TeleTrusT
Pioneers in IT security.

TeleTrusT-interner Workshop

Essen, 29./30.06.2017

Maschinelles Lernen – Was bringt dies der IT-Sicherheit?

Thomas Hemker, CISSP, CISM, CISA

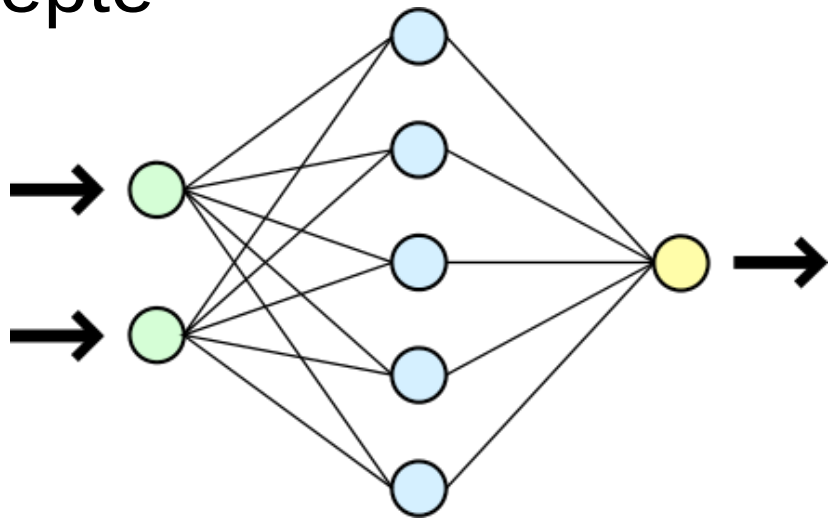
Security Strategist - Symantec (Deutschland) GmbH

Maschinelles Lernen

- "Künstliche Generierung von Wissen aus Daten" (Wikipedia)
- Nicht Neu

- Algorithmen (Motor)
- Daten/Big Data (Treibstoff)
- Parameter, Strukturen, versteckte Konzepte

- Neuronale Netze (Deep Learning)
- Entscheidungsbäume
- Vorhersagen



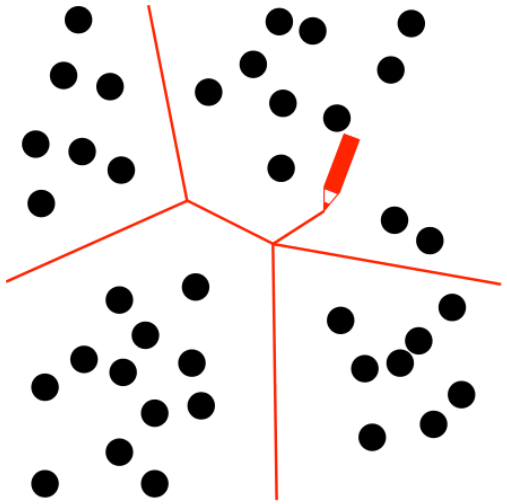
Anwendung ML – IT Sicherheit - Beispiele

Schadcode Detektion

- Ein Modul unter mehreren
- Ggf. Ersatz für signaturbasierte Erkennung
- Erkennung unbekannter Malware
- Datenbank von Dateien zum Lernen
- Statische Attribute
- Dynamisches Verhalten
- Beziehungen und Reputation
- "Ensembling" von Modellen
- Adaption – Anpassung (boosting)

Threat Intelligence

- Auswertung Telemetriedaten
- Korrelation
- Automation Sammlung von Daten
- Vorhersagen
- Modelle
- Angriffserkennung
- Forensische Analysen
- Anomalieerkennung



Diskussion

- Weitere Technologie oder "Buzzword"?
- Stand der Technik?
- Standardisierung?
- Einsatz/Verbreitung?
- Keine eigene Arbeitsgruppe
- Kompetenzaufbau Bewertung von Algorithmen und KI
- Bewertung Neue Technologien
- Deutungshoheit