Abgehängt oder aufgeklärt:
Wie gelingt digitale Aufklärung für alle Menschen?

Veränderungen im Alltag sowie neue Lösungsansätze für mehr IT-Sicherheit und Vertrauen

Stichworte für die Paneldiskussion beim DsiN-Jahreskongress 2019
am 3. Juni 2019 in Berlin

I. Grundsätzlicher Positionierungsvorschlag

- Digitalisierung durchdringt alle Lebensbereiche – privat wie beruflich. Unsere Kinder wachsen als „digital natives“ auf. Frage mich, wie wir „digital immigrants“ mitnehmen. Wir müssen eine digitale Spaltung vermeiden.
- Digitalisierung schafft Chancen – gleichzeitig aber auch Risiken für informationelle Selbstbestimmung. Wertvorstellungen sind im Wandel. Wichtig, immer wieder an die Bedeutung der „Privatheit“ zu erinnern. Das sehe ich als meine Kernaufgabe an.
- Digitalisierung erfordert vor allem neue Kompetenzen. Wir verändern unseren Medienkonsum. Nicht mehr der Zugang zu Informationen ist die Herausforderung, sondern die richtige Bewertung. Desinformation möglich. Medienkompetenz ist daher ein Schlüsselfaktor. Digitalkompetenz wird aber auch Erfolgsfaktor in Arbeitswelten (Hinweis auf Anschlusspanel „Neue Arbeitswelten 4.0“).
- Es verändert sich auch, wie wir miteinander interagieren. Beispiel: Viele digitale Freunde in Online-Communities. Sind das tatsächlich „reale“ Freunde im tradierten Sinne?
- Mir wichtig, dass diese Veränderungen „nicht einfach so passieren“. Auch Panik oder Euphorie sind fehl am Platz. Müssen die Veränderungen nüchtern begleiten und proaktiv gestalten. Notfalls auch korrigierend eingreifen.
- Wir benötigen hierfür gesamtgesellschaftlichen Konsens, was wir überhaupt wollen. Welche Zukunft wollen wir also? Finde, wir benötigen mehr digitale Selbstbestimmung. Müssen die Potenziale der Digitalisierung zum Wohle aller und für eine gute Zukunft nutzen. „Menschenfreundliche“ Gestaltung von Anfang an ist hierfür essentiell.
- Digitalisierung auch für Wirtschaft wichtiger „Enabler“. Die Wirtschaft „digitalisiert“ alle Geschäftsprozesse. Gut, denn das hebt Synergieeffekte. Gleichzeitig aber auch Gefahr. Es entstehen neue Abhängigkeiten und IT-Risiken. Zwei Beispiele: 1.) Risiken für Industriespionage steigen. Gerade für Deutschland als „Land der Entwickler“ und „KMU“ neuralgischer Punkt. Unerwünschter Know-how Abfluss ist hier existenzbedrohend. 2.) Produzie-

rendes Gewerbe: Hier lassen sich mit Industrie 4.0 völlig neue Produktionswege beschreiten. Gleichzeitig ergeben sich neue Herausforderungen durch neue Sabotagemöglichkeiten.

- Mir ist klar, dass Digitalisierung eine industriepolitische Dimension hat. Mich ärgert dabei, dass Datenschutz immer als „Bremse“ stigmatisiert wird. Ist fatal und falsch. Gegenteil kann und sollte der Fall sein.
- Europa wird zunehmend zum reinen Absatzmarkt digitaler Services. Haben es selbst nicht geschafft, weltweit agierende IT- / Internetunternehmen hervorzubringen. Müssen uns fragen, woran das liegt, auch um werthaltige Arbeitsplätze in Europa zu sichern.

Was müssen wir tun, um Chancen zu nutzen und Risiken zu reduzieren?

- Wir benötigen ein waches Auge für Risiken und Nebenwirkungen.
- Wichtig sind mehr Sensibilisierung und Aufklärung über Chancen und Risiken.
- IT-Grundwissen muss bereits in der Grundschule angelegt werden, um darauf aufbauend "IT-Sicherheit" und "Datenschutz" vermitteln zu können. Ähnliche Angebote werden für ältere Menschen benötigt (wichtig sind die grundlegenden Konzepte).
- Von DsiN, der Gesellschaft insgesamt, aber auch dem BSI oder BfDI getragene Angebote hierfür wichtiger Baustein.
- Europäische „Champions“ aktiv fördern durch anreizorientierte Industriepolitik. Hierbei Datenschutz und Datensicherheit in Europa als Wettbewerbsvorteil ausbauen. Datenschutz und IT-Sicherheit per „design“ von Anfang an mitdenken. Denn Datenschutz und IT-Sicherheit sind wichtige positive Differenzierungsmerkmale im Markt. Europa hat mit Datenschutzgrundverordnung ein Alleinstellungsmerkmal. Diesen „Vertrauensanker“ gilt es mit Leben zu füllen und auszubauen.

II. Wo stehen wir in Bezug auf digitale Aufklärung?

Stecken leider in vielen Bereichen noch in den „Kinderschuhen“. Aus meiner Sicht sind folgende Maßnahmen relevant:

- Wir brauchen verbesserten Eigenschutz. Nutzerinnen und Nutzer müssen noch stärker dafür sensibilisiert werden, wie schnell unzureichender Eigenschutz zu einem Problem führen kann, das dann auch andere in Mitleidenschaft zieht. Wichtig, dass jeder Einzelne in seinem Interesse und im Interesse Dritter die Sicherheitsanforderungen hoch hält.

- Wir brauchen in diesem Zusammenhang mehr „digitale Selbstbestimmung“: Dies schließt Kompetenz ein, selbst zu bestimmen, mit welchen Inhalten jemand in Beziehung zu seiner Umwelt tritt und wie die eigene Persönlichkeit unter Wahrung von Privatheit interaktiv entfaltet wird. Mit umfasst ist auch die selbstbestimmte wirtschaftliche Verwertungsmöglichkeit der eigenen Datenbestände.
- Gesunde Skepsis: Ansonsten hilft auch gesunde Skepsis z.B. beim Öffnen von E-Mail-Anhängen. Jeder sollte aber bei der Nutzung sozialer Medien genau überlegen, welche privaten Details veröffentlicht werden – und welche besser nicht.
- Anbieterverantwortung muss verbessert werden. Anbieter müssen ihre Systeme so sicher wie möglich gestalten. D.h. erforderlich sind eine Implementierung geeigneter Sicherheitsmaßnahmen und die Sicherstellung einer schnellen Reaktion bei Sicherheitsvorfällen. Beim Doxxing-Fall waren Internetunternehmen zu langsam und haben nicht gut genug mitgearbeitet. Wichtig wäre gewesen, sofort die betroffenen Links abzuschalten. Dann wäre die Verbreitung der Daten verlangsamt worden.

III. Wo sind die Bedarfe für digitale Aufklärung am größten?

- Wir sind mitten in einem Transformationsprozess. Ändern wird sich einiges, u.a. unser Verständnis von Demokratie, Freizeit, Arbeit, Gesundheitswesen – und möglicherweise auch der Mensch selbst.
- Ich halte es grundsätzlich für problematisch, dass wir neue Technologien immer stärker nutzen ohne sie inhaltlich zu durchdringen. Wer weiß denn schon, warum er bei einer google-Suche bestimmte Ergebnisse angezeigt bekommt? Gibt es denn ein breites gesellschaftliches Wissen über die Ertragsmodelle von Internetdiensten? Beispielsweise wie mit Nutzerdaten Geld verdient wird?
- Aufklärung ist die Basis für eine selbstbestimmte Entscheidung. Deshalb ist die digitale Aufklärung auch und gerade in diesem Bereich so erforderlich. Wie sonst sollten Menschen eine selbstbestimmte Entscheidung darüber treffen können, ob sie Dienste unter den gegebenen Konditionen nutzen wollen?

IV. Wer sind die Abgehängten – immer nur die anderen?

- Digitale Transformation und Aufklärung geht uns alle an. Das schon deshalb, weil sie alle Lebensbereiche durchdringt.

- Wir müssen uns fragen, ob bisherige Kernkompetenzen verloren gehen oder sich nur verändern? Wer kann sich heute noch an einer klassischen Landkarte orientieren? Jeder nutzt Navigations-Apps. Wenigstens eine Karte lesen können sollte man. Sonst sprechen wir nicht mehr über digitale Transformation, sondern von digitaler Abhängigkeit. Wann hatten Sie das letzte Mal einen Kompass in der Hand? *[Situativ ggf. Hinweis auf Philosoph Georg Wilhelm Friedrich Hegel, der die Rolle zwischen „Herren" und „Knecht" bereits in seiner „Phänomenologie des Geistes" von 1807 wie folgt beschrieb: Indem der „Herr" sämtliche Arbeiten auf den Knecht delegiert, verlernt er die Selbstständigkeit und wird abhängig vom „Knecht". Faktisch ist es nur noch der „Knecht", der sich weiterbildet und etwas mit eigener Hand schafft. Unmerklich drehen sich die Rollen um. Letztendlich wird der „Knecht" der Selbstständigere und Gebildete sein.]*
- In zahlreichen neuen Berufssparten benötigen Menschen IT- und Digitalkompetenz. Um eine „digitale Spaltung" zu vermeiden, muss erforderliches Wissen generationenübergreifend vermittelt werden.
- DsiN kann hier einen wichtigen Beitrag leisten. Menschen ohne Digitalaffinität droht sonst Wohlstandsverlust und sozialer Abstieg.

V. Wo steht Deutschland in Punkto Digitalisierung?

- Die analoge und digitale Welt verschmelzen zunehmend. Gewohnheiten, Arbeit, Umwelt und Freizeitgestaltung werden mehr und mehr durch die Digitalisierung transformiert.
- Der öffentliche Diskurs ist geprägt von Schlagworten wie Künstliche Intelligenz, Blockchain, Quantencomputern und Cloud Computing, die aber nur Spielarten dieser Digitalisierung sind.
- Eine performante digitale Infrastruktur ist das Rückgrat für Internet und Onlineanwendungen. Laut Breitbandatlas von Mitte 2018 sind inzwischen in Städten 50 Mbit/s und mehr für 93,5 Prozent aller Haushalte verfügbar, im ländlichen Raum dagegen nur für 50,5 Prozent, Quelle Breitbandatlas BMVI[1]. Das ist eine Basis die ausgebaut werden muss.
- Der Algorithmus ist heute schon in vielen Bereichen „besser" als der Mensch. Das ist kein neuer Befund: Am 31. August 1994 kam es zu einer Sensation, als der Schachweltmeister

1 Abrufbar unter https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/breitband-verfuegbarkeit-mitte-2018.html.

Garri Kasparow bei einem Schnellturnier in London gegen das auf einem Pentium laufende Programm Chess Genius mit 0,5:1,5 verlor. Und das ist jetzt 25 Jahre her!

- Wo geht die Reise hin? Autonomes Fahren wird es uns ermöglichen, uns viel sicherer durch den Verkehr zu bewegen. Roboter in der Medizintechnik können Operationen bald exakter als Menschen und mit gesamtem Wissen der Medizin im Hintergrund durchführen. Der Einsatz von Robotern in der Altenpflege wird diskutiert.
- Aber: Insgesamt werden immer mehr Daten generiert. Es muss sichergestellt sein, dass jedes Individuum selbst bestimmen kann, welche Daten wem offenbart werden und wofür sie genutzt werden.
- Wir müssen uns Sorgen um Kontrollverlust und Abhängigkeiten machen. *[Hinweis auf Datenethikkommission.]*
- Entscheidungen werden teilweise automatisiert getroffen. Einsatz von KI: Zu klären, wo der Einsatz von KI ethisch bedenklich ist, wo nicht. Wichtig, Letztentscheidung bei einem Menschen zu belassen und Korrekturen zu ermöglichen. Transparenz der Entscheidungsfindung ist Grundlage für Vertrauen. *[Hinweis auf Datenethikkommission.]*
- Industriepolitik: Technologisch ist Europa bereits im Hintertreffen, insbesondere hinter USA und Asien. Mit Blick auf Datenschutz aber hat Europa einen Wettbewerbsvorteil. Potenziale müssen wir nutzen und positiv vermarkten. Sollten über eigene Impulse & größeres Engagement in Standardisierung nachdenken.
- Datenschutz weiter stärken: Aufsichtsbehörden müssen durch pragmatische Rechtsauslegung und einheitliche Durchsetzung der DSGVO darauf hinarbeiten, Datenschutz weiter zu stärken. Wir müssen ganz oben anfangen! Kriegen wir Facebook, Amazon, Google und Microsoft datenschutzrechtlich nicht in den Griff, wird uns auch kein Handwerksmeister, Vereinsvorstand ober Start-Up-Unternehmen vertrauen, wenn wir ihm datenschutzrechtliche Vorgaben machen.
- Zertifizierung: Es ist wichtig, die Einhaltung der Vorgaben auch im Markt zeigen zu können. Hier spielt Zertifizierung eine große Rolle. Müssen wir stärker ausbauen.
- Es ist wichtig, IT-Sicherheit und Datenschutz von Anfang an als Teil der „DNA" eines jeden Produkts und einer jeden Dienstleistung mitzudenken. Nur so kann es gelingen, von Anfang an vertrauenswürdige Produkte und Dienstleistungen zu entwickeln.

VI. Wie stärken wir das Bewusstsein für IT-Sicherheit in Bezug auf die eigene Verantwortung?

- IT-Sicherheit und Datenschutz sind „Evergreens“: Beides neuralgische Punkte für Digitalisierung. Mit der Digitalisierung steigt auch Bedeutung der IT-Sicherheit. Einfache Gleichung: Ohne IT-Sicherheit kein Vertrauen. Und ohne Vertrauen keine Nutzung digitaler Dienste. IT-Sicherheit und Datenschutz sind wichtige Erfolgsfaktoren für Digitalisierung.
- IT-Sicherheit und Datenschutz müssen – gerade auch bei KMU – Chefsache werden. Hier sind die Unternehmen leider noch allzu oft tradiert und „hausbacken“ unterwegs. Gerade IT-Sicherheit ist aber wichtig, damit die „Kronjuwelen“ eines Unternehmens nicht in Gefahr geraten.
- Kein „Kostenfaktor“ sondern „Innovationsmotor“: IT-Sicherheit und Datenschutz dürfen nicht auf reine „Kostenfaktoren“ reduziert und „gebrandmarkt“ werden. Produkte und Dienstleistungen werden sich nur durchsetzen, wenn Sie dem Menschen dienen. IT-Sicherheit und Datenschutz sind gelebter Grundrechtsschutz und Vertrauensanker.
- IT-Sicherheit und Datenschutz als Qualitätsmerkmal begreifen: Sichere, datenschutzkonforme Produkte als Qualitätsmerkmal verstehen. Beides schafft positive Differenzierungsmöglichkeiten im Markt. Deutschland und Europa haben hervorragende Ausgangssituation. Ziel: Weltweiter Marktführer. Warum? Europa hat innovativen Rechtsrahmen. Datenschutzgrundverordnung wird weltweit als Referenz und Blaupause herangezogen. (Beispielsweise beim sog. California Consumer Privacy Act.)

VII. Welche Verantwortung tragen Politik und Wirtschaft?

- Bessere digitale Aufklärung ist wichtige gemeinsame Aufgabe von Staat, Wirtschaft und Gesellschaft. Erforderlich ist frühzeitige und fortwährende Sensibilisierung.
- Staat kann selbst mit „Leuchtturmprojekten“ als gutes Beispiel vorangehen. E-Government-Angebote müssen weiter ausgebaut werden. Nutzungsmöglichkeiten zeit- und ortsunabhängiger Verwaltungsdienste sind aktuell noch immer zu spärlich. Es reicht nicht aus, nur online einen Termin beim Amt vereinbaren zu können.
- Behörden müssen vorangehen und selbst besonders datenschutzfreundliche Dienste nutzen. *[Reaktiv: An was denken wir? Idee: Z.B. ganz bewusst einen datenschutzfreundlichen, sicheren Messenger-Dienste als Gegenspieler zu etablierten Internetdiensten schaffen. BfDI berät gerne in diesem Kontext. BfDI plant auch Aufbau eines eigenen Testcen-*

ters. BfDI prüft bei Win10/Cloud Services in der Bundesverwaltung die Möglichkeiten eines datenschutzkonformen Einsatzes.]

VIII. Wie erreichen wir alle Menschen in Bezug auf digitale Aufklärung?

- DSGVO war wichtiger Meilenstein, auch für die Sensibilisierung der Bürgerinnen und Bürger: Wir verzeichnen stärkeres Interesse am Schutz der eigenen Daten. Das ist gut. So erreichten uns im Zeitraum vom 25. Mai bis Ende 2018 insgesamt 6.507 allgemeine Anfragen und 3.108 Beschwerden. Auf den Monat heruntergebrochen entspricht dies einer Verdreifachung der Eingaben. Zusätzlich wurden von den der Aufsicht des BfDI unterliegenden Stellen noch 7.300 Datenschutzverstöße gemeldet.
- Vertrauen durch sicheren Rechtsrahmen schaffen: In diesem Zusammenhang ein Sicherheitsgesetz-Moratorium anregen. Es schafft kein Vertrauen, die sicherheitsbehördlichen Kompetenzen bei rückläufiger Kriminalstatistik auszubauen.
- Müssen generationenübergreifende und zielgruppenspezifische Angebote anbieten. Digitale Aufklärung muss Teil des Privatlebens, aber auch Berufsalltags werden, s.o.
- Der Grundstein für digitale Aufklärung muss bereits in der (Grund-)schule gelegt werden. Aber auch Angebote für ältere Menschen werden benötigt. DsiN ist hier u.a. eine geeignete Plattform.