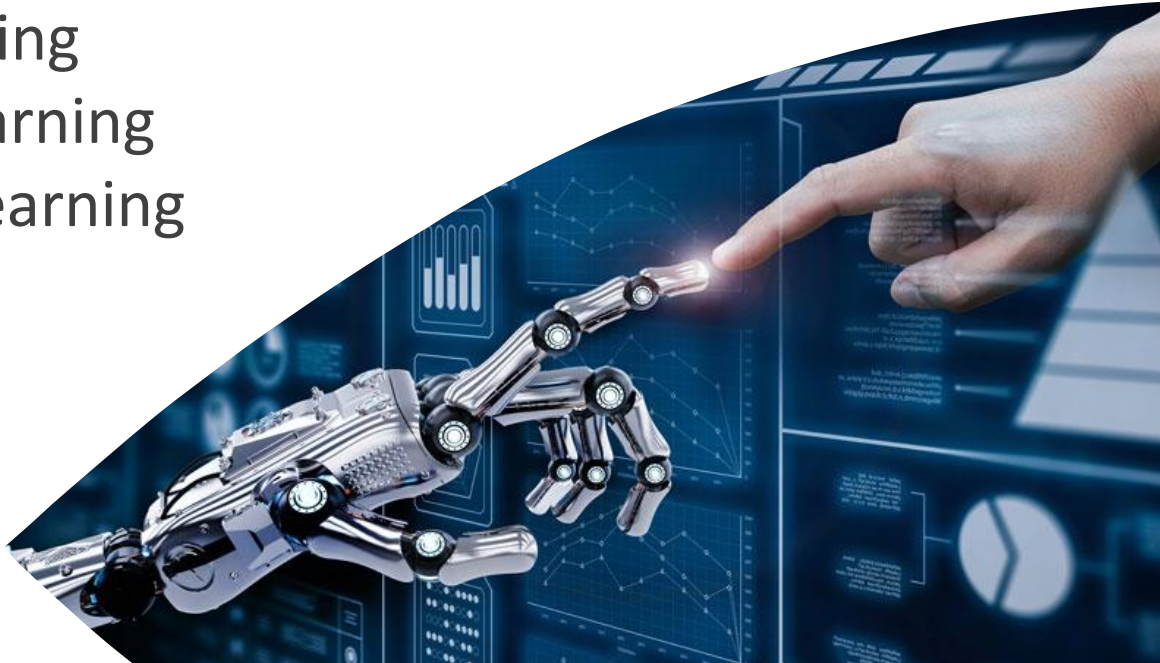
“Schwache” KI

- ▶ Machine learning



Wie werden Daten verarbeitet?

- ▶ Supervised Learning
- ▶ Unsupervised Learning
- ▶ Reinforcement Learning



regression

Ordinary Least Squares Regression (OLSR)
Linear Regression
Logistic Regression
Stepwise Regression
Multivariate Adaptive Regression Splines (MARS)
Locally Estimated Scatterplot Smoothing (LOESS)
Jackknife Regression

regularization

Ridge Regression
Least Absolute Shrinkage and Selection Operator (LASSO)
Elastic Net
Least-Angle Regression (LARS))

clustering

Single-linkage clustering
k-Means
k-Medians
Expectation Maximisation (EM)
Hierarchical Clustering
Fuzzy clustering
DBSCAN
OPTICS algorithm
Non Negative Matrix Factorization
Latent Dirichlet allocation (LDA)

decision tree

Classification and Regression Tree (CART)
Iterative Dichotomiser 3 (ID3)
C4.5 and C5.0 (different versions of a powerful approach)
Chi-squared Automatic Interaction Detection (CHAID)
Decision Stump
M5
Random Forests
Conditional Decision Trees

deep learning

Deep Boltzmann Machine (DBM)
Deep Belief Networks (DBN)
Convolutional Neural Network (CNN)
Stacked Auto-Encoders

associated rule

Apriori
Eclat
FP-Growth

neural networks

Self Organizing Map
Perceptron
Back-Propagation
Hopfield Network
Radial Basis Function Network (RBFN)
Backpropagation
Autoencoders
Hopfield networks
Boltzmann machines
Restricted Boltzmann Machines
Spiking Neural Networks
Learning Vector quantization (LVQ)

bayesian

Naive Bayes
Gaussian Naive Bayes
Multinomial Naive Bayes
Averaged One-Dependence Estimators (AODE)
Bayesian Belief Network (BBN)
Bayesian Network (BN)
Hidden Markov Models
Conditional random fields (CRFs)

dimensionality reduction

Principal Component Analysis (PCA)
Principal Component Regression (PCR)
Partial Least Squares Regression (PLSR)
Sammon Mapping
Multidimensional Scaling (MDS)
Projection Pursuit
Discriminant Analysis (LDA, MDA, QDA, FDA)

instance based

also called **case-based**, **memory-based**

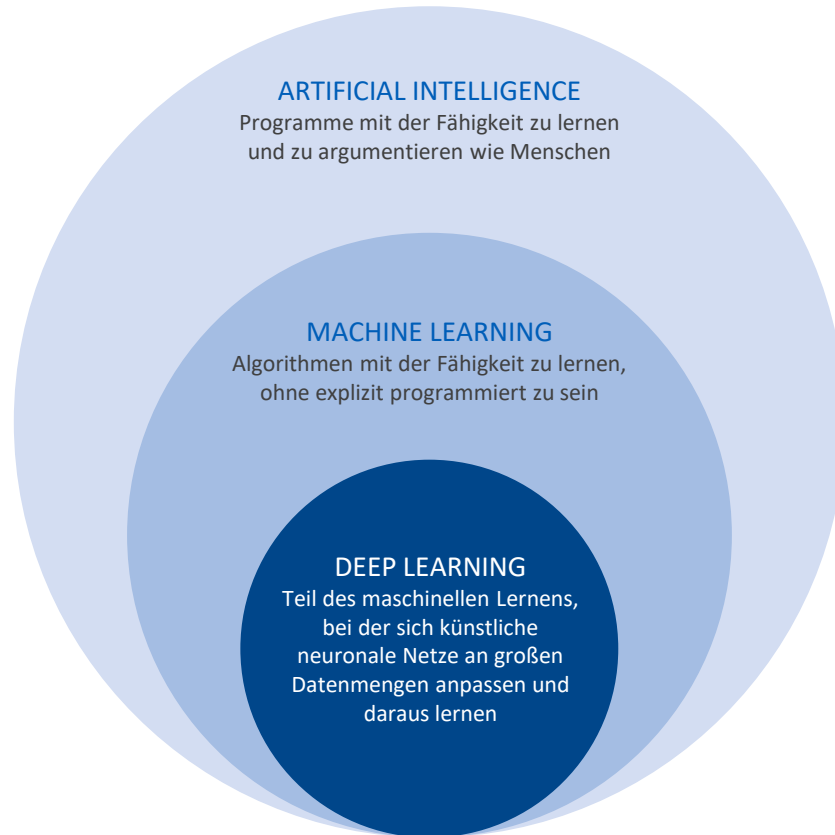
k-Nearest Neighbour (kNN)
Learning Vector Quantization (LVQ)
Self-Organizing Map (SOM)
Locally Weighted Learning (LWL)

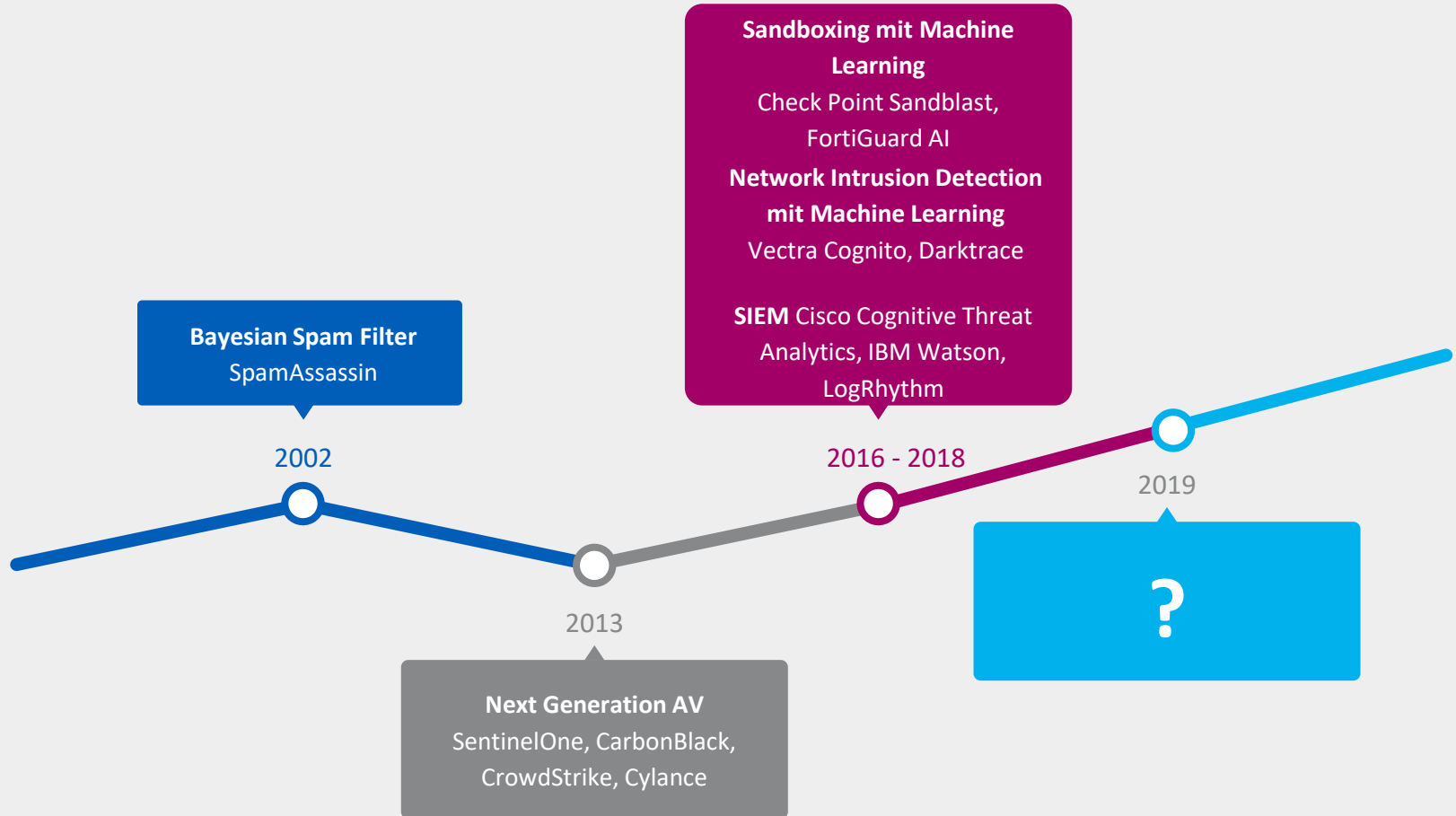
ensemble

Logit Boost (Boosting)
Bootstrapped Aggregation (Bagging)
AdaBoost
Stacked Generalization (blending)
Gradient Boosting Machines (GBM)
Gradient Boosted Regression Trees (GBRT)
Random Forest

...and others

Support Vector Machines (SVM)
Evolutionary Algorithms
Inductive Logic Programming (ILP)
Reinforcement Learning (Q-Learning, Temporal Difference, State-Action-Reward-State-Action (SARSA))
ANOVA
Information Fuzzy Network (IFN)
Page Rank
Conditional Random Fields (CRF)





- Unklar, was gelernt wird
<https://thebea.st/2z1EhR8>
- Schlechte Daten, schlechte

Fragezeichen (Microsoft &

accurate measurement of its size. Dermatologists tend to do this only for lesions that are a cause for concern. So in the set of biopsy images, if an image had a ruler

in it, the algorithm was more likely to call a tumor malignant because

presence of

Unfortunate

correlation

grounds to

Quelle: The Daily Beast



Quelle: Twitter, TayandYou

Haben Sie Fragen ?



KONTAKT

Ben Kröger
Dipl. Inf. (FH)
Leiter Professional Services
ben.kroeger@axians.de
Tel. 040 271661-32

Vielen
Dank!