Die Entwicklungsspyschologie der Intrusion Detection Systeme

— Die Zukunft vorhersagen —

Stefan Schumacher

www.Kaishakunin.com

Chemnitzer Linux-Tage 2010

解釈人

Über mich

- Selbständiger Sicherheitsberater (`www.Kaishakunin.com`)
- Fokus auf Social Engineering, Security Awareness, Unternehmenssicherheit, Systemtheorie, Konstruktivismus
- Forschungsschwerpunkt: Sicherheit messen
- Dies ist ein Vortrag zum gegenwärtigen Stand der Dinge, ich werde also keine Antworten geben, sondern Fragen stellen ;-)
- 2005: Einbruchserkennung in Netzwerke mit Intrusion Detection Systemen und Honeypots
- Forschungsprogramm zur Crime Prediction

解釈人

Table of Contents

1. Intro
2. Kybernetik
3. Genetische Epistemologie
4. Konsequenzen

解釈人

IDS?

- System zur Einbruchserkennung
- sammelt, analysiert, präsentiert Daten
- fängt Ereignisse ab die Einbrüche kennzeichnen
- **Teil** eines Sicherheitskonzepts
- **ergänzt** Zugangsschutz und andere Sicherungen
- Klassifizierung nach:
  Ort: Host, Netz, Hybrid
  Zeit: proaktiv, reaktiv, Post Mortem

解釈人

Analyse

- Signaturerkennung
  erkennt *bekannte* Angriffsmuster
  Signaturen, Vorgangsabläufe, Pattern Matching
- Heuristiken
  kann unbekannte Angriffe erkennen
  statistische Analyse (fuzzy logic)
  logische Analyse (Ereignisabfolge)

解釈人



解釈人

Warum das Ganze?

- jeder Einbruch/Sicherheitsvorfall hat eine soziale Dimension
- um Einbrüche aufzuklären muss diese Dimension untersucht werden
- um vorzubeugen müssen zukünftige Ereignisse antizipiert werden (Risikogesellschaft)
- Verhalten zu $t_n \rightsquigarrow$ *vorhergesagtem* Verhalten zu t_{n+1}
- Verhaltensvorhersage ist probabilistisch
- Benötigt Diagnostik, Prognostik, Intervention, Soziale Intelligenz, Erkenntnisfähigkeit
- Kernkompetenzen der Psychologie (und Psychiatrie, Kriminalistik, Soziologie, Philosophie)

解釈人

Warum das Ganze?

- jeder Einbruch/Sicherheitsvorfall hat eine soziale Dimension
- um Einbrüche aufzuklären muss diese Dimension untersucht werden
- um vorzubeugen müssen zukünftige Ereignisse antizipiert werden (Risikogesellschaft)
- Verhalten zu $t_n \rightsquigarrow$ *vorhergesagtem* Verhalten zu t_{n+1}
- Verhaltensvorhersage ist probabilistisch
- Benötigt Diagnostik, Prognostik, Intervention, Soziale Intelligenz, Erkenntnisfähigkeit
- Kernkompetenzen der Psychologie (und Psychiatrie, Kriminalistik, Soziologie, Philosophie)

解釈人

Nicht-technische IDS

- andere, für IDS interessante Projekte
- Amoklaufprävention an Schulen (Leaking/Risikoindikatoren)
- Analyse von Überwachungsbildern um Terroristen zu erkennen
- Rasterfahndung, Fraud Detection in Unternehmen
- Kriminologie/Kriminalistik

解釈人

Table of Contents

1. Intro
2. Kybernetik
3. Genetische Epistemologie
4. Konsequenzen

解釈人

Entscheidend ist die Entscheidung

- Heinz von Foerster: 1. Metaphysisches Postulat:
- Es gibt 2 Arten von Entscheidungen
- die, die bereits getroffen wurden (triviale E.)
- die, die nicht getroffen werden können (nicht-triviale E.)
- trivial: Ist die Erde das Zentrum des Sonnensystems? geozentrisches ./. heliozentrisches Weltbild
- nicht-trivial: nachträgliche lebenslange Sicherungsverwahrung nach Jugendstrafrecht?

解釈人

Entscheidend ist die Entscheidung

- Heinz von Foerster: 1. Metaphysisches Postulat:
- Es gibt 2 Arten von Entscheidungen
- die, die bereits getroffen wurden (triviale E.)
- die, die nicht getroffen werden können (nicht-triviale E.)
- trivial: Ist die Erde das Zentrum des Sonnensystems? geozentrisches ./. heliozentrisches Weltbild
- nicht-trivial: nachträgliche lebenslange Sicherungsverwahrung nach Jugendstrafrecht?
- nicht-trivial: ist Herr X. nur freundlich oder ist er ein Social Engineer
- nicht-trivial: Ist die Organisation »sicher«?

解釈人

Entscheidend ist die Entscheidung

- Heinz von Foerster: 1. Metaphysisches Postulat:
- Es gibt 2 Arten von Entscheidungen
- die, die bereits getroffen wurden (triviale E.)
- die, die nicht getroffen werden können (nicht-triviale E.)
- trivial: Ist die Erde das Zentrum des Sonnensystems? geozentrisches ./. heliozentrisches Weltbild
- nicht-trivial: nachträgliche lebenslange Sicherungsverwahrung nach Jugendstrafrecht?
- nicht-trivial: ist Herr X. nur freundlich oder ist er ein Social Engineer
- nicht-trivial: Ist die Organisation »sicher«?

解釈人

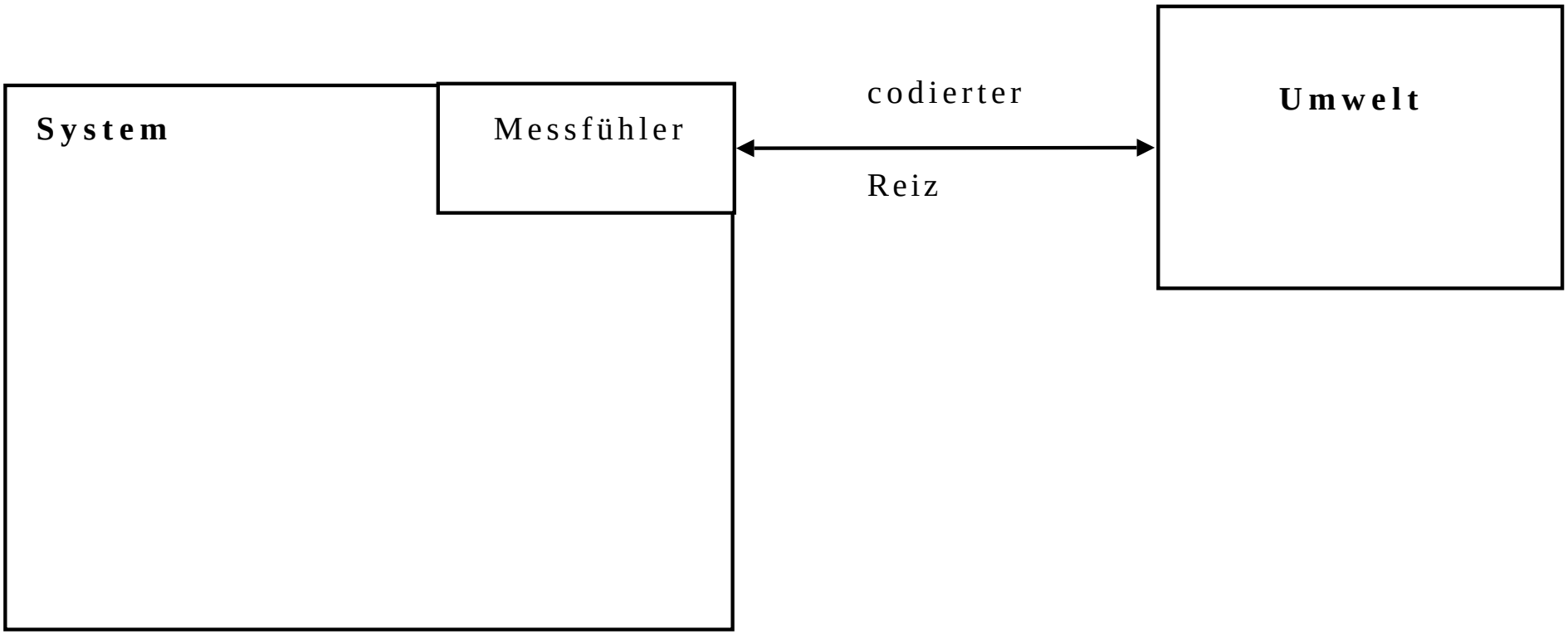
Psychologie?

Was hat das mit Psychologie zu tun?
Weltwahrnehmung (strukturelle Kopplung zwischen System und Umwelt)
Lernfähigkeit (Pädagogische Psychologie)

解釈人

Grundidee des kybernetischen Regelkreises

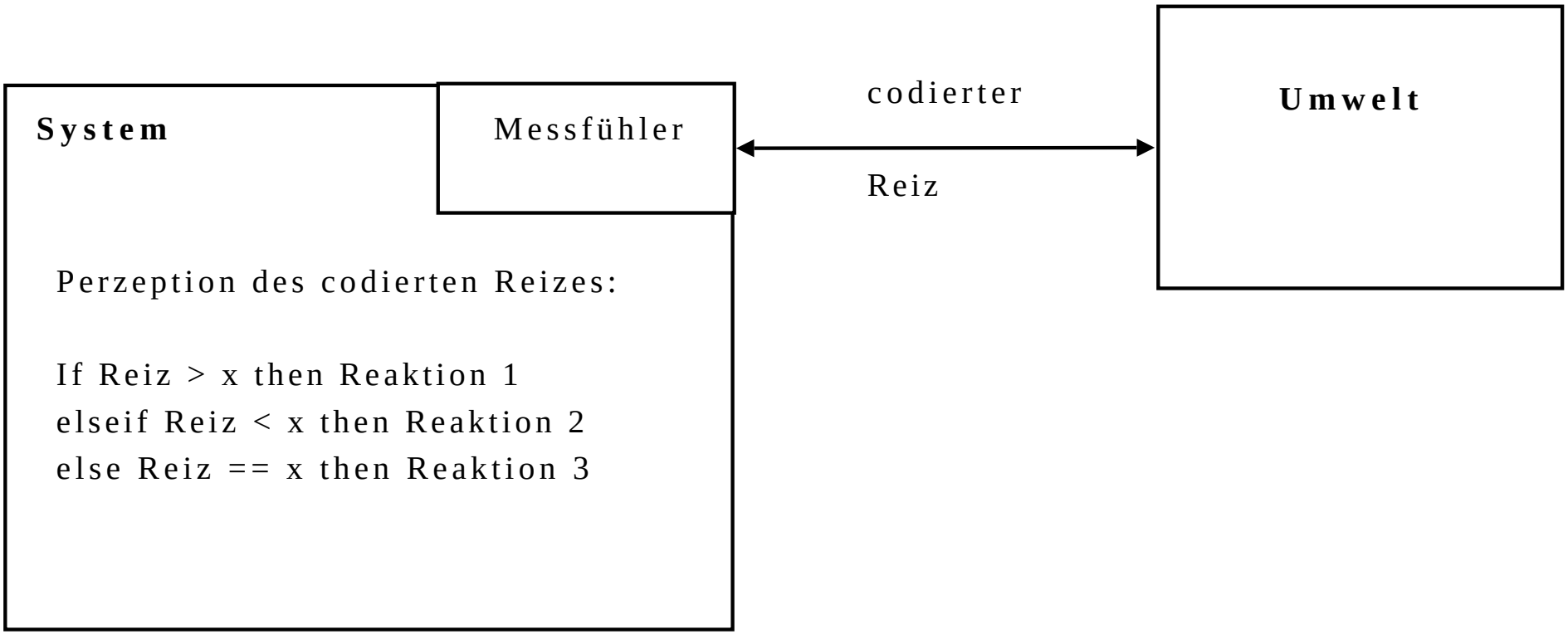
Das System nimmt über den Messfühler einen Reiz wahr



解釈人

Grundidee des kybernetischen Regelkreises

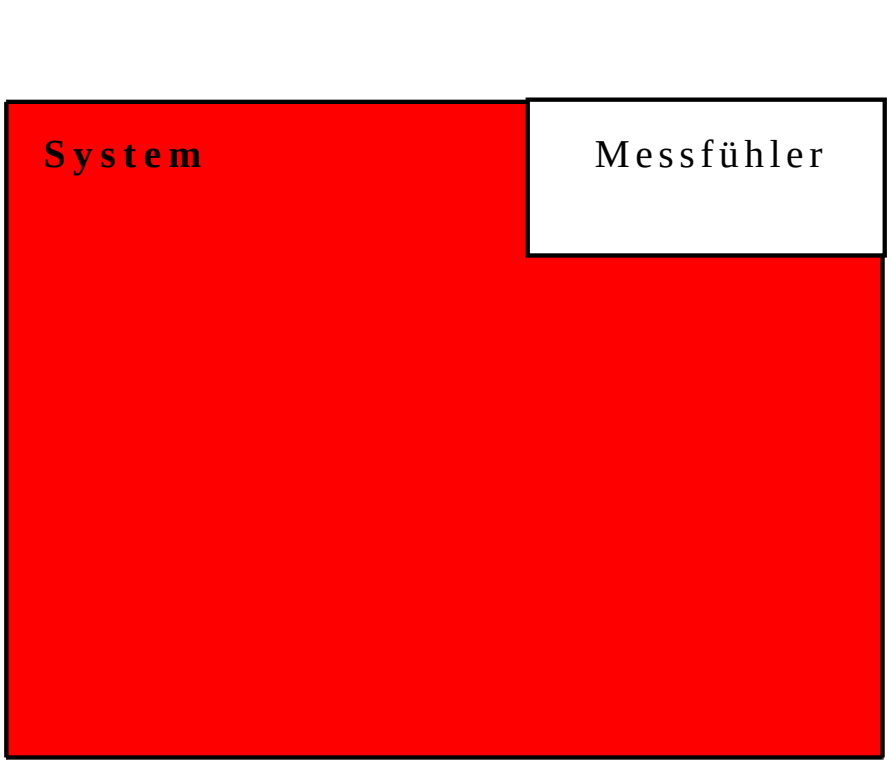
Das System reagiert auf den Reiz und verändert sich

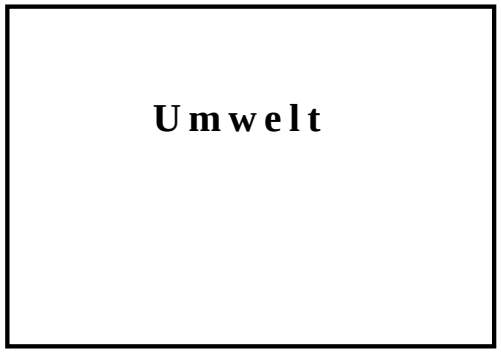


解釈人

Grundidee des kybernetischen Regelkreises

Das System entspricht nun nicht mehr dem System aus 1.





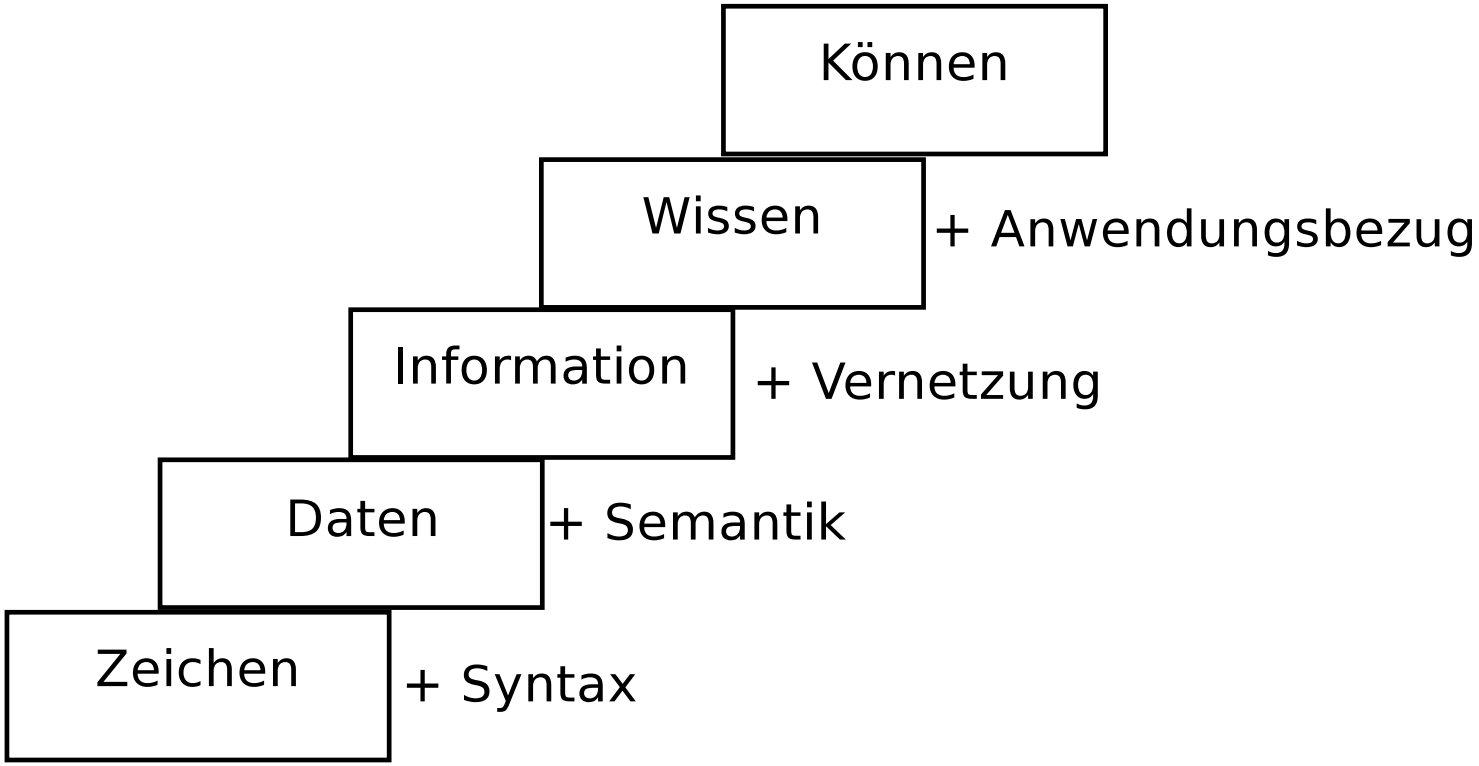
解釈人

Weltwahrnehmung

1. Das System muss seine Umwelt wahrnehmen.
2. Die wahrgenommene Umwelt muss verarbeitet werden (Diagnose), dazu muss Wissen bzw. Erfahrung über stattgefundene Sicherheitsvorfälle (post mortem) aufgebaut werden.
3. Mit der aktuell wahrgenommenen Umwelt kann anhand des erstellten Erfahrungsrahmen ein Sicherheitsvorfall, der erst noch stattfinden wird, prognostiziert werden.

解釈人

Wissenstreppe



解釈人

Table of Contents

1 Intro

2 Kybernetik

3 Genetische Epistemologie

4 Konsequenzen

解釈人

Entwicklungspsychologie

- Biologe Jean Piaget (1896 – 1980)
- interessiert darin, wie Menschen Erkenntnis erzeugen
- untersuchte Kinder und deren Entwicklung
- entwickelte die genetische Epistemologie
- beschrieb die Entwicklung des Kindes sowie des Geistes der Kinder
- begründete damit die Entwicklungspsychologie und indirekt die Pädagogische Psychologe (Aebli)

解釈人

Der Begriff »genetisch«

- Darwin führte den Begriff der Entwicklung als Evolution/Epigenetik ein
- Entwicklung ist ein Prozess, der *neue* Strukturen und Eigenschaften aus Genen erzeugt
- dabei werden neue Fähigkeiten erzeugt
- Evolution hat keinen bestimmbaren Beginn und kein bestimmbares Ende

解釈人

Struktur

- zentraler theoretischer Begriff der genetischen Epistemologie
- Kern der Entwicklung
- bestimmt die Entwicklungsrichtung vor
- inspiriert vom biologischen Holismus (Ganzheit)
- führte zur kybernetischen Theorie der Äquilibration (Gleichgewicht)
- Strukturen beschreiben Kognition über allgemeine Formen
- und Erkenntnis über ihr internes Schema
- Strukturen beschreiben wie Kognition organisiert ist

解釈人

Struktur

- Piaget beschreibt den menschlichen Geist als Organismus, der von seiner Umwelt unterschieden ist, aber mit ihr interagiert (strukturelle Kopplung nach Maturana/Varela)
- allgemein sind Strukturen Systeme von Beziehungen zwischen ihren Elementen und zwischen den Elementen und dem Ganzen.
- nicht-statisch, selbstorganisierend
- Das Ganze ist mehr als die Summe seiner Teile.
- Kognition ist mehr als die Summe einer Wahrnehmung.
- Eine Struktur kann angewendet werden auf Denken und Welt, Geist und Materie
- Jede Struktur ist das Moment einer unabgeschlossenen *und* unabschließbaren Konstruktion

解釈人

Assimilation & Akkomodation

- Wie werden Strukturen erzeugt und aktualisiert?
- grundlegende Strukturen werden durch die »Hardware« erzeugt (Gehirn, Organe, CPU)
- Strukturen assimilieren Objekte
- Objekte akkomodieren Strukturen
- Assimilation (Angleichung): Subjekt benutzt strukturen auf Objekte, die in die Strukturen assimiliert werden.
- Akkomodation (Anpassung): Objekte akkomodieren Strukturen
- Assimilation und Akkomodation bedingen einander
- jede Handlung beinhaltet Assimilation und Akkomodation
- Perzeption organisiert Ereignisse in der Umwelt mithilfe der bestehenden Perzeptionsstrukturen

解釈人

Menschliche Entwicklung









解釈人

Lernmotivation

- Piaget schuf keine Theorie der Lernmotivation
- Er ging davon aus, das die Strukturen äquilibriert sein sollen
- äquilibrierte Strukturen sind störungsunanfälliger
- nicht-äquilibrierte (perturbierte) Strukturen führen zu kognitiven Konflikten
- Strukturen werden Schritt für Schritt erweitert
- jede höhere Struktur ist mächtiger als ihr Vorgänger
- Warum will ein Computerprogramm lernen

解釈人

Lernmotivation

- Piaget schuf keine Theorie der Lernmotivation
- Er ging davon aus, das die Strukturen äquilibriert sein sollen
- äquilibrierte Strukturen sind störungsunanfälliger
- nicht-äquilibrierte (perturbierte) Strukturen führen zu kognitiven Konflikten
- Strukturen werden Schritt für Schritt erweitert
- jede höhere Struktur ist mächtiger als ihr Vorgänger
- Warum will ein Computerprogramm lernen

解釈人

reflektive Abstraktion

- Kognition ist mehr als Datensammlung
- reflektive Abstraktion nutzt Reflektion und Konstruktion
- Menschen müssen über ihre eigenen Strukturen reflektieren
- und darüber, wie die Erfahrung und Wahrnehmung beeinflussen
- Nach der Reflektion können neue Strukturen aufgebaut werden
- jeder Entwicklungsschritt wird von älteren Strukturen beeinflusst

解釈人

Table of Contents

1. Intro
2. Kybernetik
3. Genetische Epistemologie
4. Konsequenzen

解釈人

Konsequenzen

- Erkenntnisfähigkeit führt zu Identität
- Jedes IDS wird damit einzigartig sein $\rightsquigarrow$ (Un)-Vergleichbarkeit
- ein IDS kann einen Einbruch erkennen, ein anderes nicht
- Kompetenzdiagnostik benötigt
- Bewerbungsgespräche mit IDS?
- ein erkenntnisfähiges IDS hat die *Möglichkeit* einen neuen Angrifff zu erkennen

解釈人

Er-lernen neuer Fähigkeiten

- »echtes« Lernen ist notwendig, um Handlungskompetenz aufzubauen
- Lernen erfordert immer eine Rückkoplung
- man kann nicht von einem nicht-identifizierten Angriff lernen
- wir haben also immer noch das diagnostische Problem ...
- und unsere Datenbasis besteht aus schlechten (erkannten) Angriffen

解釈人

Lerntheorie: Behaviorismus

- Beeinflusst von Pawlow
- B.F. Skinner: Operante Konditionirung mit Ratten, Katzen, Hunden
- Norbert Wiener: Theory of Cybernetics
- Lernen als einfache Reiz-Reaktions-Kette

解釈人

Lerntheorie: Behaviorismus

- Beeinflusst von Pawlow
- B.F. Skinner: Operante Konditionirung mit Ratten, Katzen, Hunden
- Norbert Wiener: Theory of Cybernetics
- Lernen als einfache Reiz-Reaktions-Kette

1. lehre die Information
2. gib dem Lerner Zeit zum verstehen
3. stelle eine Frage bezgl. des Lerninhalts
4. gebe Rückmeldung auf Grundlage der Antwortqualität
5. Wiederhole ...

解釈人

Lerntheorie: Behaviorismus

- Beeinflusst von Pawlow
- B.F. Skinner: Operante Konditionirung mit Ratten, Katzen, Hunden
- Norbert Wiener: Theory of Cybernetics
- Lernen als einfache Reiz-Reaktions-Kette

1. lehre die Information
2. gib dem Lerner Zeit zum verstehen
3. stelle eine Frage bezgl. des Lerninhalts
4. gebe Rückmeldung auf Grundlage der Antwortqualität
5. Wiederhole ...

解釈人

Arbeitshypothesen

- Sicherheit ist ein latentes soziales Konstrukt
- Unterteilung in trivialer ./. trivialisierter ./. nicht-trivialisierbarer Vorfall
- Diagnose/Prognose können nur Menschen
- Turingmaschinen können keine Entscheidung treffen $\rightsquigarrow$ Operationen nur in trivialen/trivialisierten Vorfällen
- Computer sind nur Werkzeuge
- Sicherheit ist eine Dimension der Organisationskultur

解釈人

Fragen?
Stefan.Schumacher@Kaishakunin.com

解釈人