Risiko Kommunikation

Lukas Aldag,
KIT AIFB SECUSO

INSTITUT FÜR ANGEWANDTE INFORMATIK UND FORMALE BESCHREIBUNGSVERFAHREN (AIFB)
FORSCHUNGSGRUPPE SECURITY · USABILITY · SOCIETY (SECUSO)

Inhalt

- Intro
- Risiko Kommunikation?
- Risiko?!
- Extended Parallel Processing Model
- Andere Möglichkeiten? Tools!
- UMISPC
- Wie erzeugt eine Nachricht Legitimität?
  Pathos, Logos, Ethos
- Die „dunkle“ Seite
- Zusammenfassung

SECurity Usability SOciety

- Lukas Aldag
  - MSc. Psychologie, University of Twente, Enschede
  - Human Factors Engineering
  - Bei SECUSO seit Februar 2019

- Fokus: Human Factors in Security und Privacy
  - Security und Privacy Awareness Maßnahmen
  - Usable Security und Privacy Tools

- Anwendungsbereiche:
  - Authentifizierung (Passwörter, 2FA,…)
  - Kommunikation (E-Mail, Messangers,…)
  - Web
  - Smarthome/Health
  - Banking
  - Wahlen

Risiko Kommunikation?

Risiko Kommunikation

Definition:

Risk communication refers to the exchange of real-time information, advice and opinions between experts and people facing threats to their health, economic or social well-being. The ultimate purpose of risk communication is to enable people at risk to take informed decisions to protect themselves and their loved ones. Risk communication uses many communications techniques ranging from media and social media communications, mass communications and community engagement. It requires a sound understanding of people's perceptions, concerns and beliefs as well as their knowledge and practices. It also requires the early identification and management of rumours, misinformation and other challenges.

WHO: https://www.who.int/risk-communication/background/en/

Risiko Kommunikation

Definition:

Risk communication refers to the exchange of real-time information, advice and opinions between experts and people facing threats to their health, economic or social well-being. The ultimate purpose of risk communication is to enable people at risk to take informed decisions to protect themselves and their loved ones. Risk communication uses many communications techniques ranging from media and social media communications, mass communications and community engagement. It requires a sound understanding of people's perceptions, concerns and beliefs as well as their knowledge and practices. It also requires the early identification and management of rumours, misinformation and other challenges.

WHO: https://www.who.int/risk-communication/background/en/

Risiko Kommunikation

- Ziele der Risiko Kommunikation?

- Awareness erhöhen
- Schützendes Verhalten anregen
- Informieren
  - Risiken und Gefahren
  - Akzeptanz von Risiko und Management Maßnahmen
  - Richtiges Verhalten
- Warnungen vor anstehendend und derzeitigen Ereignisses
- Beruhigen
- Vertrauen aufbauen
- Dialog und Verständnis
- Einbeziehen in Entscheidungen

Wieso Risiko Kommunikation in Cyber-Security?

Wieso Risiko Kommunikation in Cyber-Security?

- Fehlende Awareness
  - Phishing
  - Passwort Policy
  - Datensicherung
- Fehlendes Wissen → Informieren
  - Wann ist eine Situation „gefährlich“? → Awareness
  - Wie kann man ich mich schützen?
    - Tatsächliche Ausführung des Verhaltens! → Schützendes Verhalten
  - Was kann ich tun wenn etwas passiert ist?
  - Wen kann ich kontaktieren? → Vertrauen aufbauen

Risiko?! → Was ist gefährlich(Risiko Szenario)?

Risiko?!

Activity or technology	League of Women Voters	College students	Active club members	Experts
Nuclear power	1	1	8	20
Motor vehicles	2	5	3	1
Handguns	3	2	1	4
Smoking	4	3	4	2
Motorcycles	5	6	2	6
Alcoholic beverages	6	7	5	3
General (private) aviation	7	15	11	12
Police work	8	8	7	17
Pesticides	9	4	15	8
Surgery	10	11	9	5
Fire fighting	11	10	6	18
Large construction	12	14	13	13
Hunting	13	18	10	23
Spray cans	14	13	23	26
Mountain climbing	15	22	12	29
Bicycles	16	24	14	15
Commercial aviation	17	16	18	16
Electric power (non-nuclear)	18	19	19	9
Swimming	19	30	17	10
Contraceptives	20	9	22	11
Skiing	21	25	16	30
X-rays	22	17	24	7
High school and college football	23	26	21	27
Railroads	24	23	29	19
Food preservatives	25	12	28	14
Food coloring	26	20	30	21
Power mowers	27	28	25	28
Prescription antibiotics	28	21	26	24
Home appliances	29	27	27	22
Vaccinations	30	29	29	25

Slovic, P. (1987). Perception of risk. *Science*, *236*(4799), 280-285.

Risiko?!

Activity or technology	League of Women Voters	College students	Active club members	Experts
Nuclear power	1	1	8	20
Motor vehicles	2	5	3	1
Handguns	3	2	1	4
Smoking	4	3	4	2
Motorcycles	5	6	2	6
Alcoholic beverages	6	7	5	3
General (private) aviation	7	15	11	12
Police work	8	8	7	17
Pesticides	9	4	15	8
Surgery	10	11	9	5
Fire fighting	11	10	6	18
Large construction	12	14	13	13
Hunting	13	18	10	23
Spray cans	14	13	23	26
Mountain climbing	15	22	12	29
Bicycles	16	24	14	15
Commercial aviation	17	16	18	16
Electric power (non-nuclear)	18	19	19	9
Swimming	19	30	17	10
Contraceptives	20	9	22	11
Skiing	21	25	16	30
X-rays	22	17	24	7
High school and college football	23	26	21	27
Railroads	24	23	29	19
Food preservatives	25	12	28	14
Food coloring	26	20	30	21
Power mowers	27	28	25	28
Prescription antibiotics	28	21	26	24
Home appliances	29	27	27	22
Vaccinations	30	29	29	25

Slovic, P. (1987). Perception of risk. *Science*, *236*(4799), 280-285.

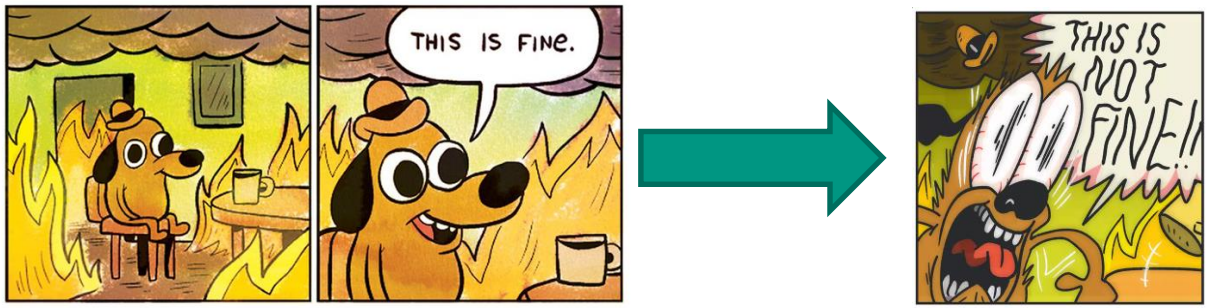
Risiko?!

- Paul Slovic (1987)
  - Risiko Bewertung
    - Experten
    - → Quantitative Analyse der Erkrankungsrate, Tötlichkeitsfaktor, finanzieller oder anderweitiger Verlust
    - Laie
    - → „Komplexere“ Analyse: Mentale Strategien und Heuristiken, soziale Gruppen, Wahrscheinlichkeit, Wahrnehmung, etc.
  - Was führt zu Problemen? Experte vs. Laie?

Slovic, P. (1987). Perception of risk. *Science*, *236*(4799), 280-285.

Risiko?!

- Paul Slovic (1987)
  - Objektiv vs. Subjektiv
  - Laien
    - Fehlende Erfahrung
    - Kognitiver Bias
    - Gruppen Effekte
- Ziel der Kommunikation: Wahrnehmung einer möglichen Gefahr



Slovic, P. (1987). Perception of risk. *Science*, *236*(4799), 280-285.

Extended Parallel Processing Model

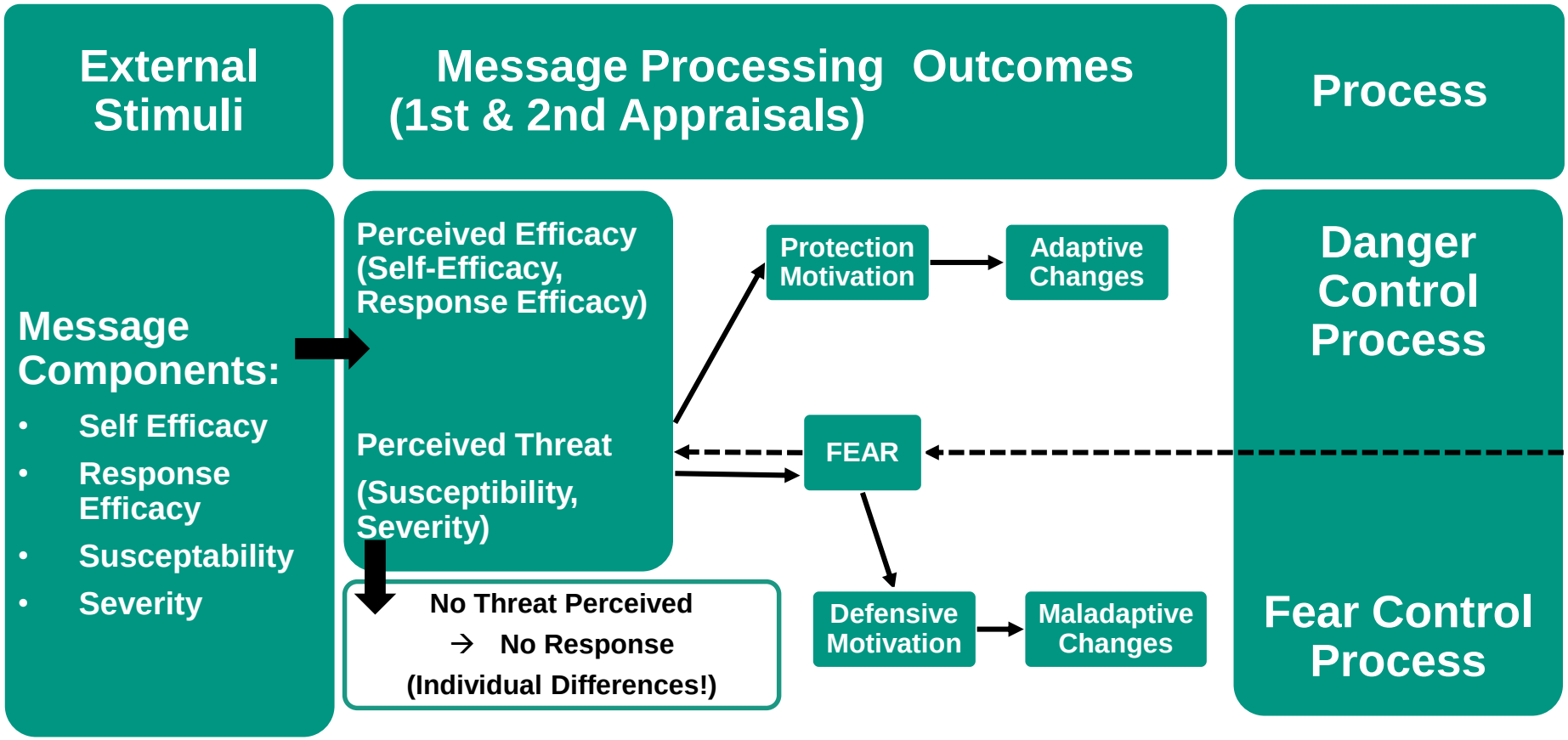
Extended Parallel Processing Model

- Was ist ein Fear Appeal?
- Fear Appeal ist nötig aber zu welchem Grad?

- Das sollte nicht passieren
  - Zu viel Angst kann sich negativ auswirken!
- Was ist das Ziel?

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs*, *59*(4), 329-349.

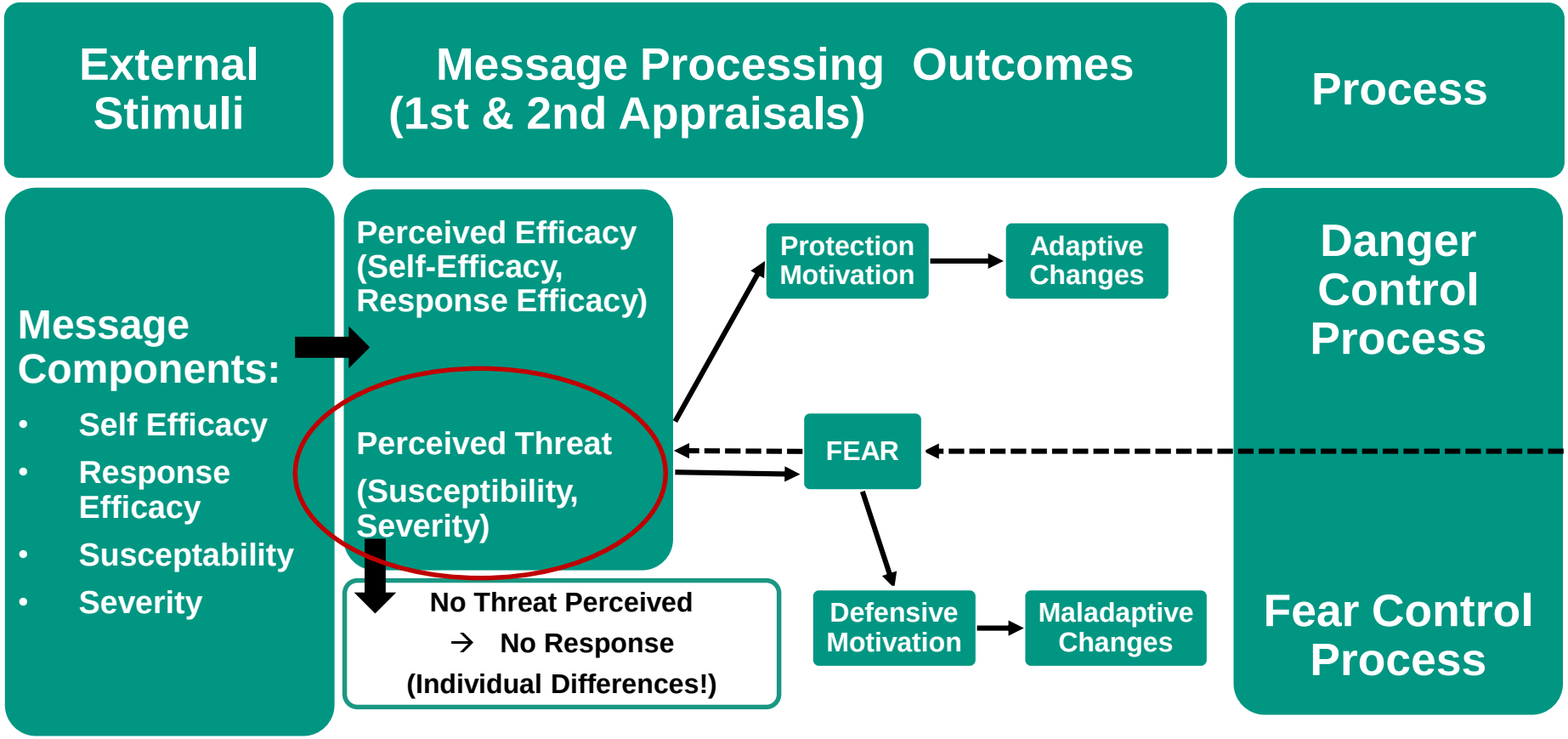
Extended Parallel Processing Model



- Was ist die erste und zweite Bewertung?

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs*, *59*(4), 329-349.

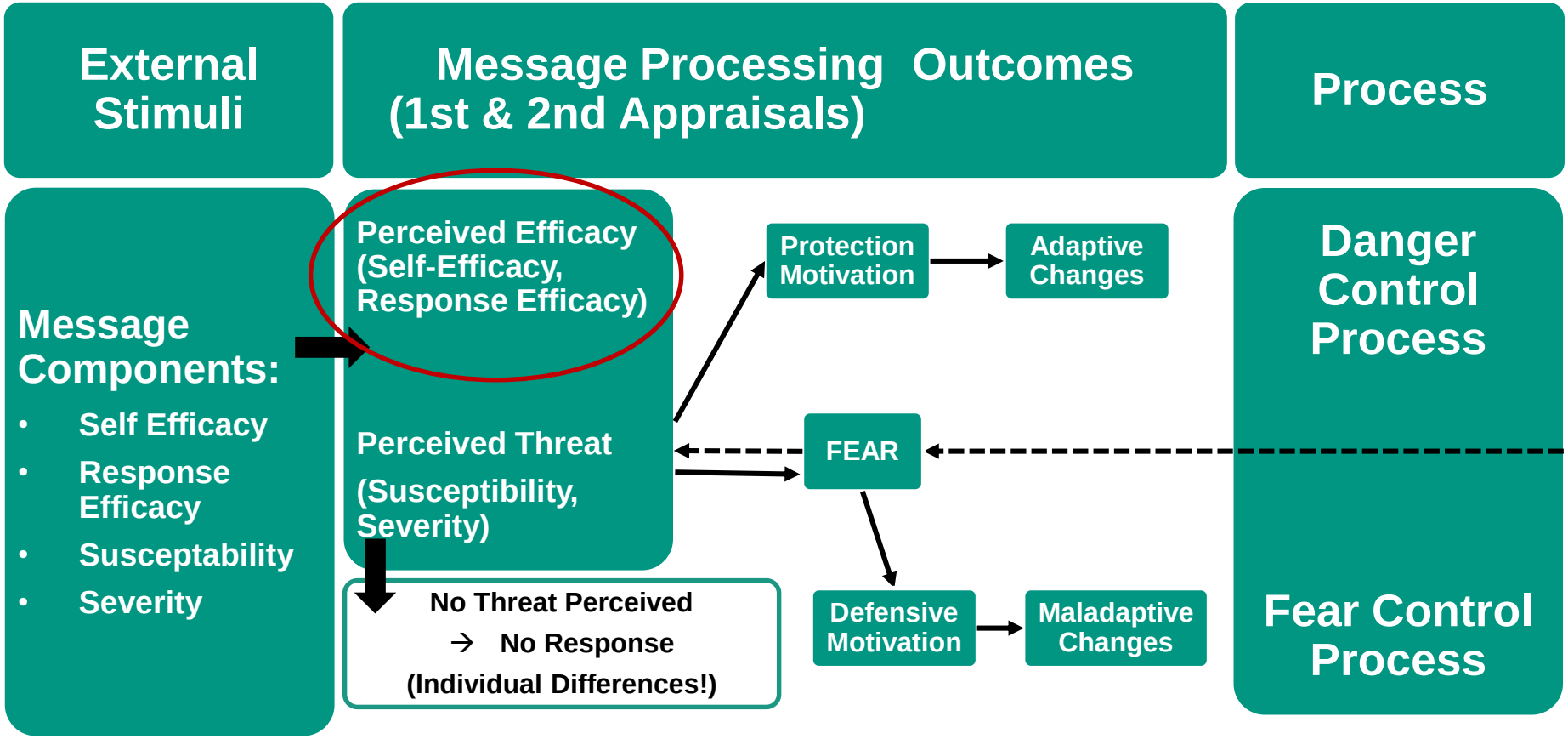
Extended Parallel Processing Model
1. Bewertung: Wahrgenommene Gefahr



- Susceptibility: Bin ich in Gefahr? → Nein: Keine Reaktion
- Severity: Könnte es mir schaden? → Ja: 2. Beurteilung

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs*, *59*(4), 329-349.

Extended Parallel Processing Model
2. Bewertung: Wahrgenommene Effektivität



- Eigen- und Repons Effektivität ist gegeben? → Ja: Danger Control Process(effektiv)
  → Nein: Fear Control Process (nicht effektiv)
- Bei Fear Control: ignorieren, vermeiden, keine Reaktion (Überforderung)

Extended Parallel Processing Model

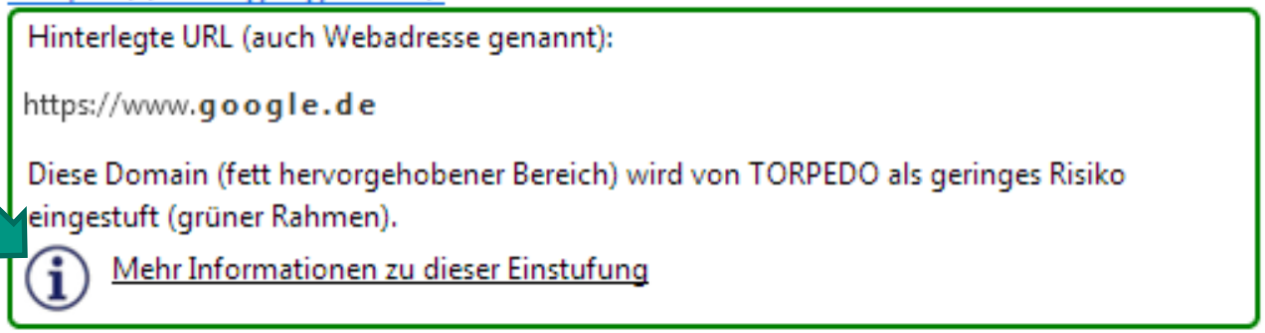
- Wo liegen die Probleme bei Cyber Security?
  - Wahrnehmung Physische und Digitale Welt
  - Risiken sind teilweise schwer zu erkennen bis es tatsächlich zu spät ist!
- Was kann man noch machen?
  - Automatische Updates
  - Sicherheitseinstellungen standardmäßig auf an gestellt
  - Usable Security
    - Tools (PassSec, Torpedo → https://secuso.aifb.kit.edu/642.php)
  - Verursacher bekämpfen

Andere Möglichkeiten? Tools!

TORPEDO – Erkennen von gefährlichen Links

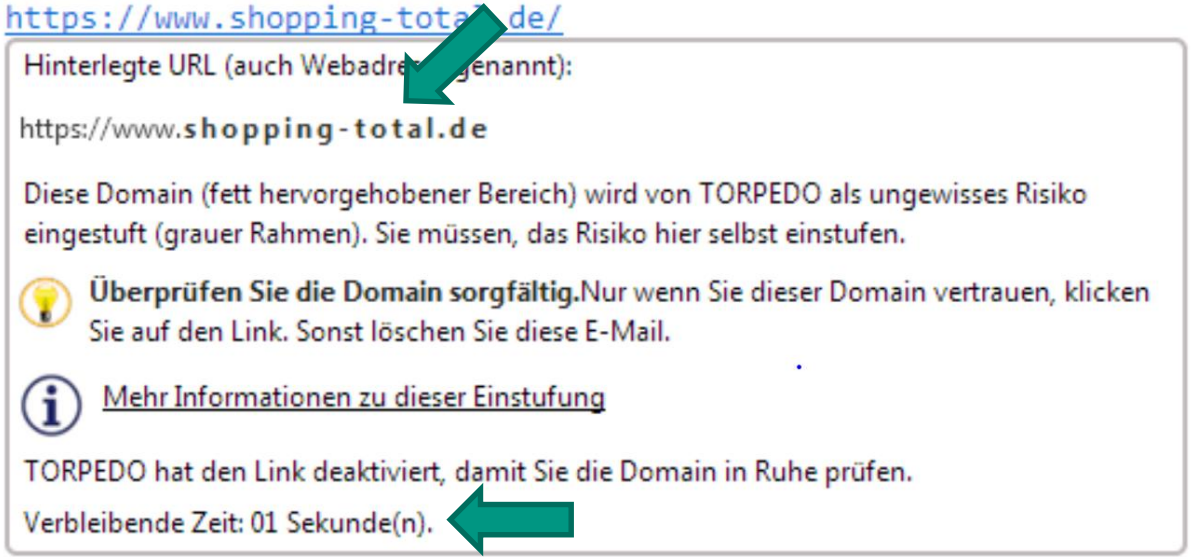
- Bekannte Webseite

https://www.google.de/



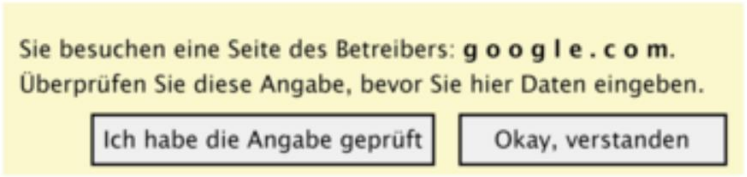
- Unbekannte Webseite oder http

https://www.shopping-total.de/



Schutz von Passwörtern, Zahlungsdaten und Privatsphäre

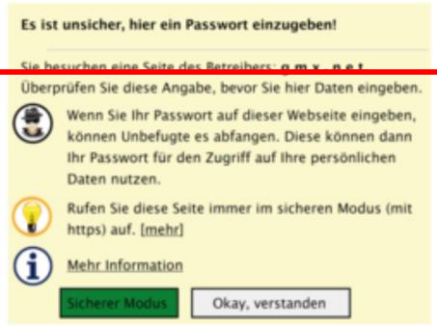
- Gesicherte aber unbekannte Seite, Domain wird nochmal gesonder angezeigt



- Nach Überprüfung

Wahrgenommene Gefahr = Symbol
Wahrgenommene Effektivität = Zusatzinformationen und Handlung (bei Bedarf)

- Webseite ohne sichere Verbindung, weitere Informationen warum nicht sicher und Handlungsempfehlung



Unified Model of Information Security Policy Compliance UMISPC

UMISPC

- Mehr Nutzung von IT
  - Digitale Daten sind einfacher zu transferieren
  - Gut und schlecht!
- Es ist wichtig diese Daten zu schützen!
- Startpunkt dafür ist eine Sicherheit Policy
- Beachtet und folgt ihr allen Policies?
- Angestellte folgen selten den entsprechenden ISS (Information systems security) Policies
  - Teilweise bevorzugen sie das unsichere Verhalten, obwohl sie das richtige kennen!
- Wieso?

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*(1).

UMISPC

- Zusammenfassung von verschiedenen Theorien:
  - Theory of reasoned action
  - Neutralization techniques
  - Health belief model
  - Theory of planned behavior
  - Theory of interpersonal behavior
  - Protection motivation theory
  - Extended protection motivation theory
  - Deterrence theory and rational choice theory
  - Theory of self regulation
  - Extended parallel processing model
  - Control balance theory

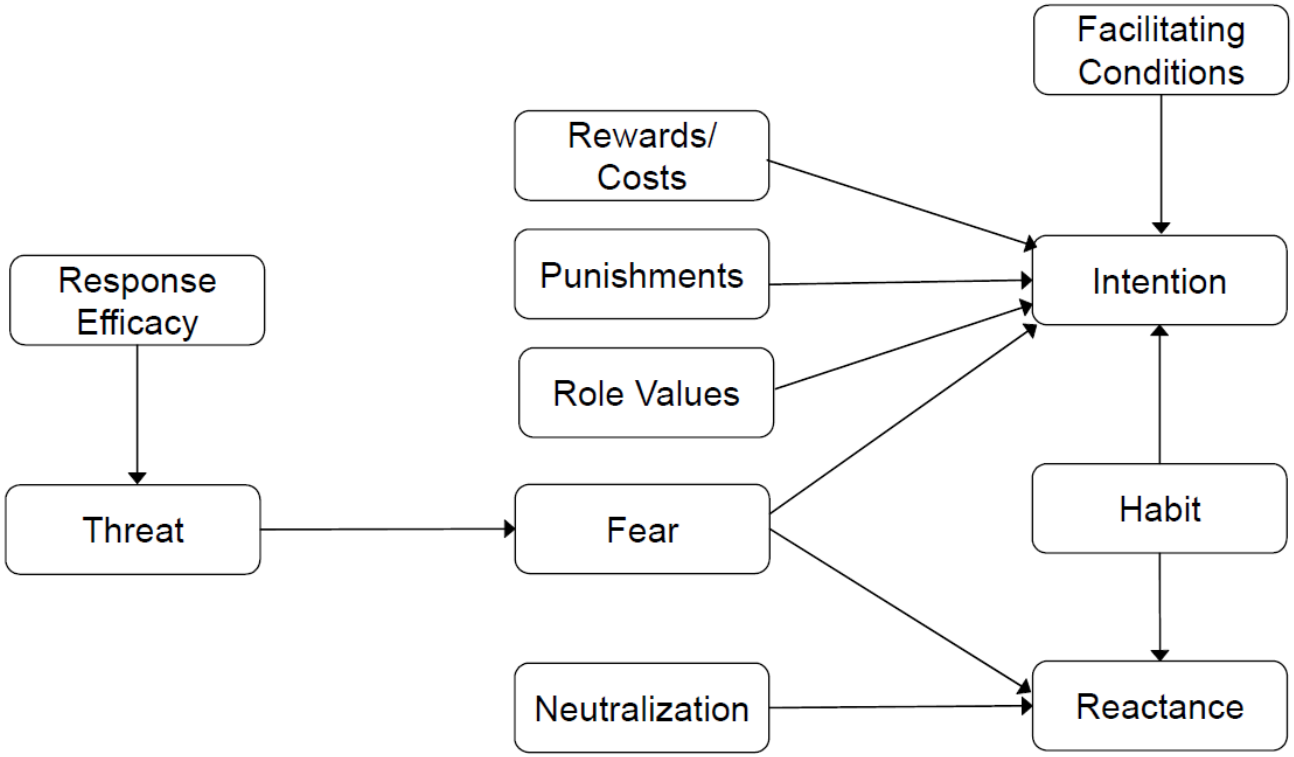
Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*(1).

UMISPC

- Vergleichen der Konstrukte und deren Faktoren
  - 11 wichtige Faktoren aus allen Theorien
- Role values: Regel wird als legitim und wichtig anerkannt
- Punishment: Wer gegen Regel verstößt wird „bestraft“
- Rewards/costs: Positive Verstärkung bei konformen Verhalten zu den Regeln
- Habit: Tendenz Änderungen zu akzeptieren
- Neutralization: Rationales Denken, abweichendes von konformen Verhalten zu unterscheiden
- Threat: Wahrnehmung der Schwere und Wahrscheinlichkeit einer Gefahr
- Fear: Negative Respons gegenüber einem Stimuli
- Response efficacy: Wahrgenommene Effektivität von Verhalten darin eine Gefahr zu umgehen oder abzuschwächen
- Facilitating conditions: Potential, das Individuen ohne Hilfe zurecht kommen
- Reactance: Leugnen eines ISS Problems
- Intention: Aufnahme eines gewünschten Verhaltens

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*(1).

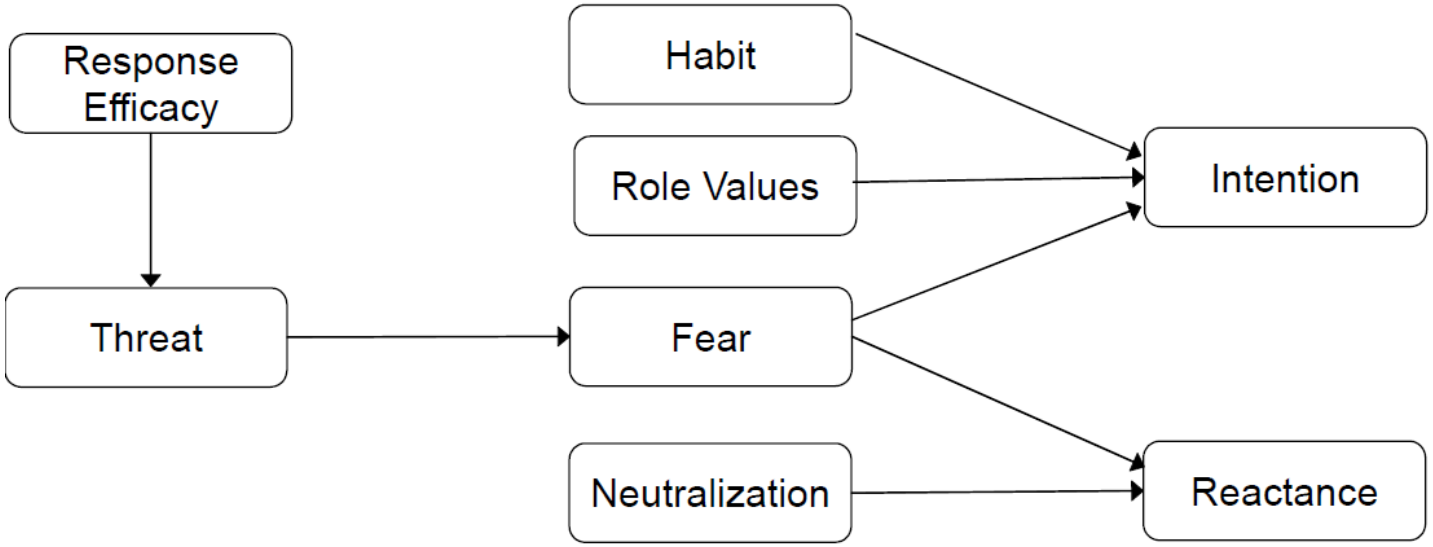
UMISPC



- Ziel ist es Intention zu erzeugen
  - Leute dazu bewegen gewisses Verhalten zu übernehmen
- Vermeiden von Reactance

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*(1).

UMISPC



- Nach Studie war es möglich, das Model weiter zu „verfeinern“
- Fokus auf die wichtigsten Faktoren

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*(1).

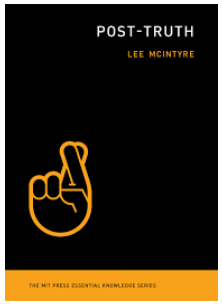
Wie erzeugt eine Nachricht Legitimität (justification)?
Pathos, Logos, Ethos

Pathos, Logos, Ethos → A rhetorical theory of diffusion

- Warum muss eine Nachricht Legitimität besitzen/erzeugen?
  - Durch eine Rechtfertigung neigen wir dazu gegebene Dinge zu akzeptieren
  - Wichtig für Aufbau von Vertrauen
- Viele Theorien die sich mit Informationsverteilung auseinander setzten betrachten selten den Rhetorischen Einfluss
  - Da oft unterschätzt
- Rationalität wird beeinflusst durch die Fähigkeit Gründe zu nennen
  - Dauerhaft entsteht eine Rechtfertigung

- Ein Text, der wenig überzeugend ist wird keine große Wirkung erzielen!
  - Bsp.: Politiker, Zeitung, Wissenschaftler, Awareness Kampagnen
    - Es spielen jeweils noch andere Faktoren mit hinein → Post Truth Ära (Post-Truth, Lee McIntyre)

- Wichtigste Ziel einer Institution ist es als selbstverständlich zu gelten



Green Jr, S. E. (2004). A rhetorical theory of diffusion. *Academy of management review*, *29*(4), 653-669.

Pathos, Logos, Ethos → A rhetorical theory of diffusion

Unterschiedliche Rechtfertigungen

- Pathos
  - Beeinflussen der Emotionen
  - Erzeugen wirksame aber nicht anhaltende Aktionen
  - Kann genutzt werden aufgrund Gier oder Angst von Zuhörer
  - Bsp.: Fear-Appeal

- Logos
  - Logische Rechtfertigung
  - Methodische Analyse des Mittels und Zwecks
  - Zeigt die Effektivität und Effizienz auf

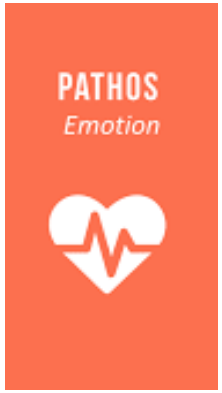
- Ethos
  - Rechtfertigung auf Grund von Moral und Ethik
  - Manche Forderungen können so gegen die eigenen Interessen legitimiert werden
  - Entscheidungen gegen das Individuum und für das Allgemeinwohl

Green Jr, S. E. (2004). A rhetorical theory of diffusion. *Academy of management review*, *29*(4), 653-669.

Pathos, Logos, Ethos → A rhetorical theory of diffusion

Pathos

- Zuhörer besitzen nur eine gewisse Aufmerksamkeit!
- Individueller Widerstand und Gruppen Konformität verhindern eine Änderung des Verhaltens
- Durch Begeisterung und Vorstellungskraft kann diese Aufmerksamkeit eingefangen werden und so zu einer Bewegung genutzt werden



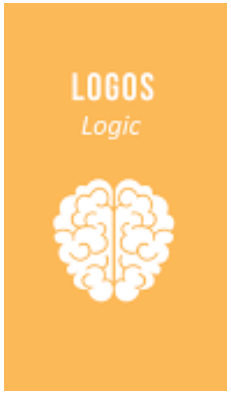
- Ein Einsatz von Pathos hat eine hohe Aufnahmerate, jedoch nach kurzer Zeit geprägt von hoher Ablehnung

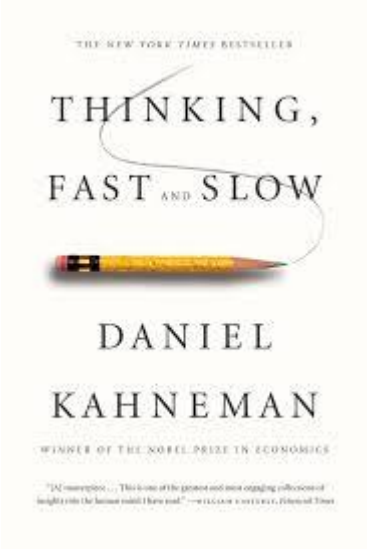
Green Jr, S. E. (2004). A rhetorical theory of diffusion. *Academy of management review*, *29*(4), 653-669.

Pathos, Logos, Ethos → A rhetorical theory of diffusion

Logos

- Baut pragmatische Rechtfertigung/Legitimität auf
- Braucht länger um Aufmerksamkeit der Zuhörer zu bekommen
  - Da ein energieaufwendigeres System angesprochen wird
  - Kahnemans: „Thinking fast and slow“
- Weniger effektiv im Vergleich zu Pathos
  - Aber länger anhaltend, da logisch begründet
- Mittlere Aufnahme und mittlere Ablehnung





Green Jr, S. E. (2004). A rhetorical theory of diffusion. *Academy of management review*, *29*(4), 653-669.

Pathos, Logos, Ethos → A rhetorical theory of diffusion

Ethos

- Rechtfertigung durch akzeptierte Normen und Werte
- Ist am stärksten und hält am längsten
  - Wieso?
- Hat den meisten Einfluss auf Selbstverständlichkeit
- Spricht auch das langsame Denksystem an
  - Da mehr verarbeitet werden muss

- Langsame Akzeptanz aber auch langsame Ablehnung

Green Jr, S. E. (2004). A rhetorical theory of diffusion. *Academy of management review*, *29*(4), 653-669.

Pathos, Logos, Ethos → A rhetorical theory of diffusion

Unterschiede

- Pathos und Logos
  - Erzeugen pragmatische Rechtfertigung
  - Appelliert an die Eigeninteressen

- Ethos
  - Erzeugt moralische Rechtfertigung
  - Normative Zustimmung und moralischer Anstand

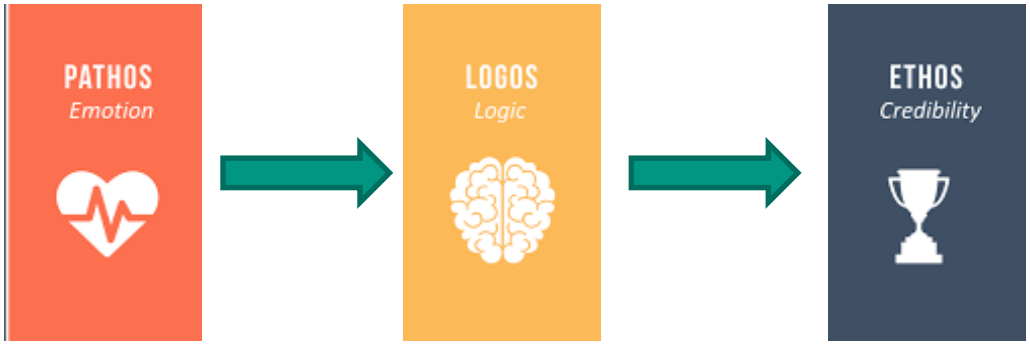
- Über Zeit wird eine kognitive Rechtfertigung/Legitimität erzeugt
  - Ergebnis: Selbstverständlichkeit

Green Jr, S. E. (2004). A rhetorical theory of diffusion. *Academy of management review*, *29*(4), 653-669.

Pathos, Logos, Ethos → A rhetorical theory of diffusion

Macht es Sinn alle anzuwenden und in welcher Reihenfolge?

- Pathos
  - Schnelle Aufnahme, schnelles Abstoßen
- Logos
  - Mittlere Aufnahme aber längeres Beibehalten
- Ethos
  - Sehr langsame Aufnahme aber längstes Beibehalten



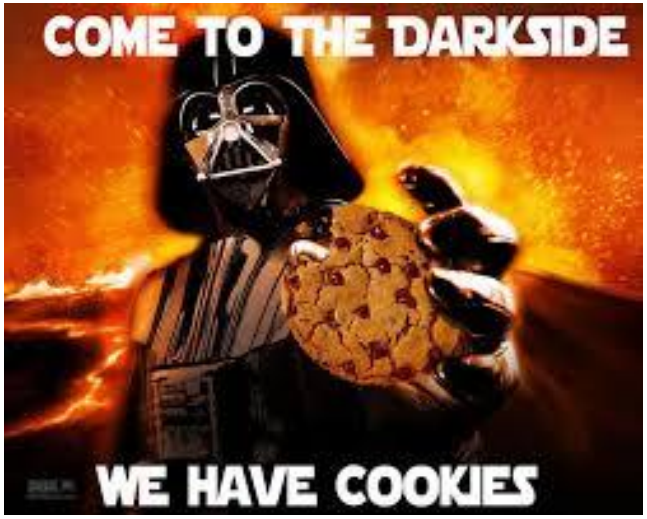
Green Jr, S. E. (2004). A rhetorical theory of diffusion. *Academy of management review*, *29*(4), 653-669.

Pathos, Logos, Ethos → A rhetorical theory of diffusion

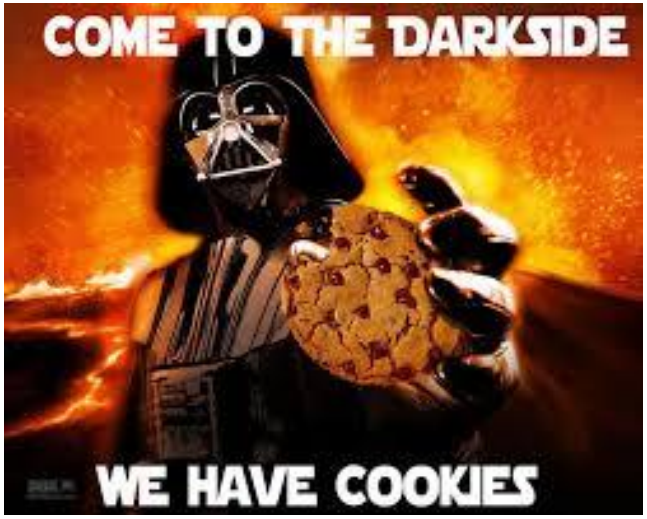
Kann man das auf jeden anwenden?

- Generell ja
- Aber
  - Kulturelle Differenzen
  - Individuelle Ziele und Bedürfnisse
  - Anpassen an Situation und Empfänger!

Green Jr, S. E. (2004). A rhetorical theory of diffusion. *Academy of management review*, *29*(4), 653-669.



Die „dunkle“ Seite



Welche Vorgehensweise wird hier verwendet?

Die „dunkle“ Seite

Wie kann das Wissen für schlechte Absichten genutzt werden?

- Social Engineering
  - Phishing

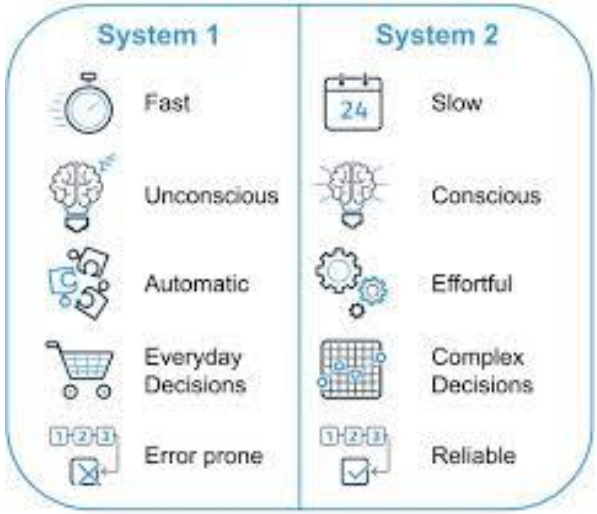
- Phisher versuchen meist das erste kognitive System anzusprechen → Kahneman

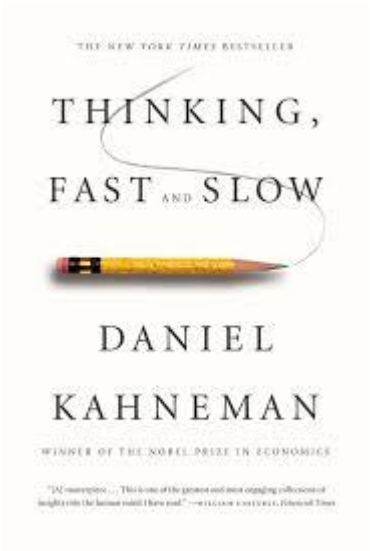
Exkurs: Kahneman, Thinking fast and slow

- Zwei Wege Entscheidungen zu treffen
  - System 1 = Intuition → Schnell und kosteneffizient
  - System 2 = Rationales Entscheiden → Zeit und kostenintensiv

- System 1 ist immer aktiv, System 2 weniger

- System 1 ist stark von kognitiven Bias beeinflusst!





Die „dunkle“ Seite

- Die typische Scam Mail

Extrinsic motivation
→ Ethos

Hello,

lett me introduce myself, I am Senator David Mark, the former Senate President of Nigeria. have retained my steemed office. I trust that you will keep everything I divulge to you under scams emanating from my country, I urge you to give me a benefit of doubt and work with n $12.8million into your custody under the guise of a valid contract payment owed to you so tl with my country.

I have a perfect plan on how we can carry this out under 3 weeks if you can give me your full willing to give you 30% of the contract payment sum. I will be ready to discuss more on your receive your return email with your consent to work with me in truth and honesty. I want to promise to deliver on it.

I hope we can discuss more on this matter soon as time is very essential and we need to act f

Please get back to me.
David.

Die „dunkle“ Seite

- Pathos, Ethos, Logos
- Extended Parallel Processing Model
- Ansprechen des ersten Systems, durch Aufbau von Angst (Kahneman)

Vertraute Institution

Pathos /Angst

Logos

Danger Control Process

PayPal
Sicherererer.

28.09.2013

Sehr geehrter Kunde,

Im Rahmen unserer Sicherheitsmaßnahmen prüfen wir regelmäßig alle Vorgänge im PayPal-System. Bei einer Überprüfung haben wir kürzlich ein Problem im Zusammenhang mit Ihrem Konto festgestellt.

Zu Ihrem Schutz haben wir den Zugriff auf Ihr Konto eingeschränkt, bis zusätzliche Sicherheitsmaßnahmen getroffen werden können. Wir bitten um Entschuldigung für eventuelle Unannehmlichkeiten.

Was mache ich jetzt ?
Bitte verifizieren Sie sich über folgenden Link durch einen Abgleich Ihrer Daten als rechtmäßiger Besitzer. Im Anschluss können Sie Ihr Konto wieder uneingeschränkt nutzen.

hier klicken

Mit freundlichen Grüßen
Ihr PayPal-Team

Zusammenfassung

- Risiko Kommunikation = Bevölkerung vor möglichen Risiken aufklären und richtiges Verhalten näher bringen
- Risiko Einschätzung von Experten und Laien ist grundsätzlich verschieden
- Extended Parallel Processing Model
  - Danger control process vs. Fear control process
- Andere Möglichkeit zum Informieren sind z.B. Tools
  - PassSec/Torpedo
- UMISPC
  - Versucht mehrere Verhaltens Theorien in einer zu vereinen
- Pathos, Logos, Ethos (Emotionen, Logik, Ethik)
- Jegliche Überzeugungsstrategien werden auch von Kriminellen verwendet und ausgenutzt