Informationssicherheit in Systemen mit künstlicher Intelligenz

Eberhard von Faber ▪ Omnisecure 2020 ▪ 21. Januar 2020

T · · Systems · Let's power higher performance

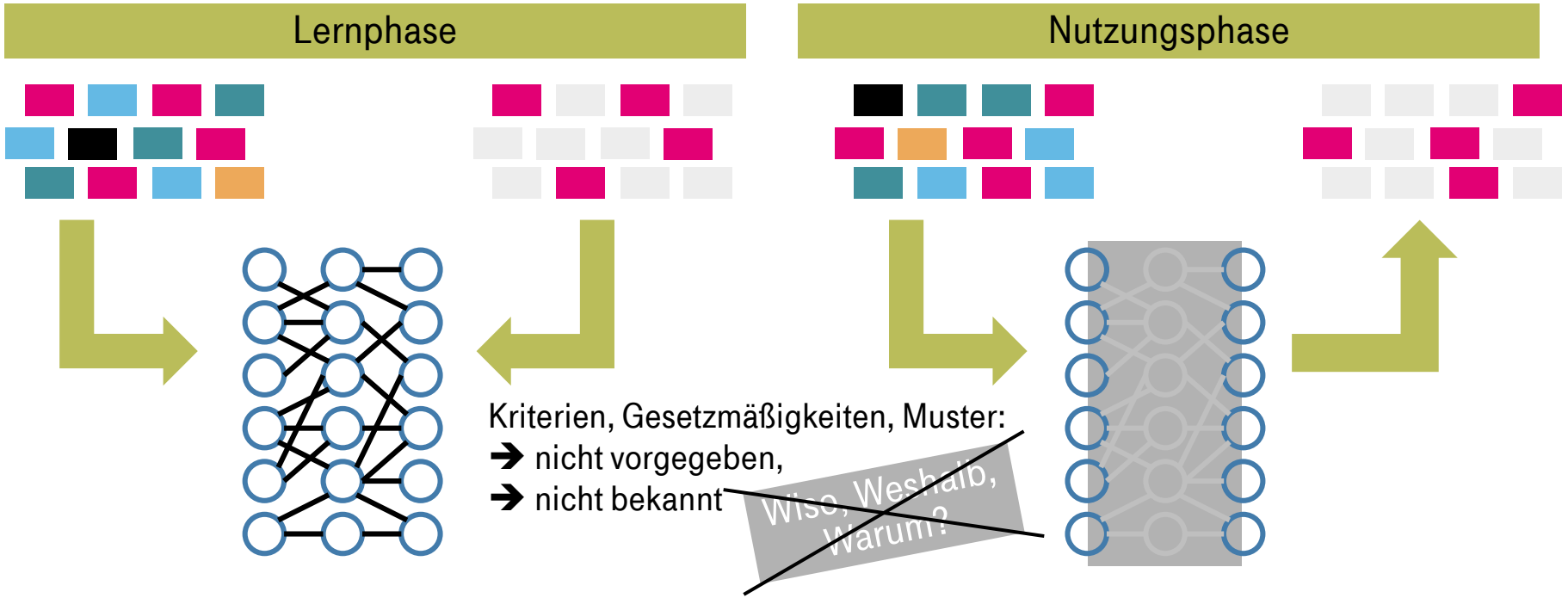
Eingrenzung.

Objekte

Subjekte

...bedrohen → ↑	Menschen	IT-Systeme/ Daten	IT mit Künstlicher Intelligenz	Maschinen
Menschen	Krieg/ Terror	**IT-Security**	**IT-Security**	Sabotage/ Terror
IT-Systeme	Qualität/ IT-Security (Safety)	Qualität	Qualität	Qualität
IT mit Künstlicher Intelligenz	(Hollywood)	Qualität	(Hollywood)	Qualität
Maschinen	Safety	Unfall	--	Cyber-Krieg

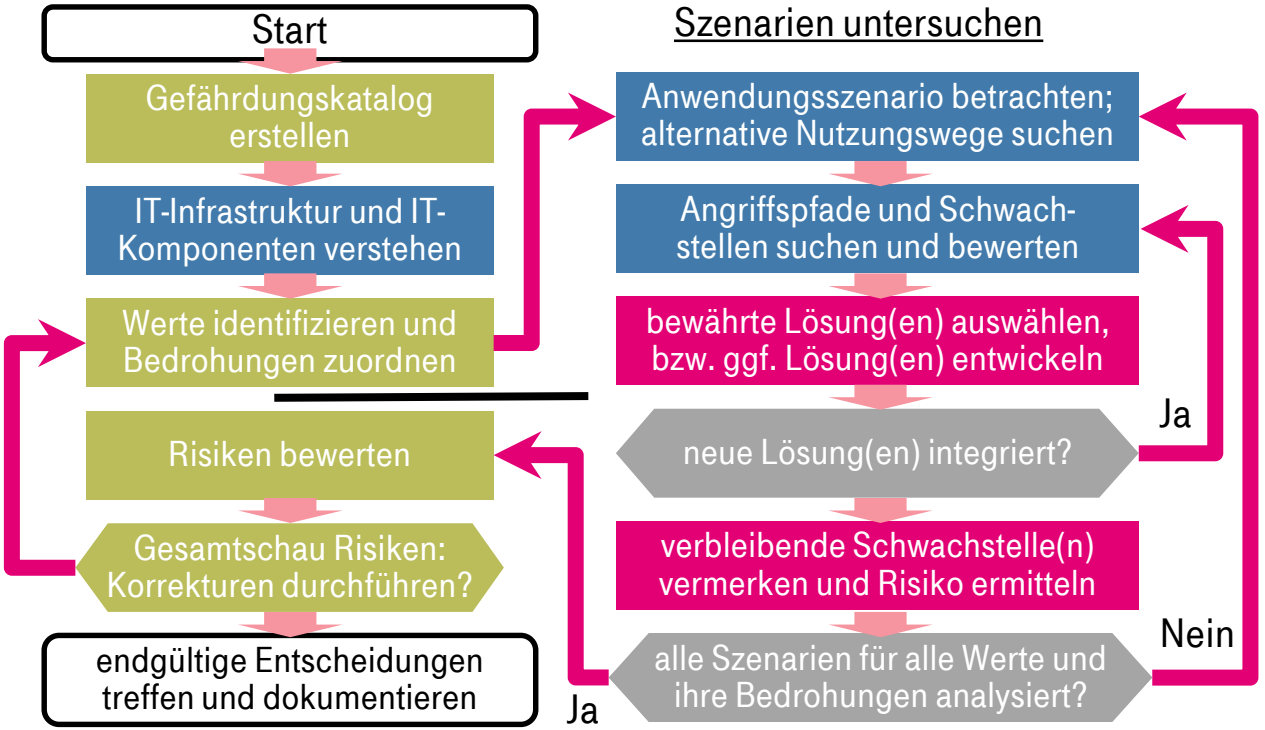
Künstliche INTELLIGENZ:
Maschinelles Lernen (ML) / Deep Learning.



IT-Sicherheit in traditioneller IT (risikobasierter Ansatz).

Voraussetzungen:

- Verständnis der IT-Architektur und IT-Komponenten,
- Verständnis der Informationsflüsse (einschl. möglicher Angriffspfade),
- Möglichkeit, gezielt einzugreifen.



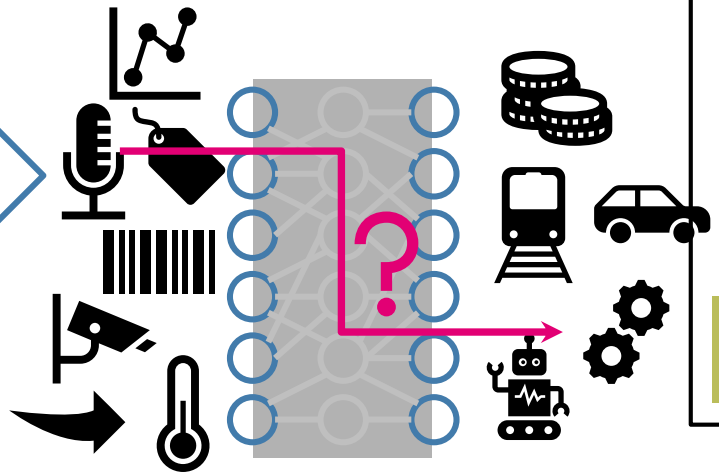
IT-Sicherheit in IT mit KI: *regellose Informationsflüsse (1).*

Voraussetzungen:

- Verständnis der IT-Architektur und IT-Komponenten,
- Verständnis der Informationsflüsse (einschl. möglicher Angriffspfade),
- Möglichkeit, gezielt einzugreifen.

„Künstl. Intelligenz“ steuert Informationsflüsse (IF) selbständig

Bsp. Produktionssteuerung, Logistik



Schwierig bzw. unmöglich:

- gewollten von verdächtigem oder feindseligem IF unterscheiden,
- bestimmte IF einfach unterbinden.

Soll-Zustand verstehen?

IT-Sicherheit in IT mit KI: *unbekannte Funktionsweise (2).*

Voraussetzungen:

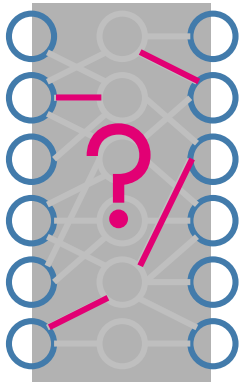
- Verständnis der IT-Architektur und IT-Komponenten,
- Verständnis der Informationsflüsse (einschl. möglicher Angriffspfade),
- Möglichkeit, gezielt einzugreifen.

?

?

„Künstl. Intelligenz“ funktioniert nicht richtlinienbasiert

Bsp. KI-Software-Komponente in einem „traditionellen“ IT-System



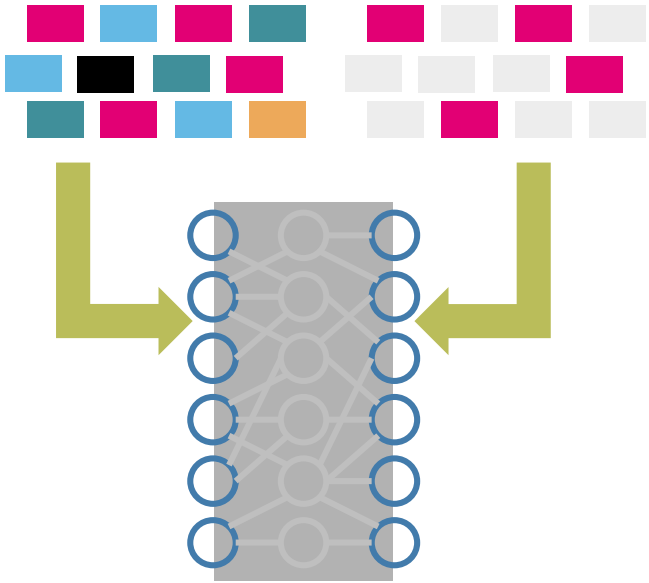
Schwierig bzw. unmöglich:

- gutartige von feindseliger Funktionsweise unterscheiden,
- manipulierte Software erkennen.

Ist-Zustand bewerten?

Einsatz von KI: *Voraussetzungen + Probleme (IT-Sicherheit)*

„Künstl. Intelligenz“ muss lernen.



Voraussetzungen:

- Stabilität,
- Relevanz der Lerndaten,
- Integrität der Lerndaten,
- Integrität des Lernvorgangs.

Problem für die IT-Sicherheit

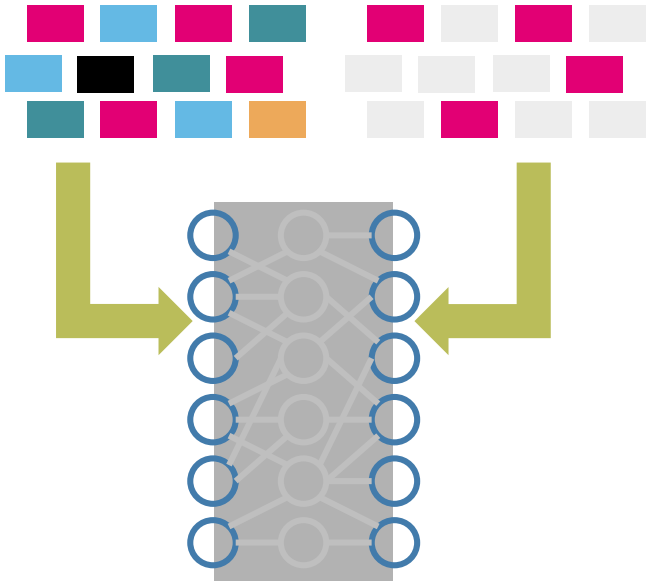
SIEM-Systeme? IDS/IPS?

- Einsatzszenario muss der Situation beim Anlernen entsprechen
- KI funktioniert nicht regelbasiert:
- KI ändert die Nutzung der IT „unverhofft“.

IDS/IPS liefern Fehlalarme

Einsatz von KI: *Voraussetzungen + Probleme (IT-Sicherheit)*

„Künstl. Intelligenz“ muss lernen.



Voraussetzungen:

- Stabilität,
- Relevanz der Lerndaten,
- Integrität der Lerndaten,
- Integrität des Lernvorgangs.

?

Problem für die IT-Sicherheit

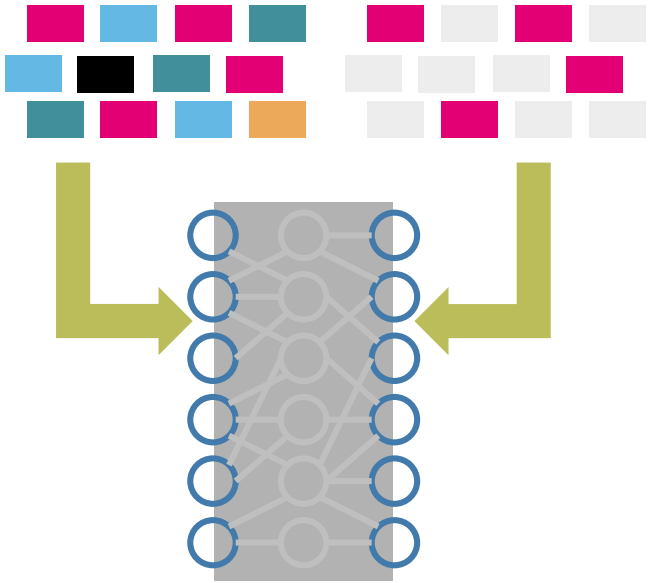
APT-Erkennung durch KI?

- Verhaltensmuster müsste bereits aufgetreten und analysiert worden sein!
- Generell: Verfügbarkeit von Beispielen für „Gut-Fall“ in dynamischen Umgebungen (Identifikation, Stabilität)

APT-Erkennung in Gefahr

Einsatz von KI: *Voraussetzungen + Probleme (IT-Sicherheit)*

„Künstl. Intelligenz“ muss lernen.



Voraussetzungen:

- Stabilität,
- Relevanz der Lerndaten,
- Integrität der Lerndaten,
- Integrität des Lernvorgangs.

?

Problem für die IT-Sicherheit

Angriff auf KI:

- Tarnung von Angriffen durch Manipulation der Lerndaten (Einschleusen von Daten; Beeinflussung der Nutzer)
- bekannt: Lieferkette der IT; jetzt jedoch bzgl. sehr komplexer Daten.

KI schützen,
ohne sie zu verstehen...

Zusammenfassung und Ausblick.

KI als „Black Box“.
- regellose Informationsflüsse,
- unbekannte Funktionsweise.

→
- Zum Schutz des Perimeters des KI-Systems zurückkehren?
- IT-Sicherheit mit KI ausrüsten: Wird diese klüger sein und die KI der IT-Anwendung verstehen können?

Neue Herausforderungen für IDS/IPS, APT & Co.
- Sensitivität des Lernvorgangs,
- Daten für Soll-Zustand?

→
- Kontrolle des Lernvorgangs!
- Konzentration auf die Verminderung der Auswirkungen?

Werden Angreifer KI verwenden können, um ihre Angriffe zu tarnen?

→
- Wird die KI der Verteidiger klüger sein?
- Werden wir KI einsetzen, um falsche Fährten zu legen und um unsere Assets zu verstecken statt sie zu schützen?

Vielen Dank.

Prof. Dr. Eberhard von Faber, T-Systems

Vortrag basiert auf einem Paper,
das entwickelt wurde zusammen mit:

Arndt Kohler, IBM, Head of IoT Security, Security Division

T · · Systems ·

Let's power
higher performance

Eberhard von Faber, Arndt Kohler: Die Lücke: Informationssicherheit in Systemen mit künstlicher Intelligenz, Wie Algorithmen und künstliche Intelligenz zur Gefahr für die IT-Sicherheit werden; in: Datenschutz und Datensicherheit - DuD, 43(7), Juli 2019, Springer Fachmedien, Wiesbaden 2019, ISSN 1614-0702, pp 434-439 https://rdcu.be/bGy3Z