RUB Faculty of Computer Science
www.informatik.rub.de

RUHR UNIVERSITÄT BOCHUM RUB

RUHR-UNIVERSITÄT BOCHUM | **FAKULTÄT FÜR INFORMATIK**
Universitätsstraße 150 | D-44801 Bochum | Gebäude ID 2.123

Deutscher Bundestag
Ausschuss für Digitales

Ausschussdrucksache
20(23)121

19.01.2023

Prof. Dr. Martina Angela Sasse

Büro: ID 2.121
Telefon: +49 (0)234 32 25028
Email: martina.sasse@rub.de

Sekretariat:
Büro: ID 2.123
Telefon: +49 (0)234 32 27600
Email: hcs-sekretariat@rub.de

www.informatik.rub.de/hcs

Bochum, 19.01.2023

Schriftliche Stellungnahme
„Cybersicherheit – Zuständigkeiten und Instrumente der Bundesrepublik Deutschland“

Sehr geehrte Damen und Herren,

anliegend übersende ich Ihnen meine schriftliche Stellungnahme zu Ihrem Fragenkatalog für die öffentliche Anhörung „Cybersicherheit – Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland“ des Ausschusses für Digitales im Deutschen Bundestag am Mittwoch, den 25. Januar 2023, 14:00-16:00 Uhr.

Mit freundlichen Grüßen

M. Angela Sasse

Prof. Dr. Martina Angela Sasse
Professorin Human-Centred Security, Horst Görtz Institut für IT Sicherheit

Schriftliche Stellungnahme:
„Cybersicherheit – Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland“
Deutscher Bundestag, Ausschuss für Digitales Öffentliche Anhörung am 25. Januar 2023
Prof. Dr. Martina Angela Sasse

Frage 1:
„Im Koalitionsvertrag haben die Regierungsparteien vereinbart, dass sie „einen strukturellen Umbau der IT- Sicherheitsarchitektur“ einleiten und das „Bundesamt für Sicherheit in der Informationstechnik (BSI) unabhängiger“ aufbauen und es als „zentrale Stelle im Bereich IT-Sicherheit“ ausbauen wollen. Wie sollte die Cybersicherheitsarchitektur auf nationaler und europäischer Ebene ausgestaltet werden, um effektiver, wirksamer und widerspruchsfreier aufgestellt zu sein und wo bedarf es einer Neuordnung oder auch Bündelung der Kompetenzen zwischen Bund, Ländern und der Europäischen Union und bedarf es auch angesichts der aktuellen Herausforderungen einer Diskussion über innere und äußere Sicherheit und der diesbezüglichen Kompetenzen und Grenzen? Welche anderen Akteure neben dem BSI (also etwa Cyber- Abwehrzentrum, Nationaler Cyber-Sicherheitsrat, ZITiS), die in Deutschland für Cybersicherheit zuständig sind, sollten reformiert werden und wie?“

Grundsätzlich ist der Ansatz, das BSI unabhängiger zu machen, und Cybersicherheits-Kompetenzen zu bündeln, zu begrüßen. Meine weitere Antwort stützt sich auf meine Beobachtungen und Erfahrungen aus der Zusammenarbeit mit dem National Cybersecurity Centre (NCSC) im UK, wo ich von 1990-2018 tätig war, und dem BSI hier in Deutschland. Im UK wurden Anfang der 2000 Cybersicherheitskompetenzen in GCHQ gebündelt, um Doppelungen zu vermeiden, und weil erwartet wurde dass durch engere Zusammenarbeit des auf ‚Externe Bedrohungen‘ und ‚Stärkung der Verteidigung‘ spezialisierten Personals Synergien und Einsparungen zu erzielen wären. Dieser Ansatz hatte aber den Nachteil, dass viele Unternehmen und Wissenschaftler wegen der Überwachungsaktivitäten nicht mit GCHQ zusammenarbeiten wollten, insbesondere nach den ‚Snowden revelations‘ 2013, die das Ausmaß der Überwachung des Internetverkehrs darlegten. 2016 wurde dann das NCSC als separate Einheit gegründet. Die klare Ausrichtung, Unternehmen, Behörden, gemeinnützige Organisationen und Bürger zu schützen, führte zu besserer Kommunikation und Kooperation. Die meisten digital aktiven Menschen im UK wissen dass man sich auf NCSC Webseiten zeitnah verlässliche Information bekommt, aufbereitet für verschiedene Zielgruppen. Das BSI ist in Deutschland den meisten großen Unternehmen und Behörden bekannt, und seine Angebote ‚von Experten für Experten‘ werden auch gut genutzt. Das BSI ist auch für KMUs und den digitalen Verbraucherschutz zuständig und bemüht sich um Zusammenarbeit, ist aber der breiten Öffentlichkeit nicht ausreichend bekannt, und die für diese Zielgruppe bereitgestellten Informationen werden als ‚sperrig‘ und ‚nicht machbar‘ (Experten-geleitet) empfunden.
Ein in der Frage nicht erwähnter Akteur ist die Bundesnetzagentur: Spam SMS, Emails und Faxe müssen dort gemeldet werden. Viele von diesen sind aber nicht nur lästig, sondern *social engineering* Angriffe, die immer häufiger werden und immer größere Schäden verursachen (z. B. als Teil eines Ransomware Angriffs). Nur eine verschwindend kleine Zahl der Bürger (die sich in solchen Fällen oft an die Polizei wenden weil sie sich persönlich angegriffen fühlen) und selbst viele Experten wissen dies nicht.

Frage 2:
Wie kann das Ziel, das BSI unabhängiger aufstellen zu wollen, konkret erreicht werden und wo bedarf es neben der Rechtsaufsicht seitens des BMI auch einer Fachaufsicht – oder anders herum gefragt: wo sind die bestehenden Abhängigkeiten das größte Hemmnis mit Blick auf die Akzeptanz und das Vertrauen in das BSI und welche Möglichkeiten sehen Sie, diese abzubauen?

Antwort auf die 2. Variante der Frage: Der Konflikt zwischen den Interessen des BMI im Namen der inneren Sicherheit und Verbrechensbekämpfung, und des BSI zur bestmöglichen Sicherheit für Unternehmen, Behörden, gemeinnützige Organisationen und Bürger. Das Recht auf Verschlüsselung (siehe Frage 4) ist ein gutes Beispiel – Verschlüsselung bietet effektiven Schutz – auch ‚bösen' Menschen. Das BMI hat sich in der Vergangenheit mit leider oft gegen das Recht auf Verschlüsselung gestellt, mit dem Argument das ‚gute' Menschen die nichts zu verbergen haben das nicht brauchen. Dieses Argument ist aus wissenschaftlich und ethisch unhaltbar, und das BSI muss weiter effektive Verschlüsselung – und andere Sicherheitsmaßnahmen empfehlen können. Daher wäre eine größere Unabhängigkeit für Unternehmen und Bürger von Vorteil.

Frage 4:
„Weitere Instrumente, die der Koalitionsvertrag adressiert, sind etwa auch

- **das Recht auf Verschlüsselung,**
- **ein Schwachstellenmanagement und die Pflicht, Sicherheitslücken zu melden,**
- **die Stärkung der digitalen Souveränität und die Beachtung der Vertrauenswürdigkeit von Unternehmen,**
- **die Vorgaben „security-by-design/default" als Standard,**
- **Stärkung der Produkthaftung und der IT-Sicherheitsforschung,**
- **das Recht auf Interoperabilität und Portabilität sowie das Setzen auf offene Standards, Open Source und europäische Ökosysteme, etwa bei 5G oder KI.**

Welche dieser Maßnahmen sollten mit welcher Priorität ungesetzt werden, wo besteht aus Ihrer Sicht darüber hinausgehender Handlungsbedarf und wo bestehen insbesondere Defizite?"

Diese Instrumente können alle zur Verbesserung der Cybersicherheit beitragen, sie setzen aber an verschiedenen Aspekten des Problems an, und sind voneinander abhängig. Daher ist eine Priorisierung nicht möglich. Präventive Maßnahmen – also die Vermeidung von Angriffsflächen und Schwachstellen – sind insgesamt langfristig effizienter als post-hoc Maßnahmen. ‚Security-by-design' ist daher der richtige Ansatz, aber nicht einfach umzusetzen. Es ist ein noch Forschungsthema, aber die bestehenden Konzepte und Maßnahmen müssen trotzdem jetzt schon Bestandteil der Aus- und Weiterbildung von Technikentwicklern werden – die Disziplin, Sicherheit (und ob sie benutzbar ist) bei der Technikgestaltung immer mitzudenken, muss noch etabliert werden. Um aktuelles Wissen für Sicherheitspraktiker und relevante technische Berufe leicht zugänglich zu machen, hat das NCSC im UK in Zusammenarbeit mit führenden Wissenschaftlern einen Cyber Body of Knowledge (CyberBok)[1] entwickelt und frei verfügbar gemacht, und damit eine Grundlage für fundierte Aus- und Weiterbildungs-Maßnahmen geschaffen.

[1] https://www.ncsc.gov.uk/section/education-skills/cybok

Aber in der Praxis agieren Entwickler im Rahmen von Vorgaben (inklusive Ressourcen) der Geschäftsleitung. In der Geschäftsleitung wird Sicherheit als unnötiger Kostenfaktor gesehen, für den Kunden nicht zahlen wollen. Die Kunden haben oft nicht genug Expertise um konkrete Risiken und Maßnahmen zu fordern, erwarten aber Sicherheit. Produkthaftung und die Pflicht, Schwachstellen zu melden schaffen einen wirtschaftlichen Anreiz auf der Geschäftsleitungsebene, ‚security-by-design' in Entwicklungsprozesse einzubauen, und adäquate Ressourcen (z.B. für Aus- und Weiterbildung der Entwickler, Testen) zu stellen.
Was unter den o.g. Instrumenten fehlt sind Maßnahmen ist effektive Vermittlung von Sicherheitsrisiken und sicheren Verhalten für die IT-Nutzer*innen (siehe Frage 17).

Frage 17:
„Anhand welcher Maßnahmen und/oder Methoden kann das Sicherheitsverständnis und -verhalten von IT-Nutzer*innen effektiv in den Mittelpunkt gerückt, eine höhere IT- Sicherheitskultur aufgebaut und das individuelle Vertrauen in die digitale Umgebung gestärkt werden?"

Sicherheitsexperten in Deutschland sind sich einig, dass das Sicherheitsverständnis und -verhalten von IT-Nutzer*innen in Deutschland mangelhaft bis ungenügend ist. Zum Beispiel gibt das Hasso-Plattner-Institut jährlich eine Auflistung der beliebtesten ‚schwachen' Passwörter heraus. In der Pressemitteilung zur Liste 2022[2] wird der ‚laxe' Umgang mit Passwörtern herausgestellt: *"Bei der Wahl des Passworts müsse Sicherheit vor Bequemlichkeit gelten und jede und jeder die möglichen Folgen bedenken, die es haben kann, wenn das Passwort in die falschen Hände gelangt."* Dies ist ein Beispiel dafür, wie die Sicherheitsindustrie, die Fachpresse, und selbst Teile der IT Sicherheitsforschung IT-Nutzer*innen die Schuld für die Wahl schwacher Passwörter - und das nicht-Befolgen von IT Sicherheitsregeln allgemein – verantwortlich machen[3] [4] [5]. Die ‚Bequemlichkeit' und ‚Ignoranz' von IT-Nutzer*innen – alias *‚Schwachstellen Mensch'* wird als die Wurzel des Problems dargestellt. Und es wird davon ausgegangen, dass dies durch ‚Security Awareness' Schulungen und Trainings - für Mitarbeiter in Unternehmen, und Angebote wie die Cyberfibel[6] für Bürger*innen und Bürger, sowie zahlreiche ‚hilfreiche' Empfehlung auf Webseiten – korrigiert werden kann. Aber in der Praxis können IT-Nutzer*innen diese Ratschläge nicht umsetzen (siehe auch Antwort zu Frage 18), was dazu führt das sie aufgeben. Die Empfehlungen zur Verwendung von starken Passwörtern ist ein Beispiel: IT-Nutzer*innen wissen aus Erfahrung dass sie sich an solche ‚starken' Passwörtern nicht erinnern können – sie erinnern sich aber an die Panik und Probleme die entstehen wenn man den dringend benötigeten Zugang nicht bekommt. Um dies zu vermeiden, wählen entweder eines der ‚schwachen' Passwörter, oder konstruieren ein oder zwei ‚starke' Passwörter, die sie dann für viele Konten verwenden – was angesichts der heute

[2] HPI, Die beliebtesten deutschen Passwörter 2022, 19. Dezember 2022, abrufbar unter: https://hpi.de/pressemitteilungen/2022/die-beliebtesten- deutschen-passwoerter-2022.html.
[3] https://new.siemens.com/de/de/unternehmen/stories/forschung-technologien/cybersecurity/human-beings-the-chink-in-the-armor.html
[4] https://www.datensicherheit.de/mensch-groesste-schwachstelle-it-sicherheit
[5] https://business-services.heise.de/security/bedrohungen-schwachstellen/beitrag/schwachstelle-mensch-im-griff-mehr-it-sicherheit-fuer-unternehmen-3156
[6] https://www.cyberfibel.de/

gängigen Angriffe äußerst riskant ist. Statt über ‚starke' Passwörter sollte zum Einsatz von Mehrfaktor-Lösungen und Passwort-Managern geraten werden[7].

Die Reichweiter dieser Ratgeber, sie sich an Konsument*innen und Bürger*innen richten, ist jedoch begrenzt. Das 2022 Digitalbarometer des BSI zeigt dass sich 23% der deutschen Bevölkerung gar nicht über IT Sicherheit informieren, und 35% *„hin und wieder."* Eine große Telefonumfrage 2021 in Deutschland mit Senioren, Jugendlichen, , Menschen mit Migrationshintergrund und niedrigem formalen Bildungsstand fand dass diese Gruppen ihre Informationen fast ausschließlich über Familie und Freunde, und Berichte in klassischen und online Medien über Cybersicherheit informieren – und fast niemand über die offiziellen online Angebote[8]. Es gibt online auch viele konkurrierende Angebote, wobei die von Verbraucherschutzorganisationen bei Befragungen am häufigsten genannt werden. Statt mehrerer allgemeiner online Angebote zum selben Thema könnte die Reichweite durch eine Aufbereitung für verschiedene Zielgruppen, Themen, und relevante Kanäle erhöht werden – z.B. über Angriffe im Online gaming auf in Gamer-Foren und -Netzwerken. Ausserdem sollten nicht nur einzelne Sicherheitsverhalten, sondern der Kontext von digitaler Souveränität und Medienkompetenz vermittelt werden.

Die meisten öffentlichen und privaten Organisationen in Deutschland stellen Sicherheits-Awareness und -Trainings-Maßnahmen für ihre Mitarbeitenden zur Verfügung. Während früher solche Veranstaltungen hauptsächlich vom IT-Sicherheitspersonal oder externen Trainern durchgeführt wurden, sind heute web-basierte Schulungen der Standard. In vielen Organisationen sind IT-Nutzer*innen verpflichtet diese zu absolvieren, z.B. weil die Organisation eine Sicherheits-Zertifikation wie ISO 27001 anstrebt oder dies in anderen Audits abgefragt wird. Manche Organisationen wählen diese sorgfältig aus und lassen Inhalte auf Risiken und Regeln des Unternehmens anpassen. In vielen Organisationen wird aber das günstigste Angebot eingekauft – relevante Module werden ausgewählt, die Inhalte aber nicht angepasst. Wenn nicht motivierte IT-Nutzer*innen sich innerhalb einer Frist durch solche Schulungen durcharbeiten müssen, stellt sich in der Regel kein Lerneffekt ein.

Selbst wenn die IT-Sicherheits-Inhalte erfolgreich vermittelt werden, führt ein besseres Verständnis allein nicht zur Verhaltensänderung. Unser Verhalten im Alltag besteht zum größten Teil aus hochgelernten Routinen, die automatisch ablaufen und uns oft nicht bewußt sind. Eine Verhaltensänderung erfordert viele Wiederholungen, und ist in der Regel nur erfolgreich wenn die Umgebung und Situation

[7] Kommunikation über Sicherheit von Passwörtern abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/digitaler_Verbraucherschutz/Beirat_DVS/Handlungsempfehlung_Sicherheit_Passwoerter.html

[8] Franziska Herbert u.v.a. „Talking to the Overlooked: A Nationwide Telephone Survey with Four Groups Under-represented in Privacy and Security" abrufbar unter https://arxiv.org/pdf/2212.12964.pdf

das neue Verhalten unterstützen[9]. Um sicheres Verhalten dauerhaft zu etablieren, muss die Einbettung von sicheren Routinen im Alltag durch Übung und Feedback unterstützt werden[10]. Viele IT-Sicherheitsschulungen setzen auf Angstmache um IT-Nutzer*innen zu sicherem Verhalten zu motivieren. Angst erzeugt jedoch führt zu Stress und Verharren in bestehenden Verhaltensmustern.

In den meisten Organisationen treffen die im Training gezeigten Verhalten jedoch oft auf Hindernisse[11]. Die meisten IT-Nutzer*innen machen jeden Tag die Erfahrung, dass sicheres Verhalten nur mit großem Aufwand, und manchmal gar nicht machbar ist[12]. In den meisten Fällen ignorieren umgehen IT-Nutzer*innen IT-Sicherheitregeln, um ihre eigene Produktivität, und die ihres Unternehmens zu schützen [13] [14] [15]. Aber statt solche Sicherheitsmaßnahmen durch bessere Technik (wie Passwort Manager, passwortlose Authentifizierung) oder bessere Integration in Arbeitsabläufe zu vereinfachen, werden mehr Awareness- und Trainingsmaßnahmen eingeführt, die wiederum Arbeitszeit kosten.

Eine besonders verbreitete Form von ‚Training' sind simulierte Phishing Emails, bei den Mitarbeitende im Arbeitsalltag durch simulierte Phishing Emails ‚angegriffen' und – wenn sie diese nicht erkennen – durch Informationen auf der Stelle noch einmal mit einer Schulung konfrontiert werden. Solche Maßnahmen sind aufwendig und mit Kosten und Risiken verbunden[16]. Sie reduzieren meist kurzfristig die Klickraten, aber eine nachhaltige Verbesserung der ‚Anfälligkeit' für solche Angriffe wurde in der bisher größten Langzeitstudie nicht beobachtet[17]. Dennoch werden sie von immer mehr Organisationen eingesetzt, oft auch mit dem Argument dass so die Fehlerkultur des Unternehmens verbessert werden kann. IT-Nutzer*innen werden oft ermutigt, Verdachtsfälle und eigene Fehler zu melden – aber die meisten Organisationen stellen keine Ressourcen für die Bearbeitung solcher Meldung zur Verfügung, so dass kein Dialog oder gemeinsames Lernen stattfindet.

---

[9] Susan Michie, Maartje Van Stralen, Robert West. "The behaviour change wheel: a new method for characterising and designing behaviour change interventions." Implementation science 6.1 (2011): 1-12.
[10] M. Angela Sasse, Jonas Hielscher, Jennifer Friedauer, Maximilian Peiffer und Uta Menges. (2022). Warum IT-Sicherheit in Organisationen einen Neustart braucht. In: 18. Deutscher IT-Sicherheitskongress 2022. Bundesamt für Sicherheit in der Informationstechnik.
[11] Maria Bada, M. Angela Sasse, and Jason RC Nurse. "Cyber security awareness campaigns: Why do they fail to change behaviour?." arXiv preprint arXiv:1901.02672 (2019).
[12] Anne Adams, M. Angela Sasse. "Users are not the enemy." Communications of the ACM 42.12 (1999): 40-46.
[13] Philip G. Inglesant, M. Angela Sasse. "The true cost of unusable password policies: password use in the wild." Proceedings of the sigchi conference on human factors in computing systems. 2010.
[14] Adam Beautement, M. Angela Sasse, Mike Wonham. "The compliance budget: managing security behaviour in organisations." Proceedings of the 2008 New Security Paradigms Workshop. 2008.
[15] Cormac Herley "So long, and no thanks for the externalities: the rational rejection of security advice by users." Proceedings of the 2009 workshop on New security paradigms workshop. 2009.
[16] Melanie Volkamer, M. Angela Sasse, Franzika Boehm "Phishing Kampagnen und ihre Fallstricke" https://www.kit.edu/kit/pi_2020_048_phishing-kampagnen-und-ihre-fallstricke.php
[17] Daniele Lain, , Kari Kostiainen, Srdjan Čapkun. "Phishing in organizations: Findings from a large-scale and long-term study." 2022 IEEE Symposium on Security and Privacy (SP). IEEE, 2022.

Sperrige Sicherheitsmaßnahmen und verpflichtende Schulungen auf der einen, wenig Bereitschaft zu Dialog oder konkreter Unterstützung im Alltag führt bei vielen IT-Nutzer*innen Sicherheitsermüdung[18] und ‚*compliance fatigue*' – ihr Interessse an, und Engagement für IT Sicherheit wird so nicht gefördert.

Frage 18
Wer bzw. was muss alles in den Blick genommen werden, wenn wir über Zuständigkeiten und Instrumente zur Verbesserung der IT-Sicherheit nachdenken, wo liegen die jeweiligen Defizite sowie Verbesserungsmöglichkeiten und wie bewerten Sie die Effektivität aktueller Informations- und (Weiter-)Bildungsmaßnahmen?

IT Sicherheit betrifft alle Menschen in die am wirtschaflichen und sozialen Leben teilnehmen wollen. Die Rolle von IT-Sicherheit ist IT-Nutzer*innen zu schützen – nicht sie zu überfordern, ängstigen, und zum Sündenbock dafür zu machen dass digitalen Plattformen und Produkte zu viele Schwachstellen haben und Angriffspunkte bieten, und die jetzigen Sicherheitslösungen einen Aufwand erfordern den sie nicht leisten können. IT-Sicherheitsexperten und der Staat müssen IT-Nutzer*innen, und ihre Zeit und Aufmerksamkeit, mit Respekt und Fürsorge behandeln – ‚Schwachstelle Mensch' ist ein Unwort das aus dem Diskurs verbannt werden muss. Vertrauen und Zusammenarbeit aller ‚guten' Akteure ist eine notwendige Voraussetzung für effektive Cybersicherheit, in Organisationen und der Zivilgesellschaft[19]. Wenn diese Akteure sich statt dessen gegenseitig ignorieren und/oder befehden, profitieren die nur den Angreifern.

IT Sicherheitsexperten brauchen zusätzliche Kompetenzen, um konstruktiv mit IT-Nutzer*innen und Führungskräften zusammenzuarbeiten. Im Unternehmenskontext kann ein konstruktiver Dialog mit IT-Nutzer*innen effiziente Lösungen finden. Besonders wichtig ist konstruktiver Dialog mit technisch versierten IT-Nutzer*innen – z. B. Software Entwicklern, um ‚security-by-design' und ‚usable security' umzusetzen[20]. Diese Umsetzung erfordert aber auch sie Ressourcen und Unterstützung von Führungskräften[21].

Führungskräfte müssen sich mehr in die Diskussion über Sicherheit, und wie wir sie für alle machbar gestalten, einbringen. Sie müssen auch verstehen, dass Sicherheit ist kein Zustand ist, der mit einem Tick bei einer Zertifizierung erreicht wird, sondern was IT-Nutzer*innen in ihren Organisationen jeden Tag praktizieren. IT-Sicherheit muss regelmäßig evaluiert und verbessert werden – die Angreifer schlafen nicht.

---

[18] Stanton, Brian, Mary F. Theofanos, Sandra Spickard Prettyman, Susanne Furman. "Security fatigue." It Professional 18, no. 5 (2016): 26-32.
[19] Lizzie Coles-Kemp, Debi Ashenden, Kieron O'Hara. "Why Should I? Cybersecurity, the Security of the State and the Insecurity of the Citizen." Politics and Governance 6.2 (2018): 41-48.
[20] Ashenden, Debi, and Darren Lawrence. "Security dialogues: Building better relationships between security and business." IEEE Security & Privacy 14.3 (2016): 82-87.
[21] Gutfleisch, Marco, et al. "How does usable security (not) end up in software products? results from a qualitative interview study." 43rd IEEE Symposium on Security and Privacy, IEEE S&P. 2022.

Auch IT-Nutzer*innen müssen - ähnlich wie in der Arbeitssicherheit - ihren Beitrag zur ihrer eigenen Sicherheit, und der von anderen, leisten. Dazu gehört die grundsätzliche Bereitschaft sich mit relevanten Risiken auseinanderzusetzen, und Verhalten, die im digitalen Zeitaltern nicht mehr sicher sind , umzustellen. Der Austausch mit anderen über den richtigen Umgang mit digitalen Risiken muss gefördert werden, im digitalen Raum, in Organisationen, aber auch Familien, Schulen, Vereinen.