Risikokompetent

in der Welt - und im Cyberspace

Was wir aus der Corona-Krise für die Informationssicherheit lernen können.

Inhalt

Vorbemerkung

Jede Krise bietet auch Gelegenheiten.

Wir, die *Sicherheitsarbeiter*, versuchen ein komplexes Produkt unter die Leute zu bringen, das keiner braucht, *wenn alles normal funktioniert.* Menschen vertrauen von Natur aus darauf, dass das Normale normal ist und es einfach immer so weiter geht. Die Tatsache, dass „wir arbeiten und leben müssen in einer Welt, die gefährlich ist“, ist aus dem Blick geraten.

Die Corona-Krise gibt uns Sicherheitsarbeitern nun die Gelegenheit in die Hand, ein erlebbares und allen Betroffen bekanntes Narrativ für den Umgang mit Informationssicherheit und Datenschutz zu entwickeln.

Informationssicherheit ist unser digitales Immunsystem

„Viren in der analogen Welt verhalten sich genauso wie Viren in der digitalen Welt“

In der analogen (offline) Welt haben wir es zu tun mit

- Bakterien, Parasiten und Viren

In der digitalen (online) Welt haben wir es zu tun mit

- Trojanern, Würmern und Viren

was die Verbreitung betrifft, gibt es keinen wesentlichen Unterschied.

Aus der Corona-Krise kann man lernen

Die Corona-Krise *kann uns etwas beibringen*. Sie sagt uns:

1. Unsere Normalität hängt von einem funktionierenden Sicherheitssystem ab.
2. Das Sicherheitssystem kann zusammenbrechen, wenn es mit einem Ereignis konfrontiert wird, auf das es nicht vorbereitet war.
3. Unvorhersehbare und unbekannte Ereignisse sind ein Definitionsmerkmal komplexer Systeme. Das Sicherheitssystem wird zusammenbrechen und damit auch die gewohnte Normalität.
4. Ein Sicherheitssystem hat *drei Komponenten*: Prävention, Überwachung und Reaktion. Alle drei Komponenten müssen gut ausgedacht, ihre Abhängigkeiten verstanden und gut implementiert sein.
5. Systempannen sind unvermeidlich. Ein mächtiges Sicherheitssystem kann die Panne begrenzen, ein ohnmächtiges Sicherheitssystem führt zu grenzenlosem Versagen.

Vier Kompetenzen sind zu erlernen

Wie bei allem, was man am Ende aus eigener Kraft bewältigen will, müssen vier Kompetenzen erworben werden - von jedem Einzelnen und von der ganzen Gesellschaft:

1. es muss *Wissen über das Ereignis* generiert werden, das zur Krise *geführt* hat und *Wissen über das System*, das auf das Ereignis mit einer Krise *reagiert* hat.
2. die *Fähigkeiten und Fertigkeiten* erworben werden, mit denen das Ereignis und seine Folgen unter *Kontrolle* gebracht werden können.
3. es muss die *Motivation und die Einstellung* ausgebildet werden, um die nötigen Maßnahmen auch *anzuwenden* und *durchzusetzen*.

4 es müssen jene *Kommunikationsstrategien* entwickelt werden, die dazu führen, dass alle von der Krise Betroffenen *am selben Strick in dieselbe* (und richtige) *Richtung* ziehen.

Die wichtigste Lehre aus der Corona-Krise?

Die wichtigste Lehre aus der Corona-Krise ist wohl, dass man die Sicht auf die Welt, in der wir leben, ändern muss, wenn wir es nicht mit Ereignissen zu tun bekommen wollen, die Menschen, Nationen und die ganze Menschheit vor Probleme stellt, die nicht mehr bewältigt werden können.

Es gibt eine Weltsicht *vor* Corona und eine Weltsicht *nach* Corona:

1 Vor Corona:

Absolute *Priorität* haben die *Effizienz und Aufwands-armes Handeln*. *„Immer weiter, schneller, billiger.“* Wir haben die Zukunft im Griff, alles ist unter Kontrolle.

Gesundheit: unser Gesundheitssystem ist zu teuer. Da wird zu viel auf Reserve vorgehalten, die Auslastung muss besser sein. Das kann alles viel schlanker sein.

Digitalisierung: Informationssicherheit und Datenschutz ist übertrieben, *„sooo schlimm ist das alles nicht“.* Und außerdem kostet es und behindert den Fortschritt. Wenn etwas passiert, „*dann anderen, die es einfach nicht bringen. Wenn bei uns etwas passiert, dann wechsle ich den Arbeitgeber.“*

2 Nach Corona:

Absolute Priorität hat es, die Kontrolle über das private, öffentliche und wirtschaftliche Leben wieder zu erlangen. Und Vorsorge zu treffen, damit wir keinesfalls wieder in eine Situation wie diese geraten.

Gesundheit: Ein gutes Gesundheitssystem mit ausreichend Reserven und motivierten Mitarbeitern ist wichtig. Es schützt uns vor Infektionen, frühem und sinnlosem Tod von geliebten Menschen und vor Pandemien, die alles zum Erliegen bringen.

Digitalisierung: Informationssicherheit und Datenschutz sind wichtig. Sie schützen uns vor Malware, dem unwiederbringlichem Verlust überlebenswichtiger Informationen und Verfahren und vor digitalen Blackouts, die alles zum Erliegen bringen.

Informationssicherheit ist wie Gesundheit. Es gibt keinen Unterschied.

Die Corona-Krise hat uns Informationssicherheitsarbeitern ein wunderbares Narrativ in die Hand gegeben:

1 Informationssicherheit ist lästig. Sie macht Mühe, kostet Geld und nimmt wertvolle Zeit weg.

   Sich so zu verhalten, dass man sich nie und nirgends irgendeine Krankheit einfängt, ist lästig. Es ist mühevoll, man muss Desinfektionsmittel und eine kleine Hausapotheke dabei haben und man ist nie sicher, ob man es richtig macht.

2 Warum ist Informationssicherheit ein Zeitdieb? Um Informationssicherheit richtig zu machen, muss man sich in der IT-Technologie auskennen. Man muss wissen, wo jene Lücken in der Arbeitsabläufen sind, die zu Fehlern führen oder Kriminellen die Türe öffnen.

   Sich so zu verhalten, dass man vor allen bekannten und noch unbekannten Schädlingen (Bakterien, Mikroben, Viren) geschützt ist, muss man sich auskennen mit Biologie, Chemie und Medizin. Man muss wissen, wo die Schwachstellen im Verhalten sind, die zu Fehlern führen oder Infektionen die Türe aufmachen.

3 Warum lohnt es sich scheinbar nicht, all das Wissen, die Fähigkeiten und Fertigkeiten zu erwerben, und – das ist ganz schwer – die Motivation aufrecht zu erhalten, Wissen und Fähigkeiten und Fertigkeiten auch immer und in jeder Situation anzuwenden? Es passiert ja selten was - und wenn doch mal was passiert, dann gibt es IT-Spezialisten, die dafür sorgen, dass es nicht so schlimm wird.

   Man wird ja selten krank und wenn schon, dann gibt es Ärzte und die Notfallmedizin. Impfen schadet mehr als es nützt und Händewaschen beschädigt in der Hauptsache den natürlichen Säuremantel der Haut.

Unsere Unterstützungssysteme sind so gut, dass Lebensgefahr oft nicht mehr als Gefahr wahrgenommen wird. Sie wird gleichgültig ignoriert oder als nervenkitzelnde Bereicherung des Lebens wahrgenommen.

Informationssicherheit ist unser digitales Immunsystem

Das sind *Lernerfahrungen, die die Herausbildung sorgloser Denk- und Verhaltensweisen begünstigen:*

1) Erfolge (im Sinne positiver Verhaltenskonsequenzen), die mit geringem Aufwand, aus Glück oder Zufall erzielt wurden, bzw. **2)** wiederholt gefährliches Verhalten ohne negative Konsequenzen führen zu der **3)** kognitivaffektiven Monopolhypothese führen: *„Alles ist gut und wird auch (von selbst) gut bleiben".*

So wird die Erwartung bestärkt, dass:
a) positive Ereignisse auch in Zukunft ohne größeres Zutun eintreten, und **b)** negative Ereignisse für die eigenen Person dagegen nicht zu befürchten sind *(„Mich trifft es schon nicht").*[i]

Erlernte Sorglosigkeit *findet man im Gesundheitsverhalten der Menschen genauso pandemisch verbreitet wie in der Informationssicherheit.*

Wir wissen, wie es immer läuft. Aber es darf nicht weiter so laufen!

Der Beginn der COVID-19-Pandemie kann auf Ende Dezember 2019 datiert werden. Berichte, dass das Virus SARS-CoV-2 schon früher bekannt war, sind bisher nicht bestätigt (eines von vielen Gerüchten und Verschwörungstheorien, die im Umkreis der Krise entstanden sind). Was seither geschehen ist, folgt einem bekannten und psychologisch erklärbaren Ablauf.

1 *Desinteresse*: Man hört von Berichten, dass in China ein Virus ausgebrochen sein soll und eine Stadt abgeriegelt wurde. Wuhan? Wo ist das überhaupt? Hat das was mit uns zu tun? So weit weg.

2 *Verleugnung*: Man liest, dass sich der Virus auch nach Europa verbreitet. Ist aber nicht schlimm. *Erkältung oder so.* Und wenn, haben wir ja unser gut ausgestattetes Gesundheitssystem.

3 *Kontrollverlust*: Das Virus verhält sich ungewöhnlich, verbreitet sich, ist nicht ungefährlich, Vertreter des Gesundheitssystems schlagen Alarm.

4 *Krisenkommunikation*: Behörden bilden Kommissionen, beängstigende Verlautbarungen werden verbreitet, die Publikumspresse übertrifft sich in Panikberichterstattung

5 *Panik*: Aktionismus, Angststarre und Panik-Narrative füllen die Informationsleere

6 *Eindämmung*: Daten sammeln, Suche nach Kompetenz und Präzision

7 *Regeneration*: Was war das? *Jetzt* sorgen wir vor. Da muss was anders werden … oder *„War da was?"* Vorbei - und *weiter wie zuvor.*

Was wir tun können

Am wichtigsten ist wohl, die Einstellung zur Welt ändern und die Tendenzen der Ausbildung von Sorglosigkeit aktiv bekämpfen. Die Welt ist nicht sauber und ordentlich. Sie ist komplex und kennt kein Mitleid mit denen, die sich nicht anpassen wollen oder können.[ii]

Es ist nicht nur so, dass die Dinge nicht immer so laufen wie geplant. Unsere Vorstellung von Plan und Kontrolle selbst ist zweifelhaft. Wie wir wissen, verwenden Organisationen viel Zeit darauf ihre zukünftigen Aktionen zu planen. Obwohl der Vorgang des Planens selbst sehr nützlich ist, die daraus entstandenen Pläne sind oft schon obsolet, bevor die finale Version verabschiedet wird.[iii]

Es gibt viele Gründe dafür. Man kann über die das Wesen der „quantum uncertainty“ spekulieren, man kann über Komplexitätstheorie und Chaostheorie sprechen. Man kann sich aber auch einfach vergegenwärtigen, dass wir in einer Welt mit Fantastilliarden Objekten und Ereignissen leben, die wir nicht einmal annähernd kennen und die sich auf uns ebenso weitgehend unbekannte Art und Weise beeinflussen. Auch wenn die Wissenschaft so weit fortgeschritten wäre, dass wir jedes einzelne Ereignis und jedes einzelne Objekt verstehen würden, gäbe es einfach zu viele Kombinationen und Perturbationen, um sie in endlicher Zeit untersuchen zu können.

Die Unvermeidbarkeit von Systempannen

Diese Sicht der Welt veranlasst zum Beispiel *Bruce Schneier*[iv] dazu, die *„Unvermeidbarkeit von Systempannen“* zu konstatieren. Für Schneier sind Systempannen der Preis für die wachsenden Komplexität von Systemen, die alle miteinander verbunden sind. Aus den Verbindungen und Interaktionen entstehen neue Eigenschaften und unbekannte Folgen. In diesem Sinne sind alle Sicherheitspannen das Resultat von unbekannten oder ungeplanten Systemeigenschaften.

Schneier unterscheidet drei Arten von Systemversagen: *aktives*, *passives* und *sicheres* Versagen. Wenn ein Sicherheitsgefüge durch einen Virusangriff in die Knie geht, dann ist das *passives Versagen*. Wenn ein System falschen Alarm schlägt und Maßnahmen eingeleitet werden, obwohl es gar keine Gefahr gibt, dann spricht man von *aktivem Versagen*.

Das Ziel aller Sicherheitsbemühungen sollte jedoch *„sicheres Versagen“* sein, eine *begrenzte Panne*. Das System fährt herunter oder schottet sich ab. Ähnlich wie bei einem Lastwagen, der durch einen Reifenplatzer auch nicht gleich umkippt oder in den Straßengraben fährt. In der Regel wird langsamer und bleibt stehen. Das ist der Moment, in dem *Redundanz-Maßnahmen* wie der Austausch mit dem Ersatzreifen greifen.

Oder – um auf die Corona-Krise zurückzukommen - ein genügend großer Bestand an nicht belegten Notfallbetten und Beatmungsgeräten.

Risikokompetenz

Der Psychologe *Gerd Gigerenzer* beschäftigt sich seit Jahrzehnten mit dem Thema Risiko und wie Menschen mit Risiken und Unsicherheiten umgehen.[v] Er stellt fest, dass Schockereignisse, das sind Situationen, in den in kurzer Zeit relativ viele Menschen ums Leben kommen, Angst und Panik auslösen – Pandemien und Flugzeugabstürze sind Beispiele dafür.

Die normale Grippe und Autounfälle ängstigen uns kaum, obwohl dadurch mehr Menschen sterben, Jahr für Jahr.

Ein Risiko wird definiert als das *Produkt aus Gefahr und Exposition*. Das heißt, nur wenn z.B. ein Virus gefährlich ist und gleichzeitig eine Exposition stattfindet besteht eine Gefahr für die Gesundheit. Und nur wenn ein Computervirus Schaden anrichten kann und er auch ein Netzwerk infiltriert, besteht Gefahr für die Informationssicherheit. Manchmal werden für „Risiko“ auch die Begriffe Wahrscheinlichkeit, Bedrohung oder (englisch) *Risk* verwendet.

Menschen haben evolutionär vorgegebene Reaktionen auf wahrgenommene Risiken. *Wenn das Risiko bekannt ist* (man hat also detailliertes Wissen über die Gefahr und kennt die Wahrscheinlichkeit der Exposition) wirkt das Risiko akzeptabel - vor allem, wenn der Nutzen größer ist als das Risiko. Wie zum Beispiel im Straßenverkehr, bei dem das statistische Bundesamt für das Jahr 2019 immerhin 3.059 Verkehrstote ausweist.

Wenn das Risiko unbekannt ist (man kennt weder die Gefahr noch die Wahrscheinlichkeit der Exposition) macht das *Angst*. Und wenn das unbekannte Risiko in kurzer Zeit viele Menschen tötet und augenscheinlich näher kommt, bricht leicht Panik aus. Fünfzig Menschen sind – evolutionär betrachtet – schon ein ganzer Verband, womit ein ganzer Stamm ausgestorben wäre.

Angst ist prinzipiell eine gute Reaktion. Sie sichert unser Überleben. Aber sie ist ein *schlechter Ratgeber*. Und wenn sie sich zur Panik auswächst, blockiert sie jede vernünftige Reaktion. Man kann sich nicht einmal mehr daran erinnern, dass vielleicht schon ähnliche Gefahren mit Erfolg gemeistert wurden, und dass man zusammen und solidarisch weiter kommt als allein – etwa mit Hamsterkäufen.

Von Marie Curie stammt der schöne Satz: *„Man braucht nichts im Leben zu fürchten, man muss nur alles verstehen“* - und das ist genau der Punkt. Wir müssen also *das Virus verstehen*: Es läuft nicht, es springt nicht, sondern *wir verbreiten es.* Entsprechend müssen wir handeln - also informiert und entspannt statt ängstlich und panisch, solidarisch statt egoistisch. Wir müssen lernen, die Informationen, die wir bekommen, richtig zu interpretieren - und wir müssen lernen, unsere evolutionär angelegten Primärreaktionen zu kontrollieren und unsere Emotionen zu managen.

Gigerenzer nennt das *„Risikokompetenz“* und meint, dass es wichtig ist zu lernen, mit Ungewissheit zu leben, statt nach Sicherheiten zu suchen, die es nicht gibt. Kleinkinder brauchen absolute Sicherheit, sagt er, Erwachsenwerden bedeute, risikokompetent zu werden und die Illusion der Sicherheit zu begraben.[vi]

Es liegt auf der Hand, dass Risikokompetenz für den Umgang mit digitalen Risiken genau so wichtig ist wie für den Umgang mit Risiken in der analogen Welt.

Kommunikationskompetenz

Wenn man nichts weiß, muss man sich auf seine Erfahrungen und auf die Informationen verlassen, die einem zur Verfügung gestellt werden. Wenn es aber keine Erfahrungen gibt oder wenn man die Erfahrungen mit ähnlichen Risiken vergessen hat, entsteht ein Informationsvakuum, das alles aufsaugt - und sei es noch so irreführend oder schlicht falsch.

Man kann leider erst hinterher feststellen, was richtig und was falsch war. Deswegen ist es wichtig zu wissen, wie Kommunikation funktioniert. Das *Kommunikationsquadrat von Schulz von Thun*[vii] sagt uns, dass jede Nachricht vier Botschaften gleichzeitig übermittelt:

1. eine Sachinformation (worüber ich informiere)
2. eine Selbstkundgabe (was ich von mir zu erkennen gebe)
3. einen Beziehungshinweis (was ich von dir halte und wie ich zu dir stehe)
4. einen Appell (was ich bei dir erreichen möchte)

Vor diesem Hintergrund sind in der Corona-Krisenkommunikation Aussagen des RKI - Präsidenten Lothar Wieler *„80% aller Fälle verlaufen glimpflich“* gefährlich. Er wollte damit vermutlich entwarnen, bedachte aber nicht, dass der Satz *auch* sagt, dass 20 Prozent aller Fälle *nicht* glimpflich verlaufen - und erzeugte somit Angst. Dabei waren die Prozentzahlen wieder nur auf die positiv Getesteten bezogen, also nicht auf alle Infizierten. Wenn der Präsident einer Bundesoberbehörde für Infektionskrankheiten (*Selbstkundgabe*) als beauftragter Sprecher der Regierung (*Beziehungshinweis*) eine falsch interpretierbare *Sachinformation* äußert, dann kann das, was er bei seinen Zuhörern erreichen möchte (*Appell*) vollkommen in die falsche Richtung gehen. Dazu kommt die unkritische und undurchdachte Verbreitung von Kriegsrhetorik, Panikpropaganda und irreführender Zahlen in vielen – ansonsten durchaus zuverlässig wirkenden – Medien, die die Situation keinesfalls beruhigen.

Es ist deshalb im Umgang mit Risiken wichtig, dass alle Beteiligten offen und ehrlich sind und sagen:
1) das wissen wir,
2) das wissen wir nicht,
3) das tun wir, um es in Zukunft zu wissen und
4) das können sie in der Zwischenzeit tun.

Security Empowerment

Die Corona-Krise hat den Blick für die Bedeutung von Infrastruktur für unser aller Wohlergehen geschärft und ein besonders helles Licht auch auf den Stand der Digitalisierung des Gesellschafts- und Wirtschaftslebens geworfen.

Kontaktverbote und Ausgangssperren haben das *Home Office* für Informationsarbeiter zum Standardarbeitsplatz gemacht, Millionen Menschen sind zu *Heimarbeitern* geworden.

Heimarbeit ist ungewohnt. Es gibt keine etablierten Routinen und es ist zweifelhaft,ob sich betriebliche Routinen überhaupt auf die Arbeit im Home Office übertragen lassen. *Die Arbeitsumgebungen zuhause sind technisch, räumlich und sozial allzu divers.*

Die Verlagerung der Arbeit vom Büro in die private Lebenswelt ist in der Umstellungsphase holprig und sieht am Anfang schwierig aus. Sie hat aber auch viele Vorteile, so viele sogar, dass Analysten den Durchbruch der Telearbeit als gegeben sehen.

Heimarbeit verschiebt auch den Fokus des Sicherheitstrainings für Mitarbeiter von der *Sensibilisierung („Awareness“)* der Anwender hin zu ihrer *Befähigung („Empowerment“)*, eigenverantwortlich für mehr Sicherheit im Umgang mit IT-gestützten Informationen zu sorgen.

Wenn man den Benutzer als schlecht konfigurierbares und schlecht kontrollierbares Element eines ansonsten gut funktionierenden technischen Systems ansieht, wirkt er tatsächlich wie ein *„weakest link“*, das regelmäßig „gepatched“ werden muss, damit es wieder seinen Dienst versehen kann - zumindest für eine begrenzte Zeit.

Führt man sich aber vor Augen, dass Informationstechnologie (wie das Gesundheitssystem) für Menschen da ist, ändert sich auch die Sichtweise: Wir haben es dann nicht nur mit Technik zu tun, sondern mit einem *sozio-technischen System.* In diesem System sind die Benutzer das Immunsystem und man kann sagen, dass die sichere Funktion des Systems durch die Benutzer aufrecht erhalten wird. Wenn das Immunsystem der Informationssicherheit zu schwach und schlecht trainiert ist, dann haben Infektionen - selbst mit eher harmlosen Keimen - katastrophale Folgen.

Der Leitsatz: *„Gib einem Mann einen Fisch und du ernährst ihn für einen Tag. Lehre einen Mann zu fischen und du ernährst ihn für sein Leben“*[viii] weist uns hier den Weg: „Ich muss meine Mitarbeiter befähigen, die technischen und sozialen Erfordernisse in seinem individuellen Kontext flexibel zu gestalten. Technische, kommunikative und soziale Kompetenz ist der Weg zu Effizienz, Sicherheit und Zufriedenheit im Home Office.“

Informationssicherheit ist unser digitales Immunsystem

Grundlegende Trainingseinheiten, die Mitarbeiter zur effizienten, sicheren und zufriedenstellenden Arbeit im Home Office (und auch im Büro) befähigen, könnten die Benennungen haben:

- *Home Office Empowerment 1*: "Miteinander reden im Home Office" -- Kommunikationskultur trotz Abstand
- *Home Office Empowerment 2:* "Risikokompetenz für Mitarbeiter" -- klarer Kopf in unklaren Situationen
- *Home Office Empowerment 3*: "Cyberhygiene im Home Office" – Gesundheit für Mensch und Maschine

Zusammenfassung

1 Die Corona-Krise ist ein Hinweis darauf, dass wir Infrastruktur als soziotechnisches System begreifen sollten, das in einer komplexen und gefährlichen Welt bestehen muss.

2 Systempannen sind unvermeidlich. Durch geeignete Methoden der Prävention, Beobachtung und Reaktion können Systempannen entschärft werden („sicheres Versagen“)

3 Nutzer sollten nicht als Problem, sondern als integraler Bestandteil der Informationssicherheit betrachtet werden.

4 Wie technische Komponenten können Benutzer nur dann sicher sein, wenn sie über die entsprechenden Kompetenzen verfügen.

5 Wichtige Kompetenzen für sicheres Verhalten auch in Krisensituationen sind
   - Risikokompetenz
   - Kommunikationskompetenz
   - Security Empowerment („Befähigung zu sicherem Verhalten“)

6 Kompetenzen entstehen durch Schulung und Training. Sie werden wirksam, wenn vier Voraussetzungen für sicheres Verhalten erfolgreich vermittelt bzw. hergestellt werden
   - Wissen und funktionale Konzepte
   - Fähigkeiten und Fertigkeiten
   - Einstellungen und Motivation
   - ein Umfeld in dem die erworbenen Kompetenzen gelebt werden können

7 Befähigte Nutzer sind das Immunsystem der Digitalisierung

Anhang: Take Away Sätze

- Emotet und andere „advanced persistent threats“ kann man sich wie das COVID-19 Virus vorstellen: lange Inkubationszeit, aber schon infektiös; Letalität stark abhängig vom Immunsystem des Wirts; hohe Mutationsrate
- und viele andere mehr …

Take Away Sätze sind Aussagen, die ein Ereignis (digitales Risiko - Emotet) in Deckungsgleichheit mit anderen Ereignissen (analoges Risiko – Corona) bringen.

Verwendbare Konnektoren sind zum Beispiel: ist wie; für … lernt man aus …; ähnelt in erstaunlicher Weise; es gibt keinen Unterschied; …

Digitale Risiken werden dadurch in die Erfahrungswelt eines (gefühlt) mit knapper Not überstandenen analogen Systemabsturzes gebracht und kann die kognitiven, emotionalen und konativen Elemente dieser Erfahrungswelt nutzen.

Endnoten

i Die Theorie der gelernten Sorglosigkeit wurde vom Sozialpsychologen Dieter Frey und anderen entwickelt (https://epub.ub.uni-muenchen.de/56815/). Schaubild 1 fasst die zentralen Aussagen der Theorie zusammen

ii „Survival of the Fittest“ bedeutet im Sinne der Darwin’schen Evolutionstheorie das Überleben der am besten angepassten Individuen und nicht – wie oft im deutschen Sprachraum verwendet und vom Google Übersetzer übersetzt – das „Überleben der Stärksten“. Wikipedia schreibt: „*Fit* oder *Fitness* beschreibt im Darwinschen Sinne den Grad der Anpassung an die Umwelt (also die adaptive Spezialisierung), oder auch die Reproduktionsfähigkeit trotz geringer Spezialisierung, und nicht die körperliche Stärke und Durchsetzungsfähigkeit im Sinne einer direkten Konkurrenzverdrängung unter Einsatz von Gewalt. Dies bedeutet, dass nicht jene Art überlebt, die allem trotzt und andere Arten verdrängt, sondern diejenige, welche sich entweder der Umwelt anpasst oder es schafft, sich trotz widriger Umweltbedingungen kontinuierlich zu vermehren.“

iii Lindblom, Charles E. (1964): „The science of "muddling through.“ In: *The making of decisions : a reader in administrative behavior*, S. 155–169.

iv Schneier, Bruce (2006): „Beyond fear. Thinking sensibly about security in an uncertain world.“ Repr. New York, NY: Copernicus Books.

v Gigerenzer, Gerd (2013): „Risiko. Wie man die richtigen Entscheidungen trifft.“ München: Random House

vi Die Arbeitsgruppe um Gerd Gigerenzer betreibt auch das Harding-Zentrum für Risikokompetenz https://www.hardingcenter.de/ und äußert sich dort auch zum Umgang mit der aktuellen Corona-Krise https://www.hardingcenter.de/de/unstatistik/unstatistik-des-monats-maerz-2020-corona-pandemie-statistische-konzepte-und-ihre

vii https://www.schulz-von-thun.de/die-modelle/das-kommunikationsquadrat

viii Konfuzius zugeschrieben

Schaubild 1: Schematische Darstellung der Theorie der gelernten Sorglosigkeit