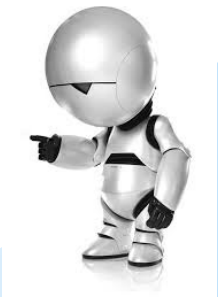
Warum ist der Wachhund immer zu spät dran?

Wirklich gute Wachhunde lernen vor der Katastrophe!



Warum ist der Wachhund immer zu spät dran?

Wirklich gute Wachhunde lernen vor der Katastrophe

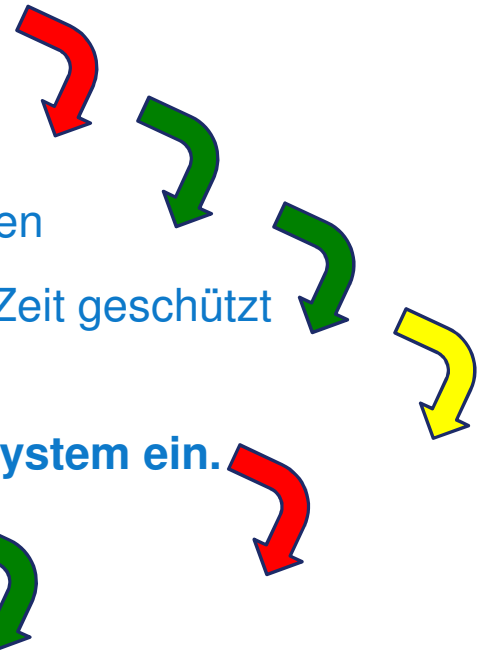
***Zyklus eines Hacker-Crashs*:**

1 **Hacker dringt in ein System ein**

2 Es entsteht ein Schaden

3 Die SW-Schwachstelle wird behoben

4 Das System scheint eine gewisse Zeit geschützt



1 **Ein neuer Hacker dringt in das System ein.**

2 Es entsteht ein Schaden ...

.....

So ein Pech !

Warum ist der Wachhund immer zu spät dran?

Wirklich gute Wachhunde lernen vor der Katastrophe

Die Geschichte vom Hasen und dem Igel

Hase =

= IT-Sicher-heits-System

Igel=

= Der Hacker

Warum ist der Wachhund immer zu spät dran?

Wirklich gute Wachhunde lernen vor der Katastrophe

Es gibt schlechte und gute Wachhunde !

Wirklich ?

Hätte der Hase nur schneller sein müssen?

Sicher nicht !

Warum ist der Wachhund immer zu spät dran?

Wirklich gute Wachhunde lernen vor der Katastrophe

***Problem bleibt*:**

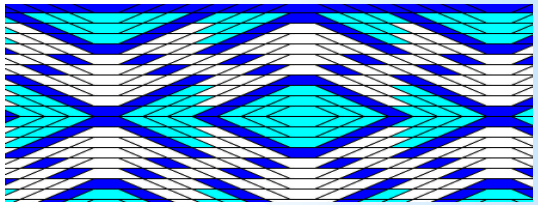
Kein sicherer Schutz vor wirklich neuen Angriffstypen Unabänderlich?

Da gab es doch eine Lösung…

Wie machte es denn die Menschheit, die Mio. Jahre alle Crashs überlebt hat? Die hat es doch gekonnt !

Warum ist der Wachhund immer zu spät dran?

Wirklich gute Wachhunde lernen vor der Katastrophe



Sensitivität:

(1) Alles, was nicht...

regelkonform, wird geprüft.

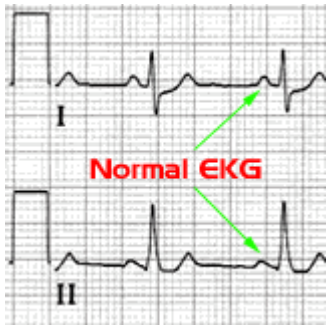
(2) Alles, was kein singuläres Zufallsereignis,

wird in Überlebensstrategie einbezogen,

z.B.

Erhöhtes Schutzverhalten

(*B. Pest*, *Ebola-Virus*).



EKG pathologisch ↑

Warum ist der Wachhund immer zu spät dran?

Wirklich gute Wachhunde lernen vor der Katastrophe

Vorschlag (1):

A **Clustern**, basierend auf gelernten (Cluster-) Strukturen mit..

- **A1 (Plus):** Input *bisher* akzeptabel → wird akzeptiert
- **A2 (Minus):** " " abgelehnt → wird abgelehnt
- **A3 (Unsicher):** Inputverlauf nicht klar zu + oder – zuzuordnen → ***weiter prüfen.***

B **Prüfgruppe**, Input wird gezwungen, aufwendigeren Zugangsweg zu gehen, der System erlaubt, eine Entscheidung zu treffen

- **B1 (Plus):** Input *jetzt* akzeptiert
- **B2 (Minus):** Input *jetzt* abgelehnt.
- **B3 (Unsicher):** Inputverlauf noch immer *nicht klar* → ***C***

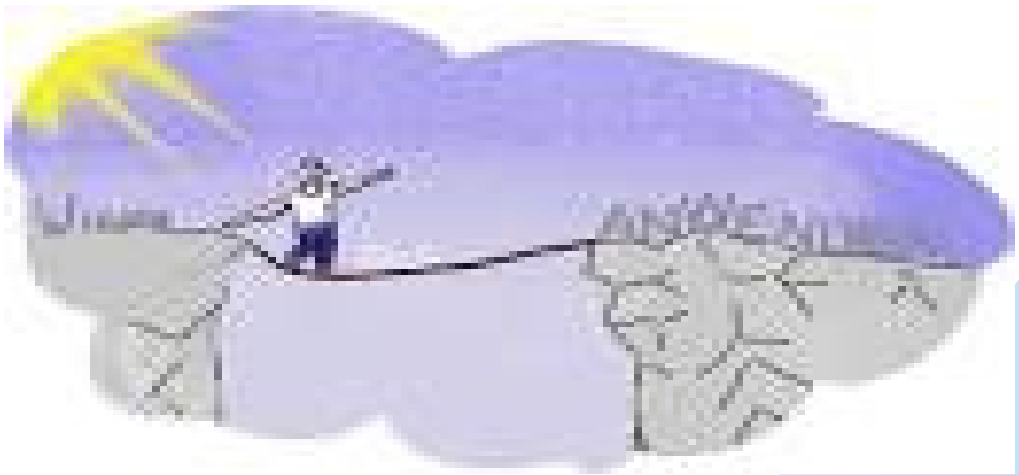
Warum ist der Wachhund immer zu spät dran?

Wirklich gute Wachhunde lernen vor der Katastrophe

Vorschlag (2):

C B wird [ökonomisch] öfter wiederholt und schließlich Restgruppe B3 an persönlichen Betreuer weitergeleitet, Berater klärt Berechtigung von Zugang + Anliegen.

D Das System bezieht aktuelle Erfahrungen vermittels eines **Lernalgorithmus** ein.



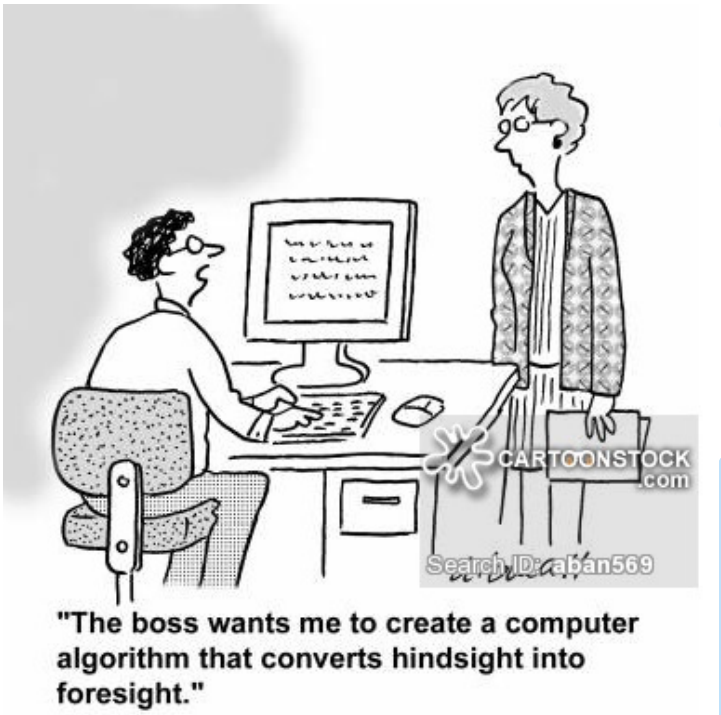
Warum ist der Wachhund immer zu spät dran?

Wirklich gute Wachhunde lernen vor der Katastrophe

Erläuterung (D):

D1 Lernalgorithmus ***strukturiert*** bei jedem Takt (= Systemzugang) den Stimulus (=Anfrage, Zugangscode, Interaktionsverlauf) neu und bewertet ihn anhand von Mittel (**Erwartungswert) + Streuung (Varianz**) bisheriger Konsequenzen).

D2 Dies verändert die Wahrscheinlichkeit der **Zuweisung** zu B1-B3, d.h. Zuweisung wird mit jedem Takt zuverlässiger.



"The boss wants me to create a computer algorithm that converts hindsight into foresight."

Warum ist der Wachhund immer zu spät dran?

Wirklich gute Wachhunde lernen vor der Katastrophe

Konsequenz:

E Selbst Insider-Information eines Hackers über akzeptierbare Zugangswege hilft ihm nicht, weil das System inzwischen weiter gelernt hat.

Dabei : Inputverlauf ist nicht nur der Zugang zum System, sondern gelernte Ablaufschritte vor + nach erfolgreichem Systemzugang.

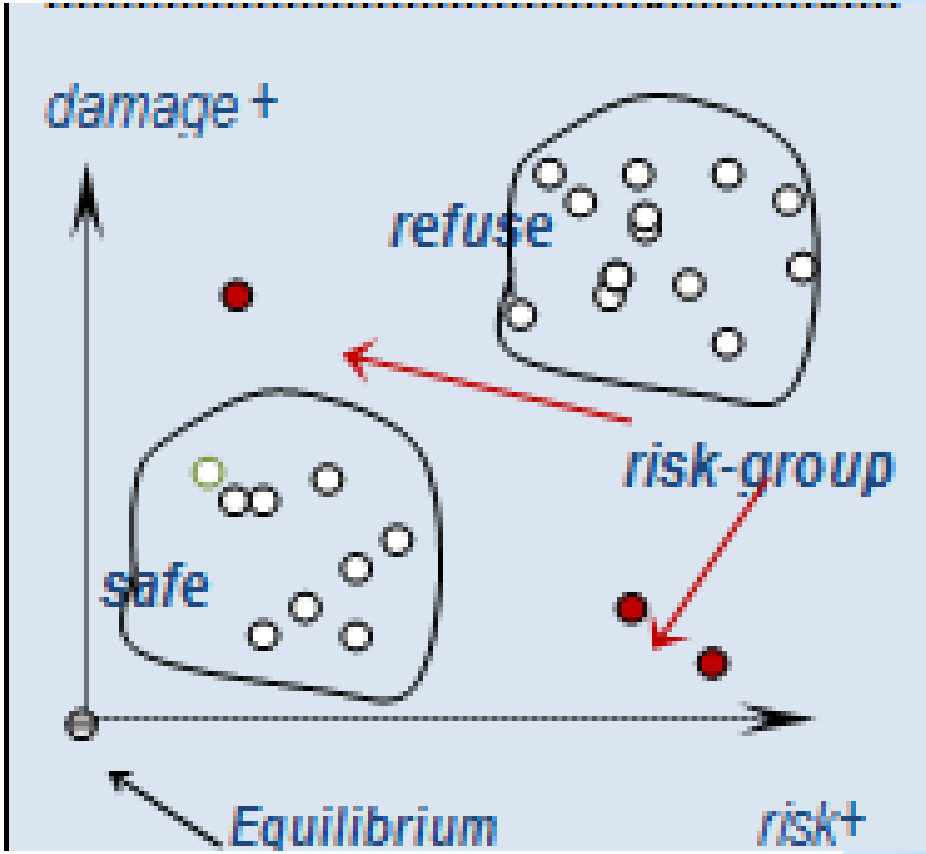
Warum ist der Wachhund immer zu spät dran?

Wirklich gute Wachhunde lernen vor der Katastrophe

Wie sieht der neue Wachhund nun aus?

1. **Lernende Risiko-Evaluation**
2. *Automatisiertes* Clustern Inputs.
3. Rglm. *statistische Validierung*
   z.B. über Diskriminanzanalyse

1. **Neuer Lernprozess** bei aktueller Risiko-Evaluation
2. .....
3. .....



Warum ist der Wachhund immer zu spät dran?

Wirklich gute Wachhunde lernen vor der Katastrophe

Wie sieht der neue Wachhund aus?

Er ist lokal überall !

weil ...

Gradienten-bezogen