

Schützen Sie Ihr wichtigstes Gut: Ihre Daten

Mit Scheer selbstbestimmt und sicher in die digitale Zukunft.



Im Rahmen unseres Security Assessments identifizieren wir Schwachstellen und mögliche Risiken Ihrer IT und implementieren entsprechende Maßnahmen. So sind wir möglichen Angreifern einen Schritt voraus und schützen Ihre wertvollen Unternehmensdaten und IT-Infrastruktur – jederzeit unter Berücksichtigung Ihrer bestehenden Security und Compliance Vorgaben.

Mehr erfahren:



scheer-group.com/security-assessment

Scheer. Die Prozess-Experten.
www.scheer-group.com

YScheer

Heft 4 | Dezember 2021

Meine Daten gehören mir!

IM+io Best & Next Practices aus Digitalisierung | Management | Wissenschaft

IM+io

BEST & NEXT PRACTICES AUS DIGITALISIERUNG | MANAGEMENT | WISSENSCHAFT

im-io.de
IM+io
Dezember 2021
Heft 04
ISSN 1616-1017
G 9765F



MEINE DATEN GEHÖREN MIR!

SOUVERÄN IN DIE DIGITALE ABHÄNGIGKEIT?

Daniela Otto

Alexa, ich bin süchtig

Wolfgang Ernst

Mit KI Datenschätze heben

Martin C. Wolff

Ich digitalisiere, also bin ich!

4

August-Wilhelm
Scheer Institut
Digital Research



FACHMAGAZIN MIT WEITBLICK



ÜBER 100 AUSGABEN



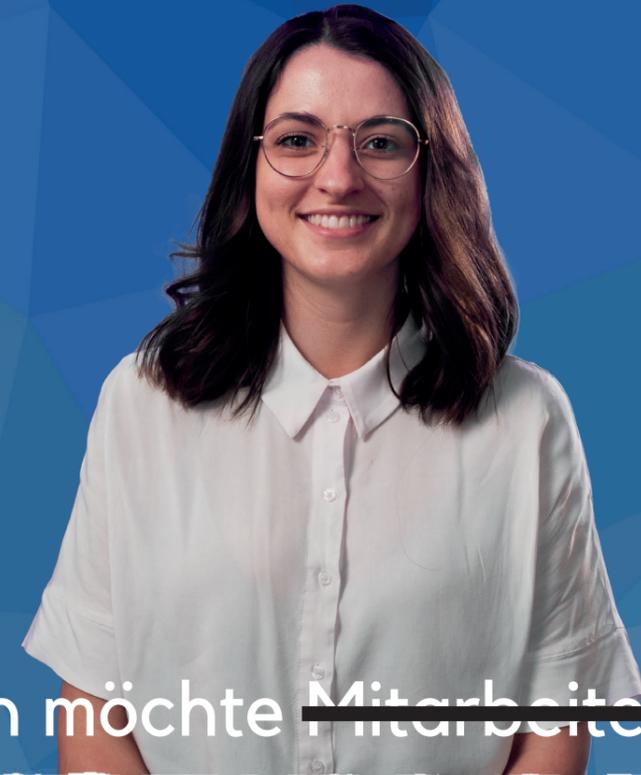
VERNETZT SEIT ÜBER 30 JAHREN



ÜBER 1000 AUTOREN
AUS ALLER WELT



**WIR HABEN PLATZ
FÜR DICH UND DEINE IDEEN.**



Ich möchte ~~Mitarbeiter:in~~

ZUKUNFTSGESTALTER:IN

sein.

Unser Motto: Stärken stärken.

Unsere Kompetenz: Potenziale entfalten. Und dafür suchen wir **DICH!**

Wir mögen es individuell, interdisziplinär und innovativ.

Gemeinsam bringen wir dein Talent an die richtige Stelle.

LET'S TRANSFORM AND PERFORM.



Jetzt Zukunftsgestalter werden!
www.aws-institut.de/karriere



Digitale Souveränität oder neue Abhängigkeit ?

Von Datenschutz, Global Playern und Medienkompetenz



Google trackt den Suchverlauf, überall müssen Cookies akzeptiert werden und Meta (Facebook) weiß von Ausbildungsplatz bis Wohnort alles über uns. Haben wir den Überblick über unsere Daten verloren? Warum machen wir uns abhängig von digitalen Global Playern. Und: Schaffen wir es, die Kontrolle zurückzugewinnen? Das Problem: Laut Studien ist nur ein Drittel der Bevölkerung digital souverän. Auf staatlicher Seite sieht es kaum besser aus. Staat und Bürger müssen befähigt werden, digitale Medien bewusster und zielgerichteter zu nutzen. Aber wie kann digitale Kompetenz gelingen? Welche Rolle spielen Datenschutz und das europäische Cloud-Projekt „Gaia-X“? Antworten auf diese Fragen liefert die neue IM+io mit dem Titel „Meine Daten gehören mir! - Souverän in die digitale Abhängigkeit?“.

Bevor Sie mit der Lektüre dieser spannenden Ausgabe starten, sollte vorher geklärt werden, was hinter dem Begriff der digitalen Souveränität steht. Im Prinzip lassen sich drei Schwerpunkte festlegen: erstens digitale Souveränität im Sinne von Datensicherheit und -transparenz und zweitens als das selbstbestimmte Arbeiten und den souveränen Umgang mit digitalen Medien, Informationen und Daten im Sinne von digitaler Medienkompetenz. Zu guter Letzt wird digitale Souveränität als digitale Konkurrenzfähigkeit bezeichnet, bei der sich sowohl Unternehmen als auch Staaten gegen Global Player in der Digitalindustrie durchzusetzen versuchen. Ein bekanntes und aktuelles Beispiel ist in diesem Zusammenhang das groß angelegte und ambitionierte Vorhaben „Gaia-X“ zur Stärkung des Standorts Europa.

Einblick in die Debatte um Datensicherheit und -transparenz gibt Patrick Henning, CEO und Mitgründer der neXenio GmbH, im Interview mit der IM+io, und er beschreibt die Entwicklung der „luca App“, die in Corona-Zeiten die schnelle und lückenlose Kontaktrückverfolgung ermöglicht. Ebenfalls häufig mit der Problematik von

Datensicherheit konfrontiert, erklärt Ville Sirviö, CEO des Nordic Institute for Interoperability Solutions aus Estland, wie im öffentlichen Sektor das hochsichere Datenübertragungssystem „X-Road“ den Durchbruch in Europa schafft.

Inwiefern eine flächendeckende, souveräne europäische Dateninfrastruktur notwendig ist, lesen Sie im Artikel: „Hoffnungsträger Gaia-X – Letzte Chance für Datensouveränität in Europa“. Daniel Krezdorn erklärt, dass „die lange geltende Laissez-faire-Politik“ die Souveränität Deutschlands gleich in mehreren Punkten gefährdet. Über Zielstellungen und Herausforderungen des Gaia-X Projektes haben wir zudem mit Dr. Johann Bizer, Vorsitzender des Dataport-Vorstands, gesprochen. Marcel Mutz und Dr. Dirk Werth beschreiben in ihrem Beitrag, was eine neue Plattform für die Batteriezellproduktion auf die digitale Souveränität in allen drei Schwerpunkten beitragen kann.

Schließlich wird das Thema der digitalen Medienkompetenz und ihrer Erlangung etwa im Artikel „Alexa, ich bin süchtig. Wie Digital Detox die Handysucht bekämpft“ von Daniela Otto beleuchtet. „Raus aus der Steinzeit. Digitalkompetenz als Schlüssel zum 21. Jahrhundert“ ist der Titel des Artikels vom Aktionsrat Bildung.

Digitale Souveränität bezieht sich also auf alles und jeden, der mit Digitalisierung und Daten zu tun hat, angefangen beim einzelnen Bürger, Unternehmen und sogar bei der Politik – in unserer heutigen Gesellschaft ist es also ein Thema, das uns alle betrifft. Doch kann man noch von digitaler Souveränität sprechen, oder befinden wir uns schon in einer gefährlichen Abhängigkeit?

Um der neuen digitalen Abhängigkeit ein wenig zu entkommen, lesen Sie das Heft und stellen sich souveräner auf!

Viel Spaß beim Lesen wünscht,

Prof. Dr. August-Wilhelm Scheer

Inhalt

Scheer Innovation Review

- 6 „Bei der Digitalisierung nicht bremsen, sondern Gas geben!“ Datenschutz als Hemmschuh für Innovation?
Ein Kommentar von August-Wilhelm Scheer, Scheer Holding
- Interview**
- 8 „Es geht darum, Abhängigkeiten zu reduzieren“. Letzte Chance für Datensouveränität in Europa
Im Gespräch mit Johann Bizer, Dataport
- 12 Vom Digital Outsider zum Digital Native. Digitale Souveränität braucht eine mutige Politik
Daniel Krezdorn, digital-souveraenitaet.de
- 16 Banking goes Blockchain. Die Transformation des Bankensektors nimmt Fahrt auf
Hartmut Giesen, Sutor Bank
- Kolumne MehrWerth**
- 21 WWW - world wide web oder Wilder Westen?
Dirk Werth, Chefredakteur IM+io

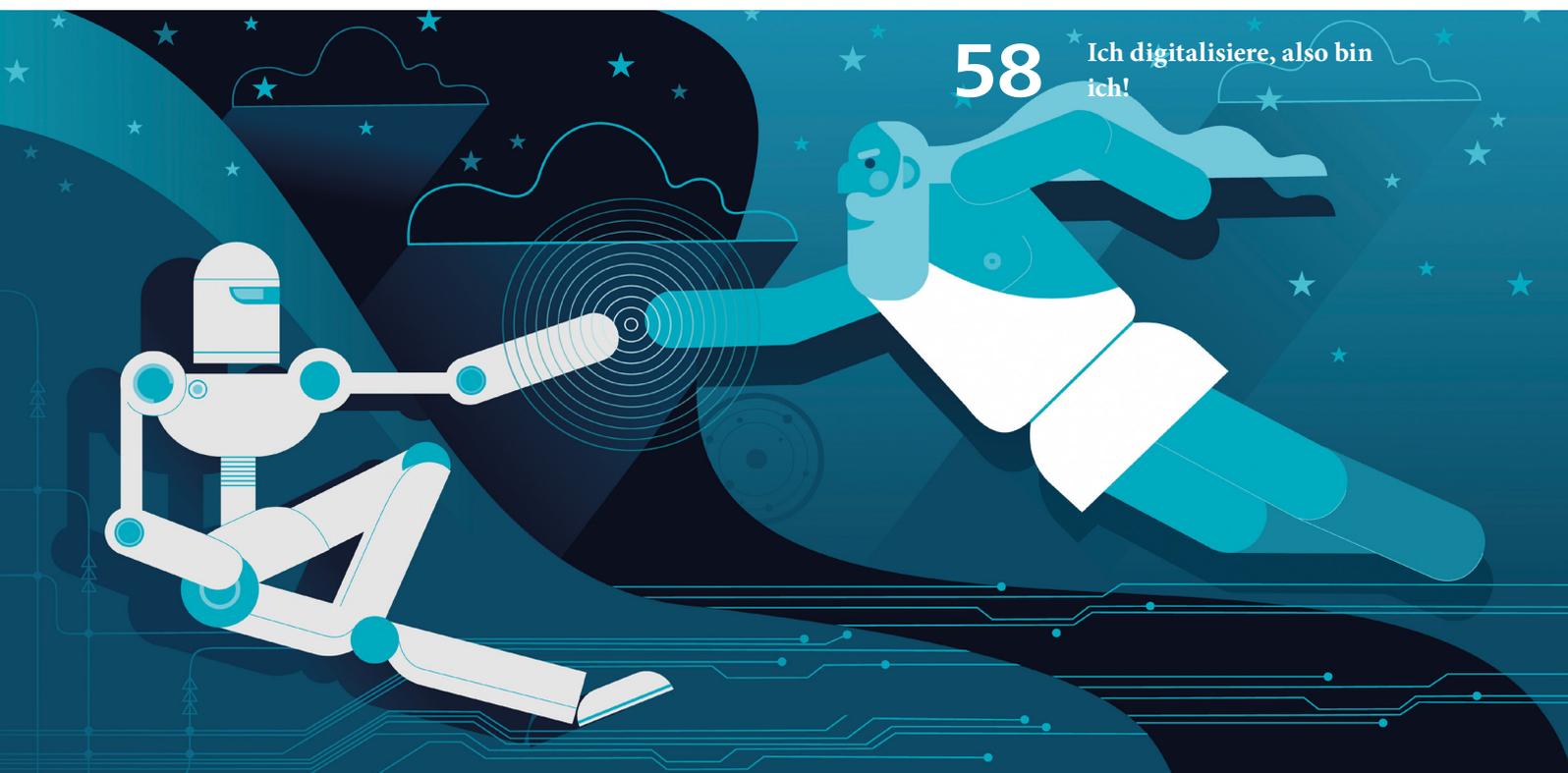
START-UP IM SPOTLIGHT

Interview

- 22 Wie luca aus der Krise hilft. Mit der luca App gemeinsam aus der Pandemie
Im Gespräch mit Patrick Hennig, neXenio

Schwerpunkte

- 26 Sicher. Souverän. Online. Warum man online nicht mit seinen Daten zahlen sollte
Sylvia Napiletzki, Julia Ringies, Bundesamt für Sicherheit in der Informationstechnik
- 30 Daten säen - Digitalisierung ernten. Wie Landwirte Datensouveränität erreichen
Bernd Rauch, Fraunhofer IESE
- 34 „Alexa, ich bin süchtig.“ Wie Digital Detox die Handysucht bekämpft
Daniela Otto, Ludwig-Maximilians-Universität München
- 38 Mit KI Datenschätze heben. Erfolgsfaktoren in der Plattformökonomie
Wolfgang Faisst, ValueWorks.ai
- 42 Datenpower macht Ionen schlauer. Wie Datascience und KI zu neuen Hochleistungsakkus verhelfen können
Marcel Mutz, Dirk Werth, August-Wilhelm Scheer Institut





98

Feierliche Eröffnung des Center for Digital GreenTech

- 48** „Ein Puzzle mit vielen Teilen“. Digitale Souveränität als gelebte Abhängigkeit
Andreas Thyen, LizenzDirekt AG
- 54** Eine Identität für alles und jeden. Mit Self-Sovereign Identities zu mehr digitaler Selbstbestimmung
Benjamin Leiding, Technische Universität Clausthal
- 58** Ich digitalisiere, also bin ich! Digitale Souveränität als gesamtgesellschaftliches Thema
Martin C. Wolff, Digital.Wolff, Plötz & Co GmbH
- 64** Datenchaos ade. Souverän durch die digitale Verwaltung
Sandra van der Hulst, Hansestadt Lübeck, und Christiane Wegner, MACH AG
- 68** Digitale Souveränität: (k)eine Frage des Alters? Raus aus der Gutenberg-Galaxis
Axel Benning, Marcell Saß, Fachhochschule Bielefeld, Philipps-Universität Marburg
- 72** Zwischen Wahrheit und Wirklichkeit. Compliance als Herausforderung für Mittelständler
Christian Löhl, W+ST CoB-IT GmbH
- 78** Lebensretter Digitalkompetenz. Digitale Souveränität für Entscheider
David Hoeflmayr
- 82** Raus aus der Steinzeit. Digitalkompetenz als Schlüssel zum 21. Jahrhundert
Aktionsrat Bildung
- 86** Dem Dreigestirn der Innovation begegnen. Digitale Souveränität beginnt im Kopf
Tomas Herzberger, Schaffensgeist
- IM+io INTERNATIONAL**
Interview
- 90** Connecting All of Europe With a Single Crossroad. The secure data-exchange layer X-Road®
Ville Sirviö, Nordic Institute for Interoperability Solutions
- OUT OF THE BOX**
- 94** Der Wald als digitales Ökosystem. Wie Gaia-X neue Datenräume eröffnet
Ingo Lück, Thomas Feld, materna
- Netzwerk**
- 98** Feierliche Eröffnung des Center for Digital GreenTech
Lisa Christl, August-Wilhelm Scheer Institut
- 100** East Side Fab. Wo Innovationen beschleunigt werden
Luisa Margies, East Side Fab e.V
- 102** Impressum
Vorschau auf Heft 1/2022

„Bei der Digitalisierung nicht bremsen, sondern Gas geben!“

Datenschutz als Hemmschuh für Innovation?

Ein Kommentar von August-Wilhelm Scheer, Scheer Holding



Die Datenökonomie ist wirtschaftliche Realität. Datenbasierte Geschäftsmodelle sind die Zukunft der Wirtschaft. Sie bieten die Grundlage für künftigen gesellschaftlichen Fortschritt und soziale Sicherheit, und das weit über die Grenzen Europas hinaus. Der Erfolg von ganzen Volkswirtschaften wird von der intelligenten Nutzung von Daten, und besonders von datengetriebenen Innovationen abhängen. Die Frage ist nun, sind wir in der Lage, eine solche intelligente Nutzung umzusetzen?

Ich teile die Kritik an den Brüsseler EU-Strategen, die die DSGVO in der vorliegenden Form auf den Weg gebracht haben. Ihnen ist es nicht gelungen, moderne und zukunftsichere Regeln für den Umgang mit Daten im 21. Jahrhundert zu schaffen. Was definitiv fehlt, ist die Konkretisierung der Verordnung, so, dass heute etablierte Geschäftsmodelle und zukünftige Möglichkeiten der digitalen Wirtschaft wettbewerbsfähig weiterentwickelt werden können.

Aber wir müssen auch dringend unsere nationalen Hausaufgaben erledigen. Es wird kaum jemand zu finden sein, der den Nutzen einer elektronischen Patientenakte für Ärzte

und Patienten infrage stellt. Dort sollen Arztberichte und Befunde von Patienten künftig über eine zentrale Software digital gespeichert werden. Ich denke, auch die Modernisierung der Verwaltungsregister, durch die verschiedene Datentöpfe, wie etwa Melderegister und KFZ-Datenbanken, die bisher dezentral gespeichert werden, unter der Steuer-ID jedes Bürgers vernetzt werden sollen, bietet kurze Wege und effizientes Handeln. Ausgebremst wird beides durch Bedenken unserer Datenschützer. Aber wir dürfen bei der Digitalisierung nicht bremsen, wir müssen vielmehr Gas geben. Die Politik hat in den vergangenen zehn Jahren durch ihre Zögerlichkeit Chancen für die Zukunft aufs Spiel gesetzt. Mahner aus Wirtschaft und Wissenschaft wurden nicht gehört, sondern eher belächelt!

Ja, der Nutzen der Digitalisierung muss gegen die potenziellen Risiken abgewogen werden und ja, der Missbrauch der Daten muss so weit als möglich verhindert werden. Sanktionen sind möglich: In Estland etwa verliert ein Arzt seine Zulassung, wenn er Patientendaten missbraucht. Es geht darum, das viel zitierte Kind

nicht mit dem Bade auszuschütten: Nur weil sich manch ein Autofahrer nicht an die Straßenverkehrsordnung hält und mit Tempo 100 durch die Innenstadt fährt, werden nicht alle Autos auf Tempo 50 gedrosselt!

Wir müssen irrationalen Ängsten und tradierten Vorbehalten durch transparente Information entgegenwirken, wir müssen die Digitalisierungsschritte durch digitale Bildung beschleunigen. Dazu gehört auch, für Klarheit beim Datenschutz zu sorgen und dabei Nutzen und Risiken in ein vernünftiges Verhältnis zueinander zu stellen. Verbissene Debatten über cloudbasierte Lernsoftware beschäftigen auch nach den Lockdownphasen noch die Kultusministerkonferenz.

Die Angst vor eben jenen hochprofessionellen aber cloudgestützten Angeboten führte während der Schulschließungen zur Nutzung von kurzfristig förmlich handgestrickten Mini-Lernplattformen, die mehr Frust als Lust am Lernen produzierten. Hier fehlte definitiv Wissen, Verständnis und Orientierung. Ich erinnere zudem an die leidenschaftlich geführte Debatte im Rahmen der Pandemie-getriebenen Verwendung von Videosoftware an Schulen. Sie war beherrscht von den überall lauenden Gefahren des Datenmissbrauchs. Erst sehr viel später haben wir über Schüler gesprochen, die vom Lernbetrieb abgehängt wurden, oder über mangelnde Lehrer-Schüler Kommunikation, die mit eben jenen Videosoftwareangeboten gleich zu Beginn des Lockdown möglich gewesen wäre. Man begnügte sich mit dem Hinweis, was aus Datenschutzgründen nicht gehe, anstatt nach Lösungen zu suchen.

Am Ende aber zeigt diese Debatte auch, dass die Modernisierung der Schulen seit Jahren vernachlässigt wurde, was sich in der Pandemie nun gerächt hat. Und damit kommen wir zum bereits angesprochenen ‚Sündenbock Datenschutz‘. Auch bei der Corona-App war wohl nicht der Datenschutz das zentrale Problem, sondern der vorsintflutliche Zustand des Gesundheitswesens hinter der App. Wäre man das Problem fehlender Leitungen, Schnittstellen und des mangelnden Know-how in der Verwaltung früher angegangen, wäre auch der Datenschutz kein zentrales Hindernis mehr gewesen. Unstreitig besteht aufgrund der komplexen Regelwerke zum Datenschutz eine große Verunsicherung.

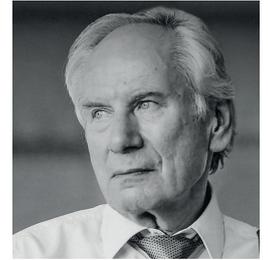
Aber es geht natürlich auch um ein problematisches Mindset: In der öffentlichen

Notwendiger Datenschutz darf sinnvoller wirtschaftlicher Datennutzung nicht entgegenstehen.

Debatte werden eher die Risiken als die Chancen der Datennutzung betont. Und ich denke, genau hier müssen wir ansetzen. Es geht nicht darum, das Grundrecht auf den sicheren Umgang mit den eigenen Daten, auf digitale Souveränität, in Frage zu stellen. Es geht darum, was wir daraus machen.

Notwendiger Datenschutz darf sinnvoller wirtschaftlicher Datennutzung nicht entgegenstehen, darüber herrscht breiter Konsens, aber bei dieser eher übergeordneten Sicht dürfen wir es nicht belassen. Was wir brauchen, ist ein ‚sowohl als auch‘. Oft verhindern Gesetze heute noch die Digitalisierung, anstatt sie zu gestalten.

Umso wichtiger ist es, die gesellschaftliche Debatte über die Notwendigkeit einer ohnehin nicht aufzuhaltenden digitalen Transformation voranzutreiben. Aber wir müssen auch die Schere aus den Köpfen der Menschen holen. Digitale Bildung und damit ein richtiges Verständnis von Datensouveränität helfen, irrationalen Ängsten in Verwaltungen, Institutionen und beim Anwender entgegenzuwirken. Wir können es uns nicht leisten, dass aus einem falschen Verständnis und einer diffusen Auslegung unseres Grundrechts auf informationelle Selbstbestimmung ein Hemmschwelle für innovative Geschäftsmodelle betoniert wird! ■



Prof. Dr. Dr. h.c. mult. August-Wilhelm Scheer

August-Wilhelm Scheer ist einer der prägendsten Wissenschaftler und Unternehmer der deutschen Wirtschaftsinformatik und Softwareindustrie. Als Unternehmer und Protagonist der Zukunftsprojekte „Industrie 4.0“ und der „Smart Service World“ der Bundesregierung arbeitet er aktiv an der Ausgestaltung der Digital Economy. Prof. Scheer hat mehrere IT-Unternehmen mit den Schwerpunkten Software-Entwicklung und IT-Beratung gegründet.

Kontakt

scheer@scheer-holding.com

www.scheer-blog.com

Kurz und Bündig

Der Nutzen der Digitalisierung muss gegen die Risiken abgewogen werden, der Missbrauch der Daten muss so weit als möglich verhindert werden. Nicht nur Datenschützer bremsen, oft verhindern auch Gesetze die Digitalisierung, anstatt sie zu gestalten, meint Prof. August-Wilhelm Scheer



Hoffnungsträger Gaia-X

Letzte Chance für Daten-
souveränität für Europa

Im Gespräch mit Johann Bizer

Deutschland muss einen eigenen Beitrag zum Cloud Computing leisten: Das verlangte bereits 2010 der damalige Präsident des Bitkom, Prof. Dr. August-Wilhelm Scheer. Er forderte Sicherheit der Daten, Standardisierung, Exzellenzentwicklung und europäische Einbindung. Doch die Zeit war wohl noch nicht reif. Erst 2019 wurde auf dem Digitalgipfel des Bundesministeriums für Wirtschaft und Energie (BMWi) der Start von GAIA-X beschlossen. GAIA-X ist eine Initiative zum Aufbau einer sicheren und transparenten Dateninfrastruktur nach europäischen Standards. Der öffentliche IT-Dienstleister Dataport ist an mehreren Vorhaben zu GAIA-X beteiligt. Mit Dr. Johann Bizer, dem Vorstandsvorsitzenden des Unternehmens, sprachen wir über Notwendigkeiten und Chancen einer souveränen europäischen Dateninfrastruktur.

IM+io Herr Dr. Bizer, noch befindet sich GAIA-X in einer Aufbauphase. Welches Ziel wird dabei verfolgt und was soll GAIA-X am Ende bieten und bewirken?

JB: Ziel von GAIA-X ist der Aufbau einer sicheren und vernetzten Dateninfrastruktur, die europäischen Ansprüchen an digitale Souveränität genügt und Innovationen fördert. Es geht darum, Abhängigkeiten zu reduzieren, LockIn-Effekte zu vermeiden und DSGVO-konforme, interoperable und für Nutzer transparente Angebote zu schaffen. Am Aufbau von GAIA-X sind mehr als 300 Vertreter aus Wirtschaft, Industrie, Wissenschaft und Verwaltung beteiligt. Inzwischen gibt es in 15 Ländern der EU zentrale und länderspezifische Anlaufstellen, die Hubs. Das partnerschaftliche Vorgehen möglichst vieler Stakeholder schon in der Aufbauphase stellt maximale Akzeptanz, Wettbewerbsfähigkeit und Innovationskraft der Initiative sicher. Wir sehen an den Use Cases der Aufbauphase jetzt schon, wie breit gefächert die Einsatzmöglichkeiten sind: Dank einer europäischen Dateninfrastruktur und mittels Verknüpfung von Datenräumen wird der Datenaustausch über verschiedene Institutionen, Staaten und bestehende Infrastrukturen möglich. Künftig können so neue Wertschöpfungsketten im EU-Binnenmarkt entstehen und neue datengetriebene Geschäftsmodelle entwickelt

werden. GAIA-X baut dabei keinen zentralen Datenpool auf. Die Daten bleiben im gesamten Prozess dort, wo sie entstehen. Und sie bleiben stets in der Hoheit der Dateneigentümer – das ist das Entscheidende. Dazu ist ein Architekturkonzept für eine technische Infrastruktur nötig. Zusätzlich benötigen wir Festlegungen für den künftigen Katalog vorhandener Cloud-Services, die Nutzungsbedingungen und die Art der Authentifizierung für den Zugang der Services sowie Compliance-Regeln. All dies orientiert sich an europäischen Werten und Vorstellungen von Datenschutz und IT-Sicherheit. Im Rahmen von GAIA-X sprechen wir dabei von federation services.

IM+io Der Initiative GAIA-X geht es also um Datensouveränität und sichere Vernetzung. Wie passt zu diesem Anspruch, dass auch die internationalen Hyperscaler Microsoft, Alibaba, Amazon und Google der Initiative beigetreten sind?

JB: Ich verstehe, dass dieser Punkt kritisch diskutiert wird. Verständigt hat man sich zunächst darauf, dass die Hyperscaler die GAIA-X-Compliance-Regeln einhalten müssen. Es bleibt das Risiko eines jeden Kunden, dass aufgrund von geopolitischen Einflüssen wie einer handelspolitischen Auseinandersetzung eine aus dem Ausland gesteuerte Cloud (zumindest



Johann Bizer

Dr. Johann Bizer ist seit November 2011 Vorsitzender des Dataport-Vorstands und verantwortlich für die Bereiche Ressourcen und Lösungen. Seine Berufslaufbahn begann er am Institut für öffentliches Recht der Universität Frankfurt am Main, wo er bis 2003 wissenschaftlicher Assistent war. Bis Ende Januar 2008 war er beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein tätig, wo er Stellvertreter des Landesdatenschutzbeauftragten Thilo Weichert war. Im Februar 2008 wechselte Dr. Bizer in den Vorstand von Dataport.

Kontakt

britta.heinrich@dataport.de
www.dataport.de

temporär) nicht mehr verfügbar ist. Das kann das Geschäftsmodell eines Kunden beschädigen oder vernichten. Wichtig ist, dass wir eine Alternative schaffen: GAIA-X soll und wird den Wettbewerb zwischen Cloud-Anbietern befeuern, indem LockIn-Effekte zwischen Anbietern ausgeschlossen werden.

Letztlich geht es darum, dass Kunden datensouverän unter Berücksichtigung ihres geschäftspolitischen Interesses entscheiden können, für welche Lösung sie welchen Anbieter und welche Lösung einsetzen wollen. Eine Entscheidung im Risikomanagement eines Unternehmens. Als öffentliches Unternehmen verfolgen wir – Dataport – im Interesse unserer Kunden und deren Nutzer seit Jahren eine Hybridstrategie: Unseren Kunden bieten wir nach Möglichkeit unterschiedliche Lösungen an, die ihrem Schutzbedürfnis, das heißt dem der Funktionen ihrer Anwendungen sowie ihrer Daten, entsprechen. Die Erfahrung zeigt, dass die Entscheidung gegen eine Cloud ausfällt, wenn ein fremdbestimmtes Abschalten der Anwendung als geschäftskritisch zu bewerten ist. Im öffentlichen Sektor ist dies der Fall, wenn das Vertrauen der Bürgerinnen und Bürger sowie der Unternehmen in die Funktionsfähigkeit der öffentlichen Verwaltung beschädigt werden könnte.

Ein Beispiel für die Hybridstrategie ist unsere dPhoenixSuite, die Module unterschiedlicher OSS-Hersteller integriert. Zusammen bilden sie einen vollständigen digitalen, cloud-basierten Arbeitsplatz, den wir aus unserem BSI-zertifizierten Rechenzentrum oder aber von

Datenschutzkonformer Austausch wird neue datengetriebene Geschäftsmodelle ermöglichen.

einem hiesigen Unternehmen aus hier betriebenen privat-wirtschaftlichen, ebenfalls BSI-zertifizierten Rechenzentrum anbieten. Die erste Lösung fokussiert die besonderen Sicherheitsbedürfnisse der öffentlichen Verwaltung: Dataport ist in öffentlicher Hand. Wir betreiben für die öffentliche Verwaltung und schützen ihre digitale Souveränität. In dem zweiten Modell wahren wir mit unserem Partner die Schutzbedürfnisse unserer Kunden. In beiden Modellen verlassen die Daten Deutschland nicht und werden DSGVO-konform verarbeitet. Im zweiten Modell kann die Veränderung der Eigentümerstruktur des Partners zu einer veränderten Bewertung seiner Vertrauenswürdigkeit führen. Die Entscheidung fällt letztlich der Auftraggeber aufgrund transparenter Informationen. Wichtig ist, dass Alternativen möglich sein müssen und Entscheidungen für ein Betriebsmodell revidiert werden können.

IM+io Cloud Computing dient als Motor für die Digitalisierung der Industrie und der Wirtschaft. Gilt das auch für den Public Sector und welchen Nutzen wird dieser aus GAIA-X ziehen?

JB: Das gilt unbedingt auch für den Public Sector. Cloud-Lösungen werden in der öffentlichen Verwaltung in Deutschland schon vielfach verwendet – und es könnten noch viel mehr sein. Sie werden etwa benötigt, um den in und für die öffentlichen Verwaltung innovativen Ansatz der „Einer für Alle“-Anwendungen erfolgreich umsetzen zu können. Dazu ist die Interoperabilität und sind Schnittstellen zwischen unterschiedlichen Cloud-Lösungen zu gewährleisten. Ermöglicht werden soll, dass eine Anwendung, die in der einen Cloud betrieben wird, ohne größeren Aufwand auch in einer anderen Cloud betrieben werden kann. Eine solche Lösung schafft Synergien, bündelt bereits bestehende Angebote unter einem Dach und gibt Standards für die Entwicklung

Infobox

Dataport ist der IT-Dienstleister für die öffentliche Verwaltung. Dazu kooperiert Dataport mit Anbietern aus der Region und unterstützt die föderale IT-Kooperation. Dazu gehören der Betrieb von Rechenzentren, Netzen und Clients sowie die Entwicklung und der Betrieb von Software. Darüber hinaus bietet das Unternehmen umfassende Dienstleistungen: Das Angebot reicht von IT-Beschaffung über Schulungen bis hin zu Projektmanagement und Beratung. Als Anstalt öffentlichen Rechts mit Unternehmenssitz in Altenholz bei Kiel wird Dataport getragen von den Ländern Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachsen, Sachsen-Anhalt und Schleswig-Holstein sowie vom kommunalen IT-Verbund Schleswig-Holstein. Dataport betreibt Niederlassungen in jedem seiner Trägerländer. Das Unternehmen hat rund 4.000 Mitarbeiterinnen und Mitarbeiter und erzielte 2020 einen Umsatz von 900 Millionen Euro.

zukünftiger Anwendungen vor. GAIA-X wird dem Public Sector nutzen, weil die dort geltenden federation services europaweit übernommen werden können. Mit anderen Worten: Übernimmt die Deutsche Verwaltungscloud diese federation services, ist die Anschlussfähigkeit an andere Lösungen breit gewährleistet – was für ein großer Schritt nach vorn.

IM+io **Das BMWi fördert 16 Leuchtturmprojekte für datengetriebene Geschäftsmodelle im digitalen Ökosystem GAIA-X. Welchen inhaltlichen Fokus haben diese Projekte, und welche Innovationen sollen gefördert werden?**

JB: Die Projekte sind Gewinner eines Förderwettbewerbs des Bundeswirtschaftsministeriums, an dem 130 Konsortien teilgenommen haben. Sie kommen aus dem Gesundheits-, Rechts-, Finanz-, Bildungs-, Energie-, Bau- und Produktionswesen, der Luft- und Raumfahrt, aus der Agrarbranche, dem maritimen sowie dem öffentlichen Sektor. Diese Use Cases sollen ganz konkret zeigen, welchen Mehrwert die souveräne Dateninfrastruktur bei der Entwicklung datengetriebener Geschäftsmodelle und KI-basierter Services sowie beim Aufbau europäischer Datenräume bietet.

Wir sind stolz, dass Dataport als Konsortialpartner – unter anderem von Unternehmen der Scheer-Group – in zwei Leuchtturmprojekten für den Public Sector dabei ist. Eines ist POSSIBLE, das eine nutzerfreundliche OSS-Cloud-Lösung für den öffentlichen Sektor zum Ziel hat. Über die Integration von Phoenix soll der digital souveräne Umgang mit Daten und Prozessen in GAIA-X möglich werden. Mit dem oben erwähnten Arbeitsplatz dPhoenix-Suite können Anwenderinnen und Anwender verschiedener Verwaltungen oder Unternehmen über einen Datenraum auf alle mit ihrer digitalen Identität verbundenen Informationen zugreifen und diese sicher und kontrolliert auszutauschen. Im Rahmen von POSSIBLE wollen wir die Zusammenarbeit regionaler Verwaltung, insbesondere der Kommunen, mit Bürgerinnen und Bürgern sowie Unternehmen erproben und pilotieren. Ziel ist die medienbruchfreie Arbeit an Dokumenten, die moderne Kommunikation via Chat und Videokonferenz sowie die Freigabe und das Teilen von persönlichen Dokumenten.

Das zweite Projekt ist MERLOT. Hier entwickeln wir Dienste und geschützte

Datenräume für den Bildungsbereich, die über Marktplätze innerhalb des GAIA-X Ökosystems abgerufen werden können. Über diese Marktplätze wollen wir Lernmanagementsysteme wie die Dataport-eigene dBildungsCloud oder iServ mit KI-gestützten Services zur Vorbereitung von Unterrichtsinhalten oder zur Leistungsauswertung zusammenführen. Dabei sind hohe Standards im Datenschutz und in der Datensicherheit zu erfüllen.

IM+io **Wie sind die Aussichten, dass GAIA-X am Ende nicht nur Datensouveränität bietet, sondern auch Marktchancen erschließt?**

JB: Die Aussichten sind zweifelsohne gut. Wie gut, wird sich zeigen. Um für unsere Branche zu sprechen: Für uns öffentliche IT-Dienstleister werden sich neue Chancen ergeben, indem wir Dienste und Leistungen aus dem GAIA-X-Netzwerk beziehen oder dort über bisherige Vertriebsgrenzen hinweg anbieten. Große Chancen ergeben sich auch für den öffentlichen Sektor, der künftig Datenräume aus Verwaltung, Bildung und Umwelt der europäischen Partnerländer erschließen kann. Unser Plädoyer für die Ausrichtung einer Deutschen Verwaltungscloud nach Gaia-X-Standards zielt genau darauf. GAIA-X wird die Abhängigkeit von internationalen Anbietern reduzieren. Datenschutzkonformer Austausch wird mehr und neue datengetriebene Geschäftsmodelle ermöglichen – und das über Branchen, Landesgrenzen hinweg und selbst dann, wenn mehrere Cloud-Anbieter involviert sind. ■

Kurz und Bündig

Am Aufbau von GAIA-X sind Vertreter aus Wirtschaft, Industrie, Wissenschaft und Verwaltung beteiligt. In 15 Ländern der EU gibt es zentrale und länderspezifische Anlaufstellen. Über GAIA-X entsteht eine europäische Dateninfrastruktur, mittels Verknüpfung von Datenräumen wird der Datenaustausch über verschiedene Institutionen, Staaten und bestehende Infrastrukturen möglich – ein Angebot, das auch für den öffentlichen Sektor interessant ist.

Vom Digital Outsider zum Digital Native

Digitale Souveränität braucht eine mutige Politik

Daniel Krezdorn, digital-souveraenitaet.de



Adobe Stock | 170578590 | vegefox.com

Die Enthüllungen Edward Snowdens vor fast einem Jahrzehnt hätten ein Weckruf für Deutschland sein können. Im Jahr 2021 scheint der Digitalraum für staatliche Institutionen hingegen immer noch „ein Stück weit Neuland“ zu sein. Die lange geltende Laissez-faire-Politik gefährdet die Souveränität des Staates gleich in mehreren Punkten. Dabei geht es neben der Infrastruktur, Sicherheit und politischer Gestaltungsmacht bei dem Thema auch um die Bürger selbst, die den Staat ausmachen. Digitale Souveränität ist daher eine gesamtgesellschaftliche Aufgabe.

Algorithmen-gesteuerte Informationsauswahl, die immer weiter zunehmende Marktkonzentration und Macht einiger weniger Konzerne, künstlich geschaffene Lock-ins im Softwarebereich und Weiteres mehr beeinflussen die digitale (und zunehmend auch die analoge bzw. reale) Souveränität von Firmen und Bürgern.

Für jeden Einzelnen als Souverän ist es daher zentral, sein eigenes Nutzungsverhalten kritisch zu hinterfragen und sich mit möglichen Alternativdiensten auseinanderzusetzen. Teil dieses Prozesses ist es, ein Bewusstsein für den Wert der eigenen Daten und die jeweiligen Konsequenzen einer Weitergabe zu schaffen. Die DSGVO bietet dabei den Rechtsrahmen für das Grundrecht auf die eigene Datenhoheit, das allerdings auch wahrgenommen werden muss. Ein solcher Prozess ist kein Selbstläufer; Alternativen müssen recherchiert werden und allzu oft sind diese hinsichtlich des Nutzererlebnisses weniger komfortabel oder eventuell sogar kostenpflichtig. Neben der Bequemlichkeit müssen also gegebenenfalls auch weitere Hürden überwunden werden, was nur gelingt, wenn einem der Zweck des Handelns bewusst ist und als erstrebenswert gilt.

Auch für Firmen ist es geboten, sich aktiv mit alternativen Anwendungen auseinanderzusetzen und diese – wo immer möglich – einzusetzen. Das kann helfen, die IT-Sicherheit zu erhöhen und die Abhängigkeit vom zukünftigen Support eines Anbieters zu reduzieren. Gerade im Open Source Umfeld gehen damit meist auch Kostenersparnisse einher.

In beiden Fällen bedarf es eines Zugangs zu Wissen, Zeit und einer existierenden Wahlfreiheit, um überhaupt im Digitalen souverän agieren zu können. Das bedeutet erstens, dass

Für jeden Einzelnen als Souverän ist es zentral, sein eigenes Nutzungsverhalten zu hinterfragen.

die Entscheidungshoheit (Souveränität) über die Verwendung der Daten vorliegen muss. Zweitens muss eine sichere (souveräne) Entscheidung aufgrund der eigenen Informiertheit überhaupt möglich sein.

Der Politik kommt in diesem Bereich somit eine tragende Gestaltungsrolle zu. So können durch entsprechende Rahmenbedingungen die nötigen Voraussetzungen für Bürger und Firmen geschaffen werden, um freie Entscheidungen im Digitalbereich zu ermöglichen.

Neben der Definition von Anforderungen hinsichtlich der Interoperabilität für staatliche Dienstleistungen/Bürgerdienste gilt es zudem, gezielt europäische Software-Entwicklungen auf Basis von Standardprotokollen und offenem Quellcode zu fördern.

Der erste Computer wurde in Berlin erfunden, das offene Betriebssystem Linux in Finnland, dennoch kommen die großen Player im Digital-Bereich (Stichwort: Big Tech) aus Amerika. Europäische Anbieter spielen bis auf einige Ausnahmen eine untergeordnete Rolle. Zudem arbeitet der Großteil der hiesigen Ämter und Behörden mit proprietären Systemen einiger weniger Anbieter. Der Versuch der Stadt München, durch Umstellung auf ein Linux-System (Projekt „LiMux“) an Souveränität



Daniel Krezdorn

Daniel Krezdorn ist promovierter Wirtschaftsingenieur und beschäftigt sich bereits seit 2013 mit der digitalen Entwicklung und deren Implikationen für sich und die Gesellschaft. 2019 begann er auf dem Blog www.digital-souveraenitaet.de über seine Erfahrungen auf dem Weg hin zu mehr digitaler Souveränität zu schreiben.

Kontakt

kontakt@digital-souveraenitaet.de

DIGITALISIERUNG

Loading...

Es ist ein gesetzgeberisches Vorgehen notwendig.

zu gewinnen, scheiterte 2017 unter anderem auch am mangelnden politischen Willen. Im Bereich der Betriebssysteme für Mobiltelefone sieht es nicht anders aus, und das Quasi-Duopol zwei amerikanischer Firmen scheint unveränderbar. Der Staat muss sich dann – wie bei den Corona-Apps geschehen – deren Bedingungen diktieren lassen und ist vom Wohlwollen zur Bereitstellung benötigter Software-schnittstellen abhängig.

Dabei gibt es zum Beispiel mit „/e/“ und dem Nokia-Nachfolger „SailfishOS“ (Jolla) vielversprechende Alternativsysteme, die allerdings bisher keine breite Unterstützung erfahren. Letzteres konnte nach finanziellen Schwierigkeiten nur durch eine Beteiligung des russischen Telekommunikationsanbieters „Rostelecom“ überleben, der jetzt Teile des Systems für ein eigenes Handybetriebssystem nutzt.

Auch andere Staaten (z.B. Bolivien) versuchen, Alternativen für ihre Verwaltungen und Bevölkerung zu schaffen. Frankreich etwa beschloss schon 2019, die interne Behördenkommunikation auf nationaler Ebene unter Nutzung des offenen Matrix-Protokolls zu organisieren. Dies ermöglicht eine verschlüsselte Kommunikation auf dezentraler Basis. In Deutschland entschied sich die Bundeswehr 2020 ebenfalls für den Einsatz dieses Protokolls in der internen Kommunikation. Auch die vor einigen Monaten getroffene Entscheidung der Gematik, für den Gesundheitsbereich einen Messenger basierend auf diesem Protokoll bereitzustellen, stimmt positiv. Daneben hat die Politik auch im Bereich der kritischen Infrastrukturen Handlungsbedarf erkannt und versucht, mit strikteren Richtlinien zur Vergabe und Unternehmensübernahmen zumindest die böswillige Einmischung anderer Staaten zu erschweren.

Dennoch: Sollen zentrale Bürgerdienste in Zukunft online und mobil angeboten werden, ist es zwingend notwendig, dass der Staat seine Bürger souverän entscheiden lässt, wie und in welchem Umfang sie diese Systeme nutzen möchten. Dazu kann auch gehören, Schnittstellen für freie Programmentwicklungen bereitzustellen und eine dezentral ausgerichtete

Architektur anzustreben. Dies ermöglicht die notwendige Interoperabilität und öffnet den Markt, sodass Alternativen entstehen können. Vor dem Hintergrund der immer älter werdenden Bevölkerung ist es aber auch von Nöten zu hinterfragen, was wirklich digital sinnvoller erbracht werden kann, respektive, was analog besser und niederschwelliger funktioniert.

Ein solches Vorgehen wird nicht nur die Akzeptanz solcher Bürgerdienste sowie deren Ausfallsicherheit erhöhen, sondern auch die Abhängigkeit von wenigen Dienstleistern – zu meist aus dem nicht-europäischen Ausland – minimieren. Die Entscheidung, für die Einsicht in die eigene elektronische Gesundheitsakte zunächst ausschließlich eine App anzubieten und die vormals angedachte Automatenlösung zu streichen, ist nicht nur das falsche Signal. Sie unterminiert auch die digitale Souveränität. Einerseits wird durch die verpflichtende Nutzung eines bestimmten Endgeräts ein Großteil der Bevölkerung ausgeschlossen und andererseits ein nicht zu unterschätzendes Sicherheitsrisiko geschaffen.

Auch abseits des staatlich-institutionellen Wirkungsbereichs ist ein beherzteres gesetzgeberisches Vorgehen notwendig, um gewünschte Rahmenbedingungen zu schaffen. Das betrifft etwa eine Anpassung des Wettbewerbsrechts hinsichtlich kostenfreier Online-dienste, um die im Digitalbereich aufgrund von Netzwerkeffekten besonders starke Tendenz zur Monopolbildung zu unterbinden. Die amerikanische Wettbewerbsbehörde FTC arbeitet bereits an einer solchen Novelle.

Zudem können durch eine verpflichtende Nutzung von Standardprotokollen sowie der Pflicht zur Bereitstellung von Schnittstellen die Interoperabilität und Öffnung von Plattformen für fremde Entwicklungen gefördert werden. Ähnlich wie bei anderen Normen zum Schutz der Verbraucher könnten zusätzlich Kriterien definiert werden, die

Es bedarf des Zugangs zu Wissen, um überhaupt im Digitalen souverän agieren zu können.

Lernen funktioniert heutzutage nicht mehr nur analog.

sicherstellen, dass z.B. Mobiltelefonanbieter analog zum PC-Markt eine freie Softwarenutzung ermöglichen müssen oder einen freien App-Marktplatz und Zugang garantieren. Das erhöht nicht nur die Auswahlfreiheit und Datenportabilität für Firmen und Kunden, sondern bietet wiederum auch neuen Marktteilnehmern Chancen.

Für den geschäftlichen Bereich gibt es neben Gaia-X und dem BMWI-Programm Smart Service Welt II bereits einige Projekte. Nur im Verbraucherbereich fehlt es bisher noch an ausreichender Unterstützung. Immerhin versucht die EU, mit dem Digital Markets Act und dem Digital Service Act (DMA bzw. DSA) ein europaweites Regelwerk zur verpflichtenden Öffnung zentraler Plattformen und für einen höheren Verbraucherschutz zu schaffen.

In diesem Zusammenhang gilt es auch zu überlegen, wie mit Datendienstleistungen umgegangen werden soll, die aufgrund hoher irreversibler Investitionskosten (sunk costs) nicht privatwirtschaftlich rentabel und marktkonform erbracht werden. Eine Möglichkeit wäre, den Staat, wie teilweise im Analogbereich auch, mit Bereitstellung und Erhalt der nötigen Infrastruktur gegen eine Nutzungsgebühr zu betrauen. Neben einem öffentlichen Internetsuchindex, auf den jeder Anbieter zugreifen kann, wären etwa auch dezentrale Datenhubs denkbar, über die Bürger ihre Daten gezielt einzelnen Firmen zugänglich machen können.

Zuletzt seien noch die Schulen und Universitäten im propagierten Bildungsland Deutschland erwähnt. Auch hier zeigte die Pandemie überdeutlich, welche Defizite nicht nur in der Hardwareausstattung vorherrschen. Lernen funktioniert heutzutage nicht mehr nur analog. Dennoch ist es nicht damit getan, jedem ein Tablet zu verschaffen. Das Thema digitale Souveränität und die Implikationen einer fehlenden Auseinandersetzung damit werden leider häufig eher stiefmütterlich behandelt und dem Einzelnen überlassen. Das mangelnde Bewusstsein dafür zeigte sich nicht zuletzt in der hastigen Umstellung auf Homeschooling, das in jedem Bundesland

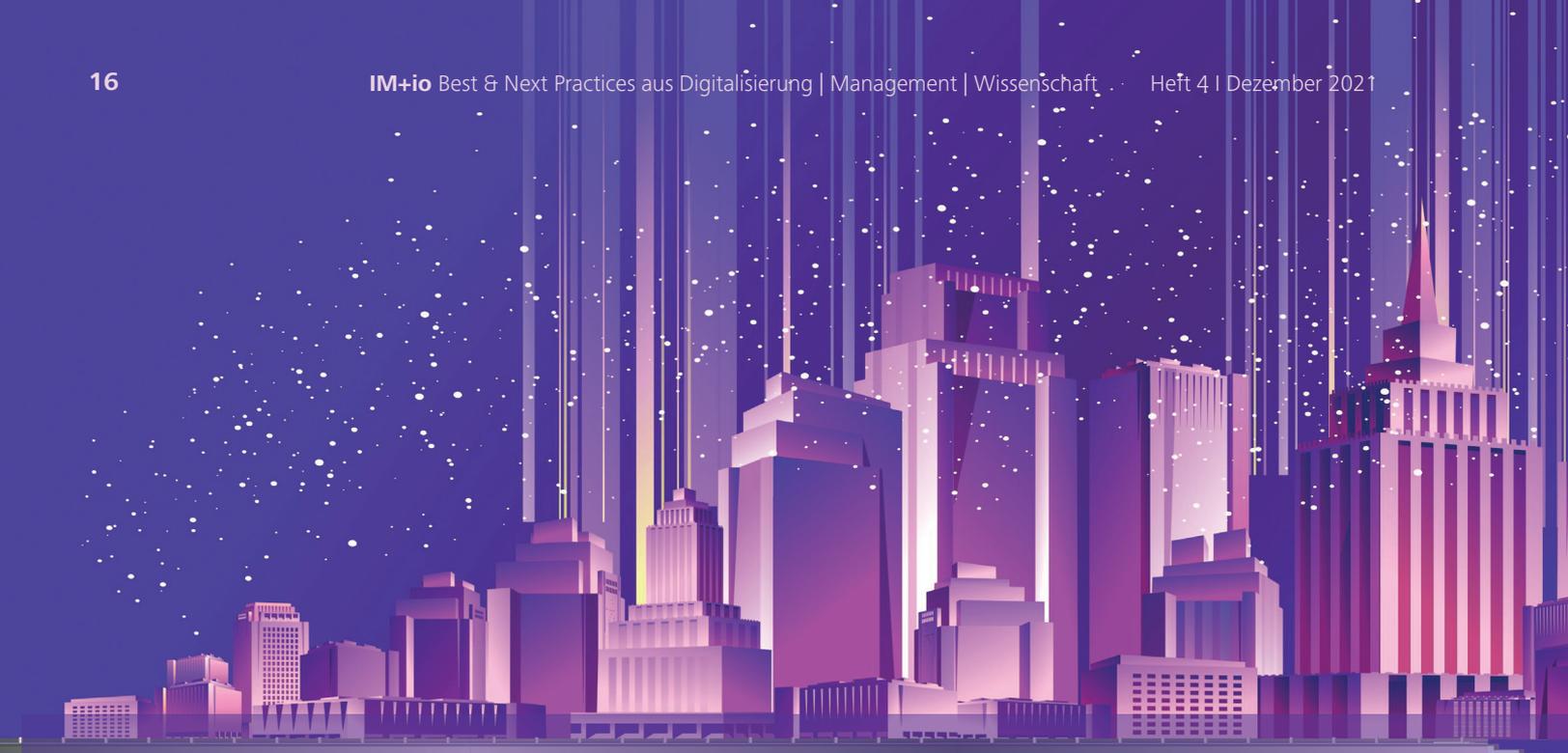
anders gehandhabt wurde und trotz Datenschutzbedenken allzu oft mit einem Rückgriff auf teure und proprietäre Systeme endete. Und auch im Unterricht stehen primär (Standard-)Anwendungen und Schulungen darin im Vordergrund. Selten werden Alternativen vorgestellt und anwendungsunabhängige Grundfunktionalitäten vermittelt. Trotzdem sind viele Schüler deutlich aufgeklärter, reflektierter und souveräner im Digitalbereich als die Elterngeneration.

Primäres Ziel der Politik sollte daher nicht nur eine stärkere Berücksichtigung von digitaler Souveränität in all ihren Facetten in Lehrkonzepten sein. Vielmehr müssen allen Menschen – unabhängig von ihrem Alter – Methoden zum kritischen Hinterfragen des Nutzungsverhaltens und mögliche Alternativen an die Hand gegeben werden. Der Erfolg des Wahl-O-Mats als staatlich initiierte Online-Orientierungshilfe zeigt dabei, dass die Bürger solche Angebote dankend annehmen.

Die Pandemie und die zahlreicher werdenden Berichte über die negativen Effekte für die Gesellschaft, insbesondere von Big Tech, zeigen überdeutlichen Handlungsbedarf im Digitalbereich. Mit politischem Gestaltungswillen und finanziellen wie personellen Anstrengungen kann es aber gelingen, Barrieren im Digitalraum abzubauen und die nötige Interoperabilität von Softwaresystemen zu etablieren. Damit kann die Politik die Voraussetzungen für die digitale Souveränität jedes Einzelnen schaffen. ■

Kurz und Bündig

Digitale Souveränität ist eine gesamtgesellschaftliche Aufgabe. Neben der Bereitschaft zur Auseinandersetzung mit der Thematik bedarf es dafür des Zugangs zu Wissen und einer tatsächlichen Wahlfreiheit, um als Einzelner auch im Digitalbereich souverän agieren zu können. Die Politik kann mit Gestaltungswillen und Einsatz die nötigen Voraussetzungen dafür schaffen und so ihrer tragenden Rolle gerecht werden.



Banking goes Blockchain

Die Transformation des Bankensektors nimmt Fahrt auf

Hartmut Giesen, Sutor Bank

In der „frühen“ Fintech-Zeit der 2010er Jahre gab es eine Grafik in unendlich vielen Versionen: darauf eine Übersicht mit Fintech-Startups, die verschiedene klassische Bankendienstleistungen schöner, schneller, digitaler anboten. Prophezeit wurde, dass die Banken damit verschwänden. Banken gibt es heute noch immer, auch wenn einige Fintechsbanken wurden oder Banken kauften. Umgekehrt haben auch Banken Fintechs gekauft. Heute kann man eine ähnliche Grafik wieder zeichnen, nur dass dort statt Fintechs Kryptotechs auftauchen. Das heißt: Für jede klassische Bankendienstleistung gibt es inzwischen einen blockchain-basierten Service, angeboten entweder durch Unternehmen – Kryptotechs – oder durch ein Ökosystem, das sich um eine Blockchain gebildet hat.

Die Blockchain-Apologeten prophezeien auch jetzt wieder, dass dezentrale (=Blockchain basierte) Finanzanwendungen, die grundsätzlich ohne zentrale Vertrauens- oder Clearingstelle auskommen, den Banken den Garaus machen werden. Vermutlich werden Banken auch diesen Digitalisierungsschub als regulierte Entitäten, Säulen des Finanzmarkts und Transmissionsriemen für die Realwirtschaft überleben. Doch die Blockchain wird die Geschäftsmodelle und die

grundlegende Technologie-Architektur von Banken wesentlich mehr verändern als die Fintech-Revolution. Die Institution Bank wird in ein paar Jahren nicht mehr viel mit dem Wesen der Bank von heute zu tun haben.

Das Führen von Konten sowie der (Besitz-) Transfer von Werten ist prinzipiell eine Art von Datenmanipulation, für die sich die nach dem Zweiten Weltkrieg auftauchenden Computer ideal eigneten. Deshalb gehörten Banken nach den Wissenschaftlern zu den IT-Anwendern der



Adobe Stock | 273445755 | marrishuanna



Hartmut Giesen

Seit 2012 realisiert Hartmut Giesen für die Sutor Bank digitale Geschäftsmodelle. Zu seinen Aufgaben gehören das Business Development Fintech, digitale Partner und Crypto/Blockchain, der Auf- und Ausbau der Sutor Banking-Plattform und die Betreuung interner Digitalisierungsprojekte. Zuvor war er im Hightech-Marketing unter anderem als Agentur-Vorstand und Gründer einer eigenen Agentur unterwegs. An der RWTH Aachen hat Hartmut Giesen Germanistik und Physik studiert. Sutor Bank ist der Banking-as-a-Service-Partner von erfolgreichen Fintechs wie Zinspilot, Growney, Fairr.de oder Fintiba. Über das Plattform-Banking hinaus ist die Sutor Bank im Private Banking, im Stiftungsmanagement und im B2B-Banking für Finanzvertriebe aktiv.

Kontakt

hartmut.giesen@sutorbank.de

ersten Stunde. Sie mussten sehr viele Daten sehr exakt möglichst schnell bearbeiten und hatten die Budgets, um die IT-Investitionen zu stemmen. Die IT machte größere Banken mit größeren Bilanzen möglich, denen effizientere Systeme für Zahlungsverkehr, Kreditwesen und Kapitalmärkte zur Verfügung standen, um komplexere Finanz- (Werte-) Transaktionen zu ermöglichen. Sieht man von Finanzproduktinnovationen für Spezialanwendungen ab, änderten sich weder das „Basismodell“ Banken noch deren Produkte und Prozesse. Nur liefen sie jetzt mehr oder weniger IT-basiert ab.

Fintechs digitalisieren Frontends

In den 10er Jahren dieses Jahrhunderts begannen Fintechs die Möglichkeiten der digital-mobilen Vernetzung zu nutzen und entwickelten tatsächlich neue Geschäftsmodelle, die Banken bisher nicht angegangen waren: Robo-Advising, Peer-to-Peer-Lending, Social Trading oder Crowd Funding sind nur einige Geschäftsmodelle, mit denen Fintechs zum Teil zu „Unicorns“ gewachsen sind. Bei näherem Hinsehen waren aber diese Geschäftsmodelle nur klassische Bankdienstleistungen, die „digital vom Kunden her“, wie die Fintechs gerne sagen, optimiert wurden. Die „Finanz-Frontends“ wurden

mobilen Apple- und Android-Standards angepasst, „Mobile First“ wurde zum Gestaltungsprinzip und Kundenprozesse, wie zum Beispiel grenzüberschreitender Geldverkehr, die Kreditvergabe oder die Geldanlage wurden effizienter und einfacher gestaltet. Hinter jedem Fintech stand aber immer noch eine Bank, die die eigentlichen Finanztransaktionen ausführte und überwachte, mithin die Aufgaben wahrnahm, die sie seit ihrem Entstehen in der Renaissance ausführte.

Nicht-digitalisierte Werte und Regulierung schützten Banken

Dass Banken weiterhin im Zentrum jedes Fintech-Geschäftsmodells standen, hatte einen technischen und einen (aufsichts-) rechtlichen Grund. Der technische Grund ist, dass Werte sich bislang zwar schon digital als Daten darstellen ließen, ihr Vorhandensein und ihr Transfer aber weiterhin den vertrauensvollen Dritten benötigen, der dies beglaubigt. Dieser Akt ließ sich nicht digitalisieren. Deshalb blieben die Banken mit ihren Core-Banking-Systemen auch technisch im Zentrum der „neuen“ Finanzwelt. Darüber hinaus wollten Staaten weiterhin – und darin liegt der rechtliche Grund –, dass Finanzgeschäfte nur Unternehmen durchführen, die

von ihnen streng beaufsichtigt werden. Zu wichtig ist ein funktionierender, stabiler Finanzsektor für die Realwirtschaft und die Geldwertstabilität in einer funktionierenden Volkswirtschaft. Deshalb blieb Fintechs nichts anderes übrig, als mit Banken zu kooperieren, was die meisten taten, oder selbst zu Banken zu werden – ein Weg, den auch einige gingen. Dies hat auch verhindert, dass in der Finanzbranche wirklich disruptive Geschäftsmodelle entstehen konnten, wie etwa Streaming oder Social-Media-Plattformen im Medienbereich, Software-as-a-Service oder Cloud-Computing im Technologie-Sektor oder Plattform-Geschäftsmodelle in Werbung, Handel, Tourismus etc.

Blockchain verändert bei Banken Geschäftsmodelle und Technologie

Mit der Blockchain, hier synonym für alle dezentrale Technologien genutzt, ändert sich die technologische Lage jetzt aber auch in der Finanzbranche grundlegend: Das Konzept, das Satoshi Nakamoto für den Bitcoin erstmals entwickelt hat und das durch inzwischen ungezählt weitere Blockchain-Architekturen weiter verfeinert wurde, ermöglicht erstmals die digitale Schaffung, Verbreitung und Verarbeitung von nicht-dinglichen Werten, ohne dass eine Bank diese Aktivitäten ausführt oder beglaubigt. Die digitalen Konsensprozesse, die Teil jeder Blockchain sind, übernehmen jetzt die Aufgabe der Banken. Vertrauen wird digitalisiert, und damit wird die vollständige Digitalisierung, von Werten möglich. Werte lassen sich nun wie Informationen schaffen, verarbeiten und verbreiten. Und da die Blockchains sich als Schicht auf die existierende Internet-Infrastruktur legen, gibt es auch schon die Bahnen für den unbegrenzten Wertetransfer.

Die zuerst mit Ethereum entwickelte Blockchain-Erweiterung, mit der Werterzeugung oder -transfer in technisch codierte Bedingungsketten – sogenannte Smart Contracts – eingebettet werden kann, reduziert die Rolle der Banken als Instanz, die alleine Finanztransaktionen ausführen kann, weiter. Obwohl die Digitalisierung von Werten wahrscheinlich die

gleichen umwälzenden Auswirkungen haben wird wie die Digitalisierung von Informationen, werden Banken weiter bestehen. Denn die Staaten werden wie bisher darauf bestehen, dass die Finanzwelt reguliert bleibt. Sie sind als Regulierungshubs und makroökonomische Transmissionsriemen, über die sich das gesamte Finanzsystem kontrollieren und steuern lässt, unverzichtbar. Staaten benötigen Banken weiterhin als Kontrollinstanzen, die dafür sorgen, dass Geldwäsche, Terrorismusfinanzierung und sonstige Straftaten im Sinne des GWG verhindert werden. Genauso werden sie von Zentralbanken benötigt, die durch das Setzen von geldpolitischen Parametern die Geldschöpfung und Kreditvergabe von Geschäftsbanken beeinflussen und damit für die Stabilität von Wirtschaft und Geld sorgen.

Neue Technologiearchitektur für Banken

Aber die technische Infrastruktur von Banken wird künftig wahrscheinlich komplett anders aussehen: Statt Core-Banking- und Wertpapier-Handelssystemen betreiben sie Blockchain-Knoten und bieten Wallets an, in denen digitale Währungen gehalten werden. Die Parameter für die Geldschöpfung und Kreditvergabe werden von Zentralbanken in die Protokolle der entsprechenden Blockchains programmiert. Kapitalmarktakteure sind über Blockchains vernetzt, die Schnittstellen zu den Geldblockchains besitzen. Die Vergabe von Krediten oder der Handel von Wertpapieren werden durch Smart Contracts automatisiert ausgeführt.

Dass die Banken als regulierte Entitäten erhalten bleiben, heißt nicht unbedingt, dass die heutigen Banken als Unternehmen bestehen bleiben. Denn sie müssen die technische Transformation von der heutigen zentralen „Core-Bankingarchitektur“ zu dezentralen Blockchainnetzwerken schaffen und ihre Prozesse darauf hin ausrichten. Tun sie dies nicht, laufen sie Gefahr, von den heute noch unregulierten Kryptotechs abgelöst zu werden. Schon jetzt ist sichtbar, dass erfolgreiche Kryptounternehmen Lizenzen erwerben oder Banken kaufen, um ihr Geschäft regulierungsfest zu machen.

Banken sind als Regulierungshubs und makroökonomische Transmissionsriemen unverzichtbar.

Optimierungspotenzial der Blockchain zwingt zur Innovation

Nun wird bereits sichtbar, welche gewaltigen Optimierungspotenziale die Blockchaintechnologie hat. Klar wird dies, wenn man beispielsweise betrachtet, welchen Wandel eine Blockchain-basierte digitale Zentralbankwährung bedeuten würde, an der heute bereits eine Reihe von Staaten inklusive der EU arbeiten (Central Bank Digital Currency = CBDC). Im Gegensatz zu anderen längst im Gebrauch befindlichen digitalen Geldformen auf Konten, Karten oder Wallets, die eine Forderung der Kunden gegenüber Geschäftsbanken auf die Herausgabe von Bargeld (=Papiergeld) darstellen, sind die CBDC wie Bargeldforderungen gegenüber Zentralbanken. CBDC ersetzen Papiergeld als bisher einzige Form von Zentralbankgeld. CBDC können von ihren Besitzern in eigenen Wallets statt auf Bankkonten gehalten werden. Sie können sie direkt transferieren, ohne dass jede Transaktion durch das Bankensystem gezogen wird und erst nach ein bis drei Tagen abgeschlossen ist. Damit werden Konten und Einlagen bei Banken überflüssig, genauso wie die gesamten Zahlungsverkehrssysteme, die Banken mit großem Aufwand unterhalten. So fallen wesentliche Säulen des traditionellen Bankengeschäftsmodells weg.

Weitere Prozesse und damit verbundene Systeme entfallen, weil CBDC-Transaktionen in Echtzeit ablaufen und Gegenparteirisiken verschwinden, die bisher Banken als vertrauenswürdige Intermediäre – als Geldnotare gewissermaßen – gemanagt haben. Zu diesen verschwindenden Gegenparteirisiken gehört, dass Kunden nicht um ihre Einlagen bangen müssen, falls eine Bank einmal in Schieflage geraten sollte; Einlagensicherungsfonds verlieren damit ihren Sinn. Banken werden so – zumindest zum Teil – von Bilanz- zu Service-Unternehmen.

Von der technischen Frontend- zur End-to-End-Revolution

War die Fintech-Revolution in erster Linie eine Frontend-Revolution, ist die sich anbahnende Blockchain-Revolution eine End-to-End-Revolution, die Geschäftsmodelle, Kernprozesse und -technologien betrifft. Die wahren Auswirkungen der Blockchain-Revolution werden wir – Unternehmen und Kunden – aber vielleicht erst in ein paar Jahren erleben und

spüren. Andrew McAfee und Erik Brynjolfsson haben in „Machine, Platform, Crowd“ dargestellt, dass disruptive Technologien erst in der jeweils nächsten Unternehmensgeneration ihr volles Potenzial entfalten.

Nach der Erfindung der Elektrizität ersetzen die Unternehmen die zentralen Dampftriebe zunächst einfach durch zentrale Elektromotoren. Erst später lernten sie das Dezentralisierungspotenzial einzusetzen und Elektromotoren direkt in die Maschinen an den Aktoren einzubauen und damit Industrieanlagen mit ganz neuen Ausmaßen zu konstruieren. Ähnlich wurden in der ersten Digitalisierung in allen Branchen zunächst nur die Prozesse digitalisiert, bevor damit begonnen wurde, neue Geschäftsmodelle zu entwickeln – dies waren dann in der Regel die Newcomer, die damit mobile Smartphones oder Plattformen bauten.

Dies beobachten wir auch in der Adaption der Blockchain-Technologie: Im ersten Schritt werden bestehende Prozesse ‚blockchainisiert‘, erst dann kommen die Blockchain-basierten Geschäftsmodelle, mit dem Unterschied, dass die Regulierung für diese Geschäftsmodelle Lizenzen vorschreiben wird. Die Möglichkeiten von dezentraler Geldschöpfung, programmierbarem Geld, Smart Contracts oder der ‚Tokenisierung‘ von Werten aller Art werden erst die Banken der nächsten Generation erkennen und in neue Geschäftsmodelle umsetzen, die wir heute noch gar nicht absehen können. Der Bankensektor wird damit in den nächsten Jahren zu einer der spannendsten Arenen für den digitalen Wandel werden. ■

Kurz und Bündig

Der Bankensektor wird in den nächsten Jahren zu einer der spannendsten Arenen für den digitalen Wandel werden. Jetzt nutzen Kryptotechs ihre Chance: Mit der Blockchain ändert sich die technologische Lage in der Finanzbranche grundlegend: Das Blockchain Konzept ermöglicht erstmals die digitale Schaffung, Verbreitung und Verarbeitung von nicht-dinglichen Werten, ohne dass eine Bank diese Aktivitäten ausführt oder beglaubigt.

WEBINARE & SEMINARE

LIVE. TOP BEWERTET. INDIVIDUELL BUCHBAR.



**WE TRANSFORM.
YOU PERFORM.**

Mit unseren Webinaren und Seminaren verwandeln wir Ihr digitales Denken. Strategische Planung und praxisnahe Anwendungsszenarien stehen bei uns im Mittelpunkt. Ob live, remote, hybrid oder individuell, wir bieten Ihnen maximale Information in kürzester Zeit.



Erfahren Sie mehr unter
www.aws-institut.de/webinare

August-Wilhelm
Scheer Institut
Digital Research 

WWW – world wide web oder wilder Wilder Westen?

Dirk Werth, Chefredakteur IM+io



Dr. Dirk Werth

Dr. Dirk Werth ist seit 2016 Chefredakteur der IM+io. In der Kolumne „MehrWerth“ schreibt er in pointierter Form Meinungsbeiträge zum Schwerpunktthema des Heftes und stellt diese zur Diskussion.

Kontakt

dirk.werth@aws-institut.de
www.aws-institut.de

Es ist ein viel kolportierter Vergleich, dass Daten das neue Öl sind. Und es ist auch viel Wahres daran: Nicht nur, weil Daten zu einem Wirtschaftsgut geworden sind – wenn auch mit Blick auf die Rechtslage noch nicht richtig, aber dazu später mehr, sondern auch, weil Daten eine neue Industrie begründet haben, die zu einer Wirtschaftsmacht geworden ist – und die zu mono- bzw. oligopolartigen Verwerfungen geführt hat. Ähnlich wie ein Rockefeller im Boomzeitalter des Erdöls mit seiner Standard Oil Company den Markt beherrschte, so haben heute die GAFAMs (Google, Apple, Facebook, Amazon, Microsoft) eine ähnliche Marktstellung. Und es mehren sich die kritischen Stimmen, gerade in Europa.

Unbestrittene Tatsache bleibt, dass die Daten explodieren: Sowohl im Umfang – das erzeugte Datenvolumen wächst aktuell exponentiell – als auch in der Qualität. Die oben genannten GAFAMs kennen uns besser, als es die eigene Familie tut. Das kann positive aber auch negative Wirkung haben. Insofern ist es folgerichtig und konsequent nach dem Motto „Meine Daten gehören mir“ die Datensouveränität in den Mittelpunkt zu stellen. Wenn Daten zunehmend und vielfältig genutzt werden, so ist es essenziell, hierüber die Kontrolle zu behalten. Diese Kontrolle zu erreichen ist alles andere als trivial: Herausforderungen sind dabei sowohl technischer als auch konzeptioneller und rechtlicher Art. Bleiben wir beispielsweise beim „Meine Daten gehören mir“. Ist das wirklich so? Hochinteressant und vielleicht etwas befremdlich ist die rechtliche Behandlung von Daten. Hier kann nämlich von einem neuen Öl, also einem Wirtschaftsgut, keine Rede sein. Tatsächlich betrachtet das deutsche Rechtssystem Daten nicht als Sache – mit weitreichenden Folgen. Denn damit gibt es kein Eigentums- oder Besitzrecht an Daten, also kein absolutes Recht, das für jedermann gleichermaßen gilt. Vielmehr müssen in Bezug auf spezifische Daten die beteiligten Parteien

bilateral vertraglich vereinbaren, was und in welcher Form gelten soll. Ein immenses Hindernis, das nicht nur aufwendig in der Umsetzung ist, sondern vielfach auch eine Datennutzung verhindert – mangels rechtlicher Sicherheit.

Ich kann diesen Umstand historisch gut nachvollziehen: Schließlich hat sich im 19. Jahrhundert, als die Grundzüge der Rechtsordnung geschrieben wurden, sicher niemand Gedanken über digitale Daten als Wirtschaftsgut gemacht. Aus heutiger Sicht betrachtet, muss ich klar kritisieren, dass es der Gesetzgeber bislang nicht für notwendig erachtet hat, hier nachzuziehen, und das, obwohl die Bedeutung von Daten und datengetriebenen Geschäftsmodellen seit mehr als einer Dekade bekannt ist. Denken wir mal, was gewesen wäre, wenn man Erdöl die Eigenschaft als Wirtschaftsgut abgesprochen hätte. Irgendwie schwer vorstellbar...

Wenn aber die Daten das Öl sind, was ist dann der Motor? Denn Daten alleine liefern per se ja noch keinen Mehrwert. Vielmehr geht es um die Frage, was mache ich mit den Daten? Nutze ich sie zur Analyse und Optimierung von Produkten, zur Vorhersage von Verschleiß oder zum Profiling von Benutzern? Kurzum, der Mehrwert entsteht durch das, was man mit den Daten erreichen kann. In Denglisch „Services“ genannt. Der kometenhafte Aufstieg der „künstlichen Intelligenz“ in den letzten Jahren (im eigentlichen Sinne des maschinellen Lernens) hängt direkt mit der Verfügbarkeit großer Datenmengen zusammen. Insofern ist es auch nicht verwunderlich, dass diejenigen, die die meisten Daten besitzen, – Entschuldigung, gesammelt haben, – die führenden KI-Unternehmen darstellen.

Wenn wir beim Vergleich mit dem Öl bleiben wollen, so hat das, was ich aktuell beobachte, schon etwas vom Wilden Westen. Das zu ändern, ist die Kernherausforderung dieses Jahrzehntes. Also, lasst uns den Colt umschnallen und uns aufs digitale Pferd schwingen. ■



Wie luca aus der Krise hilft

Mit der luca App gemeinsam aus der Pandemie

Im Gespräch mit Patrick Hennig, neXenio

Bei der Erwähnung der neXenio GmbH begegnet man gemeinhin fragenden Blicken, denn bei dieser Ausgründung des Hasso-Plattner-Instituts ist das Produkt der Markenkern, die luca App. Gemeinsam mit einigen Kulturschaffenden, wie der Band „Die Fantastischen Vier“ gründete das Team von neXenio die luca-Initiative. In Corona-Zeiten soll so die schnelle und lückenlose Kontaktrückverfolgung im Austausch mit den Gesundheitsämtern erfolgen, unterdessen ist die App in vielen Bundesländern im Einsatz, in Hamburg etwa ist sie flächendeckend Voraussetzung zum Check-in in der Gastronomie. Wie und ob die Datenübermittlung funktioniert, hat Patrick Hennig, CEO von neXenio im Gespräch mit der IM+io erläutert.



Patrick Hennig

Patrick Hennig ist CEO und Mitgründer der neXenio GmbH sowie seit 2020 einer der Geschäftsführer der culture4life GmbH, der Firma hinter luca. Nach einem Master in IT-Systems Engineering und mehreren erfolgreichen Forschungsprojekten am Hasso-Plattner-Institut in Potsdam gründete er zusammen mit Philipp Berger im Jahr 2015 neXenio. Gemeinsam verfolgen sie mit ihrem Team das Ziel, Sicherheit, Data Privacy, Integration und UX in Produkten zu vereinen.

Kontakt

hello@luca-app.de

IM+io Herr Hennig, bei Ihrer Gründung im Jahr 2015 konnte noch niemand ahnen, dass man pandemiebedingt eine engmaschige Kontaktnachverfolgung brauchen würde. Was war Ihr ursprüngliches Businessmodell?

PH: Unser Unternehmen neXenio ist eine Ausgründung des Hasso-Plattner-Instituts in Potsdam, an dem mein Partner Philipp Berger und ich studiert haben. Unsere Vision war es, die Erkenntnisse der dortigen Forschung für die Wirtschaft zugänglich zu machen, durch Produkte, die in Unternehmen genutzt werden können. Vor diesem Hintergrund wurden auch unsere anderen Projekte entwickelt, wie z. B. das neXboard, SEAMLESSme und die Cloudlösung bdrive der Bundesdruckerei. Das Ziel von unserem Team bei neXenio ist es, Sicherheit, Data Privacy, Integration und User Experience in diesen Produkten zu vereinen – Nutzerfreundlichkeit und Sicherheit, zwei Themen, die sich ergänzen müssen. Als Corona kam, haben wir uns gefragt, wie wir mit unseren Kenntnissen und Ressourcen einen Mehrwert schaffen können und die Gesundheitsämter sicher und möglichst unkompliziert in der

Pandemie unterstützen können. So entstand im Spätsommer 2020 die Idee, die Gesundheitsämter digital mit den Bürgerinnen und Bürgern zu verbinden – luca war geboren. Übrigens stand am Anfang kein Businessmodell hinter luca.

IM+io Mit der luca App soll eine schnelle und lückenlose Kontaktrückverfolgung im Austausch mit den Gesundheitsämtern über eine verschlüsselte und sichere Datenübermittlung erfolgen. Wie funktioniert das?

PH: Luca ist viel mehr als nur eine App, hinter luca steckt ein komplettes System, das ineinandergreift und so dafür sorgt, dass Infektionsketten schnell unterbrochen werden. Dazu zählen die App, die die Gäste auf ihrem Handy nutzen, aber auch „luca-Locations“, der Zugang für die Betriebe und vor allem die „luca-Software“ für die Gesundheitsämter. Diese digitale Verbindung zwischen Nutzern und Nutzerinnen, den Locations und den Gesundheitsämtern ist das, was luca einmalig macht. Hinter diesem System steht ein komplexes Sicherheitskonzept, die Daten der Nutzer sind sicher, und nur das

Luca App- Registrierte Bürger

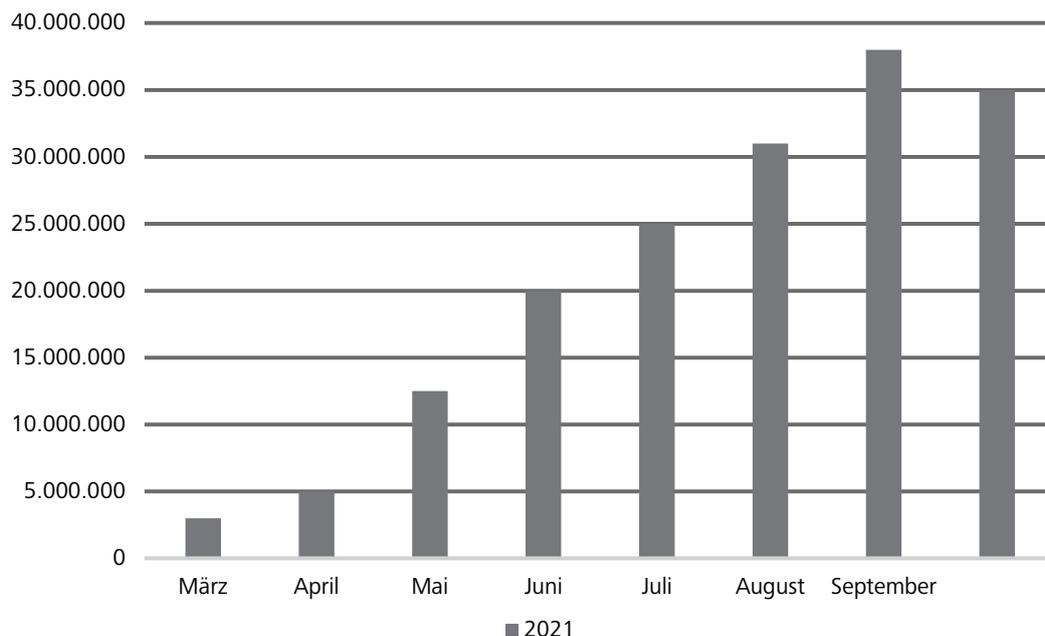


Abbildung 1: Registrierte Nutzer der luca App in 2021. Stand: Oktober 2021. © luca

Gesundheitsamt kann sie im Falle einer Kontaktnachverfolgung entschlüsseln. Erst durch die Eingabe der benötigten Sicherheitsschlüssel können die entsprechenden Daten eingesehen und so die betroffenen Gäste gewarnt werden. Wir führen gerade Schritt für Schritt unser bisher größtes Update luca+ ein. Mit diesem Update passen wir uns den neusten Entwicklungen der Pandemie an. Wir berücksichtigen die Schwerpunktnachverfolgung für 2G und 3G sowie eine intelligente Kontaktrückverfolgung und Cluster-Erkennung. Damit wird es in Zukunft für die Gesundheitsämter einfacher, und Anwender können noch schneller informiert werden.

IM+io Manche Gesundheitsämter beklagen, dass die luca App Daten für sie kaum nutzbar seien. Zum einen müssen sie händisch in die dort im Einsatz befindliche Software Sormas übernommen werden, zum anderen definieren Veranstalter und Gastronomen nicht selten die einzelnen luca Erfassungsgebiete zu großräumig, um eine realistische Gefährdung einzelner Personen einschätzen zu können. Was entgegnet Sie diesen Kritikern?

PH: Die Gesundheitsämter sind der Schlüssel in dieser Pandemie. Durch sie können Infektionsketten erkannt und unterbrochen werden. Und genau dabei möchte luca ihnen unter die Arme greifen, um diese Aufgabe so einfach wie möglich zu machen. Für viele Gesundheitsämter ist es erstmal ungewohnt, ein

neues System anzuwenden, das haben wir in den letzten Wochen immer wieder gemerkt. Uns ist es aber wichtig, dass die Gesundheitsämter wissen, dass wir nicht einfach nur ein Programm bereitstellen, sondern selbstverständlich auch den entsprechenden Support dazu anbieten. Wenn ein Gesundheitsamt Fragen oder Probleme bei der Nutzung von luca hat, kann es uns jederzeit erreichen. Dazu haben wir eine E-Mail-Adresse und auch eine Telefonnummer ausschließlich für die Gesundheitsämter eingerichtet, am Wochenende werden die Anrufe auf Philipp und mein Handy weitergeleitet – luca ist also quasi 24/7 erreichbar. Außerdem versuchen wir natürlich, den Gesundheitsämtern, aber auch den Betreibern, soweit wie möglich entgegenzukommen und sie bestmöglich über die Nutzung von luca zu informieren. Dafür bieten wir jede Woche Schulungen an, in denen das System detailliert und mit Video erklärt wird, damit eben solche Probleme gar nicht erst auftreten und die Betreiber aufgeklärt werden, wieso eine kleinflächigere Einteilung ihrer Location sinnvoll ist.

Übrigens können die Daten in verschiedenen Formaten exportiert werden, sodass sie auch in anderen Systemen weiterverarbeitet werden können. Auch dabei unterstützen wir die Gesundheitsämter gerne, wenn es Schwierigkeiten gibt.

IM+io Manche Datenschützer hinterfragen Ihr Leistungsversprechen einer „verschlüsselten, sicheren und verantwortungsvollen Datenübermittlung“. Wo liegt hier das Problem?

PH: Die Frage ist komplexer, als sie zunächst klingt. Viele Kritikpunkte, die im luca-Kontext diskutiert wurden, behandeln eigentlich eine Grundsatzfrage: Zentrale oder dezentrale Datenspeicherung? Dabei wird schnell vergessen, dass die allermeisten Plattformen, auf denen wir uns täglich bewegen, die Daten zentral speichern. Hinter luca steht wie gesagt ein komplexes Sicherheitskonzept, und wir sind weiterhin davon überzeugt, dass luca aktuell die beste und sicherste Möglichkeit ist, wenn Kontaktdaten übermittelt werden sollen. Das bestätigten uns auch Datenschützer. Datensicherheit war von Anfang an der Fokus bei luca, der nach wie vor bei jeder Neuerung bedacht wird.

Etwas anderes sind Fehler, die im Prozess gemacht wurden und für die wir uns entschuldigen. Für alle ist es die erste Pandemie, auch für uns. Die Daten der Nutzer und Nutzerinnen waren aber nie gefährdet, denn die sind über zweiteilige Schlüssel jederzeit abgesichert.

IM+io Derzeit ist die luca App vielfach im Einsatz, aber die Pandemie wird ja hoffentlich auf lange Sicht durch breite Impfungen beherrschbar. Haben Sie Pläne für die Zukunft?

PH: Momentan weiß niemand, wie es mit der Pandemie weitergeht und welche Entwicklungen uns noch bevorstehen, auch wir nicht. Wir haben luca entwickelt, um hier und jetzt einen Unterschied zu machen und gemeinsam als Gesellschaft diese Pandemie in den Griff zu bekommen. Ich denke, wir haben in den letzten Monaten viel erreicht: Das gesellschaftliche Leben kehrt zurück, es finden Veranstaltungen statt, Menschen können wieder ins Restaurant gehen – und luca hat dazu beigetragen. Darauf sind wir stolz. Wir haben in dieser Zeit viel gelernt und lernen auch jetzt noch immer weiter dazu. luca ist ein Prozess, ein System, das sich den Entwicklungen und Bedürfnissen der Menschen in dieser Pandemie anpasst.

IM+io Hinter dem luca Team stehen nicht nur die IT-Experten von neXenio, sondern auch Kulturschaffende wie die „Fanta 4“. Wie ist diese Zusammenarbeit entstanden? Welches Interesse und welchen Einfluss hatten diese Kulturschaffenden in der luca Initiative?

PH: Bei luca geht es uns darum, Infektionsketten

Das gesellschaftliche Leben kehrt zurück – und luca hat dazu beigetragen.

zu unterbrechen und somit das Gesellschaftsleben in Deutschland trotz andauernder Pandemie wieder möglich zu machen. Dazu stehen wir in ständigem Austausch mit Epidemiologen, Gesundheitsämtern und Ärzten. Aber auch Menschen aus der Gastronomie und Kulturschaffende, die von der Pandemie besonders betroffen sind und etwas tun möchten, beziehen wir mit ein. Schließlich möchten wir luca den Bedürfnissen der Menschen anpassen, daher ist uns ihre Meinung sehr wichtig. Die Fantastischen Vier waren von Anfang an dabei und sind direkt an der Entwicklung von luca beteiligt. Durch den ständigen branchenübergreifenden Austausch stellen wir sicher, dass wir dort ansetzen, wo luca benötigt wird.

IM+io Wird neXenio künftig wieder allein agieren oder liegt die Zukunft in hybriden Konstellationen wie mit „Fanta 4“?

PH: Unser Ziel bei neXenio ist es immer, das bestmögliche Produkt zu kreieren. Um dieses Ziel zu erreichen, stellen wir unser Team aus Menschen mit hervorragenden Kenntnissen in den entsprechenden Fachgebieten zusammen. Ich halte es generell für sehr wichtig, über den Tellerrand hinauszuschauen und nicht vor hybriden Konstellationen bzw. Input von außen zurückzuschrecken. Daher arbeiten wir bei neXenio stets nach dem Motto: „WeQ is better than IQ.“ ■

Kurz und Bündig

Als Ausgründung des Hasso-Plattner-Instituts ist neXenio das Unternehmen hinter der luca App. Sie soll in der Corona Pandemie eine schnelle und lückenlose Kontaktverfolgung im Austausch mit den Gesundheitsämtern über eine verschlüsselte und sichere Datenübermittlung ermöglichen. Dabei wird deutlich, dass bei der Optimierung der Anwendung noch Luft nach oben ist.

Sicher. Souverän. Online.

Warum man online nicht mit seinen Daten zahlen sollte

Sylvia Napiletzki, Julia Ringies, Bundesamt für Sicherheit in der Informationstechnik (BSI)



Wie kaufe ich sicher online ein? Kann mein Smart-TV gehackt werden? Reicht ein Passwort für alle meine Accounts? Mit der Kampagne #einfachBSIchern will das Bundesamt für Sicherheit in der Informationstechnik Nutzerinnen und Nutzer dafür sensibilisieren online ihre Daten zu schützen, und zwar möglichst nah am digitalen Alltag der Menschen. Aber welche Bedingungen müssen erfüllt sein, damit Verbraucherinnen und Verbraucher souverän mit digitalen Produkten und Diensten umgehen? Diese Fragestellung ist komplex und wird sowohl in der Praxis als auch Forschung intensiv diskutiert.

Der Begriff „digitale Souveränität“ steht für die Handlungsfähigkeit und die Entscheidungsfreiheit der Verbraucherinnen und Verbraucher. Bezogen auf den Alltag und im gesamtgesellschaftlichen Rahmen sind sie dann sowohl Marktteilnehmerinnen und -teilnehmer, Konsumentenbürgerinnen und -bürger als auch „Prosumer“, die in Netzwerken agieren.

In seinem Gutachten „digitale Souveränität“ hat der deutsche Sachverständigenrat für Verbraucherfragen (SVRV) unter anderem Leitlinien und Handlungsfelder der digitalen Souveränität skizziert: Wahlfreiheit, Selbstkontrolle und Sicherheit, aber auch Selbstbestimmung sind wesentliche Aspekte digitaler Souveränität. Selbstbestimmtheit heißt hier, dass Verbraucherinnen und Verbraucher die Hoheit über Entscheidungen im digitalen Raum haben, indem sie beispielsweise die gezielte Einflussnahme mittels Dark Pattern oder KI-gestützter Bewertungen erkennen und entsprechend resiliente Handlungsmuster entwickeln.

Es besteht Handlungsbedarf

Eine zentrale Voraussetzung dafür ist die Entwicklung digitaler Kompetenzen. Durch Sensibilisierungs- und Informationsangebote rund

**Verbrauchern soll
auf Augenhöhe
begegnet werden.**

um die (sichere) Nutzung von digitalen Produkten und Diensten können diese Kompetenzen ausgebaut werden. Doch ist im Bereich der Verbraucherbildung und -information längst bekannt, dass standardisierte „one-size-fits-all“-Ansätze kein hinreichendes Mittel darstellen, um Verbraucherinnen und Verbraucher bei der Ausbildung und Entwicklung digitaler Verbraucher*innenkompetenz zu unterstützen. Dass der Handlungsbedarf für Sensibilisierungs- und Informationsangebote zur Förderung der digitalen Souveränität der Verbraucherinnen und Verbraucher wächst, zeigen auch die Intensität und die Vielzahl von Sicherheitsvorfällen auf dem digitalen Verbrauchemarkt. Dennoch können Verbraucherinnen und Verbraucher mit grundlegenden Sicherheitsmaßnahmen, wie einem guten persönlichen Passwortmanagement und regelmäßigen Updates, ihre persönliche IT-Sicherheit sowie die IT-Sicherheit der Gesellschaft erhöhen.

Für das BSI stellen IT-Sicherheit und eine erfolgreiche Digitalisierung zwei Seiten derselben Medaille dar. Hersteller sollen mit dem Ansatz „Security by Design“ ihre Produkte absichern, und Verbraucherinnen und Verbraucher müssen Sicherheitsmaßnahmen selbstbestimmt anwenden können. Doch wie können sie dazu noch stärker motiviert werden? Gefragt sind im übertragenen Sinne kommunikative Transmissionsriemen, welche die Welt der Nutzenden mit den IT-Sicherheitsanforderungen verbindet und im Idealfall in Einklang bringt.



Sylvia Napiletzki

Sylvia Napiletzki ist seit 2019 Projektleiterin der Kampagne zur Information und Sensibilisierung in der IT-Sicherheit im BSI. Fachlich ist Frau Napiletzki im Referat BL 21 „Nationales Verbindungswesen“ verortet. Dort hat sie sich unter anderem dem strategischen Thema der Kampagnenfähigkeit des BSI gewidmet.

Kontakt

projektkampagne@bsi.bund.de
www.einfachabsichern.de

Hersteller sollen mit dem Ansatz „Security by Design“ ihre Produkte absichern.

Die #einfachaBSIchern-Kampagne

Hier setzt die vom Bundesministerium des Innern, für Bau und Heimat (BMI) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) initiierte „Kampagne zur Information und Sensibilisierung der Bevölkerung in der IT-Sicherheit“ unter dem Motto „#einfachaBSIchern“ an. Verbraucherinnen und Verbrauchern soll dabei auf Augenhöhe begegnet werden – mit einer Ansprache, die sie in Nutzungssituationen des privaten Alltags abholt und so für IT-Sicherheitsthemen sensibilisiert. Als Absender tritt dabei das BSI als die Cyber-Sicherheitsbehörde des Bundes in Erscheinung. Im Rahmen der Hauptkampagne, die im März 2021 startete, orientieren sich die thematischen Schwerpunkte der Kampagne und deren kreative Umsetzung an ausgewählten Lebenswelten des privaten digitalen Alltags. Dazu zählen: das Home-Office, die Social Media-Nutzung, das Online-Shopping, das

Gaming und das Smarthome.

Das Ziel der Kampagne ist, das Risikobewusstsein der Verbraucherinnen und Verbraucher rund um Themen der IT-Sicherheit zu erhöhen und zugleich ihre Fähigkeiten zu stärken, auftretende Probleme kompetent, langfristig wirksam und selbstbestimmt zu lösen. Die Kampagne führt zur Webseite des BSI, auf der gezielt ein Bereich im Rahmen der Kampagne mit einem niederschweligen Einstieg in das Thema IT-Sicherheit aufgebaut wurde. Dieser wird stetig weiterentwickelt und stellt ein Bindeglied zu den bestehenden tiefergehenden Informationen der weiteren BSI-Webseiten dar, auf denen ein breites Informationsangebot für Verbraucherinnen und Verbraucher zu finden ist.

Über den Alltag an die Menschen

Die zugehörigen Motive der Hauptkampagne zeigen Szenen aus dem digitalen Alltag. Dort werden IT-Anwendungen scheinbar unbesorgt genutzt, lediglich die Headline-Mechanik wirft die Frage nach der IT-Sicherheit auf. Wichtig dabei ist, dass keine Angstszenerien geschaffen werden. Vielmehr soll die Kampagne zum Nachdenken anregen. Sie möchte Nutzerinnen und Nutzer dazu motivieren, sich dem Thema IT-Sicherheit anzunähern. Der Grundgedanke ist: Cybersicherheit ist wichtig

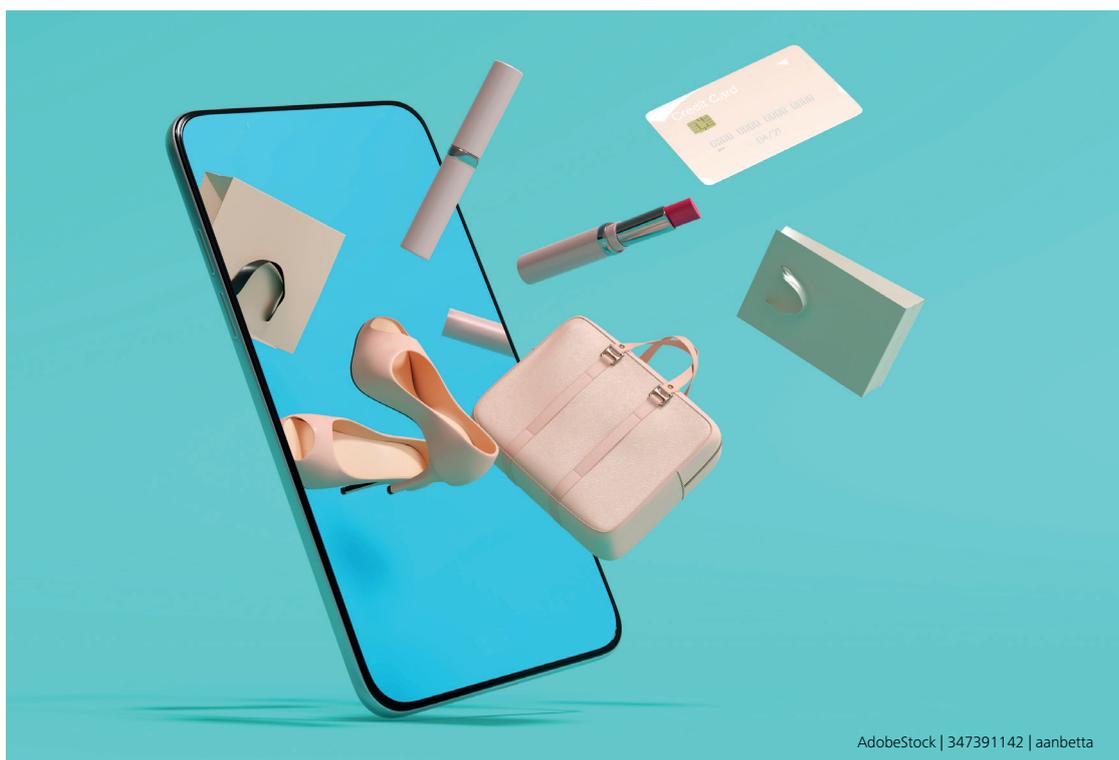




Abbildung 1: Die fünf Motivthemen der Hauptkampagne: Online-Shopping, Gaming, Social Media-Nutzung, Home-Office und Smarthome. © Bundesamt für Sicherheit in der Informationstechnik

und für alle machbar. Wie zentral eine positive Herangehensweise ist, hat sich bereits durch die Recherchen im Planungs- und Kreativprozess der Kampagne gezeigt.

Um die Zielgruppen besser zu verstehen, wurde unabhängig von klassischen alters- oder auch geschlechterspezifischen Einteilungen vielmehr ein Ansatz gesucht, der Rückschlüsse auf das IT-Sicherheitsverhalten in der Bevölkerung insgesamt zulässt und die Ableitung von Zielgruppen anhand der Kriterien Risikobewusstsein, Sicherheitswissen und Lösungskompetenz zulässt. So konnten auf Grundlage einer spezifischen Milieustudie, welche die Internetnutzung und Sicherheitsthemen mit einer vergleichsweise breiten lebensweltlichen Betrachtung verknüpft, verschiedene Sicherheits- und

Gegensatz dazu sind andere Personengruppen zwar aufgeschlossen gegenüber der Onlinenutzung, fühlen sich durch das Wissen um Risiken jedoch häufig überfordert und in der Anwendung von adäquaten Sicherheitsmaßnahmen verunsichert. Für die kreativ-kommunikative Umsetzung ist für uns als BSI daher wichtig, innere Widerstände wie den Verdrängungsmechanismus oder die Überforderung zu überwinden.

Daran knüpft das Motto der Kampagne an: #einfachaBSichern. Die Kernbotschaft bildet die kreative Klammer der Kampagne. Es wird deutlich gemacht, dass sich jede und jeder – unabhängig vom eigenen Wissensstand – vor den potenziellen Gefahren im digitalen Raum schützen kann. ■

Der Grundgedanke ist: Cybersicherheit ist wichtig und für alle machbar.

Nutzungstypen abgeleitet werden.

Beispielsweise gibt es Personengruppen, die neben ihrer Experimentierfreudigkeit und Neugier am Neuen ein eher abstraktes Bewusstsein für Sicherheitsrisiken haben und diese in ihren Alltagspraktiken eher verdrängen oder nicht sonderlich ernst nehmen. Im

Kurz und Bündig

Mit seiner Kampagne #einfachaBSichern will das Bundesamt für Sicherheit in der Informationstechnik das Bewusstsein von Verbrauchern beim Thema IT-Sicherheit erhöhen. Dabei werden von Online-Shopping bis zum Smart-TV eine Vielzahl an Themen aus dem digitalen Alltag abgedeckt. Dank einer Millieustudie konnten Nutzer in ihrem Onlinerverhalten kategorisiert werden und so eine spezifische zielgruppengerechte Ansprache gefunden werden.



Julia Ringies

Julia Ringies ist seit 2019 Projektleiterin der Kampagne zur Information und Sensibilisierung in der IT-Sicherheit im BSI. Fachlich ist Frau Ringies im Referat WG 33 „Cybersicherheit für den Bürger und die Gesellschaft“ verortet. Dort hat sie sich unter anderem dem strategischen Thema der Bürgerkommunikation sowie dem Marketing gewidmet.

Kontakt

projektkampagne@bsi.bund.de
www.einfachabsichern.de

Daten säen – Digitalisierung ernten

Wie Landwirte Datensouveränität erreichen

Bernd Rauch, Fraunhofer IESE



Adobe Stock | Pugin & Photo Studio | 1371029365

Datensouveränität spielt im landwirtschaftlichen Kontext eine immer stärkere Rolle. Im Fokus stehen dabei zwar häufig Daten aus Landwirtschaftsbetrieben, doch wäre die Einschränkung auf diese zu kurzfristig. Landwirtschaftliche Produktionsprozesse sind hochkomplex, und das gesamte Wertschöpfungsnetzwerk reicht von der Produktion landwirtschaftlicher Maschinen bis zum Lebensmittelangebot im Einzelhandel. Während Unternehmen und die Öffentlichkeit großes Interesse an der Verwertung und Nutzung betrieblicher Daten haben, fürchten Landwirtinnen und Landwirte um „ihre“ Daten.

Die moderne Landwirtschaft nutzt hoch technologisierte Produktionsverfahren für Ackerbau und Viehzucht, der Trend zur Digitalisierung [1] hält an, und Daten gewinnen dabei eine immer größere Bedeutung. Sie dienen einerseits der Dokumentation und Steuerung von Produktionsprozessen, können aber auch selbst als digitale Güter gehandelt werden. So werden mittels hochauflöser Bilddaten von Pflanzkulturen Machine-Learning-Modelle trainiert, die Unkräuter von Nutzpflanzen unterscheiden oder Pflanzenkrankheiten erkennen können. Prognoseapplikationen benötigen umfassende Datenbestände, um das Pflanzenwachstum vorherzusagen und die Düngemittelgabe situativ anzupassen. Die Möglichkeiten zur Nutzung von Daten in der Landwirtschaft sind so vielfältig wie die Landwirtschaft selbst. Im Mittelpunkt vieler digitaler Lösungen stehen dabei Daten, die aus dem Kontext landwirtschaftlicher Betriebe stammen. Unternehmen zeigen ein zunehmendes Interesse an diesen Daten, um daraus digitale Dienstleistungen und Lösungen zu entwickeln oder Marktentwicklungen einzuschätzen. Auch die Forschung benötigt große Datenmengen, die Öffentlichkeit möchte über die Nachhaltigkeit der Lebensmittelproduktion informiert sein, und Handelsunternehmen können mit dem Wissen über Erntemengen und -zeitpunkte ihr Einkaufsverhalten und damit ihre Einkaufspreise steuern. Das letzte Beispiel zeigt dabei stellvertretend für viele weitere, wie es zu widerstreben den Interessen kommen kann: Kann ein Handelsunternehmen Einkaufspreise zu seinem Vorteil beeinflussen, ist das in der Regel zum Nachteil der Landwirtschaftsbetriebe. Solche und ähnliche Beispiele wie auch die Unklarheit darüber, welche Konsequenzen die unkontrollierte Nutzung betrieblicher Daten tatsächlich hat, weckt Befürchtungen um die eigene digitale Souveränität unter Landwirtinnen und Landwirten. In Diskussionen ist dabei immer öfter die Rede von einem allbestimmenden landwirtschaftlichen Google, Facebook oder Amazon. Selbst wenn diese Vorstellung diffus und unbegründet sein mag, trägt sie in einem gewissen Maße zur Skepsis gegenüber digitalen Technologien bei. Und das kann fatal sein, nicht nur für die Branche selbst, sondern auch für aktuelle und zukünftige Herausforderungen. Denn digitale Technologien in der Landwirtschaft ermöglichen nicht nur die Erhöhung der Prozesseffizienz, sie bieten auch ein enormes Potenzial für die nachhaltige landwirtschaftliche Produktion.

Datensoeveränität wird zwar gefordert, wurde aber bisher kaum definiert.

Führt Datensoeveränität für Landwirtinnen und Landwirte zu mehr Vertrauen in digitale Technologien, wird sie damit essenziell für die Landwirtschaft der Zukunft.

Datensoeveränität ist mehr als Zugriffskontrolle

Bei der Datensoeveränität in der Landwirtschaft geht es dabei um mehr als nur Zugriffskontrolle auf betriebliche Daten. Sie soll Landwirtinnen und Landwirten ermöglichen, dass sie souverän über „ihre“ Daten verfügen, d.h., diese auch in ihrem Sinne nutzen und einsetzen können. In der digitalen Landwirtschaft werden viele verschiedene Fachapplikationen eingesetzt, um Produktions- und Managementprozesse durchzuführen. Diese Fachapplikationen erfassen, speichern und verarbeiten Daten im Rahmen der jeweiligen Applikationszwecke. Auch wenn Softwarelösungen zunehmend in Cloudumgebungen betrieben werden, existiert noch keine umfassende Vernetzung über die eigenen Systemgrenzen hinweg. Eine solche Vernetzung, etwa über offene Schnittstellen, ist aber eine wichtige Voraussetzung für Innovation und Wettbewerb. Ein Start-up mit einem neuen Algorithmus zur Optimierung des Düngemitelesatzes benötigt dazu Daten über die Äcker der Landwirtschaftsbetriebe. Diese werden in der Regel in sogenannten Ackerschlagkarteien verwaltet, und bieten diese keine Schnittstellen, kann das Start-up seine Dienstleistung nicht erbringen. Fehlende Schnittstellen unterbinden darüber hinaus die Möglichkeit, beim Anbieterwechsel eigene Daten „mitzunehmen“. Auch wenn hier nicht in allen Fällen Anbietern Absicht unterstellt werden darf, wird durch die Bindung betrieblicher Daten an Fachapplikationen der Wettbewerb gehemmt werden und es kommt zum Vendor-Lock-in-Effekte. Solche Effekte bekommen eine noch größere Tragweite, wenn landwirtschaftliche Maschinen an herstellerbetriebene Flottenmanagementsysteme gebunden werden, durch die ein



Bernd Rauch

Bernd Rauch ist Digitalisierungsexperte am Fraunhofer IESE in Kaiserslautern und beschäftigt sich mit digitalen Ökosystemen und Plattformökonomien. Er schloss sein Informatikstudium an der Universität des Saarlandes mit Diplom ab und erwarb einen Master of Business Administration an der TU München. Bei seiner Arbeit als Projektmanager und Softwarearchitekt ist es ihm wichtig, Projekte und digitale Lösungen ganzheitlich sowie aus verschiedenen Perspektiven zu betrachten. Schwerpunkt seiner aktuellen Forschungs- und Entwicklungsprojekte ist die digitale Landwirtschaft.

Kontakt

bernd.rauch@iese.fraunhofer.de
www.iese.fraunhofer.de

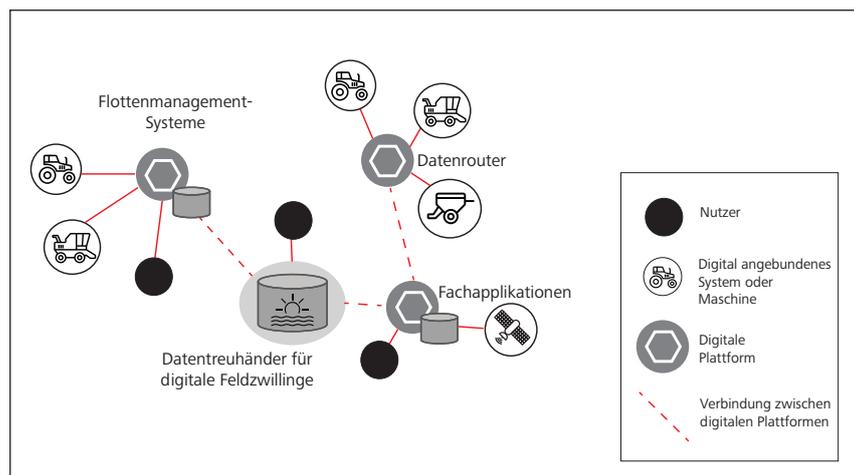


Abbildung 1: abstrahierte Darstellung des digitalen Ökosystems Landwirtschaft.
© Fraunhofer IESE

exklusiver Zugriff auf Maschinendaten erfolgt.

Verständnis von Datensouveränität in der Landwirtschaft

Die inhaltliche Bedeutung von Datensouveränität für Landwirtinnen und Landwirte ist nicht gut ausgearbeitet oder definiert, obgleich sie an vielen Stellen diskutiert wird. Um Datensouveränität oder synonym Datenhoheit in der Landwirtschaft greifbarer zu machen, wurde im Rahmen des Forschungsprojekts „COGNAC“ (Cognitive Agriculture) der Fraunhofer-Gesellschaft [2] eine Definition erarbeitet, die drei wesentliche Elemente vorsieht:

- **Datennutzung nur mit Zustimmung:** Obwohl eigentlich selbstverständlich, ist diese Forderung nicht durchgängig erfüllt. Daten sollen durch Dritte nur nach expliziter Zustimmung durch Landwirtinnen und Landwirte genutzt werden können. Erreicht werden kann das durch Zugriffseinschränkungen, die idealerweise über eine einmalige Erlaubnis hinaus gestaltbar sind. So könnte Datennutzung auch im zeitlichen, räumlichen oder inhaltlichen Umfang eingeschränkt werden. Eine räumliche Einschränkung ist beispielsweise sinnvoll, wenn ein Unternehmen eine Dienstleistung auf einem Acker durchführt und Zugriff auf benötigte Datenbestände nur bei Arbeiten vor Ort erhält.
- **Transparenz der Datennutzung:** Werden betriebliche Daten durch Dritte genutzt, soll die Nutzung detailliert nachvollziehbar sein. Dazu können eine Protokollierung einzelner Datenzugriffe zählen, die vorherige Festlegung auf erlaubte Nutzungszwecke oder auch die verständliche Darstellung

der Konsequenzen aus der Datennutzung. Der letzte Punkt kann für Landwirtinnen und Landwirte bedeutend sein, da nicht immer einfach nachvollziehbar ist, welche Bedeutung eine spezifische Datennutzung hat. Auf der Basis von betrieblichen Daten könnten beispielsweise entscheidungsunterstützende Systeme entwickelt werden, die in der fernen Zukunft die Arbeit von Landwirtinnen und Landwirten überflüssig machen.

- **Souveräne Datennutzung:** Landwirtinnen und Landwirte sollen betriebliche Daten auch über datenhaltende Fachapplikationen hinaus in ihrem Sinne nutzen und einsetzen können. Hierzu wird einerseits ein diskriminierungsfreier Zugang zu Datenbeständen für die Verwendung durch Dritte benötigt. Darüberhinausgehend soll es aber auch möglich sein, Daten bei einem Anbieterwechsel in ein neues System zu übertragen (Datenportabilität).

Ansätze zur Schaffung von Datensouveränität

Mit der vorgeschlagenen Definition von Datensouveränität ist es möglich, den Begriff durch konkrete Anforderungen und Beispiele verständlicher zu machen. Zur Umsetzung in der Landwirtschaft werden verschiedene Ansätze diskutiert. Eine Möglichkeit bietet die rechtliche Gestaltung der Datennutzung, die in Gesprächen regelmäßig mit einer missverständlichen Formulierung beginnt: „Die Daten gehören der Landwirtin oder dem Landwirt“. Was häufig als Forderung oder Marketingversprechen ausgedrückt wird, ist rechtlich nicht haltbar, da das deutsche Recht kein Eigentum an Daten kennt. Demzufolge können Landwirtschaftsbetriebe auch keine Eigentumsrechte an betrieblichen Daten geltend machen [3]. Häufig wird auch die Datenschutz-Grundverordnung (DSGVO) als Lösungsansatz herangezogen, doch fokussiert diese sich auf personenbezogene Daten und regelt mehr den Schutz als den Umgang damit - zur Ausgestaltung von Datensouveränität ist sie nicht geeignet. Möglich sind letztendlich privatvertragliche Regelungen zum Umgang mit Daten, doch in der Praxis stehen Landwirtinnen und Landwirte von Unternehmensanwälten ausgearbeiteten AGBs gegenüber, die sie, wenn überhaupt, nur sehr selten in ihrem Sinne beeinflussen können.

Branchenweite Verhaltenskodizes wie beispielsweise der „EU Code of conduct on agricultural data sharing by contractual agreement“ [4] führten bisher ebenfalls zu keiner befriedigenden Situation für Landwirtinnen und Landwirte, so dass sich aktuell Rufe nach einer stärkeren Regulierung durch den Gesetzgeber mehren [5]. Diese könnte zwar den Umgang mit betrieblichen Daten durch Anbieter von Fachapplikationen und landwirtschaftlichen Systemen verbindlich regeln, es ist aber fraglich, ob dabei die für dynamische Digitalisierungsprozesse notwendige Flexibilität erreicht werden kann.

Neue Konzepte für das digitale Ökosystem Landwirtschaft

Ein Lösungsweg kann in der Kombination von organisatorischen und technologischen Ansätzen liegen. Die Verteilung betrieblicher Daten auf verschiedene Fachapplikationen ist eine grundsätzliche Herausforderung in der Domäne, nicht nur für die Datensouveränität. In COGNAC werden Konzepte entwickelt und prototypisch evaluiert, in denen sämtliche einen Acker beschreibende Daten in einem digitalen Feldzwilling zusammengeführt und durch Technologien zur Datennutzungskontrolle geschützt werden. Ein solcher Feldzwilling kann beispielsweise durch einen Datentreuhänder betrieben und über eine digitale Plattform angeboten werden. Fachapplikationen und digitale Dienstleister können so diskriminierungsfrei und anbieterneutral auf betriebliche Daten der Landwirtschaftsbetriebe zugreifen und diese in deren Sinne nutzen. Dank der zentralen Architektur dieses Ansatzes können Landwirtinnen und Landwirte an einer Stelle konfigurieren und nachvollziehen, wer welche Daten in welchem Umfang nutzen darf und wie sie tatsächlich genutzt werden. Aufgrund der Entkopplung von Daten und Fachapplikationen wird zusätzlich ein Vendor-Lock-in vermieden, wobei dies natürlich auch für die Datentreuhänder selbst auszuschließen ist. Abbildung 1 zeigt eine abstrahierte Darstellung des digitalen Ökosystems Landwirtschaft. Typische Elemente sind Flottenmanagementsysteme, Datenrouter und Fachapplikationen, die als digitale Plattformen umgesetzt wurden. Diese binden jeweils weitere digitale Systeme ein und könnten prinzipiell miteinander zum Datenaustausch verbunden werden. Häufig kommt es aber zu

Bisherige Lösungsansätze brachten noch keine Datensouveränität.

Abgrenzungen zwischen einzelnen Angeboten, Initiativen und Anbieterverbänden. In der Folge entsteht die verteilte Speicherung in Datensilos, welche durch einen Datentreuhänder für betriebliche Daten aufgebrochen werden könnte.

Auch wenn der vorgestellte Ansatz die Herausforderungen der landwirtschaftlichen Datensouveränität in der Theorie lösen kann, steht der Transfer in die Praxis noch aus. Die digitale Landwirtschaft ist hochkomplex, und es gibt viele Anbieter von Softwarelösungen, die dazu an einem Strang ziehen müssten. Möglicherweise führt die Kombination vieler Ansätze und Faktoren zum Erfolg, wesentlich ist dabei auch die Rolle von Landwirtinnen und Landwirten, die als souveräne Kunden den Markt in ihrem Sinne mitgestalten können. Hierzu kann und muss die weitere Diskussion der Datensouveränität in der Landwirtschaft beitragen. ■

Kurz und Bündig

Im Zuge fortschreitender Digitalisierung werden Daten immer wichtiger: Sie sind Grundlage von Dienstleistungen, beschreiben und steuern Prozesse oder werden als digitale Güter gehandelt. Der Umgang mit Daten führt dabei nicht selten zu widerstreitenden Interessen, etwa wenn ungeklärt bleibt, wem sie gehören, wessen Rechte sie berühren oder wer davon profitiert. Auch die Landwirtschaft beschäftigt sich intensiv mit diesen Fragen. Bieten digitale Technologien für Datensouveränität Antworten?



Weitere Infos und Literaturangaben zum Artikel finden Sie unter folgendem Link: <https://bit.ly/3mgR6PY>



„Alexa, ich bin süchtig.“

Wie Digital Detox die Handysucht bekämpft

Daniela Otto, Ludwig-Maximilians-Universität München

Wie lange sind Sie zurzeit täglich online? Seit Corona liegt die durchschnittliche Bildschirmzeit bei bis zu elf Stunden. Das kommt auch schnell zusammen, wenn man sich einen normalen Tag anschaut: Morgens klingelt der Handywecker und wenn man das Smartphone schon einmal in der Hand hat, kann man gleich Mails checken, und den Social Media Feed durchscrollen. Dann das Frühstück. Statt Zeitung lesen lieber die News auf dem Tablet überfliegen. Danach den Rechner an und arbeiten. Die Mittagspause ist mit ein bisschen YouTube schnell vorbei. Und abends geht's weiter mit Binge Watching auf Netflix. Ein Leben in modernen Zeiten ist ein Leben vor vielen Bildschirmen – häufig nutzen wir diese sogar gleichzeitig. Wie oft müssen Sie Ihre Lieblingsserie zurückspulen, weil Sie nebenher aufs Handy geschaut haben?

Der Sog dieser leuchtenden Bildschirme ist enorm, sie ziehen uns förmlich an. Mehr noch: Sie machen süchtig. Es ist an der Zeit, diese Sucht ernst zu nehmen, denn viel zu oft wird sie noch relativiert, bagatellisiert, abgetan als bloße, leicht in den Griff zu bekommende Spielerei. Das ist fatal. Die Wahrheit ist: Wer sein Handy nicht mehr weglegen kann, ist krank. Und da immer mehr Menschen vom Smartphone abhängig sind, können wir ohne Übertreibung sagen: Die digitalisierte Gesellschaft hat das größte kollektive Suchtproblem aller Zeiten.

Smartphones verändern das Gehirn

Wie immer steckt unser Gehirn dahinter. Dieses ist neuroplastisch, das heißt, es kann das, was wir ihm beibringen, es passt sich unseren Gewohnheiten an. Wir können unser Gehirn trainieren, je nachdem, welche Bereiche wir besonders beanspruchen. Derzeit geben wir uns ganz der narzisstischen Gier nach Aufmerksamkeit hin. Jedes kleine Handysignal, jedes Like, jeder neue Follower, gibt uns zu verstehen, dass wir wichtig sind. Es ist ein Ego-Booster. In unserem Gehirn wird dadurch das Belohnungszentrum aktiviert, das sogenannte „Glückshormon“, der Neurotransmitter Dopamin wird

ausgeschüttet, und das fühlt sich zunächst gut an. Wir wollen dieses Gefühl wieder und wieder spüren – der Suchtkreislauf beginnt.

Smartphones können krank machen

Die seelischen Folgen dieser Onlinesucht sind nicht zu überschätzen. Immer mehr Studien belegen den Zusammenhang von psychischen Krankheiten und intensiver Smartphonennutzung. Die Depressionsraten steigen, sogar die Suizidalität nimmt zu, insbesondere bei jungen Menschen. Über 60 Prozent geben an, dass sie ohne Handy ein Gefühl der Angst überkommt. Es gibt sogar einen Fachbegriff dafür: Nomophobie (No-Mobile-Phone-Phobia). Für fast 90 Prozent der 14- bis 19-Jährigen ist ein Leben ohne Smartphone undenkbar. Unter dem Phänomen „Snapchat-Dysmorphia“ versteht man die traurige Tatsache, dass immer mehr



Daniela Otto

Dr. Daniela Otto ist Expertin für Digital Detox. Sie promovierte über das Thema „Vernetzung“ und schrieb das erste deutsche Buch zu diesem Thema. Ihr neues Buch „Digital Detox für die Seele“ (Irisina Verlag) ist das erste Buch, das Achtsamkeit und Digital Detox kombiniert.

Kontakt

mail@danielaotto.com

www.danielaotto.com

Wir müssen erwachsen werden und uns endlich digital abnabeln.

wer sich ohne Ablenkung ganz auf sein Gegenüber einlässt, kann den anderen voll und ganz wahrnehmen. Auch Mitgefühl entsteht im Gehirn. So wie ein Handy automatisch nach Netz sucht, wenn es keines hat, so sucht unser Gehirn automatisch nach einem empathischen Austausch mit einem anderen Gehirn. Kein Gehirn ist in Isolation glücklich – wir können nicht anders, als nach neuronaler Vernetzung streben. Sogenannte „Spiegelneurone“ sind dafür zuständig, diese empathischen Verbindungen herzustellen. Spiegelneurone, auch Empathie Neurone genannt, sind visuo-motorische, also für die Koordination zuständige Nervenzellen in unserem Gehirn, die ein Resonanzsystem bilden. Durch Spiegelneurone verstehen wir andere, denn, wie der Name sagt, sie spiegeln die Handlungen und Gefühle anderer in uns selbst. Sie erzeugen in uns die Emotionen des anderen, bringen diese zum Schwingen. Unsere Gefühle werden intuitiv übertragen, wir stecken einander emotional an. Wenn wir zum Beispiel jemand weinen sehen, werden die Spiegelneurone aktiv; sie „feuern“ in unserem Gehirn und lösen in uns das Gefühl aus, das der andere empfindet. Sie kennen den Effekt, dass Sie zucken, wenn Sie sehen, wie sich jemand in den Finger schneidet? Genau das erzeugen Spiegelneurone. Wenn wir aber ständig in Bildschirme starren, wird ein solcher mitfühlender Austausch erschwert. Die Folge: eine zusehends unempathischere Gesellschaft – dabei ist Mitgefühl der Kitt, der uns zusammenhält.

Digital Detox führt sie zurück ins Leben

Mitgefühl brauchen wir insbesondere auch in sozialen Netzwerken, die maximales Suchtpotenzial haben. Wer im virtuellen Wettbewerb bestehen will, braucht digitale Resilienz – denn der Vergleich mit anderen, deren Leben vermeintlich schöner und besser ist, macht nachweislich unglücklich. Mit Digital Detox können Sie eine neue, selbstliebende innere Haltung kultivieren. Im Fokus steht ein gesunder Selbstwert. Das Digital Detox Mantra für Social

Mitgefühl ist der Kitt, der uns zusammenhält.

Zeit ohne Handy ist Zeit, die wir uns selbst schenken.

Media lautet: Sie sind gewollt, Sie sind geliebt, egal, wie viele Likes oder Follower Sie haben. Überhaupt: Es ist nur Social Media. Nicht das echte Leben. Auch beim Online-Dating, das für viele der perfekte Ego-Booster ist, gilt: Tindern Sie sich nicht die Seele aus dem Leib. Wenn Sie selbst ein Date nach dem anderen haben, fragen Sie sich, ob Sie das wirklich erfüllt. Machen Sie sich bewusst, was Sie eigentlich suchen, wenn Sie online daten und dass Ihr Leben auf jeden Fall ein glücklicheres ist, wenn Sie es in gesundem Maß tun und nicht süchtig sind. Egal, wo Sie jemanden kennenlernen: Daten Sie respektvoll. Hinter jedem Profil steht ein Mensch mit Gefühlen. Behandeln Sie andere so, wie Sie selbst gerne behandelt werden wollen – Dating-sucht verdirbt schnell den Charakter.

Egal, ob in der Liebe, im Beruf oder der Freizeit, Digital Detox betrifft alle Lebensbereiche, denn unser Leben ist in Gänze von Smartphones durchdrungen. Schalten wir also öfter gezielt ab, und kümmern wir uns um unser Wohlergehen. Im digitalen Zeitalter müssen wir den unbezahlbarsten Wert überhaupt verteidigen: den Wert einer gesunden Seele. Mit Digital Detox gelingt uns das. ■

Kurz und Bündig

Mails, Chats, Posts, Home Office – die Bildschirmzeiten explodieren. Denn mit der Coronapandemie ging noch eine andere Pandemie einher: Smartphonesucht. Diese psychische Erkrankung müssen wir endlich ernst nehmen und überwinden. In diesem Artikel werden Risiken und potenzielle Lösungen für die Sucht nach dem Digitalen vorgestellt. Es muss auch in digitalen Zeiten eine eigene gesunde Seele geben.

Mit KI Datenschätze heben

Erfolgsfaktoren in der Plattformökonomie

Wolfgang Faisst, ValueWorks.ai



Das digitale Zeitalter verändert weltweit Produktionsprozesse und Wertschöpfungsketten – und stellt Unternehmen vor große Herausforderungen. Auch kleine und mittlere Betriebe müssen ihre Geschäftsmodelle anpassen. Entscheidend dabei ist es, die Daten verschiedener Akteure entlang der Wertschöpfungskette intelligent miteinander zu kombinieren. So entstehen Wertschöpfungsnetzwerke, in denen die beteiligten Akteure ihre Datenschätze teilen und daraus mithilfe von künstlicher Intelligenz (KI) neue Geschäftsmodelle entwickeln.

Aktuell zeigen sich Mittelständler beim Einsatz von KI-Systemen noch zurückhaltend. Lediglich knapp sechs Prozent der KMU in Deutschland setzen KI-Technologien bereits in allen Geschäftsbereichen ein. Dabei handelt es sich insbesondere um größere, bereits stärker digitalisierte Mittelständler. Das zeigt eine 2020 veröffentlichte Umfrage des Bundesverbands mittelständische Wirtschaft (BVMW) und des Mittelstand 4.0-Kompetenzzentrums Berlin. Knapp 30 Prozent der befragten kleinen und mittleren Unternehmen (KMU) nutzen KI-Technologien danach in einzelnen Projekten, rund 25 Prozent haben es vor. Rund 40 Prozent der Mittelständler indessen nutzen aktuell weder KI-Technologien noch planen sie deren Einsatz. Insbesondere kleinere Unternehmen erkennen häufig noch nicht den Nutzen, den KI-basierte Lösungen für ihren Betrieb versprechen; konkrete Anwendungsfälle sind ihnen oft nicht bekannt.

Dabei ist künstliche Intelligenz längst nicht nur eine Technologie für große Unternehmen. Auch dem Mittelstand eröffnen KI-basierte Systeme enorme Potenziale entlang der gesamten Wertschöpfungskette.

Künstliche Intelligenz ermöglicht es, durch die Verknüpfung und Analyse von Daten neues Wissen zu generieren. Auf diese Weise lassen sich bestehende Produkte und Dienstleistungen immer weiter individualisieren und damit für den Nutzer verbessern bzw. ganz neue (digitale) Leistungen erschaffen. KMU verfügen selten allein über die notwendigen Daten und Technologien, um solche datengetriebenen Geschäftsmodelle zu realisieren. Die Zusammenarbeit und das Teilen von Daten, Technologien

und Kompetenzen in Geschäftsnetzwerken sind daher für Unternehmen künftig unerlässlich.

Noch aber fehlen häufig sowohl die Bereitschaft in vielen Unternehmen als auch eine sichere, vertrauenswürdige Infrastruktur für den Datenaustausch. In unserer Publikation „Von Daten zu Wertschöpfung: Potenziale von Daten- und KI-basierten Wertschöpfungsnetzwerken“ der deutschen KI-Initiative Plattform Lernende Systeme und acatech beleuchten wir, wie datenbasierte Wertschöpfungsnetzwerke funktionieren und welche Hürden sich für Konzerne und KMU in der unternehmensübergreifenden Zusammenarbeit stellen können. Mögliche Ausprägungen von Datenökosystemen werden anhand von praktischen Beispielen aus unterschiedlichen Branchen illustriert.

Relayr, Produktionsunternehmen, MunichRe:

Ungeplanter Stillstand der Anlagen wird verhindert, und die Risiken potenzieller Schäden durch Produktionsausfälle werden minimiert. Als Teil der MunichRe-Gruppe kann Relayr auf eine Vielzahl von möglichen Finanzierungs- und Versicherungsmodellen und -partnern zurückgreifen, um ein geeignetes Wertschöpfungsmodell anbieten zu können.

Fresh energy, Energieversorger, Privathaushalte:

Basierend auf Smart-Meter-Daten bietet Fresh Energy in einem B2B2C-Modell eine innovative Kundenbeziehung zwischen Energieversorger und Privathaushalt. Die Endkunden



Wolfgang Faisst

Dr. Wolfgang Faisst ist Co-Founder und CEO der ValueWorks GmbH in Karlsruhe. Davor war er Leiter von S/4 NEXT - Next Generation Business Processes & Practices bei der SAP SE. Er war seit 2005 im Konzern tätig und hat dort zahlreiche strategische Innovationsthemen vorangetrieben. Er leitet die Arbeitsgruppe Geschäftsmodellinnovationen in der Plattform Lernende Systeme.

Kontakt

wolfgang.faisst@valueworks.ai
www.plattform-lernende-systeme.de

erhalten eine App im Design des Energieversorgers, in der der Stromverbrauch in Echtzeit einzusehen ist. Der summierte Stromverbrauch kann durch KI-Methoden disaggregiert werden, um einzelne Geräte zu erkennen

Ada health, Ärzte, Patienten:

Ada Health bietet eine KI-gestützte Anamnese. Eine selbst entwickelte Softwarelösung, von 50 angestellten Ärztinnen und Ärzten im Hinblick auf verbreitete und seltene Krankheitsbilder hin ausgebildet, gibt Patientinnen und Patienten durch einfache Fragen eine Vordiagnose basierend auf einem probabilistischen System.

Die Erkenntnisse gelten für viele andere Sektoren, vor allem für die heute führenden Unternehmen aus Europa, also insbesondere für den B2B-Bereich, der in der so genannten „zweiten Halbzeit“ der Digitalisierung im Fokus steht.

Kooperation und Vertrauen

Die Beispiele für datenbasierte Wertschöpfungsnetzwerke mögen unterschiedlich sein, gemeinsam ist ihnen die Herausforderung, die Geschäftspartner initial zu gewinnen und dauerhaft einzubinden, quasi in Form eines „virtuellen Unternehmens“ mit einer gemeinsamen Dateninfrastruktur. In solchen Kooperationsverbänden kommt dem „fokalen“ Unternehmen (oftmals mit gutem Endkunden-Zugang) die zentrale Aufgabe zu, aus einer losen Gruppe

eine funktionierende Einheit zu formen.

Die technischen Herausforderungen lassen sich gut lösen und es gibt geeignete Referenz-Architekturen (inkl. Schnittstellen und gemeinsamen Datenformaten), an denen man sich orientieren kann. Über den Erfolg entscheidet am Ende, ob die Geschäftspartner die notwendige Vertrauensbasis aufbauen und ein geeignetes Geschäftsmodell definieren können, das Nutzen für alle Beteiligten stiftet.

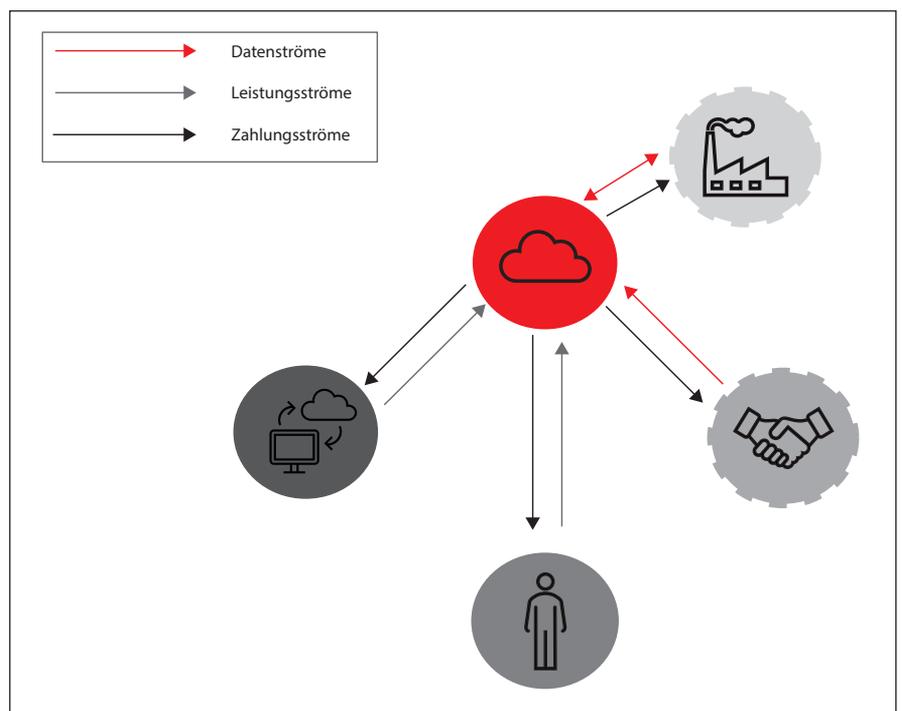
Typischer Ausgangspunkt bei der Definition innovativer Geschäftsmodelle ist, ein vom Endkunden ausgehendes klares und direktes Nutzenversprechen („Value Proposition“) für jeden einzelnen Beteiligten zu schaffen.

KI-Expertise von außen

Viele Unternehmen lassen sich durch die notwendige KI-Expertise abschrecken oder wegen des Fehlens von Data Scientists. Dieser Mangel lässt sich aber kompensieren, indem die Unternehmen mit KI-Expertinnen und -Experten von Hochschulen oder aus der Forschung kooperieren oder mit KI-Fachleuten von Unternehmensberatungen zusammenarbeiten.

Eine größere Herausforderung ist dagegen, die für die Anwendung von KI-Verfahren notwendigen Daten in geeigneter Form bereitzustellen. Deshalb sollten die beteiligten Unternehmen eine Inventur ihrer Datenbestände vornehmen und eine Datenlandkarte für die später in den KI-Verfahren genutzten Datenobjekte (zum

Abbildung 1: Wechselwirkung von Plattform und Benutzer.
© Plattform Lernende Systeme



Unternehmen sollten sich nicht scheuen, auch mit traditionellen Wettbewerbern zu kooperieren.

Beispiel „Kunde“, „Produkt“) und deren Quellsysteme (zum Beispiel Unternehmenssoftware, mobile bzw. Webanwendungen, IoT-Systeme mit Sensoren zu technischen Geräten und deren Nutzern) und -Formate erarbeiten.

Während die traditionellen IT-Abteilungen im Bereich der relationalen Datenbanken gute Kenntnisse mitbringen, werden für den Einsatz von KI typischerweise viel größere Datenmengen verarbeitet, so dass hier auf Technologien aus dem Bereich „Big Data“ oder Datenmanagementplattformen zurückgegriffen werden muss, welche eher selten im Repertoire einer typischen IT-Abteilung enthalten sind. Sollen personenbezogene Daten verarbeitet werden, so sind die Vorgaben der DSGVO zu beachten. Dazu ist die Zustimmung der privaten Datenerzeuger einzuholen und diese nachvollziehbar abzuspeichern, etwa in Form eines „Datenvertrages“, der einem Datenpool zugeordnet ist.

Wie bei jedem Start-up, so ist es auch hier erfolgskritisch, einen so genannten Minimum Viable Product (MVP)-Scope zu definieren, und zwar im Zusammenspiel mit initialen, oftmals eng in die Produktentstehung eingebundenen „Co-Innovationskunden“. Der MVP ist der minimale Produktumfang, für den die ersten Kunden bereit sind, Geld zu bezahlen.

Da sich die Ökosysteme der avisierten Wertschöpfungsnetzwerke sehr dynamisch verändern können, sollten die Projekte durch einen agilen Roll-out möglichst frühzeitig auf den Markt gebracht werden. So können Methoden und Erwartungen der Teilnehmer – beispielsweise bezüglich Effizienzvorteilen und Nutzerversprechen des Produkts – früh geprüft, angepasst und so gewährleistet werden. Daher sollte das Wertschöpfungsnetzwerk initial so zusammengestellt werden, dass es schnell handlungsfähig ist und sich bei Markterfolg sukzessive erweitern lässt. Dabei sollte man sich nicht scheuen, auch mit traditionellen Wettbewerbern zu kooperieren und gemeinsamen ge-

gen die digitalen Wettbewerber aufzutreten.

Während gegenüber dem Endkunden ein „As-a-Service“-Geschäftsmodell immer beliebter wird, werden die in der Wertschöpfung beteiligten Parteien über eine Erfolgsbeteiligung in Form eines Umsatzanteils dazu motiviert, ihre Daten zu teilen – der wesentliche Produktionsfaktor in der Datenökonomie.

Fünf Empfehlungen, wie aus Daten erfolgreiche Geschäftsmodelle entstehen

Zusammenfassend lassen sich fünf Empfehlungen für den erfolgreichen Aufbau von datenbasierten Wertschöpfungsnetzwerken geben:

1. Transparenter Aufbau des Netzwerks mit klar formulierten Wertversprechen aller Beteiligten
2. Definition einer klaren Datenstrategie, welche Qualität, Relevanz und Verfügbarkeit der für die Wertschöpfung nötigen Daten festlegt
3. Strategisch und langfristig angelegte (Forschungs-) Kooperation zur Generierung von eigenen Kompetenzen im Bereich Data Science
4. Agiler Roll-out des Produkts, um Hürden frühzeitig zu erkennen und das Produkt anpassen zu können
5. Kontinuierliche Prüfung und Anpassung des Geschäftsmodells und geeigneter Finanzierungsmodelle, z. B. Umsatzbeteiligung ■

Kurz und Bündig

Um sich in Zeiten rasanter technologischer Entwicklungen im Wettbewerb zu behaupten, müssen Unternehmen ihre Geschäftsmodelle anpassen. Das Gebot der Stunde lautet, Mehrwert aus Daten zu schöpfen – und zwar gemeinsam mit Partnern. Nur selten verfügen Betriebe allein über die notwendigen Daten und Technologien, um datengetriebenen Geschäftsmodelle zu realisieren. Der Gastbeitrag zeigt, wie datenbasierte Wertschöpfungsnetzwerke funktionieren und welche Hürden sich für Konzerne und KMU in der unternehmensübergreifenden Zusammenarbeit stellen können.

Datenpower macht Ionen schlauer

**Wie Datascience und KI zu neuen Hochleistungsakkus
verhelfen können**

Marcel Mutz, Dirk Werth, August-Wilhelm Scheer Institut



Batterien müssen leistungsfähiger, zuverlässiger und langlebiger werden, um den rasant steigenden Anforderungen der Zukunft gerecht zu werden. Elektroautos, Smartphones, Tablets oder Laptops sind heute batteriegetrieben, und bei Ihrer Herstellung stellen sich Fragen, wie: „Durch welche Veränderung im Produktionsprozess kann ich die Kapazität der Batterie erhöhen?“. Das gemeinnützige August-Wilhelm Scheer Institut arbeitet mit Partnern im Forschungsvorhaben „DigiBatMat - Plattform für Batteriematerialdaten, -wissen und deren Verknüpfung“ an der Verbesserung der Batteriezellproduktion. Die in dem Projekt entwickelte Plattform für Batteriematerialdaten stellt eine innovative Lösung dar, um die Entwicklung und Transparenz von Batterien, deren Herstellung sowie die eingesetzten Materialien weiter voranzutreiben – ein Ansatz für steigende digitale Souveränität in der Branche.



Marcel Mutz

Marcel Mutz, Projektleiter DigiBatMat AWSi, hat Wirtschaftsinformatik (M.Sc.) an der Universität in Saarbrücken studiert. Heute arbeitet er am August-Wilhelm Scheer Institut im Smart Quality Lab im Bereich der Qualitätsdatenanalyse und im Mittelstand 4.0 Kompetenzzentrum Saar als KI-Trainer.

Kontakt

marcel.mutz@aws-institut.de
www.aws-institut.de

Digitale Souveränität

Wer dem Begriff „digitale Souveränität“ begegnet, erkennt schnell: die eine Definition von „digitaler Souveränität“ stellt sich als schwierig heraus. Digitale Souveränität, so zeigt auch das vorliegende Heft, bedeutet im Grunde dreierlei:

1. Digitale Medienkompetenz: Das selbstbestimmte Arbeiten und der souveräne Umgang mit digitalen Medien, Daten und Informationen im Alltag, Privatleben, Beruf und innerhalb von Organisationen und Unternehmen.
2. Datensicherheit: Datensicherheit als selbstbestimmte Regulation und die selbstbestimmten Zugriffsmöglichkeiten auf die eigenen Daten und Informationen in einer digitalisierten Welt. Diese Daten können sowohl personenbezogene als auch solche sein, die innerhalb einer Organisation oder eines Unternehmens vorliegenden. Die Sicherheit dieser Daten muss für den Nutzer gewährleistet und darf nur für ihn transparent sein.
3. Digitale Konkurrenzfähigkeit: Die meisten

digitalen Global Player sind weder aus Deutschland noch anderen Staaten der Europäischen Union. Unternehmen wie Amazon, Facebook, Google oder Ali Baba sind in Ländern wie den USA oder China entstanden. Um den Anschluss an diese Länder nicht zu verlieren und völlig abhängig von ihnen zu werden, versuchen sich Staaten und Unternehmen in Sachen Digitalisierung souveräner aufzustellen. Die Stärkung der Standorte Europa und Deutschland wird beispielsweise im großangelegten und europaweiten Vorhaben Gaia-X gebündelt.

Elektroauto, Laptop, Akkustaubsauger - alles batteriegetrieben

Heutzutage kommen moderne Lithium-Ionen-Batterien (LIB) in einem Großteil der elektronischen Geräte zur Anwendung. Ob in einem Elektroauto, einem Akkustaubsauger, einem Laptop oder einem Smartphone: Die Batterieherstellung hat einen maßgeblichen Einfluss auf die Leistungsfähigkeit und Qualität des Produktes. Die aktuellen, zum Teil nicht digitalisierten Vorgänge innerhalb der Materialforschung hemmen die Möglichkeiten

zur unternehmensübergreifenden Forschung und Kooperation. Ultimativ können dadurch die Potentiale der Forschung nicht ausgeschöpft werden, was der Beantwortung relevanter Fragen in der Batterieproduktion im Weg steht. An dieser Problemstellung knüpft das Forschungsprojekt „Plattform für Batteriematerialdaten, -wissen und deren Verknüpfung“ (DigiBatMat) an. Durch das im Forschungsprojekt entwickelte System werden Daten und Informationen unterschiedlichster Quellen und Unternehmen unter Berücksichtigung der Datensicherheit zusammengeführt.

einer mehrteiligen Prozesskette zu Batteriezellen verarbeitet. Die Leistungsdaten der Batteriesysteme hängen entscheidend von den Eigenschaften der Materialien und ihrem Zusammenspiel ab. Deshalb werden sie bei den Herstellern in aufwändigen Serienversuchen verbessert und geprüft. Diese Serienversuche gehen mit einem enormen Kostenaufwand und einer Verschwendung von Rohstoffen aufgrund der Produktion unbrauchbarer Batterien einher. Die Anwender solcher Batterien (beispielsweise Hersteller elektrischer Fahrzeuge) analysieren die Materialien ebenfalls und versuchen

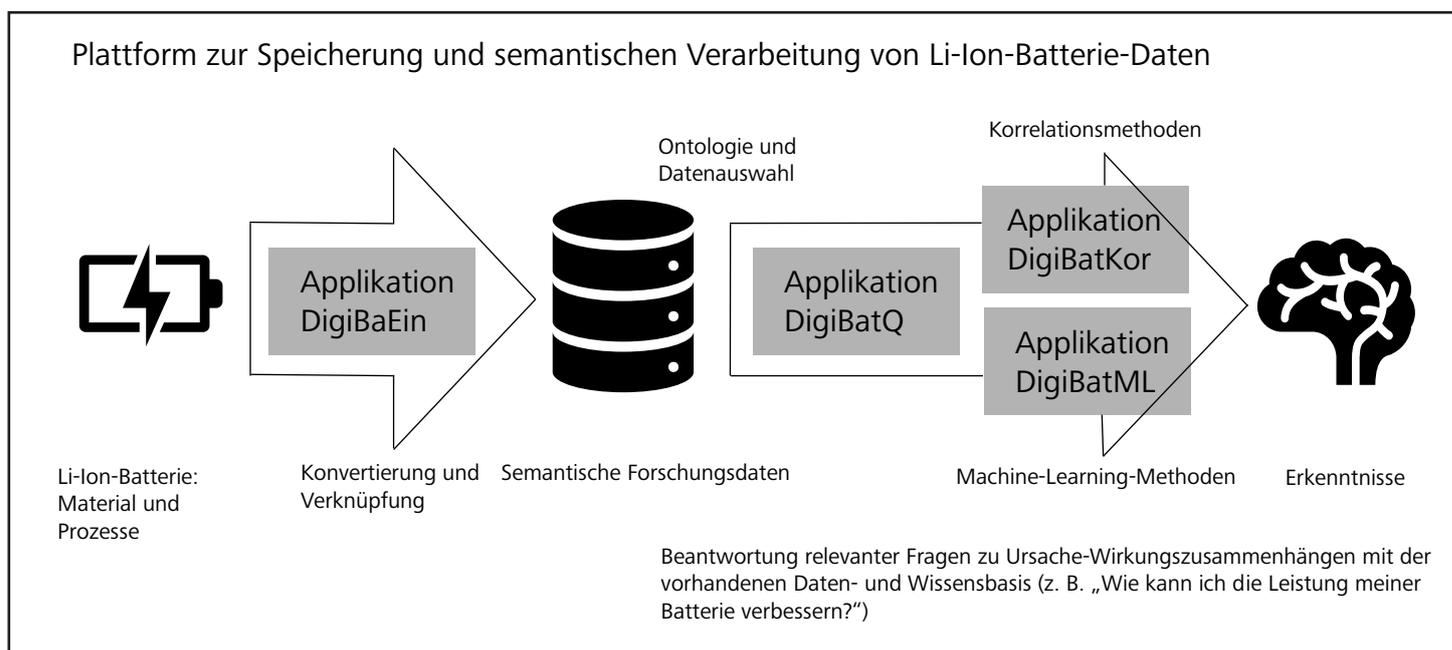


Abbildung 1: Schema Plattform „DigiBatMat“.

Dies ermöglicht den Nutzern der Plattform die umfangliche Analyse der vorliegenden Daten und die Qualitätsvorhersage produzierter Batterien in Abhängigkeit von relevanten Kennzahlen während der Produktion. Das vorliegende und erarbeitete Wissen wird zusammengeführt und für den Nutzer unmittelbar abrufbar gemacht. Somit ermöglicht die Plattform eine ressourcenschonende Batterieforschung zur Entwicklung leistungsfähiger Batterien. Nutzer des Systems werden in die Lage versetzt, zuvor ungenutzte Datenbeziehungen aufzudecken und Synergien zu schaffen.

Aktueller Forschungsstand

Moderne Lithium-Ionen-Batterien (LIB) für aktuelle technologische Geräte enthalten hochspezialisierte, komplexe Materialien. Binder, Leitadditive, Elektrolyten und die Aktivmaterialien der Kathode und Anode werden in

Beziehungen zur Leistung und Haltbarkeit herzustellen. Auf Systemebene bemühen sich innovative Start-Ups, möglichst zutreffende Vorhersagen über den Ladezustand und die Lebensdauer der Batteriesysteme zu treffen. Aufwändige Auswertungssoftware ist Teil heutiger Batterie-Management-Systeme. Daten sind die „Rohstoffe“ all dieser Bemühungen. In der Wissenschaft werden Batteriematerialien (nicht nur von LIB) mit großem Aufwand erforscht, wobei sowohl Eigenschaften der etablierten Materialien untersucht als auch neue Materialien gesucht werden.

Wozu der Schritt zur Digitalisierung?

Im Bereich der Materialwissenschaft werden Projekte üblicherweise getrennt voneinander geplant und durchgeführt. Die Aggregation der erhobenen Daten in einer gesammelten Datenbank ist hierbei nicht möglich. Da Analysen

DigiBatMat bewirkt perspektivisch die Stärkung der digitalen Souveränität.

maschinellen Lernens erst mit größerer Datenbasis zu verwertbaren Ergebnissen kommen, ist die Schaffung einer projektübergreifenden Datenbasis eine Grundvoraussetzung. Bei der Entwicklung neuer Lithium-Ionen-Batterien (LIB) und der Analyse von Qualitätsmängeln existierender LIB stellen sich der Industrie konkrete Fragen, wie „Kann ich eine Batterie schneller laden, wenn ich das Material X verändere“ oder „Durch welche Veränderung kann ich die Kapazität der Batterie erhöhen?“. Solche Fragestellungen sind wirtschaftlich bedeutsam und können entscheidend für die Realisierbarkeit neuer Anwendungen sein. Sie sind heute aber oft schwer zu beantworten und bleiben deshalb offen oder müssen mit großem Aufwand in Serienversuchen beantwortet werden. Wichtige Ursachen dieses Problems liegen in der mangelnden Zusammenspiel existierender Daten und der unsystematischen Darstellung bestehenden Wissens. So werden Veränderungen in Versuchen teilweise nicht genau erfasst und dokumentiert. Auch das Anwenden von Analysemethoden zur Bestimmung von Eigenschaften ist unzureichend beschrieben, wodurch eine Vergleichbarkeit nur schwer möglich ist. Erhobene Daten werden in unterschiedlichen Formaten, nicht standardisiert und oft lokal gespeichert. Diese in der Materialforschung herrschenden Probleme sollen mit dem Forschungsprojekt DigiBatMat angegangen werden.

Die Plattform zur Lösung des Problems

Das Projekt „Plattform für Batteriematerialdaten, -wissen und deren Verknüpfung“ (DigiBatMat) wird durch das vom Bundesministerium für Bildung und Forschung (BMBF) geförderte akademische Förderprogramm „MaterialDigital“ begleitet. Außerdem ist DigiBatMat im Kompetenzcluster zur Batteriezellproduktion „ProZell“ verankert. Für das über drei Jahre geförderte Forschungsvorhaben werden Mittel in einem Volumen von ca. 2,2

Mio. € bereitgestellt. Das Projekt startete im März 2021. DigiBatMat schafft als Teil von „MaterialDigital“ eine Plattform, mit der Daten unterschiedlicher Akteure zusammengeführt und verknüpft werden können. Hierbei tritt das August-Wilhelm Scheer Institut als Experte im Bereich der Digitalisierung und Qualitätsdatenanalyse auf und wirkt unmittelbar auf die Digitalisierung der Batteriematerialforschung ein, indem ein Datenbanksystem entwickelt wird, auf dessen Basis Forschung betrieben werden kann. Zuvor unstrukturierte und nicht zusammengeführte Daten werden in dem System aufbereitet und durch weitere Applikationen analysiert. Das Institut ist für die Softwareentwicklung der Plattform und die Entwicklung der Komponente des maschinellen Lernens zuständig. Erst dadurch sind umfangreiche, projektübergreifende Untersuchungen der Batterien möglich. Um Praxisrelevanz zu garantieren, nutzt das Projektkonsortium eine Datenbasis aus Industriekooperationen und Batterieforschung. Zusätzlich werden Versuchsdaten erzeugt, die im Projekt entlang der gesamten Kette vom Rohstoff bis zur Zelle charakterisiert und dokumentiert werden. Simulationsdaten aus der Kooperation und von externen Partnern ergänzen die Datenbasis und füllen Lücken, wo nicht gemessen werden kann. Integraler Teil der Plattform sind innovative Applikationen, mit denen die Daten komfortabel analysiert werden können. Zur Vorhersage von Qualität (predictive quality) aufgrund von Materialdaten einer bestimmten Zelle wird im Projekt ein Maschinenlern-Algorithmus mit historischen und Referenzdaten trainiert, der zum Schluss Bestandteil der Plattform wird. Zur Identifikation relevanter kausaler Zusammenhänge wird eine Applikation zur linearen und nichtlinearen Korrelationsanalyse der Daten zur Verfügung gestellt. Neben dem August-Wilhelm Scheer Institut sind vier weitere Partner an DigiBatMat beteiligt:



Dr. Dirk Werth

Dr. Dirk Werth ist Geschäftsführer und wissenschaftlicher Direktor des August-Wilhelm Scheer Instituts für digitale Produkte und Prozesse, einem interdisziplinären privaten Forschungszentrum mit Schwerpunkt Digitalisierung. Er arbeitet seit mehr als 15 Jahren an der Frage, wie digitale Technologien Einzug in die betriebliche Praxis finden können und wie Forschung in marktfähige Produkte überführt werden kann. Dr. Werth ist außerdem Chefredakteur der institutseigenen Fachzeitschrift IM+io.

Kontakt

dirk.werth@aws-institut.de
www.aws-institut.de

In der Materialforschung werden Projekte üblicherweise getrennt durchgeführt.

Elektroautos, Akkustaubsauger und Co. haben heutzutage moderne Lithium-Ionen-Batterien.

Im Bereich der Materialwissenschaften und der Batterieforschung ist das Leibniz Institut für neue Materialien (INM) federführend. Das Leibniz Institut beteiligt sich mit zwei Fachbereichen (Energy Materials und Structure Formation) an diesem Projekt. Der Programmbereich Strukturbildung des INM koordiniert das Gesamtprojekt und untersucht die Funktions- und Bildungsmechanismen, die den Eigenschaften von Batteriematerialien zugrunde liegen. Die Technische Universität Braunschweig engagiert sich mit dem Institut für Partikeltechnik und dem Institut für Werkzeugmaschinen und Fertigungstechnik. Die Institute verfügen als zentrale Institution der Battery Labfactory Braunschweig (BLB) über eine vollständige Prozesskette zur Herstellung von Elektroden und Zellen mit inline, online und offline-Erfassung von mehr als 600 Prozess- und Produktdaten. Die Hochschule Aalen – Technik und Wirtschaft untersucht kommerzielle und selbst hergestellte LIB-Zellen aus etablierten Materialien und sammelt dazu seit 10 Jahren umfangreiche Daten, die die Machine Learning Group der Hochschule zur Detektion von Fehlstellen und Gefügekenngößen untersucht. Das Institut für Angewandte Informatik und

Formale Beschreibungsverfahren (AIFB) des Karlsruher Instituts für Technologie (KIT) unterstützt das Konsortium bei der Schaffung der Organisation der Definitionen und Terminologien bis hin zur Erstellung von verknüpften Wissensgraphen, insbesondere im Hinblick auf deren Anschlussfähigkeit.

Systemkomponenten

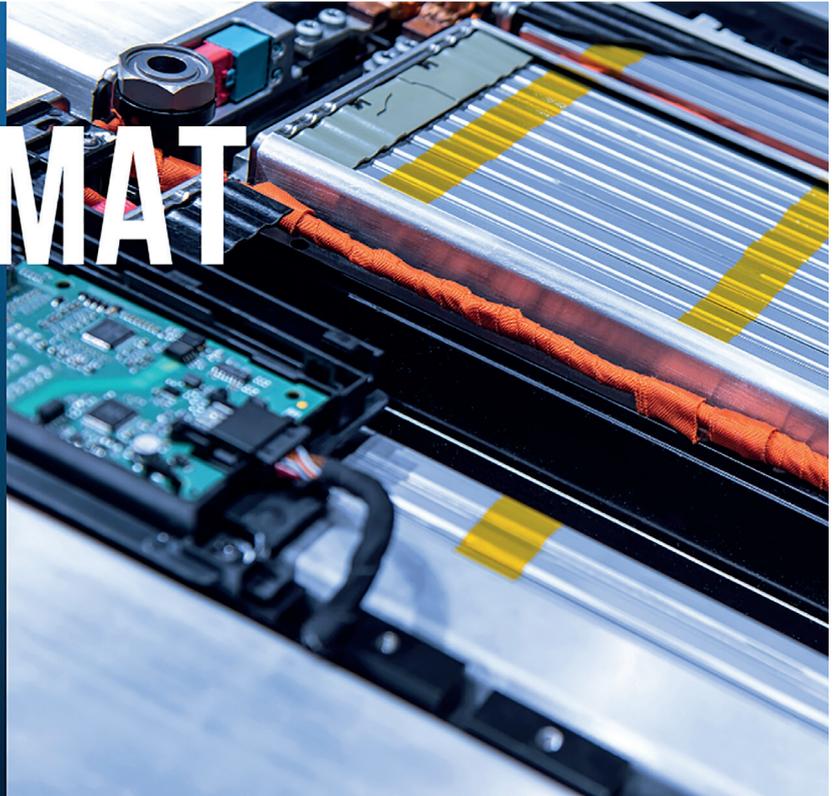
Im Projekt werden vier Hauptkomponenten betrachtet. Im ersten Schritt soll basierend auf mit allen Partnern festgelegten Definitionen und Kenntnissen eine Datenbankstruktur erstellt werden. Mit der in DigiBatMat entwickelten Datenbank sollen Forschungseinrichtungen und industrielle Unternehmen die Möglichkeit haben, Forschungsdaten zur Materialforschung zu pflegen und zu verwalten. Im DigiBatEin-Modul (Dateneingang) werden die Datenbank, sowie entsprechende Schnittstellen zum einfachen Import und Export von Batterie-Materialdaten und -Prozessdaten entwickelt. Über das DigiBatQ-Modul (Question) können Fragen an die Plattform gestellt werden, die basierend auf schon prozessierten Daten Informationen bereitstellen kann. Somit besteht die Möglichkeit, schnell auf vorhandene Erkenntnisse zurückzugreifen. In den Modulen DigiBatKor (Korrelation) und DigiBatML (Maschinelles Lernen) werden vorliegende Daten in der Datenbank prozessiert und analysiert. So werden beispielsweise durch Veränderungen von Prozess- oder Materialparametern die Auswirkungen auf die hergestellte Batterie analysiert. Dies ermöglicht die Qualitätsvorhersage der produzierten Batterie auf Basis vorliegender Einstellungen und Daten im Produktionsprozess.

Infobox

Das Projekt „Plattform für Batteriematerialdaten, -wissen und deren Verknüpfung“ (DigiBatMat) wird durch das vom BMBF geförderte akademische Förderprogramm MaterialDigital begleitet. Außerdem ist DigiBatMat im Kompetenzcluster zur Batteriezellproduktion ProZell verankert. Für das über drei Jahre geförderte Forschungsvorhaben werden Mittel in einem Volumen von ca. 2,2 Mio. € bereitgestellt. Das Projekt startete am 01.03.2021. Daran beteiligt sind fünf Partner: Neben dem gemeinnützigen August-Wilhelm Scheer Institut unterstützen das Leibniz Institut für neue Materialien, die Technische Universität Braunschweig, die Hochschule Aalen und das Institut für Angewandte Informatik und Formale Beschreibungsverfahren die Entwicklung der Plattform im Projekt DigiBatMat.

DIGIBATMAT

**DIGITALE PLATTFORM FÜR
BATTERIEMATERIALDATEN,
- WISSEN UND DEREN
VERKNÜPFUNG**



Fazit und Ausblick

DigiBatMat wirkt perspektivisch in allen oben genannten Aspekten auf die Stärkung der digitalen Souveränität ein. Durch die Verwendung des Systems befinden sich Unternehmen der Materialwissenschaften in der Lage, selbstbestimmt mit den vorhandenen Daten und deren vielseitige Nutzung umzugehen. Zusätzlich entsteht die Möglichkeit der Zusammenarbeit verschiedener Unternehmen zum Zwecke der gemeinsamen Forschung oder des Datenaustausches. Dabei steht die selektive Datenveröffentlichung nach den Vorgaben des jeweiligen Unternehmens im Fokus, wobei die Datensicherheit gewährleistet wird. Zusätzlich soll durch die Verwendung der Plattform die digitale Struktur in Deutschland gestärkt werden, um die Konkurrenzfähigkeit gegenüber großen internationalen Playern aufrecht zu halten.

In den verbleibenden zweieinhalb Jahren des Projektes soll das DigiBatMat-System entwickelt und bereits produktiv von den Partnern der Materialforschung verwendet werden. Hierbei wird ein Fokus auf die Benutzerfreundlichkeit der Applikation gelegt. Neben den wissenschaftlichen Verwertungen in Publikationen und auf Konferenzen soll ein Systemrahmen

entwickelt werden, welcher ohne großen Aufwand auf andere Bereiche der Materialforschung angepasst werden kann. Sowohl Forschungseinrichtungen als auch industrielle Unternehmen sollen über dieses System als Unterstützungskomponente Forschung betreiben können. Der Einsatz des Systems stellt einen bedeutenden Schritt in der Digitalisierung der Materialforschung dar. ■

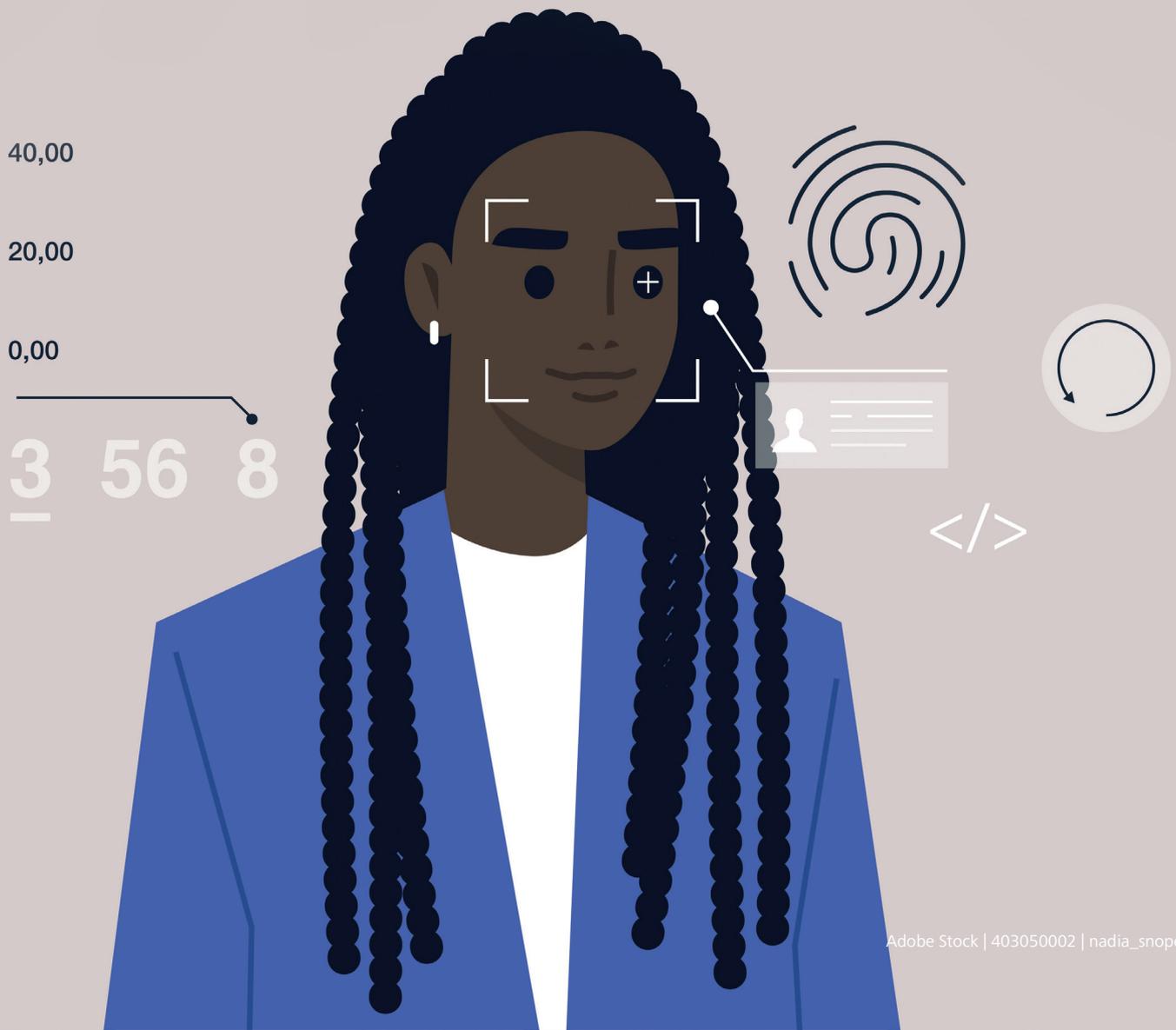
Kurz und Bündig

Das Projekt „Plattform für Batteriematerialdaten, -wissen und deren Verknüpfung“ (DigiBatMat) wird über das vom BMBF geförderte akademische Förderprogramm MaterialDigital begleitet. Das August-Wilhelm Scheer Institut arbeitet gemeinsam mit Partnern in diesem Vorhaben an der Verbesserung der Batteriezellproduktion. Die entwickelte Plattform für Batteriematerialdaten stellt eine innovative Lösung dar, um die Entwicklung und Transparenz von Batterien, deren Herstellung sowie die eingesetzten Materialien weiter voranzutreiben – ein Ansatz für steigende digitale Souveränität in der Branche.

Eine Identität für alles und jeden

Mit Self-Sovereign Identities zu mehr digitaler Selbstbestimmung

Benjamin Leiding, TU Clausthal



Beflügelt durch die fortschreitende und tiefgreifende Digitalisierung unseres Alltages werden auch traditionell-analoge Konzepte in die digitale Welt übertragen – z.B. Identitäten. Wobei wir in diesem Kontext nicht nur von menschlichen Identitäten sprechen, sondern den Begriff verallgemeinern und auch auf (intelligente) Maschinen, Software Services, etc. anwendbar machen. Ähnlich wie die analogen Identitäten sind auch deren digitale Gegenstücke sowie deren Transition hin zu digitalen Identitäten nicht frei von Problemen und Herausforderungen.

Klassische Identitätslösungen wie Personal-Kausweise oder Firmenausweise sind zentralisiert strukturiert und werden entsprechend von einer Zentraleinheit verwaltet und gesteuert – z.B. dem Staat bzw. einer Firma. Deren digitale Pendant funktionieren nach demselben Prinzip, wobei die Verfahren zur digitalen Repräsentation der Benutzeridentität sowie zur Validierung und Authentifizierung in der Regel auf einem asymmetrischen Schlüsselkonzept aufbauen, bei dem das Schlüsselmateriale die digitale Identität eines Nutzers darstellt.

Infrastrukturen für öffentliche Schlüssel (Public Key Infrastructures – PKIs) sind nicht nur das gängigste System für die Verteilung und Verwaltung öffentlicher Schlüssel, sondern auch für die Sicherstellung einer korrekten Zuordnung zwischen einem öffentlichen Schlüssel und dessen Besitzer. Das zentralisierte Vertrauensmodell für die Identitätsauthentifizierung nutzen hierbei hierarchisch strukturierte zentrale Behörden, während etwaige Alternativlösungen wie das PGP Web of Trust (WoT) einen dezentralen Ansatz verfolgen.

Die meisten PKI-Systeme stützen sich auf zentrale Datenbanken und eine Kontrollinstanz zur Verwaltung sowie Speicherung der Schlüssel, welche eine einfache und effiziente Handhabung erlauben. Zentrale Kontrollstrukturen sind in der Regel aber auch Single-Point-of-Failure (SPOF) – wenn diese kompromittiert werden, stellt es eine direkte Bedrohung für die digitalen Identitäten der Benutzer dar. Ähnliche Sicherheitsprobleme könnten auch auftreten, wenn eine nationale Behörde eine Zertifizierungsstelle aus Überwachungsgründen zur Zusammenarbeit zwingt. Ein weiterer Nachteil zentralisierter

Datensilos und des zentralisierten Identitätsmanagements ist die fehlende Interoperabilität zwischen den einzelnen Datensilos. Was aus Sicht des Anbieters zu einem günstigen – und gewünschtem – Lock-in-Effekt und aus Sicht des Endnutzers zu diversen Nachteilen führt.

Im Gegensatz zu den zentralisierten PKI Systemen gibt es bei dezentralen Lösungen wie beispielsweise dem PGP WoT keinen SPOF. Dennoch hat es einige andere Nachteile, wie z.B. fehlende Anreize für die Schlüsselüberprüfung und fehlende Bestrafungen, um die Benutzer zu motivieren, sich an die Überprüfungsregeln zu halten.

Selbstbestimmte Identitäten – Self-Sovereign Identities

Als Alternative zu den altherwürdigen Identitätskonzepten positionieren sich die sogenannten Selbstbestimmten Identitäten (Self-Sovereign Identities – SSI). Eine SSI überträgt den eigentlichen Endnutzern und nicht den Organisationen, die traditionell die Identität zentralisiert managen und verwalten, die Verantwortung für Entscheidungen über ihre eigene Privatsphäre und die Offenlegung von persönlichen Informationen und Berechtigungsnachweisen.

SSI Systeme, die auf dezentralen Identifikatoren (Decentralised Identifiers – DID) basieren, nutzen Ledgers oder Blockchains als verteilte Speichersysteme, die zentralisierte und inkompatible Datensilos durch eine kooperative gemeinsame Speicherressource ersetzen.

Wie sieht das Ganze in der Praxis aus? Nehmen wir das Beispiel des Altersnachweises



Benjamin Leiding

Prof. Dr. Benjamin Leiding ist Inhaber der Juniorprofessur "Software Services for the Circular Economy" an der TU Clausthal und forscht an der Schnittstelle von Digitalisierung und Nachhaltigkeit. Zu seinen Themenschwerpunkten gehören die Circular Economy, die Machine-to-Everything Economy (M2X Economy), Blockchain Technologie, verteilte Systeme und digitale Identitäten.

Kontakt

benjamin.leiding@tu-clausthal.de

zum Konsum von Alkohol. Üblicherweise wird im Zweifel die Vorlage eines Personalausweises verlangt, welcher für die Überprüfung des Alters viel zu viele irrelevante private Informationen enthält, z.B. Geschlecht, Adresse, Geburtsort, Staatsangehörigkeit, Augenfarbe, Körpergröße. Notwendig wäre nur das Alter oder – wenn man es noch genauer nimmt – nur ein Nachweis der Volljährigkeit.

Dezentrale Identifikatoren

Das Konzept der DIDs wurde vom W3C vorgeschlagen und standardisiert. DIDs bieten eine Identität, die von der besitzenden Entität kontrolliert wird, während sie gleichzeitig unabhängig von einem zentralisiertem Identitätsanbieter oder einer Zertifizierungsstelle ist.

Ein DID (`did:example:123456789abcdefghi`) besteht aus drei Teilen: Erstens dem so genannten Schema “did”, zweitens der Methode “example” und schließlich dem methodenspezifischen Bezeichner “123456789abcdefghi”. Der Schema-Teil erklärt ganz einfach, dass es sich um ein DID handelt. Eine DID-Methodenspezifikation legt fest, wie ein DID und das dazugehörige DID-Dokument erstellt, gelesen, aktualisiert und gelöscht werden. Im letzten Abschnitt des Beispiels wird der eigentliche eindeutige Bezeichner beschrieben.

DID Dokumente

Ein DID selbst ist im Wesentlichen eine URL, die einem Nutzer zugeordnet ist und zu einem sogenannten DID-Dokument auflöst. DID-Dokumente beschreiben, wie der entsprechende

DID zu verwenden ist. Diese bestehen aus einer Referenz (ID), die sie mit dem entsprechenden DID verknüpft, öffentlichen Schlüsseln (public keys), die zu Überprüfungszwecken verwendet werden können, Authentifizierungsmethoden (authentication) zur Authentifizierung eines DID oder der besitzenden Entität.

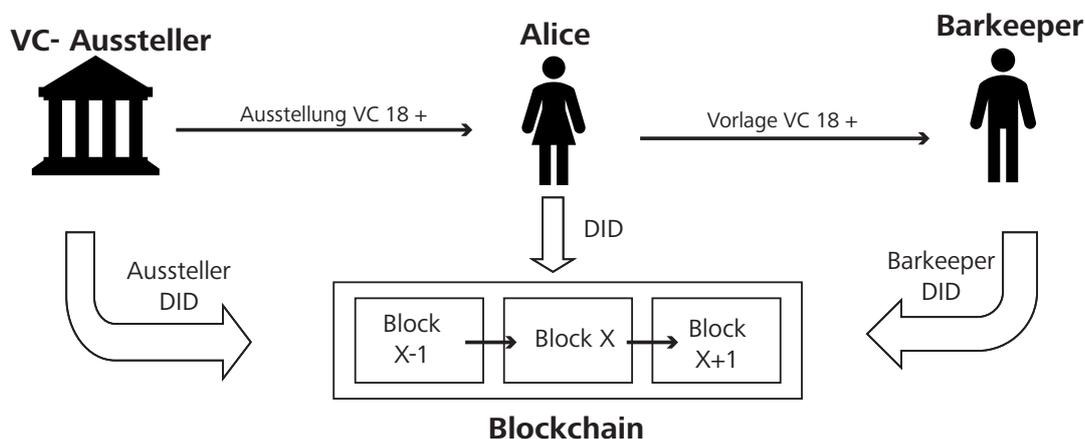
Mittels der Authentifizierungsmethoden kann ein DID-Subjekt kryptografisch nachweisen, dass es mit einem DID assoziiert ist. Der Nachweis erfolgt durch Auflösung des DID in ein DID-Dokument gemäß seiner DID-Methodenspezifikation. Der Nachweis der Kontrolle über den in einem DID-Dokument angegebenen öffentlichen Schlüssel erfolgt über einen signaturbasierten Anforderung-Antwort-Mechanismus.

Verifiable Claims

Allerdings reichen DIDs und DID-Dokumente allein noch nicht aus, um eine digitale Identität zu erschaffen – es fehlt ein Konzept zur Beschreibung der Attribute der Nutzer, z.B. Alter und Bildungsabschluss. Überprüfbare Behauptungen (Verifiable Claims) überwinden dieses Problem und ermöglichen es einer Entität, selektive Verifiable Claims auf sich selbst zu sammeln, die dann mit der DID und dem DID-Dokument verknüpft werden und so eine Identität abbilden. Verifiable Claims werden von einem Verifiable Claim Aussteller (Staatliche Behörde für das Alter, oder Universität für den Uni-Abschluss) ausgegeben und können kryptografisch verifiziert werden.

Wenn wir zurück zu unserem vorherigen Beispiel gehen, könnte ein solcher Verifiable Claim lauten: Alice ist älter als 18 und darf

Abbildung 1: Beispiel Verifiable Claim zur Überprüfung der Volljährigkeit.



SSI bietet ein vom Nutzer gesteuertes Modell zur Bereitstellung einer Identität.

daher Alkohol konsumieren. Das exakte Alter ist nicht relevant, solange es über einem bestimmten Schwellenwert liegt, der Barkeeper prüft lediglich den Verifiable Claim und kontrolliert, dass dieser mit der von Alice kontrollierten DID verbunden ist. Wichtig ist, dass der Verifiable Claims Aussteller dem Barkeeper als vertrauenswürdige Institution bekannt ist, z.B. als staatliche Einrichtung. Ein von Alice selbst ausgestellter Verifiable Claim wäre dementsprechend nicht ausreichend.

Identitäten für intelligente Maschinen

Während die bisherigen Beispiele sich auf menschliche Identitäten beziehen, bedarf es in einer hochgradig technologisierten Welt auch adäquater Konzepte, die intelligente Maschinen und Software Services berücksichtigen. Als Beispiel soll hier die Machine-to-Everything (M2X) Economy dienen. Die M2X Economy ist das Ergebnis von Interaktionen, Transaktionen, Kollaborationen und Geschäftstätigkeiten zwischen Menschen, autonomen und kooperativen intelligenten Maschinen, Software-Agenten und physischen Systemen.

Ein essenzieller Bestandteil sämtlicher wirtschaftlicher Beziehungen der M2X Economy sind die Identitäten der beteiligten Kooperationspartner. Von der jeweiligen Identität des Gegenübers hängt ab, wie viel Vertrauen wir ihm/ihr entgegenbringen, welches Rechtssystem anwendbar ist. Was auf den ersten Blick trivial klingt, ist komplizierter als angenommen, schließlich können wir nicht einfach jede Maschine mit einem Personalausweis ausstatten. Wir benötigen eine Art Maschinenausweisdokument als funktionelles Äquivalent zum Personalausweis. Darüber hinaus müssen Menschen und Maschinen in der Lage sein, sich gegenseitig zweifelsfrei zu identifizieren.

Im Zusammenhang mit dem M2X-Ökosystem kann eine DID-basierte Identitätslösung in Kombination mit Verifiable Claims auf vielfältige Weise genutzt werden. In erster Linie

können DIDs und entsprechende Identitäten für alle Teilnehmer des M2X-Ökosystems erstellt werden, z.B. eine DID/Claim-Kombination für die Fahrzeugidentifikationsnummer (VIN) eines Autos oder ein DID für einen Menschen, der Dienstleistungen nutzt oder anbietet. Mit DIDs können wir auch digitale Zwillinge von analogen Objekten oder Entitäten für digitale geschäftliche Kollaborationen, Interaktionen und Transaktionen erstellen. Darüber hinaus ermöglichen DID-basierte SSIs auch einen sicheren und privatsphäre-wahrenden Ansatz für die gemeinsame Nutzung von Daten, da jede Einheit nicht auf eine Identität (DID) beschränkt ist, sondern Tausende von DIDs, DID-Dokumenten und Verifiable Claims haben kann, die in verschiedenen Szenarien nützlich sind und mit verschiedenen Teilnehmern geteilt werden können.

Fazit

Im Gegensatz zu den klassischen zentralen Identitätsmanagementkonzepten ermöglichen Self-Sovereign Identities ein nutzergesteuertes Identitätsbereitstellungsmodell, bei dem die User den Zugriff und die gemeinsame Nutzung ihrer Daten auf der Grundlage des Wissensbedarfs mithilfe der Konzepte von DIDs, DID-Dokumenten und überprüfbaren Angaben steuern. Darüber hinaus können mittels DID-basierter SSI Systeme auch Identitäten für intelligente Maschinen und Software Services realisiert werden. ■

Kurz und Bündig

Im Gegensatz zu den klassischen zentralen Identitätsmanagementkonzepten ermöglichen Self-Sovereign Identities ein nutzergesteuertes Identitätsbereitstellungsmodell, bei dem die User den Zugriff und die gemeinsame Nutzung ihrer Daten auf der Grundlage des Wissensbedarfs mithilfe der Konzepte von DIDs, DID-Dokumenten und überprüfbaren Angaben steuern. Darüber hinaus können mittels DID-basierter SSI Systeme auch Identitäten für intelligente Maschinen und Software Services realisiert werden.

„Ein Puzzle mit vielen Teilen“

Digitale Souveränität als gelebte Abhängigkeit

Andreas E. Thyen, LizenzDirekt AG

Das Thema digitale Souveränität ist dieser Tage in aller Munde. Zuletzt hat sich auch die Politik hierfür in zunehmendem Maße ausgesprochen. Aber ist es leicht oder gar überhaupt möglich, diese zu erlangen? Und wenn ja, ist sie überhaupt erstrebenswert? Genügt ein entsprechender politischer Wille, um das proklamierte Ziel digitaler Souveränität zu erreichen?

Digitale Souveränität – Maßstab und Denkansatz

Pauschalisierungen helfen sicher nicht, um Antworten zu finden, aber allzu häufig dürfen die Teilnehmer der Diskussionen nicht einmal von derselben Bedeutung des Begriffs und dessen Dimension ausgehen. Hinzu kommt, dass regelmäßig auch ein technischer Sachverstand erforderlich für eine Orientierung ist. Aber auch ökonomische, soziologische bis hin zu ökologischen Aspekten gehören maßgeblich zu diesem Komplex. Dann wird sich die Frage stellen: „Inwieweit ist eine digitale Souveränität überhaupt möglich oder geben wir uns mit diesem Ansinnen nur noch einer Illusion hin?“

Ein wissenschaftlich-theoretischer Bezugsrahmen sowie entsprechende Hypothesen werden nachfolgend nicht aufgestellt. Vielmehr geht es darum, einige Aspekte und Szenarien exemplarisch herauszustellen, um die Relevanz, Komplexität, aber auch Gegensätzlichkeit aufzuzeigen und vor allem einen Appell zu richten, das Thema für sich zu entdecken und sich in den gesellschaftlich-politischen Diskurs einzubringen.

Digitale Souveränität – Eine Orientierung

Bevor eine Meinungsbildung möglich ist oder Lösungsansätze evaluiert werden können, muss eine Orientierung im Zusammenhang mit dem Begriff der digitalen Souveränität erfolgen. Dabei fällt schon bei der Meinungsschau auf, dass es nicht nur keine klare Definition hierfür gibt, sondern jeder Beitragende einen eigenen Ausgangspunkt mit entsprechendem Verständnis wählt. Folglich ist die Auswahl von Definitionsversuchen denkbar groß und die inhaltliche Reichweite allumfassend und kontextabhängig ausgeprägt.

Souveränität zielt vom Wortverständnis auf Selbstbestimmung ab, welche sich durch

Unabhängigkeit und Eigenständigkeit vom Zustand der Fremdbestimmung abgrenzt [1]. Im digitalen Kontext wird hiermit ein gesellschaftliches Ziel beschrieben, wodurch politische, wirtschaftliche und auch individuelle Abhängigkeiten in der sich digitalisierenden Welt reduziert werden sollen; das gelte etwa für Schlüsseltechnologien, Geschäftsmodelle und digitale Ökosysteme [2]. Umfasst werden Abhängigkeiten von Infrastrukturen, Daten, Hard- und Software wie auch Bildung [3].

Aus dem weiten und komplexen Definitionsansatz wird deutlich, dass die Frage einer digitalen Souveränität niemals universell beantwortet werden kann und vom individuellen Standpunkt aus als äußerst paradox empfunden wird. Was für den einen Souveränität bedeutet, bedeutet paradoxerweise das Gegenteil – nämlich eine Einschränkung von Freiheit – für manch anderen. Gleiches folgt aus den unterschiedlichen Idealen und Zielrichtungen von Politik, Wirtschaft und Geisteswissenschaften.

Bei allen Bestrebungen nach Unabhängigkeit ist zudem zu bedenken, dass eine vollständige Digitale Souveränität in einer vernetzten Welt gemeinhin als weder realistisch noch zielführend angesehen wird, jedoch zumindest in kritischen Bereichen immer eine Risikoabwägung zu erfolgen habe [4].

Ebenso elementar ist aber auch, dass digitale Souveränität nicht isoliert zu betrachten ist. Unmittelbar spielen hier zu diskutierende gesellschaftliche, demokratische und politische Fragen mit, aber es werden auch Zielkonflikte und widerstreitende Interessen nicht zu vermeiden sein. Aus diesen Gründen bestehen gesamtgesellschaftliche Betrachtungserfordernisse in jedem

Eine Software ist kein statisches Werk.



Andreas E. Thyen

Dipl. Volkswirt Andreas E. Thyen studierte in Hamburg Wirtschafts-, Rechtswissenschaften und Soziologie sowie Internationale Wirtschaftsbeziehungen und Sozialökonomie. Seit über 20 Jahren berät Thyen zu zahlreichen Planungs-, Prozess und Management-Themen u.a. bei einer internationalen Unternehmensberatung und publizierte in diesem Kontext. Heute ist Thyen Präsident des Verwaltungsrats der LizenzDirekt AG. Hierbei schöpft er von seinem Erfahrungsschatz aus über 14 Jahren in führenden Positionen auf dem Gebrauchtssoftware-Markt. Weit über die rechtlichen Grundlagen dieses Marktes hinaus vermittelt Thyen routiniert, engagiert und mit Weitsicht die Tragweite damit verbundener wirtschaftlicher und gesellschaftlicher Aspekte und Interessen.

Kontakt

andreas.thyen@lizenzdirekt.com

Einzelfall der Ausgestaltung Digitaler Souveränität. Damit geht es darum, einseitige und unvollständige Ansätze sowie Ausgrenzungen bei der eigenen Meinungsbildung zu vermeiden.

Digitale Souveränität – Bestandsaufnahme

Um ein realistisches Bild zum Stand der Digitalen Souveränität zu erhalten, ist aufgrund der Weite des „neuen“ Themenfelds notwendigerweise eine Konkretisierung erforderlich. Im Zusammenhang mit Standardsoftware und zugehörigen Diensten fällt eine (nicht-repräsentative) Erhebung relativ leicht. Die Abhängigkeit von Betriebssystem- und Office-Software aus dem Hause Microsoft ist denkbar hoch und hat sich während des Lockdowns dramatisch ergänzt und um Cloud-Dienste wie Teams noch gesteigert. Eine Studie der Unternehmensberatung PwC für das deutsche Bundesministerium des Inneren ergab bereits im Jahr 2019, dass die zunehmende Abhängigkeit von wenigen Softwareanbietern die digitale Souveränität der deutschen Bundesverwaltung erheblich gefährde. Souveränität ist hier kaum zu erkennen und in Zukunft trotz großer Agenden begrenzt zu erwarten, und dies trotz beachtlicher Anstrengungen wie derzeit in Schleswig-Holstein [5] sowie im Ansatz in Bezug auf Basisfunktionen von weiteren Bundesländern und des Bundes zu sehen ist [6].

Bekanntnisse zur Steigerung Digitaler Souveränität gibt es sowohl in Deutschland als auch auf europäischer Ebene. Im Jahre 2020 erklärte die deutsche Ratspräsidentschaft, „Digitale Souveränität als Leitmotiv der europäischen Digitalpolitik etablieren“ zu wollen [7]. Auch die Europäische Kommission hat die „Gestaltung der digitalen Zukunft Europas“ neben dem „Grünen Deal“ zur Leitlinie erklärt [8]. Allerdings treten wegen der Vielfalt an Konzepten für digitale Souveränität und der unterschiedlichen Handlungsebenen - Staat, Wirtschaft und Individuum - immer wieder Zielkonflikte bereits in der Konzeptionsphase auf [9]. Richtigerweise spricht die Kommission daher von einem komplexen Puzzle mit vielen Teilen [10].

Digitale Souveränität – Bestrebungen

Insbesondere auf Infrastrukturebene gibt es zunehmend staatlich initiierte Bestrebungen - wie von der Europäischen Kommission in Bezug auf 5G-Netze und Deep-Tech wie Cloud-Kapazitäten,

Blockchain und Quantentechnologien [11]. Damit soll dem Trend entgegengewirkt werden, dass neben Microsoft Clouddiensten auch in Europa insbesondere auf Amazon Web Services auf Infrastrukturebene, zumindest im Privatsektor, zunehmend zurückgegriffen wird, anstatt noch eigene Server zu betreiben. Denknottwendig nimmt die Abhängigkeit auf Datenebene zu - und damit die Souveränität weiter ab. Nicht einmal Wechselmöglichkeiten sind hier noch ohne Weiteres möglich, wodurch sich die Initiative der EU erklärt, hier entsprechende Rechte für Kunden zu schaffen [12].

Was häufig bei der großen Programmatik vergessen wird, ist jedoch, dass die Abhängigkeiten nicht ohne Grund bestehen und nicht ohne Grund noch zunehmen. Zwar gibt es beachtliche Anstrengungen, europäische Lösungen wie das GAIA-X-EU-Cloudprojekt aufzubauen, und es bestehen zahlreiche Open-Source-Lösungen, die mit den kommerziellen Produkten mithalten können. Dennoch gilt das nicht uneingeschränkt.

Eine Software ist kein statisches Werk, sondern lebt von der Fortentwicklung und Anpassung an aktuelle Bedürfnisse. Hieran hapert es häufig im Open-Source-Bereich genauso wie an Supportmöglichkeiten und Kompetenzen. Hinzu kommen wichtige Maßgaben an Verfügbarkeit, Performance und Skalierbarkeit.

Aus diesem Grund überrascht es wenig, dass dem europäischen GAIA-X Projekt ausgerechnet das auf Big-Dataanalysen spezialisierte US-Unternehmen „Palantir“ angehört, das auch für die US-Geheimdienste tätig sein soll. Ebenso befriedigend ist die Tatsache, dass zuletzt wiederum auch die US-Giganten Microsoft und Amazon einbezogen wurden [13]. Gleichwohl sieht die von der Europäischen Kommission ausgearbeitete europäische Datenstrategie weiterhin noch alle Möglichkeiten der EU als offen an, da ein Großteil der Daten künftig aus industriellen und beruflichen Anwendungen, aus Bereichen von öffentlichem Interesse oder aus Alltagsanwendungen des Internets der Dinge stammen, also aus Bereichen, in denen die EU stark sei [14]. Diese Erwartung erscheint jedoch recht optimistisch, da die Vergangenheit diesen Effekt vermissen ließ.

Digitale Souveränität – Zurück im Unternehmen

Schließlich darf nicht übersehen werden, dass

Prognose bis 2025

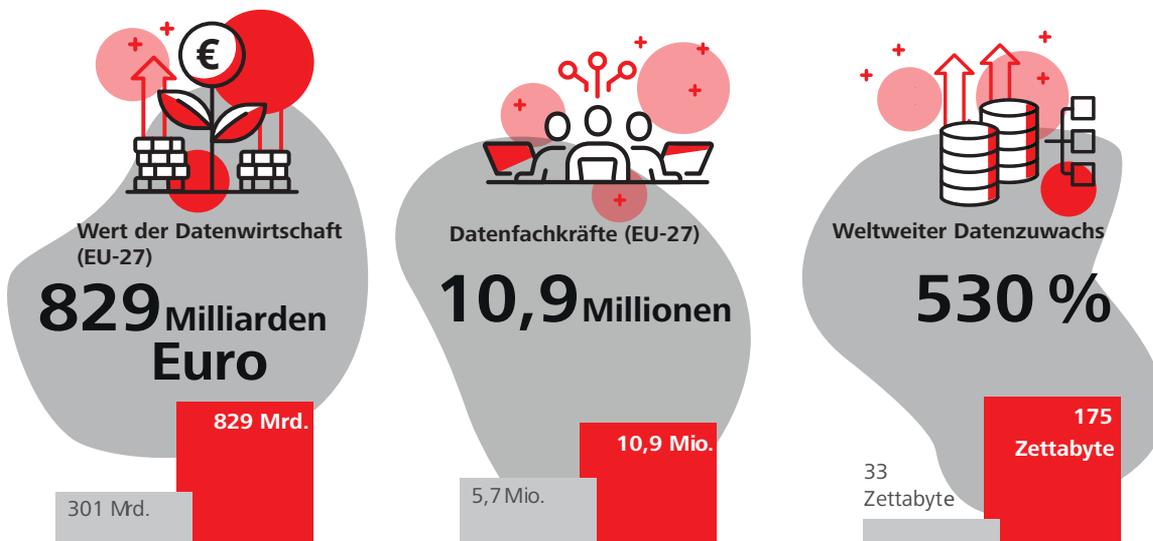


Abbildung 1: Prognosen der Datenveränderungen in 2025 [14]. ©LizenzDirekt AG by Claudia Herpich, NeueWelten Design.

jedes Unternehmen schon lange unter enormen Digitalisierungsdruck steht. Hier geht es nicht um zukünftige Visionen der Politik, sondern um die praktische Gegenwart. Im Ergebnis gilt Ähnliches für den Staat. Die Möglichkeiten der eigenen Digitalisierung sind hingegen ökonomisch ebenso unterschiedlich wie auch die Anforderungen abweichen.

Lokal installierte „On-Premise“ Software wie auch Cloud-Dienste dienen zuvorderst der Erledigung der alltäglichen Aufgaben und Bewältigung der technischen Prozesse. Der Anspruch ist hierbei nicht von regionalen Gegebenheiten abhängig, sondern muss sich in der Regel am globalen Niveau orientieren. Auf Infrastrukturebene bestimmen entscheidend Leistungsfähigkeit und skalierbare Verfügbarkeit. Hier können also europäisch-regionale Limitationen überaus unerwünscht sein. Wer in diesem Komplex den Anschluss verpasst, ist schneller abgehängt als je zuvor. Das hat auch mit der nahezu in allen Wirtschaftszweigen enormen Zunahme der Relevanz von Daten und deren Auswertung für die eigene Wertschöpfung zu tun. Dies hat wiederum auch die EU-Kommission erkannt. Hier wird von einem Wert der Datenwirtschaft von 829 Mrd. Euro und einer weltweiten Datenzunahme um 530 % (seit 2018) zu 175 Zettabyte im Jahr 2025 ausgegangen [15].

Hinzu kommt die regelmäßige Abnahme eigener Kompetenzen im Unternehmen und Server und die Fähigkeit eigene Infrastruktur zu administrieren. Die Kompetenzen im

staatlichen Umfeld sind ebenfalls durch das bisherige Engagement beschränkt. Abgerundet wird das Unterfangen mit gestiegenen Anforderungen an Datenschutz und Datensicherheit.

Aus diesen Gründen könnten heutige Initiativen, für eigene konkurrenzfähige europäische Lösungen zu schaffen selbst bei deren erfolgreicher Vollendung zu spät für viele Unternehmen kommen und ohne rechtliche Notwendigkeit kaum Relevanz entfalten. Der nunmehr von der EU intendierte rechtliche Rahmen kommt zu spät. Selbst scheinbar datenschutzfreundliche Angebote von US-Anbietern in Zusammenarbeit mit der „Deutschen Telekom“ als Treuhänderin wurden zunächst eingestellt. Insofern darf sich nicht der Naivität hingegeben werden, dass Jahrzehnte des Rückstands und mangelnder eigener digitaler Schöpfungskraft in Europa über Nacht aufgeholt werden können. Auch anderen Rechtsrahmen wie der DSGVO ist das nicht entscheidend geglückt. Zwar diente die DSGVO manch anderem Land als Vorbild. Dennoch stehen heute Unternehmen praktisch vor unlösbaren Risiken, da umgekehrt der EU-US-Privacy Shield als Grundlage für Datentransfers in die USA noch dazu weggefallen ist.

Digitale Souveränität – Komplex bleibt komplex

In unserer hochgradig globalisierten und digitalisierten Welt wird vollkommene Digitale Souveränität gemeinhin weder als realistisch

noch pauschal erstrebenswert erachtet. Das mag an der angedeuteten Komplexität des Themas liegen, welches nicht frei von Paradoxen ist und unsere gesamte Gesellschaft prägt. Wie die Europäische Kommission konstatiert, sei der stattfindende Wandel ebenso fundamental wie der Wandel, der durch die industrielle Revolution ausgelöst wurde [16]. Gleichwohl muss es gar nicht um absolute digitale Souveränität gehen, sondern darum, bestimmte Abhängigkeiten der Bedeutung gegenüber in angemessenen Maße graduell abzubauen, um diese durch europäische Werte und Inhalte im Rahmen einer Gesamtstrategie auszufüllen.

In bestimmten – etwa hochsicherheitsrelevanten Bereichen – dürfte das zu fordernde Souveränitätslevel entsprechend hoch anzusetzen sein. In anderen gesellschaftlichen Bereichen wird es hingegen erst einmal um mehr Transparenz und Wettbewerbsfähigkeit gehen. Im Übrigen bedeutet und verlangt Digitalisierung in aller Regel höchstmögliche Vernetzung und Dynamik. Das Maß an Abhängigkeit und die damit verbundenen Einflussnahmemöglichkeiten von einigen wenigen globalen US-Unternehmen sind aber ohne Zweifel besorgniserregend.

Am Beispiel der sogenannten „gebrauchten Software“

Trotz der Not gibt es keine pauschale Lösung der Problematik, um Abhängigkeiten zu reduzieren. Jede knappe Empfehlung hierzu wird unterkomplex sein. Jedoch lohnen sich jeder Denkansatz und jede Initiative. Vor allem müssen aber auch das konkrete praktische Szenario und entsprechende flankierende Maßnahmen betrachtet werden. Anfangen kann hierbei jeder bei sich selbst, indem anstelle des Reflexes zugunsten von kommerziellen US-Produkten zumindest auch Alternativen evaluiert werden und die gebotene Risikobetrachtung erfolgt. Genauso zählt hierzu, nicht nur aus Trendgründen auf Cloud-Produkte zu setzen.

Zumindest im Officebereich genügen Behörden wie auch Unternehmen oftmals „On-Premise“ Lizenzen. Diese dauerhaften Lizenzen („Perpetual“) bieten zudem den Vorteil absoluter (einmaliger) Kosten mit entsprechenden Möglichkeiten der Abschreibung anstelle von kontinuierlichen Kosten und etwaigen Änderungen, aber noch dazu die Möglichkeit, bei Bedarf weiterverkauft zu werden. Nicht zuletzt

die Europäische Union als freiheitlicher Rechtsraum bietet hiermit dank der EuGH-Rechtsprechung aus 2012 einen entscheidenden Vorteil in Form der sogenannten gebrauchten Softwarelizenzen. Auch durch Wahrnehmung solcher Möglichkeiten und allenfalls lediglich ergänzender Abolizenzen wird ein Stück Souveränität bewahrt. Gleichzeitig ist der negative ökologische Effekt von Cloud-Serverfarmen nicht zu unterschätzen.

Dort, wo es keine konkurrenzfähigen Lösungen gibt oder keine eigenen Kompetenzen bestehen, diese konkurrenzfähig zu machen, sind Vorwürfe verfehlt und politische Agenden gefragt, Kompetenzen zu entwickeln und zu fördern. Dort, wo aber Ignoranz herrscht, etwa indem Ausschreibungen in der IT aus Gewohnheit oder gar Bequemlichkeit auf bestimmte Produkte oder Anbieter zugeschnitten werden und damit offener Wettbewerb und Alternativen faktisch ausgeschlossen werden oder aus fadenscheinigen Gründen Möglichkeiten wie der An- und Verkauf gebrauchter Software versäumt werden, ist vor dem Hintergrund des Ansinnens digitaler Souveränität Kritik angebracht und ein höheres Maß an Selbstreflexion geboten.

Das Selbstbestimmungsrecht des Einzelnen - mag es im digitalen Kontext auch beschränkt sein - unterliegt der eigenen Obliegenheit, sich zugunsten dessen Wahrung zu verhalten. Dies ist sich stets zu vergegenwärtigen und bei Abwesenheit fortwährend anzumahnen, wozu nicht zuletzt dieser Artikel aufrufen will. Politisch wurde dem von der EU-Kommission Nachdruck verliehen. Es geht gerade nicht nur um die Förderung des europäischen Wettbewerbs, sondern es zeigt sich am Beispiel gebrauchte Software erstaunlicherweise die Synthese und wechselseitige Stimulierung der beiden Hauptanliegen der Europäischen Union (Grüner Deal und digitale Zukunft), indem entsprechend der Kreislaufwirtschaft sowohl ökologisch nachhaltige Werte erworben und veräußert werden. Damit wird auch die Souveränität in Form des europäischen Wettbewerbs und der involvierten Kunden gestärkt.

Insofern bestehen einige Gemeinsamkeiten und ein gleich gerichtetes Engagement zwischen der Herausforderung durch die digitale Souveränität und die globale Klimakrise. Gleichmaßen kann jeder seinen Beitrag hierzu leisten, wenngleich große Veränderungen politische Umsetzung verlangen.

Die Tat des Einzelnen zählt (auch)

Dabei kann sich das Engagement des Einzelnen sehr wohl lohnen. Nichts zu tun und sich nur zu echauffieren oder aufzugeben, ist sicher nicht die richtige Wahl. Auch kleine Anstrengungen können sich lohnen und gemeinsam zu einer beeindruckenden Aktion werden und Vorbildcharakter erreichen. So wurde der Softwarerie- se Microsoft in seine Schranken gewiesen, nachdem im letzten Jahr trotz des vom Hersteller gewünschten Umstiegs von On-Premise-Lizenzen auf entsprechende Abonnementlizenzen schlagartig entgegen europäischen Grundsätzen ein Verkauf der alten Lizenzen nicht mehr erlaubt sein sollte. Diese Änderung der Produktbestimmungen durch Microsoft inmitten der Corona-Krise fiel dem Autor umgehend auf, der als erfahrener Händler nicht vergessen hat, mit welcher Intensität Hersteller den Gebrauchthandel verhindern wollten. Dennoch sollte es mehr als ein Jahr mit zahlreichen Publikationen und Aufrufen des Autors und anderer dauern, bis Microsoft den Zusatz kassierte.

Das ist sicherlich nur ein vergleichsweise einfaches Beispiel, aber ein solches mit Signalwirkung. Persönliches Engagement kann sich lohnen und Grenzen müssen gerade auch US-Monopolisten zumindest dort gesetzt werden, wo europäische Rechte untergraben werden, und Linien heimlich verschoben werden. Umgekehrt soll damit kein Aufruf für protektionistische oder sonstige wettbewerbsbeschränkende Maßnahmen verbunden sein. Auch eine solche Einseitigkeit würde der Komplexität der digitalen Souveränität nicht gerecht werden und wirtschaftlichen Interessen kaum entsprechen.

Es bleibt abzuwarten, was die europäische Agenda zur digitalen Souveränität bis zum Ende der deutschen Ratspräsidentschaft tatsächlich konkret erreichen wird. Aber auch die Evaluierung deutscher Bestrebungen der digitalen Verwaltung wird spannend sein. Nicht zuletzt wird es hierbei auf eine Auswertung der Nachhaltigkeit genauso wie auf Interoperabilität und eine Kosten-Nutzen-Analyse ankommen. Wie sich hier der dieser Tage ebenfalls gelegentlich diskutierte Föderalismus und länderübergreifende Kooperationen auswirken werden, bleibt abzuwarten.

Erst eine Auswertung der Erfolge der Maßnahmen wird zeigen, ob und in welchen Bereichen überhaupt eine qualitative Verbesserung digitaler Souveränität erreicht wurde. Es

ist anzuerkennen, dass das Thema politisch spät, aber deutlich ambitionierter angegangen wird als bisher. Hier tut sich aktuell sehr vieles, aber nur rechtstheoretisch und abstrakt. Daher werden die konkrete Umsetzung und der praktische Effekt entscheiden. Eine grundlegende Umordnung der aktuellen Machtverhältnisse der Akteure in diesem Komplex ist kurz- und mittelfristig kaum zu erwarten. Auch in anderen Bereichen wird digitale Souveränität unter Umständen eine Illusion bleiben. Dennoch zählen auch die bereits in der Gegenwart möglichen Entscheidungen und Maßnahmen zugunsten einer Zunahme von digitaler Souveränität. Hier können Wechsel zu freier Office Software genauso wie die nachhaltige Beschaffung gebrauchter Software eine gewichtige Rolle spielen. Das gilt für den Staat genauso wie für die Privatwirtschaft. Die Summe solcher Einzeltaten kann einen signifikanten Beitrag leisten und den gesellschaftlichen Wandel mitprägen. Der einzelne Benutzer ist also selbst gefordert, nicht auf das Wahrwerden der absoluten Souveränität zu warten, sondern seine eigenen Möglichkeiten auszuschöpfen und genauso wie in Umweltfragen die Tragweite und Konsequenzen des eigenen Tuns zu begreifen. Es geht damit darum, eigene Initiativen zu entfalten und sich entsprechend diesem Appell, wie eingangs als Maßstab und Denkansatz für diesen Ansatz postuliert, den großen Herausforderungen im Alltag zu stellen und eigene Handlungsmöglichkeiten zu bewerten. ■

Kurz und Bündig

Digitale Souveränität ist aktuell ein großes politisches Anliegen ohne eindeutige Definition und zu komplex, um an einfache, universelle und absolute Lösungen zu Förderung dessen zu glauben. Hingegen bestehen auch eigene Möglichkeiten, um einen Beitrag hierzu zu leisten. Am Beispiel gebrauchter Software zeigt sich etwa die Synthese und wechselseitige Stimulierung der beiden derzeitigen Hauptanliegen der Europäischen Union (Grüner Deal und Digitale Zukunft), indem sowohl ökologisch nachhaltig Werte erworben und veräußert werden wie auch damit Souveränität in Form des europäischen Wettbewerbs und der involvierten Kunden gestärkt werden.

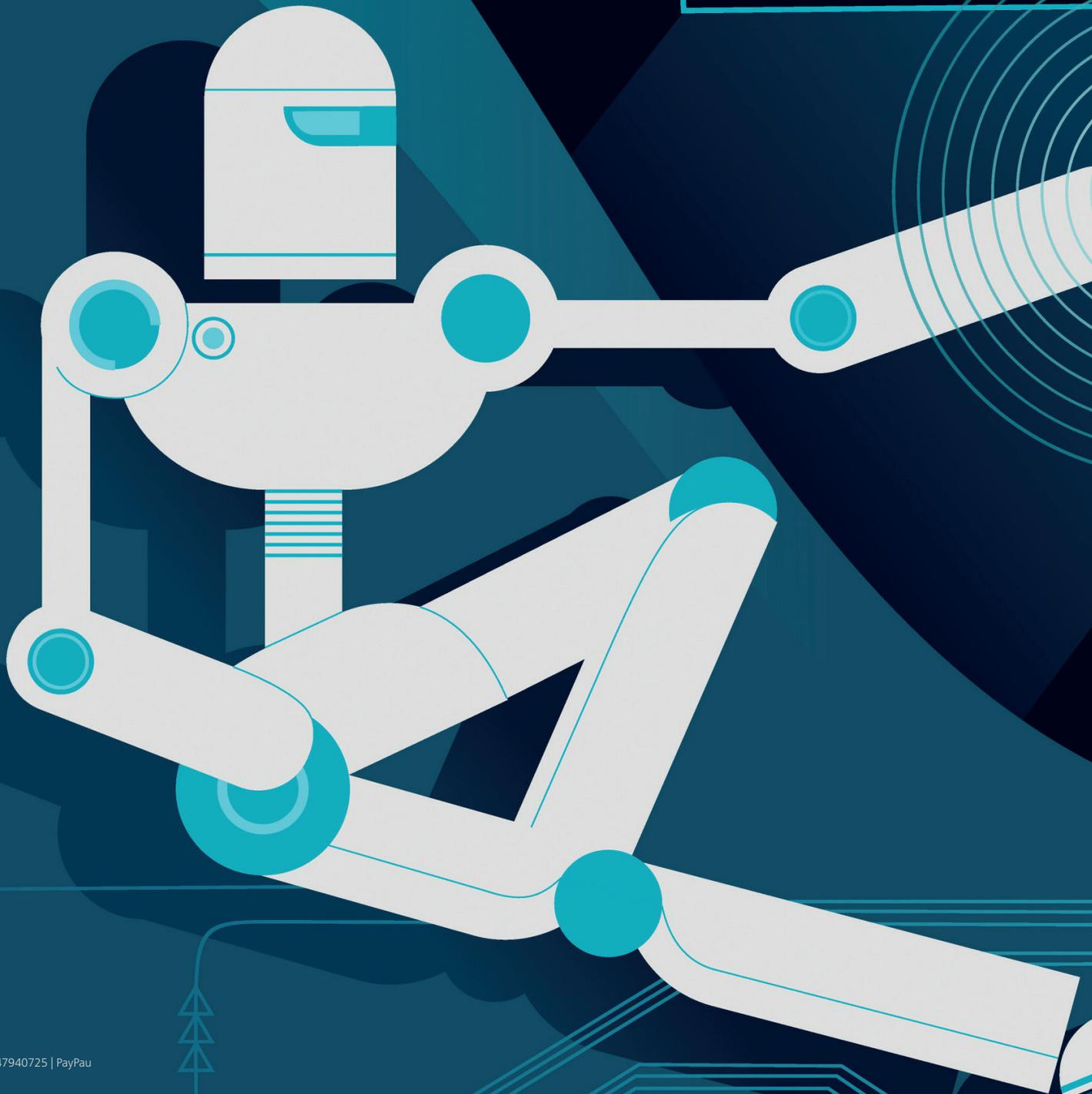


Weitere Infos und Literaturangaben zum Artikel finden Sie unter folgendem Link: <https://bit.ly/3kwdChH>

Ich digitalisiere, also bin ich!

Digitale Souveränität als gesamtgesellschaftliches Thema

Martin C. Wolff, Digital.Wolff, Plötz & Co GmbH





Der Begriff „digitale Souveränität“ wird sehr unterschiedlich aufgefasst. Entsprechend hilflos und chaotisch wirken einzelne Umsetzungsversuche. Die fehlende Konzeptbildung hat eine historische Tiefendimension an Technikskepsis, die deutlich nachwirkt. Der Artikel zeigt die Innovation des Digitalen in der Souveränität und somit den Bedarf der fehlenden, aber notwendigen Konzeptionsbildung auf.



Martin C. Wolff

Dr. Martin C. Wolff ist Unternehmer und Wissenschaftler. Er lehrt Philosophie und Digitale Ökonomie an der Humboldt Universität zu Berlin, berät Behörden und Non-Profit-Organisationen zur Digitalisierung und entwickelte den „Digitalen Klingelbeutel“. Er forscht zur Theorie und Praxis von Digitalisierung & Cyber, leitet an der Führungsakademie der Bundeswehr das Internationale Clausewitz Zentrum und das Clausewitz Netzwerk für strategische Studien.

Kontakt

martin@digitalwolff.de
digitalwolff.de

Erbe und Innovation der digitalen Souveränität

Digitale Souveränität ist in aller Munde. Unter ihr werden Datenschutz und „digitale Selbstverteidigung“ ebenso sehr gefasst wie die Bestrebungen, mittels mehr Open-Source-Lösungen weniger abhängig von US-amerikanischen Produkten zu werden; mal meint man Investments in KI oder geradezu tragische Ambitionen für Cloud-Services wie Gaia-X; oder wöchentliche Blockchain-Lösungen mit Heilscharakter, die kurz darauf zurückgezogen werden. Die Vielzahl der Diskurse zeigt: Es fehlt ein gemeinsames Verständnis. Tatsächlich erscheint mir sogar fraglich, ob überhaupt irgendein Verständnis existiert. Diese Kakophonie ist Ausdruck einer Orientierungslosigkeit.

Es ist die Logik des Mehr-vom-Selben, die sich trotz offenkundigen Scheiterns aufgrund des Mangels an Alternativen wiederholt. „Die Definition von Wahnsinn ist, immer wieder das Gleiche zu tun und andere Ergebnisse zu erwarten (Albert Einstein).“ Es fehlt die kleinteilige und mühsame Grundlagenarbeit und Konzeptbildung, was man überhaupt lösen möchte; was die Ziele sind. Die fehlende Konzeptbildung hinterlässt Mahnmale aus Investitionsleichen, sei es beim digitalen Führerschein, der DE-Mail, dem besonderen elektronischen Anwaltspostfach und so einigem mehr. Die Aktivisten des Chaos Computer Clubs werden als Boten schlechter Nachrichten abgelehnt („Don't shoot the messenger!“). Und doch muss man feststellen: Auch sie haben kaum konstruktive Vorschläge, wie man digitale Souveränität entwickelt. Um nicht in dieselbe Falle zu tappen, ist ein kleiner ideengeschichtlicher Überblick notwendig.

Die problematische Debatte zur digitalen Souveränität

Souveränität ist kein technisches oder digitales Thema, sondern ein philosophisches und ein politisches. Es geht um Herrschaft. Das ist hierzulande heikel, wir beobachten die deutschsprachige Entwicklung von Machtversessenheit zur Machtvergessenheit, in der wir die erlernte Hilflosigkeit mit moralischer Überheblichkeit kompensieren. Beim Begriff Herrschaft ist zu hinterfragen: Worauf und wogegen richtet sie sich? Wie ist das Verhältnis von Gewaltmitteln zu den Rechtsmitteln? Wie

legitimiert und wie schützt sie sich? Und – bei der Digitalen Souveränität am wichtigsten – Wie ist das Verhältnis von Staat zu privat?

Die profanen Ansätze scheitern an ihrer jeweiligen Tradition. Der technische/digitale Ansatz einerseits hält alle Technologie für einen Heilsbringer und behauptet, dass der Zweck die Mittel heilige. Das löst Widerstände aus.

Die ministeriell-juristische Administration andererseits macht, was sie schon immer gemacht hat. Das ist ihr Auftrag: Innerhalb bestehender Prozesse, fester Rechtsrahmen und getrennter Ressortprinzipien versucht sie ein vernetztes, innovatives, ergo normabweichendes und kostenintensives Thema juristisch zu erschlagen. Das ist wie Pudding an die Wand nageln.

Digitalisierung wird fälschlicherweise für ein technologisches Thema, nicht für ein gesellschaftliches gehalten – und entsprechend von Technologie-Diskursen dominiert. Das bindet wertvolle Zeit und Ressourcen an den falschen Stellen. Die Digitalisierung der Schulen beispielsweise hat nur mit Regulation, Verwaltung, Vergaberecht und Kultur zu tun, **nicht** mit Technologien. Ohne eine Erneuerung der zugrunde liegenden Konzepte werden die juristischen Ansätze weiterhin in den bestehenden Traditionen gefangen bleiben. In der Folge bleibt Deutschland ein digitales Entwicklungsland, gefangen in einem systematischen Reformstau, den eine moralisch und historisch aufgeladene Technikskepsis noch verstärkt.

Die moralische Überfrachtung der Digitalen Souveränität

Die fehlende Konzeptbildung ist ein Symptomträger tieferer Ursachen: Es fehlt am kulturellen Verständnis; wir wissen nicht, womit wir es zu tun haben. Schlimmer noch, wir versuchen nicht einmal es zu erfahren. Blicken wir zum

Digitalisierung wird fälschlicherweise für ein technologisches Thema gehalten, nicht für ein gesellschaftliches.

Vergleich auf andere Kompetenzfelder: Die Literatur zur künstlerischen Bildung und Pädagogik umfasst mehrere Dutzend Regalmeter. Fügt man die musische Bildung, Musikpädagogik und ästhetischen Ausbildung hinzu, füllen sie ganze Bibliotheksetagen.

Sucht man hingegen nach Literatur und pädagogischen Anleitungen für das technologische Verständnis, bekommt man kaum ein Regal voll. Das ist weder Zufall noch ein Unfall, sondern Ausdruck unserer Geschichte: Seit den alten Griechen tragen wir die Hypothek, Technik als billige, ergo minderwertige Nachahmung der Natur zu betrachten. Sie ist etwas für Laien, Handwerker und moralisch Desinteressierte, also für Praktiker. Als Unnatürliches ist sie automatisch widernatürlich, potentiell dämonisch und böse – genau so, wie wir künstliche Intelligenz, Drohnen, Automatisierung und Datenverkehr diskutieren.

Wir beerben diese Tradition: Oft ist die Rede von billigen Chinaimitaten als qualitativ und moralisch minderwertige Raubkopien gegenüber den ethischen und qualitativ besseren Originalen hierzulande. Der eigentliche Treppenwitz der Geschichte liegt in der britischen Brandmarkung der billigen deutschen Raubkopien als „made in germany“ während der Industrialisierung. Das verkehrt sich nun in die moralische Überlegenheit der deutschen Ingenieure, die ihrerseits auf China herabblicken – eine gefährliche Arroganz. Zum Kontrast: In China schreiben Bauverordnungen Drohnenlandeplätze für jede Wohnungsimmoblie vor. Die führenden Hersteller und Innovatoren für Drohnen sind chinesisch, ebenso wie für die Chipherstellung, Präzisionsmechanik und einige mehr. Darauf wies schon in den 90ern Jahren der DARPA-Chef Jacob T. Schwartz hin [1].

„Die Definition von Wahnsinn ist, immer wieder das Gleiche zu tun und andere Ergebnisse zu erwarten.“ (Albert Einstein)

Souveränität ist kein technisches oder digitales Thema, sondern ein philosophisches.

Ebenfalls von den Griechen übernehmen wir die Vorstellung von Kunst als Ausdruck göttlicher Wahrheit. Zusammen mit der Natur gilt sie als Ausdruck göttlicher Schöpfung und göttlichen Ordnungswillens, also als heilig. Die Kunst zu erlernen ist moralische Pflicht, sie bringt uns näher ans Heilige und Reine, näher ans Ursprüngliche und Göttliche. Die aktuellen Naturschutzdebatten bedienen diese Tradition: Die Natur als Heiligtum, Umweltverschmutzung als Sünde durch Abfall vom Ursprünglichen, Umweltschutz als moralische Pflicht am Heiligen.

Die Kollision dieses Erbes erleben wir gegenwärtig beim Impfschutz, bei der Atomkraft oder der Digitalisierung: Die Technologie als Schandmal gegenüber dem Natürlichen, als (moralisch) minderwertige Nachahmung und Kontaminierung der heiligen Natur. Entsprechend begegnen wir dem Themenfeld nicht mit einem Kompetenzaufbau, sondern mit einer systematischen Abwehr. Wir misstrauen dem Fortschritt, betonen die Gefahren und verwechseln Bedenken mit Ethik.

So bleiben die Diskurse segregiert. Gesellschaft und Technologie werden nur über Bedenken miteinander verbunden. Folgerichtig fällt es uns schwer, Qualitätskriterien für Software und für Softwareausbildung anzugeben. Besonders in der Security von IT beziehungsweise Cyber wird das deutlich. Wie bei Ärzten müssten einzelne Spezialisierungen gebündelt in Expertenhäusern (z. B. Krankenhäusern) unterfüttert und mit maßgeblichen gesellschaftlichen Ressourcen institutionell ausgestattet werden. Ausbildung, Praxis und Lehre aus einer Hand an einem Ort, abgesichert durch die Qualitätssicherung der Staatsexamina sind das Ziel.

Souveränität und digitale Souveränität

Souveränität fragt nach der guten und rechtmäßigen Herrschaft zum Zwecke des geregelten Zusammenlebens [2]. Nach innen soll sie gute



Technik ist unnatürlich und damit automatisch dämonisch und böse.

Gesetze machen und durchsetzen. Nach außen soll sie verteidigen. Dafür braucht sie Gewaltmittel, Polizei und Militär. Ohne diese guten Gesetze wären sie Tyrannei [3], ohne die Gewaltmittel impotent [4]. Kämpfe um Souveränität sind nach innen hin Kämpfe um die Gewaltmittel nach außen hin Kämpfe mit den Gewaltmitteln. Souveränität verbindet also Gewaltmittel und Rechtmäßigkeit.

Das Besondere der digitalen Souveränität liegt in der irreversiblen Integration der Infrastruktur und der privaten Akteure. Die Pandemiebewältigung funktionierte nicht aufgrund eines exzellent organisierten Staates mit guten Gesetzen und guter Verwaltung. Im Gegenteil, sie funktionierte trotz der Begrenzungen des Staates dank der Kompensation durch private Akteure.

Das Verbindungsglied ist die ökonomische Dimension, die gesellschaftliche Realitäten ausdrückt: Die Digitalisierung gelingt aufgrund der privaten, konsumentengetriebenen Verbreitung von vernetzten Computern in klein und groß, fest und mobil, am Armband oder als Smartphone. Nicht die Staaten bauten die Infrastruktur, sondern die ebenso privaten digitalen Konzerne. Diese Art ökonomischer-souveräner Wechselwirkungen ist für digitale Souveränität konstitutiv.

Das ist die tiefere Bedeutung des Allgemeinwissens: Die Digitalisierung ist eine durch und durch zivilgetriebene Technologie, sowohl bezüglich der Entwicklung als auch der Nutzung. Sie drückt sich in der flächendeckenden individuellen Infrastruktur und Weiterentwicklung aus. Die Pandemiebewältigung gelingt im 21. Jahrhundert trotz aller menschlicher Fehler so gut, weil es ebendiese fertig ausgerollte, zivil feingranular verbreitete Infrastruktur gibt. Es sind die staatlichen Institutionen, welche rückständig sind.

Die Infrastruktur wird selbst zum Teil des Souveränitätsbegriffes: Souveräne Güter wie die Clouddienstleistungen und Smartphones funktionieren nur aufgrund einer breiten

Konsumentenbasis. Dafür gibt es ökonomische Schwellenwerte, die geschätzt bei 300 Millionen Nutzern liegen, wie am Beispiel der Amazon-Web-Services sichtbar wird. Ihr Umsatz betrug 2020 46 Milliarden Euro [5], was dem Verteidigungsetat Deutschlands entsprach, dem zweitgrößten Posten im Bundeshaushalt. Für die Souveränität bedeutet das eine Weiterentwicklung um die politische Ökonomie von Infrastruktur und Privateers – in Anlehnung an die vergleichbare Entwicklung in der Geschichte der Seefahrt [6]. Gaia-X braucht **jährliche** Investitionen in Höhe von 10-20 Milliarden Euro, um überhaupt Aussicht auf Erfolg zu haben. Oder eben einen Privaten, der bereit ist, das zu leisten.

Digitale Souveränität nivelliert das Über- und Unterordnungsverhältnis zwischen Privaten und Staat. Es ist paritätisch, es nähert sich ökonomisch und infrastrukturell an. Der Staat und seine Ressorts müssen diese neue Rolle des Privaten überhaupt erst zur Kenntnis nehmen, um sie zu erlernen und Prozesse, Ministerien und Administrationen zu integrieren. Die Volkssouveränität muss im Parlament gute Gesetze für eben diese Umstände verabschieden, statt die Privaten wieder und wieder substituieren zu wollen. Doch die Realität zeigt das Gegenteil: Eine Abwehr mittels einer regulatorischen Überkompensation und die täglich reproduzierte Hypothek als Schuldzuschreibung des Bösen gegenüber Google, Facebook und Amazon [7]. ■

Kurz und Bündig

Digitale Souveränität ist eine Synthese von privaten und staatlichen Akteuren. Digitalisierung ist zivilgetrieben, sie schafft die Infrastruktur durch Unternehmen, durch Konsumenten und Nutzer der digitalen Geräte. Der klassische staatliche Souverän muss diese Synthese zur Kenntnis nehmen und seine Expertise in Form von guten, zeitgemäßen Gesetzen und Regularien einbringen. Jedoch reproduziert er stattdessen eine gefährliche Tradition der Dämonisierung der Technik.



Weitere Infos und Literaturangaben zum Artikel finden Sie unter folgendem Link: <https://bit.ly/3cmo008>

Datenchaos ade

Souverän durch die digitale Verwaltung

Sandra van der Hulst, Hansestadt Lübeck und Christiane Wegner, MACH AG



Adobe Stock | TankVision | 3993433351

Für die erfolgreiche Digitalisierung der Verwaltung ist die digitale Souveränität von allen Beteiligten ein entscheidender Faktor. Ein interdisziplinäres Projektteam arbeitet an Lösungen, um Datenströme transparenter und Prozesse verständlicher zu machen. In diesem Beitrag wird das Projekt „Digitale Souveränität durch E-Government“ vorgestellt.

In der digitalen Welt den Überblick über den Weg der eigenen Daten zu behalten, ist in der heutigen Zeit schwierig geworden. Auch im öffentlichen Sektor gibt es aufgrund der föderalen Strukturen in Deutschland viele behördenübergreifende Prozesse mit intensivem Datenaustausch und hoher Intransparenz der Datenweitergabe. So wundern sich Eltern nicht selten darüber, dass ihr Neugeborenes bereits wenige Tage nach der Geburt Post vom Bundeszentralamt für Steuern mit einer eigenen Steueridentifikationsnummer erhält, sie aber den Kindergeldantrag noch bei der Familienkasse ihres Wohnortes stellen müssen.

Digitale Souveränität durch eine digitale Öffentliche Verwaltung

Mit der Verabschiedung des Gesetzes zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz, OZG) wurde festgelegt, dass Bund, Länder und Kommunen 575 Verwaltungsleistungen bis Ende 2022 digital anbieten sollen. Mit der Umsetzung des OZG sollen Verwaltungsleistungen bürgerfreundlicher und Prozesse effizienter werden. Allerdings gaben 21 Prozent der Befragten in einer Studie des Bitkom [1] an, nicht gerne in einer Gemeinde mit vielen digitalen Angeboten zu leben. 76 Prozent davon nennen als Grund Angst vor einer Entwicklung zum gläsernen Menschen; 66 Prozent fürchten Datenmissbrauch. Diese Auskünfte deuten ein Misstrauen gegenüber der Verwaltung an, die einer breiten Nutzung der Online-Dienste im Wege stünde.

Eine Stärkung der digitalen Souveränität kann hierfür eine Lösung sein. Digitale Souveränität meint das „selbstbestimmte Handeln und Entscheiden von Personen, Organisationen und Staaten im digitalen Raum“ [2][3], (S. 3).

Sowohl bei der Digitalisierung von Verwaltungsdiensten als auch für die Smart City-Angebote, die in immer mehr Städten wie Lübeck angeboten werden, ist ein bewusster und reflektierter Umgang mit den eigenen Daten notwendig [3], damit Bürgerinnen und Bürger die Dienste nutzen können und wollen. Ebenso wichtig ist die Gestaltung der Dienste in der Form, dass sie ihnen am besten dienen. Die sensiblen Daten, die dabei gesammelt und verarbeitet werden, fordern einen sehr verantwortungsvollen Umgang. Die öffentliche Verwaltung hat nicht nur die Aufgabe, datenschutzrechtlich und verantwortungsvoll mit diesen Daten umzugehen, sondern auch mit gutem Beispiel voranzugehen. Es gilt, mit transparenter Gestaltung von Datenströmen und Datenschutzhinweisen die Souveränität der Bevölkerung hinsichtlich ihrer Daten zu stärken. Bürgerinnen und Bürger sollten wissen und hinterfragen, wie Organisationen im öffentlichen und privaten Bereich Daten sammeln, was mit diesen Daten passiert und warum sie erhoben werden, damit sie im Sinne der digitalen Souveränität selbstbestimmt über ihre Daten und deren Nutzung entscheiden können.

Um die digitale Souveränität zu fördern, hat sich die Hansestadt Lübeck mit weiteren Partnern vor Ort zusammengetan. Zwei Institute der Universität zu Lübeck und die MACH AG,



Sandra van der Hulst

Sandra van der Hulst ist seit Februar 2021 Projektmanagerin für das Projekt „Digitale Souveränität durch E-Government“ bei der Stabstelle Digitalisierung, Organisation und Strategie der Hansestadt Lübeck. Den Bezug zu Digitalisierungsthemen hat sie seit ihrem Studium in ihrer Heimat, den Niederlanden. Danach war sie unter anderem als IT-Beraterin und Gründungsberaterin tätig.

Kontakt

sandra.vanderhulst@luebeck.de

www.luebeck.de

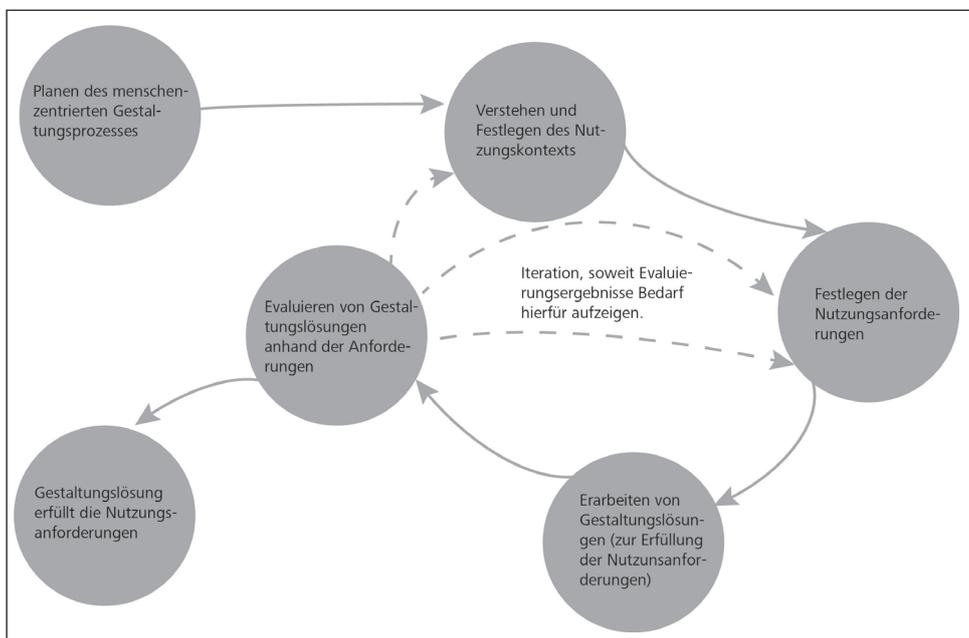


Abbildung 1: Schematische Darstellung des menschenzentrierten Entwicklungsprozesses nach DIN EN ISO 9241-210. © [6]

Ziel des Projektes ist es, Informations- und Interaktionsangebote zu schaffen.

ein Lübecker Softwareunternehmen, arbeiten mit der Hansestadt in dem vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Verbundprojekt "Digitale Souveränität durch E-Government" zusammen. Das Projekt läuft im Rahmen des BMBF-Forschungsprogramms „Mensch-Technik-Interaktion für digitale Souveränität“ [4].

Dr. Stefan Ivens, CDO der Hansestadt Lübeck, sagt dazu: „Mit den Lösungen, die im Projekt digitale Souveränität durch E-Government entwickelt werden, kann die Akzeptanz von digitalen Verwaltungsanwendungen erhöht werden, was positive Auswirkungen auf die öffentliche Leistungserstellung bewirken kann. Darüber hinaus sind informierte und digital souveräne Bürgerinnen und Bürger besser in der Lage, die digitale Transformation in ihrer Stadt mitzugestalten.“ Ziel des Projektes ist es, Informations- und Interaktionsangebote zu schaffen, welche die digitale Souveränität der Nutzerinnen und Nutzer fördern und sie auch im Umgang mit kommerziellen Anbietern zu mehr Datensouveränität ermächtigen.

Zusammenarbeit in einem interdisziplinären Team

Die Zusammenarbeit im Verbundprojekt ist in hohem Maße interdisziplinär. Jeder Projektpartner kann seine Stärken einbringen und

Teilaufgaben des Vorhabens federführend adressieren. Die Hansestadt Lübeck bietet den Zugang zur Verwaltung und sammelt Informationen für das Projekt. In der iterativen Entwicklung der Lösungen hat die Stadt vor allem die Möglichkeit, die Lösungen mit den Zielgruppen zu testen.

Die Wissenschaft ist vertreten durch die Universität zu Lübeck mit dem Institut für Interaktive und Multimediale Systeme (IMIS) sowie mit dem Ethical Innovation Hub (EIH). Schwerpunktthemen des IMIS sind die Forschung zu Konzeption, Realisierung und Evaluation von interaktiven Mensch-Maschine-Systemen sowie psychologische Grundlagen von gelungenen Interaktionsdesigns und Usability-Engineering. Der EIH forscht zu ethischen und sozialen Aspekten technischer Entwicklungen.

Die MACH AG ist ein Software- und Beratungsunternehmen aus Lübeck mit über 35 Jahren Erfahrung bei der Modernisierung und Digitalisierung von Prozessen in der öffentlichen Verwaltung. Als mittelständisches Unternehmen, das sich auf den öffentlichen Sektor konzentriert, entwickelt die MACH AG Software für die spezifischen Anforderungen der öffentlichen Verwaltung.

Datenströme im Fokus

Das Projekt fokussiert behördenübergreifende Datenströme aus einer Vielzahl an Verwaltungsprozessen, bei denen Daten aufgenommen, weiterverarbeitet und ausgetauscht werden. Dabei hat das Projektteam drei Lebenslagen exemplarisch ausgewählt: Geburt, Umzug und soziale Notlage (hier ist insbesondere die Situation der Arbeitslosigkeit gemeint).



Abbildung 2: Mitglieder des interdisziplinären Projektteams bei einem Design Sprint Workshop.
© Projektteam

Zwei Aspekte zeichnen das Vorgehen im Projekt aus:

1. ein menschenzentrierter Entwicklungsprozess (DIN EN ISO 9241-210) unter Einbeziehung der Nutzerinnen und Nutzer von der Konzeption bis zur Evaluation (Abbildung 1)
2. eine wissenschaftliche Begleitung mittels Nutzerstudien und Labor- sowie Feldexperimenten, welche die erarbeiteten Lösungen auf ihre Wirksamkeit hin untersuchen.

Dem menschenzentrierten Entwicklungsprozess folgend, startete das Projektteam eine Analysephase, um den jeweiligen Nutzungskontext und die Anforderungen zu verstehen und festzulegen. In dieser wurden Bürgerservice-Webseiten und E-Government-Angebote hinsichtlich Datensouveränität untersucht. Dabei zeigten die Online-Services der öffentlichen Verwaltungen auf kommunaler Ebene keine besonderen Maßnahmen zur Erhöhung der Datensouveränität ihrer Nutzerinnen und Nutzer [3]. Neben Recherchen zu gesetzlichen Grundlagen und Fachverfahren fanden Experteninterviews mit Verwaltungsmitarbeitenden und Datenschutzbeauftragten statt, sodass eine gute Übersicht der Datenströme, beispielsweise bei einer Ummeldung in der Meldebehörde, entstand. Besuche vor Ort, unter anderem im Standesamt, ermöglichten einen Blick auf die konkreten Abläufe. Hier zeigten sich bei der Verwendung von handschriftlichen Registerbüchern auch die Grenzen der fortschreitenden, aber noch lange nicht abgeschlossenen Digitalisierung der Verwaltung. Wissen über diese Grenzen hilft dabei, Prozesse und Datenströme zu verstehen und aktiv mitzugestalten.

Iterativ zum Ziel

Mit den detaillierten Einblicken und ermittelten Anforderungen aus der Analysephase konnte eine interdisziplinäre Gruppe wie in Abbildung 2 gezeigt in einem Design Sprint [5] erste Gestaltungslösungen erarbeiten. Für die Bedürfnisse und Ressourcen des Teams war es dabei passender, das Konzept anzupassen und nur die ersten drei statt der originalen fünf Tage im Sprint durchzuführen. Gemeinsam wurden so die ersten drei Etappen eines Sprints erarbeitet: Das Ziel verstehen und festlegen, mehrere Ideen zur Lösung sammeln und schließlich aus den Ideen die Richtung zum Ziel auswählen und in einem Storyboard skizzieren. Die Storyboards

werden derzeit von einer studentischen Mitarbeiterin zu Prototypen umgesetzt und in mehreren Iterationen weiter ausgearbeitet. Einer der Prototypen ist eine interaktive Visualisierung der Datenströme nach der Ummeldung mit Gamification-Elementen, da die Anwendenden in einer Art Wissensspiel später Rückmeldung darüber erhalten, inwieweit sie die Weitergabe der Daten richtig eingeschätzt haben.

Ein zentraler Aspekt des menschenzentrierten Entwicklungsprozesses ist das iterative Anpassen der Gestaltungslösungen anhand von Evaluationen und Feedback von der Zielgruppe. Trotz aller Planung im Vorfeld, der Recherche in der Analysephase und der Expertise und Kreativität, die im Designsprint eingebracht werden – erst durch das Feedback der Nutzerinnen und Nutzer wird deutlich, wie gebrauchstauglich eine Anwendung ist [6]. So plant das Projektteam in den nächsten Monaten mehrere Iterationszyklen mit den Prototypen, bei denen die Evaluationen mit den Bürgerinnen und Bürgern und Verwaltungsmitarbeitenden durch die Universität zu Lübeck als Projektpartner wissenschaftlich begleitet und ausgewertet werden. Schritt für Schritt nähert man sich so dem Punkt, an dem die Gestaltungslösung die Anforderungen bestmöglich erfüllt und auf Webseiten oder Portalen der öffentlichen Verwaltung zur Verfügung gestellt werden kann. In weiteren Untersuchungen wird abschließend analysiert, ob die digitale Souveränität der Anwenderinnen und Anwender messbar gefördert wird und ob ein Transfereffekt zu privaten Anbieterinnen und Anbietern hinsichtlich des souveränen Umgangs mit den eigenen Daten erfolgt. ■



Christiane Wegner

Christiane Wegner studierte Angewandte Mathematik in Medizin und Lebenswissenschaft an der Universität zu Lübeck und forschte dort nach ihrem Masterabschluss als wissenschaftliche Mitarbeiterin zu Methoden der Künstlichen Intelligenz. Im Jahr 2018 wechselte sie zur MACH AG als Innovation Engineer. Bei Projekten zur Digitalisierung und Modernisierung der öffentlichen Verwaltung sind ihre Schwerpunktthemen Datenanalyse und Visualisierung.

Kontakt

christiane.wegner@mach.de
www.mach.de

Kurz und Bündig

Für die erfolgreiche Digitalisierung der Verwaltung mit E-Government- und Smart City-Angeboten, bei denen auch personenbezogene Daten gesammelt, ausgewertet und ausgetauscht werden, ist die digitale Souveränität von Bürgerinnen und Bürgern ein entscheidender Faktor. Um diesen Prozess und die Nutzung der digitalen Angebote zu unterstützen, arbeitet ein interdisziplinäres Projektteam an Lösungen, um Datenströme transparent darzustellen, Beteiligte zu informieren und damit die digitalen Verwaltungsangebote zu verbessern.



Weitere Infos und Literaturangaben zum Artikel finden Sie unter folgendem Link: <https://bit.ly/3C6AgYK>

Digitale Souveränität: (k)eine Frage des Alters?

Raus aus der Gutenberg-Galaxis

Axel Benning, Marcell Saß, Fachhochschule Bielefeld, Philipps-Universität Marburg



Ist es wirklich ein Kampf zwischen Digital Natives und Silver Surfern? Oder können die einen gar von den anderen lernen? Stellen sich Silver Surfer mehr Fragen zur Souveränität? Und wie sieht es mit der Nutzung von digitalen Plattformen in den verschiedenen Altersgruppen aus? Das Projekt SoDiLe der Universität Marburg und der Fachhochschule Bielefeld soll Klarheit schaffen. Mithilfe von integrierter Forschung werden unsere digitale Souveränität auf die Probe gestellt und etwaige Differenzen zwischen Altersgruppen ermittelt.



Dr. Axel Benning

Dr. Axel Benning ist Professor für Wirtschaftsrecht, insbesondere Handels-, Gesellschafts- und Arbeitsrecht am Fachbereich Wirtschaft der Fachhochschule Bielefeld. Er forscht zu rechtlichen Problemen der Digitalisierung.

Abschied von der Gutenberg-Galaxis

Gut eineinhalb Jahre nach den ersten Berichten über ein „neuartiges Coronavirus“ sind wir immer noch in einer Pandemie und alle irgendwie – so konnte man in der Süddeutschen Zeitung vor einiger Zeit lesen – „mütend“, das heißt müde und wütend. Die Corona-Pandemie fordert Gesellschaft und Politik, Schulen und Hochschulen, Forschung und Unternehmen zutiefst heraus. Neben ökonomischen, kulturellen und sozialen Folgen für die Einzelnen und die Gesellschaft verdichten sich die Herausforderungen im Bereich einer großen gesellschaftlichen Herausforderung in besonderer Weise. „Digitale Erleuchtung“ titelte die Wochenzeitschrift „Der Spiegel“ bereits 2013 und zeigte zwei Bilder aus Rom. Sie stammten aus den Jahren 2005 und 2013: „Beim Tod von Johannes Paul II. schauten die Menschen gebannt Richtung Petersdom. Bei der Wahl von Papst Franziskus wiederholte sich die Szene - und war doch ganz anders“. [1] Auf dem zweiten Bild nämlich halten die Menschen zahlreiche Mobiltelefone hoch! Gleichsam symbolisch erkennbar ist schon 2013 die endgültige Abreise aus der Gutenberg-Galaxis und unsere pandemiebedingt beschleunigte private und berufliche Ankunft in einem neuen digitalen Zeitalter. Der Prozess der Digitalisierung ist unaufhaltsam, eine neue Kultur der Digitalität (F. Stalder) [2] hat Einzug gehalten, die Medienevolution der letzten Jahre erscheint uns als bisweilen dramatische Medienrevolution. Die Folgen dieser Transformationen werden vielfältig erforscht, immerhin mit der mittlerweile anerkannten

Einsicht, dass monodisziplinäre Zugänge kaum weiterführen, sondern inter- beziehungsweise transdisziplinäre Zugänge notwendig sind. Das vom BMBF im Rahmen eines Clusters „Integrierte Forschung“ geförderte Projekt „Souveränität in digitalisierten Lebenswelten“ (SoDiLe) der Fachhochschule Bielefeld und der Philipps-Universität Marburg bearbeitet die Frage, ob und wie junge Menschen sich souverän in einer Kultur der Digitalität bewegen, wenn zugleich unübersehbar ist, dass sie als Digital Natives bereits unauflösbar in einen Prozess der Digitalisierung verwoben sind. Der Forschungsansatz beider Hochschulen führt anthropologisch-bildungstheoretische und rechtswissenschaftliche Perspektiven zusammen und integriert empirische sowie hermeneutische Perspektiven. Zunächst wird die potenzielle Tragfähigkeit tradierter Souveränitätskonzepte aus den Diskursen des Staatsrechts beziehungsweise aus Herrschaftsverhältnissen früherer Zeiten analysiert und dem Selbstverständnis von 13-15-Jährigen entgegengestellt. In Gruppendiskussionen mit Schülerinnen und Schülern sollen deren Vorstellungen vom Selbst und damit von Souveränität als konjunktive Erfahrungsräume (R. Bohnsack) rekonstruiert werden. Erste Ergebnisse der Studie werden im kommenden Jahr vorliegen. Diese Befunde können dann mit

Kontakt

benning@fh-bielefeld.de

Wie gestaltet sich die Nutzung digitaler Technologien in unterschiedlichen Altersgruppen?

Die Medienevolution der letzten Jahre erscheint uns als dramatische Medienrevolution.

Studien zur digitalen Souveränität im Alter [3] ins Gespräch gebracht werden, um folgende Hypothese zu prüfen: Wie ist das Verhältnis der Nutzung digitaler Technologien zu einem souveränen, kompetenten Umgang mit diesen in unterschiedlichen Altersgruppen? Lässt sich hier ein doppelter gap in Bezug auf das Alter der Nutzerinnen und Nutzer und die Intensität der Nutzung beobachten? Geht eine verstärkte Nutzung digitaler Technologien unter Umständen gar nicht mit einem „starken“ Konzept von Souveränität einher?

„Däumlinge“ in posthumanistischen Zeiten

Das Forschungsprojekt SoDiLe greift Arbeiten auf, die die gegenwärtigen Transformationen als anthropologische Neuvermessung deuten. Dass diese Neuvermessung nicht nur verfallstheoretisch gedeutet werden muss, lässt sich auf unterhaltsame Weise von M. Serres [4] lernen.

Seine „Liebeserklärung“ an die von ihm als „Däumlinge“ bezeichneten jungen Menschen betont die Chancen digitaler Umbrüche. Der ältere „Silver Surfer“ Serres beneidet die „Digital

Natives“ um deren aktive Gestaltungsmöglichkeiten. Serres Ode leistet für unsere Grundlagenforschung zweierlei: eine institutionenkritische Argumentation und einen Technik- bzw. Forschungsoptimismus. Die in SoDiLe geplante Rekonstruktion von Souveränitätskonzepten nimmt damit empirisch eine postmoderne Binsenweisheit auf, nämlich die Einsicht, gegenwärtig mit einem Umbruch konfrontiert zu werden.

Übrigens: M. Foucault hatte vor 50 Jahren schon das „Verschwinden des Menschen“ vorausgesagt [5]. Auch die Frage nach Souveränität wird sich dem heute kaum entziehen können und muss vermutlich neu oder zumindest anders beantwortet werden. Aktuelle posthumanistische und transhumanistische Perspektiven in verschiedenen Wissenschaftsdisziplinen bieten hierzu Anregungen, da sie konzeptionell die gegenwärtigen (technischen) Entwicklungen als einen Bruch mit grundlegenden Annahmen westlicher Kulturen deuten. Dabei geht es um ein neues Verständnis des Verhältnisses des Menschen zur Welt und Natur mit dem Ziel, menschenbezogene Deutungen so zu bearbeiten, dass neue Sichtweisen auf die Grenzen zwischen Mensch, Tier und Technik möglich werden [6].

Post- und Transhumanismus unterscheiden sich jedoch erheblich [7]: Im Transhumanismus wird ein Projekt der „Verbesserung“ des Menschen verfolgt. Der Mensch als unvollkommenes sterbliches, leidendes Lebewesen soll optimiert werden, Krankheit, Tod und Alter sollen beseitigt werden. Anders verfährt ein kritischer Posthumanismus, der mit Namen wie R. Braidotti, D. Haraway oder B. Latour verbunden ist. Hier wird der Platz des Menschen auf



„Was ist der Mensch?“

der Erde als Gefährder und Gefährdeter zugleich lokalisiert. Wir sind folglich dringend herausgefordert, neu zu klären, was schon I. Kant fragte: „Was ist der Mensch?“ [8] Die in zahlreichen Studien dokumentierte Verbreitung digitaler Medien [9] belegt diese Beobachtungen und markiert Herausforderungen für Schule und Hochschule, für Ausbildung und Bildung gleichermaßen. Aus juristischer Perspektive haben wir zudem davon auszugehen, dass ein digital-souveräner Umgang mit Technologie nur dann möglich ist, wenn den Handelnden verständlich ist, wie diese funktioniert. Deshalb verstehen wir digitale Souveränität eben auch als kompetenten Umgang mit digitalen Technologien. Aus der Veränderung von Selbst-Konzepten folgen Überlegungen, inwieweit eine – insbesondere juristische – Regulierung erforderlich ist, um als Individuum überhaupt digital souverän bleiben zu können, etwa im Persönlichkeits- und Datenschutzrecht, bei der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, bei Datensicherheit, vertraglichen und haftungsrechtlichen Fragen sowie letztlich auch erbrechtlichen Problematiken.

Souveränität in der Krise? Zur Forschungspraxis integrierter Forschung in SoDiLe

Da das Forschungsprojekt SoDiLe noch am Anfang steht, können belastbare Ergebnisse an dieser Stelle noch nicht vorgelegt werden. Ob Individuen nun im Sinne eines posthumanistischen Menschenbildes wirklich souverän sind, sie also kompetent digitale Technologien verstehen und beherrschen oder aber ob spätmoderne Menschen von den Technologien bereits beherrscht werden, werden die hermeneutischen und empirischen Klärungen zeigen.

In jedem Fall benötigt man aber, das zeigt sich schon bei der Durchsicht aktueller Forschungen, neben tragfähigen Konzepten und Begriffen (Person, Souveränität, Kompetenz) handhabbare Instrumente, die die Individuen befähigen, digitale Souveränität auch als eine Kompetenz zu erwerben. Und zwar in einem bildungstheoretischen Sinne als „die

bei Individuen verfügbaren oder durch sie erlernten kognitiven Fähigkeiten und Fertigkeiten, um bestimmte Probleme zu lösen, sowie die damit verbundenen motivationalen, volitionalen und sozialen Bereitschaften und Fähigkeiten, um die Problemlösungen in variablen Situationen erfolgreich und verantwortungsvoll nutzen zu können“ [11].

Weiterhin muss durch die Definition des Begriffs Souveränität aus verschiedenen wissenschaftlichen Perspektiven (Transdisziplinarität) geklärt werden, inwieweit digitale Technikprojekte eigenständig sein können, sodass diese gegebenenfalls für „Fehlverhalten“ selbst verantwortlich gemacht werden können. Im Falle eines autonom fahrenden Autos mag man sich dies durchaus vorstellen können. Letztlich muss aber geklärt werden, ob nicht der dahinterstehende Algorithmus selbstständig ist, was insbesondere in der rechtswissenschaftlichen Diskussion eine besondere Herausforderung darstellt. Weiterführend ist auch die Frage, inwieweit sich Souveränität im fortschreitenden Alter wandelt. Hierzu hat die bereits erwähnte Bertelsmannstudie zur digitalen Souveränität im Alter erste Ergebnisse geliefert, die wir mit unseren empirischen Eindrücken zum Selbstbild von „Digital Natives“ gegenüberstellen werden. Eine uns antreibende Suchbewegung soll hier geteilt werden: Menschen, die erst spät in ihrem Leben einen kompetenten Umgang mit Prozessen der Digitalisierung erworben haben, könnten eine höhere Affinität zu Fragen der Souveränität haben und Nutzungsintensitäten von daher abwägen. Ob sich dies bei denen, die im Digitalzeitalter geboren und sozialisiert sind, andersherum verhält, wird uns interessieren. ■



Dr. Marcell Saß

Dr. Marcell Saß ist Professor für Praktische Theologie mit dem Schwerpunkt Religionspädagogik an der Philipps-Universität Marburg und stellvertretender Vorsitzender des dortigen Zentrums für Lehrerbildung. Er forscht zu Fragen digitaler Bildung und zu deren bildungstheoretisch-anthropologischen Grundlagen.

Kontakt

m.sass@uni-marburg.de

Kurz und Bündig

Posthumanistische digitale Zeiten stellen hohe Anforderungen an menschliche Souveränität im Umgang mit Technik und neuen Technologien. Integrierte Forschung hilft zu verstehen, ob unsere Konzepte von Souveränität noch stimmig sind und ob es dabei Unterschiede zwischen Digital Natives und Silver Surfern gibt.



Weitere Infos und Literaturangaben zum Artikel finden Sie unter folgendem Link: <https://bit.ly/3EwEXgh>



Zwischen Wahrheit und Wirklichkeit

Compliance als Herausforderung für Mittelständler

Christian Löhl, W+ST CoB-IT GmbH

Digitale Souveränität ist die Summe aller Fähigkeiten und Möglichkeiten die Individuen und Institutionen benötigen, um ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können. Die Digitalisierung betrifft alle Lebensbereiche. Dabei lassen sich potentielle Gefahren, z.B. aus der massenhaften Sammlung und Speicherung digitaler Daten und der immer stärkeren Vernetzung informationstechnischer Systeme, nicht nur auf den beruflichen und privaten Alltag, sondern



Christian Löhl

Christian Löhl ist als Dipl.-Betriebswirt (FH) Geschäftsführer der W+ST CoB-IT GmbH für Compliance Beratung des Mittelstandes. Er arbeitet seit 1999 bei der W+ST Wirtschaftsprüfung AG & Co. KG am Hauptsitz in Dillingen. Löhl verfügt über umfangreiche und fundierte Fachkenntnisse im IT-GRC Themenumfeld ("Governance, Risk & Compliance"). Er besitzt langjährige Erfahrungen in der Beratung und Prüfung mittelständischer und größerer Unternehmen aus den unterschiedlichsten Branchen und somit im Umgang mit individuellen IT-Anwendungen bis hin zu komplexen ERP-Systemen.

Kontakt

christian.loehl@w-st.de

auch auf das Firmen-Know-how und die unternehmerischen Prozesse projizieren. Bereits heute sehen sich Unternehmen durch den rasanten technologischen Fortschritt und die wachsende globale Vernetzung der Gefahr einer Informationsüberflutung und Komplexitätsüberlastung bis hin zu einer "digitalen Demenz" ausgesetzt.

Mit der Digitalisierung und im Zusammenhang mit der rasanten technologischen Entwicklung entstehen immer schneller neue Geschäftsmodelle, die einen hohen Anspruch an Sicherheit und an die Zuverlässigkeit im Hinblick auf die Datensouveränität als Teil der digitalen Souveränität mit sich bringen. Dabei nimmt der Umfang der verarbeiteten Informationen stetig zu. Änderungen am Kunden- bzw. Geschäftsportfolio und damit einhergehend Risiko-Entwicklung und -Gestaltung haben hohe Ansprüche an die Informationsqualität und deren Erhebungszeiten zur Folge.

Dieser stetige Wandel und damit die Komplexität der individuellen Geschäftsvorfälle haben tiefgreifende Auswirkungen auf Unternehmen, da sie eine kontinuierliche Anpassung der internen Compliance-Strukturen erfordern. Daneben kann durch die Verknappung und/oder eine unausgewogene Lastverteilung von Ressourcen eine weitere Zielkonkurrenz entstehen. Die ständige Anpassung der Systeme an geänderte Anforderungen führt zu Zielkonflikten zwischen Verlässlichkeit und Veränderung. Denn während Verlässlichkeit Beständigkeit verlangt, fordern Veränderungen Flexibilität.

Welche Compliance-Anforderungen gilt es zu beachten?

Gesetze, Normen und Grundsätze beeinflussen dabei zunehmend die Unternehmenstätigkeiten. Gerade in jüngster Vergangenheit geraten verstärkt Compliance-Skandale ans Licht der Öffentlichkeit (z.B. Wirecard und Deutsche Bank). Durch den steigenden öffentlichen Druck und Forderungen an die Nachhaltigkeit (z.B. Umwelt) und Transparenz (z.B. Ethik) sowie durch die damit einhergehenden neuen Regularien (wie z.B. das Lieferkettengesetz, die EU-Hinweisgeberrichtlinie und das Geldwäschegesetz) sehen sich aber auch mittelständische Unternehmen gestiegenen Anforderungen ausgesetzt.

Insbesondere in den Bereichen Korruption und Kartellverstöße kann es zu hohen, die Existenz bedrohenden Bußgeldern und

Gewinnabschöpfungen kommen. Zusätzlich droht den handelnden Mitarbeitern und der Geschäftsleitung persönliche Strafbarkeit. Mit der zunehmenden Anwendung des Legalitätsprinzips - in Abkehr vom Opportunitätsprinzip - müssen die Verfolgungsbehörden beim Vorliegen eines Anfangsverdachts über die Begehung einer Straftat zwingend ein Ermittlungsverfahren einleiten.

Neben der verschärften rechtlichen Sanktionierung und etwaiger branchenspezifischer Regularien sehen sich Unternehmen auch dem Druck seitens ihrer Kunden und Lieferanten, von Kreditinstituten und Versicherungen ausgesetzt.

Welche Gefahren birgt die Digitalisierung?

Der digitale Wandel, als Integration von



Compliance-Strukturen müssen ständig angepasst werden.

Information, Daten und Systemen verstanden, rückt die Bedeutung von IT-Sicherheit weiter in den Vordergrund. Diese ist essentiell um Personen, Unternehmen und Prozesse zu schützen und beispielsweise Sabotage und Systemmanipulationen zu verhindern. Ebenso sind Bedrohungen durch Angriffe auf IT-Systeme keine Seltenheit, sondern tägliche Realität.

Bei Cyberangriffen werden Unternehmen vielfach Daten entwendet und verschlüsselt. Häufig versuchen die Straftäter auf diese Weise „Lösegeld“ – oft in Form von Kryptowährungen – zu erpressen. Nach einer solchen Attacke sind zahlreiche Aspekte wie beispielsweise die interne und externe Kommunikation, Strafverfolgung, Datenschutzmeldungen und weitere rechtliche Implikationen des Vorfalls zu beachten. Es geht nicht mehr ausschließlich um IT-Fragen, sondern auch um wirtschaftliche und rechtliche Themenstellungen, die es zu eruieren und beurteilen gilt. Letzten Endes müssen sich Leitungs- und Aufsichtsorgane ihrer Eigenverantwortung insb. im Hinblick auf die Einhaltung ihrer Sorgfaltspflicht bzw. der Unterlassung von Aufsichtsmaßnahmen und somit der grundsätzlichen Frage „Opfer oder doch eigentlich Täter“ bewusstwerden.

Die neuen Regularien etablieren faktisch eine Beweislastumkehr. Für die Enthftung bzw. Exkulpation (z.B. „Selbstreinigung“ nach § 125 GWB) braucht es gemäß der Business Judgment Rule zur Wahrung der Sorgfaltspflicht bei der Ausübung von Geschäftstätigkeiten, insb. ein Handeln auf der Grundlage angemessener Informationen eine sorgfältige Ermittlung aller verfügbaren Entscheidungsgrundlagen, die eine umfassende Abwägung von Chancen und Risiken der jeweils anstehenden Handlungsoptionen möglich macht.

Um hier gewappnet zu sein und gegebenenfalls reagieren zu können (etwa durch Selbstanzeige), ist es dringend erforderlich, dass sich ein Unternehmen so schnell wie möglich einen detaillierten Überblick darüber verschafft, welche „sensiblen“ Daten betroffen sind, da ein solches Leakage schlimmstenfalls existenzbedrohend werden kann. In der Praxis

ist häufig problematisch, dass nicht oder zumindest nicht unmittelbar nach einem Datenvorfall zu ermitteln ist, welche Daten entwendet worden sind. Selbst wenn Einfallstore schnell identifiziert werden können, bereitet es mitunter große Schwierigkeiten, den Umfang der entwendeten Daten festzustellen.

Eine weitere Gefahr besteht aufgrund der stetig zunehmenden Menge an Daten und der Kommunikationskanäle, die immer mehr Möglichkeiten bieten praktisch jede Meinung fokussiert als „Wahrheit“ zu generieren. Auf der einen Seite ist der dazu passende Ausschnitt der „Wirklichkeit“ in der Fülle der Daten schnell zu generieren, aber umgekehrt bedarf es zur späteren Verifizierung bzw. zum transparenten Nachvollzug einer hohen Ambiguitätstoleranz.

Worin liegen die Besonderheiten bei kleinen und mittleren Unternehmen

Gerade kleine und mittlere Unternehmen verfügen in der Regel über stark heterogene Organisationsstrukturen und IT-Landschaften sowie ein für sie typischerweise wenig ausgeprägtes internes Kontrollsystem („IKS“). Zusätzlich führen insbesondere die in der Regel unzureichenden oder fehlenden Prozess- und IKS-Dokumentationen oftmals zu einer unklaren und nicht nachvollziehbaren Datenaggregation. Der Zugang zu wichtigen Informationen, Erfahrungswissen und Spezialkenntnissen ist zumeist nur auf eine geringe Anzahl von Mitarbeitern begrenzt und wird nicht durchgängig dokumentiert.

Zur Sicherstellung des Wissenserhalts und des Wissenstransfers fehlen entsprechende organisatorische Rahmenbedingungen und unterstützende Softwarelösungen im Unternehmen. Mängel in der Stammdatenpflege, resultierend aus einer fehlenden Definition von Informations- oder Dateneigentümern (i.S.v. Zuständigkeit) sowie damit einhergehend wenig ausgeprägten und zumeist organisatorischen Kontrollen (i.S.v. Verantwortlichkeit), werden oftmals erst im Zuge von notwendigen (Stamm-)Datenmigrationen, z.B. bei Versionswechseln der ERP-Software, ersichtlich.

Im Hinblick auf die Umsetzung der Compliance Anforderungen bei KMU scheuen gerade mittelständische Unternehmen oftmals die in diesem Zusammenhang erforderlichen monetären Aufwendungen und die notwendige personelle Ressourcenbindung oder sonstigen

Maßnahmen zur Sicherstellung der IT-Sicherheit und der Unternehmens-Compliance. Umgekehrt sehen sich gerade international und innovative mittelständische Unternehmen einem höheren Risiko aus Cyberangriffen und einem höheren Bedarf an Compliance (insb. aus sinkenden Schwellenwerten analog der Umsetzung der EU-DSGVO im deutschen BDSG-neu) ausgesetzt.

Bei der Umsetzung bzw. Implementierung notwendiger Kontrollen und Maßnahmen bedarf es einer strikten risikoorientierten Vorgehensweise zur Vermeidung einer Überregulierung insb. bei Unternehmensrichtlinien, Organisationsanweisungen und Verfahrensbeschreibungen, auch wenn dies bedeutet, dass ein Verstoß in einem Bereich mit niedrigem Risiko nicht verhindert wird, da in der Regel mehr Aufmerksamkeit und Ressourcen auf Bereiche mit höherem Risiko gelenkt werden.

Was ist zu tun?

Zur Wahrung der digitalen Souveränität und zur Sicherstellung der Datensouveränität bedarf es grundsätzlich einer Weiterentwicklung des klassischen IT-Sicherheitsmanagements zum Informations- und Kommunikationssicherheitsmanagement. Daneben erfordert der zunehmende Wettbewerbsdruck die digitale Weiterentwicklung, insb. die Schaffung einheitlicher und klarer Strukturen ("Transparenz") sowie die Verbesserung der internen und externen Kommunikation ("Informationserhebung und -bereitstellung"). So bezieht sich der Begriff der "Cyberresilienz" auf die Fähigkeit eines Umgangs mit den Daten in einer Kombination aus organisatorischer Resilienz und IT-Sicherheit, um sich gleichzeitig vor Angriffen schützen und in Krisenfällen schnell und effektiv reagieren zu können.

Dabei genügt es nicht, ein rein risikobasiertes System und entsprechende Wirksamkeitskontrollen vorzuhalten bzw. einzurichten.

Vielmehr liegt die Herausforderung in der Implementierung eines "gelebten Systems" bzw. einer "gelebten Unternehmenskultur" unter Einbezug sämtlicher Komponenten des Informationsverbundes mit dem Ziel des Schutzes von relevanten Informationen, die im Zusammenhang mit Informationsverarbeitung stehen - gleichwohl in welcher Form dies geschieht. Zur risikoorientierten Umsetzung bedarf es im Vorfeld einer sorgfältigen Risikoanalyse vor der Einrichtung und Dokumentation zusätzlicher oder notwendiger Kontrollen. Außerdem benötigt man Maßnahmen zur Sicherstellung des Regelbetriebs und der kritischen Geschäftsprozesse (i.S.e. Risiko- und Informationssicherheitsmanagements), der Aufrechterhaltung des laufenden Geschäftsbetriebs, zum Wiederanlauf (i.S.e. Notfallmanagements) sowie zur Identifizierung beim Umgang mit auftretenden und aufgetretenen Störungen und Fehlern (i.S.e. Problem- and Incident-Managements).

Dabei gilt es die Kontrollen und Maßnahmen sinnvoll in die Geschäfts- und Unternehmensprozesse zu integrieren, ohne dass sich diese störend oder hemmend auf den Geschäftsbetrieb auswirken. Denn nachhaltige Durchsetzung von Compliance bedarf bewusster Orientierung an den Geschäftsmodellen statt der Implementierung nachgelagerter Kontrollmaßnahmen, Genehmigungsstufen und Anweisungen. Ebenso lässt sich ein mögliches Risikopotential über prozessimmanente Kontrollen von der nachgelagerten Stufe der Risikofeststellung (z.B. durch Identifizierung von Ergebnisauswirkungen im Controlling) auf die Ebene der Risikoprävention vorverlagern, d.h. Risiken können ggf. bei der Entstehung identifiziert werden.

Insgesamt gewinnt damit das Risikomanagement an Wirkungskraft. Darüber hinaus bietet die Vorgehensweise auch immer wieder Anhaltspunkte für die Weiterentwicklung der Sicherheit aber auch der Effizienz der betrachteten Unternehmensprozesse im Sinne eines aktiven Geschäftsprozessmanagements ("PD-CA-Prozess") und somit letzten Endes zur Gewährleistung der Datensouveränität.

Ebenso sind entsprechende Regelungen und Maßnahmen zur fortlaufenden Risikoanpassung/-analyse ("Forecast") im Hinblick auf neue Projekte, Produkte, Prozesse und Prozeduren inkl. der Anpassung der Überwachungspläne zu notwendigen

Internationale und innovative mittelständische Unternehmen haben ein höheres Risiko für Cyberangriffe und einen größeren Bedarf an Compliance.

Neue Regularien etablieren faktisch eine Beweisumkehr.

Kontrollhandlungen und Maßnahmen (i.S.e. "Veränderungsmanagements"), ggf. unter Einbezug vorhandener Funktionsbeauftragter und zur Vermeidung von überbordenden Dokumenten und Berichten sowie inhaltliche Redundanzen, zu definieren und einzurichten.

Die Wahrung eines "gelebten" Ansatzes lässt sich im Hinblick auf die faktische Beweislastumkehr über die Definition und Implementierung "fortlaufender Überwachungsmaßnahmen" als zentraler Aspekt zur Exkulpation (i.S.e. "kontinuierlichen Verbesserungsprozesses") sowie in der Form von regelmäßigen Schulungen und Sensibilisierungsmaßnahmen von Mitarbeitern sowie regelmäßige Tests und Übungen ("Walk-the-Talk") sicherstellen.

Ein weiterer zentraler Aspekt bei der Gestaltung eines gelebten Ansatzes liegt in der Schaffung offener Kommunikationskanäle (insb. "Whistleblowing") angesichts von Verstößen, laufenden Verfahren sowie internen und externen Risiken auf horizontaler Ebene bzw. zwischen den Mitgliedern eines Leitungsorgans (i.S.e. Informationsrisikomanagements). Zur Sicherstellung der Kommunikation auf vertikaler Ebene gilt es neben der Sorgfaltspflicht und der nicht vollumfassend delegierbaren Pflicht zur Überwachung zumindest ein konkludentes Bekenntnis im Sinne des Vorlebens von regelkonformem Verhalten (nicht nur mit Blick auf Aussagen, sondern auch auf die Handlungen und Entscheidungen bzw. Sanktionen) zur Stärkung des Ordnungsrahmens und der Glaubwürdigkeit konsequent ("Ton-at-the-Top" oder "Conduct-at-the-Top") umzusetzen.

Fazit

Grundsätzlich empfiehlt sich - in Analogie zu den zumeist bekannten Anforderungen an Qualitätsmanagementsysteme (ISO 9001) - eine Orientierung an der Entwicklung der Anforderungen an Compliance-Systeme. Der neue Standard ISO 37301 als Typ A Standard lässt somit auch eine Zertifizierung eines übergeordneten Compliance-Managements zu. Aufbauend auf diesem lassen sich weitere

Managementsysteme in der Folge sinnvoll und effizient umsetzen bzw. integrieren.

Integrierte Managementsysteme als Resultat digitaler, gesellschaftlicher und auch regulatorischer Anforderungen an Unternehmen ermöglichen gerade KMU die Bewältigung komplexer bereichsübergreifender Führungsaufgaben über einen ganzheitlichen integrativen systemgestützten Ansatz. Die Vorteile der Effizienzsteigerung resultieren aus der Vermeidung von Redundanzen bzw. der Nutzung von Synergieeffekten und somit aus der Reduzierung des Dokumentationsaufwands. Dabei führt die aktive Einbindung der operativen Geschäftseinheiten zu einer hohen Akzeptanz bei Mitarbeitern und zur Vermeidung von Reibungsverlusten im Führungszirkel.

Allerdings bedarf es zur Umsetzung dem regelmäßigen Einsatz eines interdisziplinären Teams, das sich neben den Mitarbeitern aus den involvierten Fachabteilungen, insb. aus Mitarbeitern der IT, dem Controlling, aus Anwälten und Funktionsbeauftragten zusammensetzt. Die größten Herausforderungen bestehen in der strikt risikoorientierten Herangehensweise zur Reduzierung Komplexität sowie der Schaffung eines einheitlichen Wording zwischen den Projektbeteiligten. Es ist oftmals ratsam - neben externen Experten - auch neue Mitarbeiter mit noch wenigen Unternehmenskenntnissen in das Projekt einzubeziehen, um einer gewissen Voreingenommenheit bzw. Betriebsblindheit zu begegnen. ■

Kurz und Bündig

Bei Cyberangriffen werden Unternehmen Daten entwendet und verschlüsselt. Es geht nicht allein um IT-Fragen, sondern auch um wirtschaftliche und rechtliche Themenstellungen. Leitungs- und Aufsichtsorgane müssen sich dabei ihrer Eigenverantwortung und Sorgfaltspflicht bewusst werden. Dieses Beispiel zeigt, wie wichtig integrierte Managementsysteme als Resultat digitaler, gesellschaftlicher und auch regulatorischer Anforderungen an Unternehmen sind. Sie ermöglichen gerade KMU die Bewältigung komplexer bereichsübergreifender Führungsaufgaben über einen ganzheitlichen integrativen systemgestützten Ansatz.

Adobe Stock | Elnur | 212639969



Lebensretter Digitalkompetenz

Digitale Souveränität für Entscheider

David Hoeflmayr

In diesem Artikel wird digitale Souveränität als Mittel zur Erreichung langfristiger Überlebensfähigkeit von Unternehmen in der mehr und mehr digitalisierten Ökonomie verstanden. Digitalkompetenz bei Entscheidern umfasst die Themenfelder Strategie, Organisation, marktseitige und innengerichtete Digitalisierung. Studien zufolge haben Unternehmen, deren Aufsichtsräte mit Digitalexperten besetzt waren, eine höhere Ergebnismarge und stärkeres Wachstum aufgezeigt. Entscheider mit Digitalkompetenzen machen Unternehmen souveräner.

Das Jahr 2000 war ein Erfolgjahr für die Fotobranche. Nach 20 Jahren kontinuierlichen Wachstums wurden in Deutschland 191 Mio. Filme verkauft [1]. Fotolabore wie AGFA Fotoservice, V-Dia, Südcolor oder Cewe feierten Rekordergebnisse. Fünf Jahre später wurden nur noch 90 Mio. Filme verkauft, und AGFA, V-Dia und Südcolor hatten Insolvenz angemeldet. Auch Cewe hatte mit Umsatzrückgängen zu kämpfen, konnte aber 2010 – als im Markt gerade noch 18 Mio. Filme verkauft wurden – nach 10 Jahren Transformation einen neuen Umsatzrekord von 446,8 Mio. EUR melden. Die Erfolgsgeschichte des Branchenprimus setzt sich bis heute fort – im Jahr 2020 wurde ein Umsatz von 727,3 Mio. EUR gemeldet.

Cewe musste sich in wenigen Jahren vom Fotolabor zum Digitalfoto-Finisher transformieren. Wie konnte das Unternehmen meistern, woran andere gescheitert sind? Ein frühzeitiges Erkennen der Trends und entschiedenes Handeln in drei Bereichen waren entscheidend:

- Kapazitätsabbau: 11 von 23 Betrieben wurden geschlossen, und die Belegschaft wurde um 1.200 Mitarbeiter reduziert.
- Investitionen von über 320 Mio. EUR in neue Fertigungstechnologien
- Innovationsführerschaft in den Bereichen Produkte (z.B. Fotostationen, Fotobücher) und Vermarktung (z.B. Internetvertrieb, B2B-Geschäft).

Viele Organisationen haben den Luxus, die digitale Transformation nicht in solch einem kurzen Zeitraum absolvieren zu müssen und das Kerngeschäftsmodell schrittweise steigern zu können. Trotzdem müssen sie sich transformieren.

Digitale Souveränität ist hier verstanden als langfristige Überlebensfähigkeit. Das Cewe-Beispiel verdeutlicht, dass es dabei eben nicht nur um isolierte Maßnahmen geht, sondern um grundsätzliche Strategieentscheidungen, die jeden Unternehmensbereich betreffen.

Digitalkompetenz bei Entscheidern

In erfolgreichen Organisationen wird die Verantwortung für die digitale Transformation ganz oben wahrgenommen. Die Strategien werden durch Vorstände und Geschäftsführer und im öffentlichen Bereich z.B. durch Behördenleiter und Präsidenten erarbeitet. In Wirklichkeit sind es aber oft bei einem Unternehmen der Aufsichtsrat oder Beirat, in der Politik z.B. die Abgeordneten, bei einem Verein der ehrenamtliche Vorstand, die die abschließenden Strategieentscheidungen treffen. Ein leistungsfähiges Gremium ist Impulsgeber und Sparringpartner, der die Digitalstrategie auf Augenhöhe diskutieren kann. Und es dient als Kontrolleur, der die Umsetzung und die Risiken der digitalen Transformation beurteilen kann.

Vorstände und Geschäftsführer sprechen sich selbst eine hohe Digitalkompetenz zu. 16 Prozent benoten sie mit „sehr gut“, 34 Prozent bewerten sich mit „gut“ [2]. Allerdings beklagen 73 Prozent der Manager mangelnde Zeit, um sich mit neuen digitalen Technologien zu beschäftigen. 28 Prozent fühlen sich manchmal durch digitale Technologien überfordert, und 21 Prozent befürchten sogar, durch die Beschäftigung mit der Digitalisierung das Kerngeschäft aus den Augen zu verlieren. Leider passt das Selbstbild der Manager nicht immer zu den



Dr. David Hoeflmayr

Dr. David Hoeflmayr ist im Beirat und im Aufsichtsrat verschiedener Unternehmen. Nach über 20 Jahren in mittelständischen Vorstands- und Geschäftsführungspositionen begleitet er heute Unternehmer bei digitalen Transformationsvorhaben und investiert in Start-Ups.

Kontakt

david@hoeflmayr.de

Ein leistungsfähiges Gremium ist Impulsgeber.

Ergebnissen, die sie erzielen. Deutschlands Unternehmen landen in Digitalisierungsrankings ja bekanntermaßen oft im hinteren Drittel [3].

Dünnere wird die Digitalkompetenz in den Gremien. Börsennotierte Unternehmen versuchen, diese auch in schriftlichen Kompetenzprofilen zu fixieren. Der Gesamtaufsichtsrat von Fresenius soll beispielsweise „über das gebotene Verständnis für die Digitalisierung verfügen“ [4]. Die Allianz fordert „Mindestens ein Mitglied, das über Sachverstand auf dem Gebiet digitale Transformation verfügt“ [5]. 2019 waren zwei Drittel der Aufsichtsräte von Dax30-Unternehmen mit mindestens einem ausgewiesenen Digitalexperten besetzt [6]. Bei Familienunternehmen dagegen lag der Anteil von familienexternen Gremienmitgliedern mit Expertise in Digitalisierung oder neuen Technologien bei nur 3 Prozent [7].

Themenfelder der Digitalisierung

Es besteht offensichtlich Nachholbedarf. Was aber macht Digitalkompetenz aus, was muss das digital souveräne Gremienmitglied können? Die Unklarheit beginnt schon bei den unterschiedlichen Meinungen darüber, was Digitalisierung eigentlich ist. Grob lassen sich vier Themenfelder herausarbeiten: Strategie, Organisation, marktseitige und innengerichtete Digitalisierung.

1. Strategie

Die Digitalstrategie von Organisationen lässt sich heute kaum mehr von der Gesamtstrategie trennen. Das Marktumfeld beschleunigt sich zusehends, und das Ausmaß an disruptiven Veränderungen steigt. Gleichzeitig wird es bei geringerer Pfadabhängigkeit und steigender Komplexität schwieriger, die Veränderungssignale richtig zu interpretieren.

Digital geprägte Strategien müssen anders gedacht werden. Einerseits werden sie umfassender, beispielsweise transformiert sich Daimler vom Automobilhersteller zum vernetzten Mobilitätsdienstleister. Andererseits werden Langfriststrategien immer weniger planbar [8]. Die richtige Strategie kann dann

sein, auf die Steigerung der Anpassungsfähigkeit und Lernfähigkeit des Unternehmens zu setzen. Neue Werteströme können es sinnvoll machen, morgen mit Wettbewerbern von gestern zu kooperieren [9].

2. Organisation

Digitalisierung betrifft fast alle Abläufe im Unternehmen. Methoden wie Kanban, Lean oder Design Thinking werden nicht mehr als Inselösungen eingesetzt, sondern verändern die Arbeitsweise von Firmen ganzheitlich. Produkte werden schneller und „unfertiger“ auf den Markt gebracht („Fail-Fast“) und die Kunden in die Weiterentwicklung einbezogen.

Digitalisierung beeinflusst auch die Aufbauorganisation. Silodenken und starre Strukturen müssen aufgebrochen werden. Dabei treten neue Zielkonflikte auf. Beispielsweise soll einerseits die Ausgliederung von Innovation die Innovationskraft und Umsetzungsgeschwindigkeit steigern, andererseits will man den Nutzen digitaler Innovationen zeitnah dem Kerngeschäft zukommen lassen.

Eine der grundlegendsten Voraussetzungen erfolgreicher Transformation ist das Humankapital. Der Fachkräftemangel belastet auf allen Ebenen – vom digitalaffinen Vorstand bis zum App-Entwickler. Für die Gesamtbelegschaft ist Digitalisierung mit vielen Verbesserungen, aber oft auch mit Veränderungsdruck und Zukunftsangst verbunden [10].

3. Marktseitige Digitalisierung

Die kundenseitigen Unternehmensbereiche, z.B. Produktmanagement, Marketing, Vertrieb und Kundenservice, werden durch die Digitalisierung gravierend verändert. Produkte werden zunehmend „smart“, also über ihre physischen Eigenschaften hinaus mit digitalen Mehrwerten versehen. Ein Erfolgsbeispiel ist der Thermomix von Vorwerk. Das Unternehmen musste die Fähigkeit aufbauen, die digitalen Mehrwerte zu entwickeln, zu produzieren und zu vermarkten. Solche Technologieentwicklungen sind oft mit hohen Investitionen und langen Entwicklungszyklen verbunden.

Im Marktsegment B2C gewinnen neue Kanäle wie Onlineshopping, mobiles Marketing und soziale Medien zunehmend an Bedeutung. Auch im B2B-Geschäft verändert sich das Einkaufsverhalten. Kunden erwarten, sich online informieren zu können, Produkte selbst zu konfigurieren und komfortable Bestellprozesse

nutzen zu können. Die neuen Kanäle sind mit erheblichen Investitionen und Risiken verbunden, die es zu bewerten gilt. Letztlich wird auch die Kundenbeziehung digitalisiert. Kunden wollen ihr Konto online verwalten, in Realzeit den Reparaturstatus überprüfen und über Social Media Serviceanfragen gelöst bekommen. Gleichzeitig erschließt die steigende Menge an Daten immer neue Potenziale zur Kundenbindung und Umsatzsteigerung.

4. Innengerichtete Digitalisierung

Der Transformationsprozess „Industrie 4.0“ hat schon große Erfolge verzeichnet. Dass er auch mit Risiken behaftet ist, zeigen die Speed Factories von Adidas, in denen in Europa und den USA Kleinserien und 3-D-gedruckte Einzelschuhe produziert wurden. 2019, nur zwei Jahre nach Eröffnung der Fabriken, wurde die Produktion nach Asien zurückverlegt [11].

Die Digitalisierung endet nicht mit der Produktauslieferung. Digitale Zwillinge begleiten physische Produkte durch ihren Lebenszyklus. Technologien wie prädiktive Instandhaltung und Remote-Updates verlangen teils erhebliche Investitionen. Betroffen sind praktisch alle Unternehmensprozesse. Am Beispiel der Zentralfunktionen reicht das von der automatischen Belegerfassung in der Buchhaltung bis zum Bewerbermanagement in der Personalabteilung. Die menschliche Arbeit wird dabei vermehrt substituiert.

Eine stets wachsende Rolle kommt der Informationstechnologie zu. Einerseits gilt es, für die Kern-Geschäftsprozesse steigende Anforderungen an Performanz und Verlässlichkeit bei kontrollierten Kosten bereitzustellen. Andererseits müssen auch die Anforderungen der innovationsnahen Unternehmensbereiche nach Schnelligkeit, Agilität und Skalierbarkeit bedient werden.

Fazit: Entwicklung von digitaler Souveränität

Bei dieser Bandbreite stellt man sich die Frage, wie man nun die nötige Digitalkompetenz im Gremium und die digitale Souveränität in der Organisation verankert. Ein Ansatz ist die gezielte Besetzung des Gremiums mit einem oder mehreren Digitalexperten, analog zum Financial Expert in Aktiengesellschaften. In einer aktuellen US-Studie haben Unternehmen, deren Aufsichtsräte mit drei oder mehr

Dünnere wird die Digitalkompetenz in den Gremien.

Digitalexperten besetzt waren, eine 17 Prozent höhere Ergebnismarge und 38 Prozent stärkeres 3-Jahres-Wachstum aufzeigt [12].

Nur sehr wenige Menschen können allerdings die ganze Bandbreite an Digitalisierungsthemen abdecken. Statt den Vorstand mit dem einen „Chief Data Officer“ (CDO) oder das Gremium mit dem einen Experten zu besetzen, wäre eine breitere Streuung und zielgerichtete Auswahl der Expertise empfehlenswert. Der konkrete Kompetenzbedarf richtet sich vorrangig nach den Zielen, dem Marktumfeld und den existierenden Ressourcen der Organisation [13].

Fortbildungsmaßnahmen sind ein weiterer Ansatz. Die Komplexität von Themen wie Informationssicherheit oder künstliche Intelligenz macht es oft schwierig, die Teilnehmer mit vertretbarem Zeitaufwand sattelfest zu machen. Die Qualifizierung sollte daher gezielt auf die Ausbildung des Urteilsvermögens ausgerichtet sein, also beispielsweise Methoden zur Erfassung von Marktdynamiken, Werkzeuge zur Bewertung von Digitalstrategien und Metriken für Investitionsentscheidungen vermitteln.

Letztlich aber drückt sich die digitale Souveränität eines Gremiums in seiner inneren Haltung aus, in dem Mut der Mitglieder, die Strategie auf den Prüfstand zu stellen, in ihrer Unabhängigkeit, das Management zu hinterfragen und ihrer Klarheit, die richtigen Entscheidungen zu treffen. ■

Kurz und Bündig

Erfolgreiche digitale Transformation verlangt nach weitreichenden strategischen Entscheidungen. Um dafür gerüstet zu sein, müssen Organisationen gezielt die digitalen Entscheidungskompetenzen im Management und im Aufsichtsgremium aufbauen. Dabei entscheiden die strategischen Ziele genau, welche Kompetenzen die Organisation benötigt und wie sie sie erwirbt.



Weitere Infos und Literaturangaben zum Artikel finden Sie unter folgendem Link: <https://bit.ly/3whTbPc>



Raus aus der Steinzeit

Digitalkompetenz als Schlüssel zum 21. Jahrhundert

Aktionsrat Bildung

Die digitale Transformation durchdringt nahezu alle Lebensbereiche. Der souveräne Umgang mit digitalen Medien wird damit zur Grundlage von Bildungsprozessen und zur Voraussetzung dafür, Bildungsteilnehmer auf die sich wandelnden Anforderungen in Beruf und Gesellschaft vorzubereiten. Um auch zukünftig sowohl individuellen Erfolg als auch wirtschaftlichen und gesellschaftlichen Wohlstand zu sichern, muss es gelingen, digitale Souveränität als übergreifendes Bildungsziel in allen Bildungsphasen zu verankern.

Digitale Souveränität meint die Möglichkeit, digitale Medien selbstbestimmt und unter eigener Kontrolle zu nutzen, die Konsequenzen des Handelns einschätzen zu können und sich an die ständig wechselnden Anforderungen in einer digitalisierten Welt anzupassen. Digital-souveränes Handeln ist einerseits an individuelle Voraussetzungen gebunden, also an eine hinreichende Medienkompetenz der Person, und andererseits an die Bereitstellung entsprechender Technologien und Produkte. So setzt etwa die Kontrolle des Nutzens über die Darstellung der eigenen Person in der digitalen Welt zunächst Wissen über verschiedene Medien, relevante Sicherheitsaspekte und potentielle Gefahren ihrer Verwendung voraus (Medienkompetenz).

Außerdem sind zertifizierte IT-Produkte, Datenschutzrichtlinien und Systeme notwendig, die eine sichere Datenübermittlung garantieren. Der Begriff „digitale Souveränität“ wird vor allem mit Bezugnahme auf die in einer Gesellschaft lebenden Personen und die gesellschaftlichen Rahmenbedingungen verwendet, die einen souveränen Umgang mit digitalen Medien gewährleisten.

Bildung in einer digital vernetzten Welt erweitert somit Medienkompetenz um den Begriff der digitalen Souveränität. Neben dem Erlernen der Kulturtechniken Lesen, Schreiben und Rechnen ist der souveräne Umgang mit digitalen Medien die Voraussetzung für eine systematische Verankerung der Medienbildung im Handeln jedes Einzelnen. Zur Entwicklung digitaler Souveränität gehört neben der Diskussion der Chancen auch die kompetente Auseinandersetzung mit Fragen zu relevanten Sicherheitsaspekten und möglichen Gefahren, die mit der Nutzung digitaler Medien verbunden sind. Ein wesentlicher Lerninhalt ist es zudem, für die eigene digitale Information Verantwortung zu übernehmen und folglich die Wirkungen des eigenen Handelns nicht nur zu kennen, sondern auch reflexiv zu bewerten.

Lernende aller Altersgruppen sollen als selbstbestimmte Persönlichkeiten in einer sich ständig verändernden Gesellschaft bestehen und souverän sowie verantwortlich am

gesellschaftlichen, politischen und beruflichen Leben teilnehmen können. Darum zählt die sichere Beherrschung der Informations- und Kommunikationstechnologien heute zu den Schlüsselkompetenzen. Vollständige digitale Souveränität wird erst möglich, wenn auch auf ethisch-reflexiver Ebene eine verantwortungsvolle Auseinandersetzung mit digitaler Information und Kommunikation stattfindet.

Chancen und Risiken der Nutzung digitaler Medien für das Lernen

Digitale Kompetenzen sind, wie oben beschrieben, also zum einen eine übergeordnete Notwendigkeit, die sich aus gesellschaftlichen Wandlungsprozessen ergibt. Zum anderen wird die Digitalisierung des Bildungssystems als Mittel zur Verbesserung der Bildungsqualität gesehen und eingefordert. Negative Auswirkungen digitaler Medien auf das Lernen sind unter ungünstigen Randbedingungen möglich, z. B. wenn der Lernende nur über eine geringe Selbstregulationskompetenz verfügt.

Zudem gibt es eine gewisse Evidenz dafür, dass bestimmte Eigenschaften digitaler Medien einen exzessiven Gebrauch begünstigen und entsprechend auch andere entwicklungsförderliche Aktivitäten, wie z. B. sportliche Betätigung, „verdrängen“ können. Digitale Medien haben also nicht per se positive Auswirkungen auf Lernen und Leistung, sondern nur wenn tatsächlich die spezifischen Vorteile genutzt werden, die sie bei der Unterstützung von Lehr- und Lernprozessen gegenüber konventionellen Lehr-/Lernmethoden bieten. Die Forschung hat viele Erkenntnisse darüber hervorgebracht, wie Lernmotivation erzeugt oder gesteigert werden kann: Klar definierte und für den Lernenden etappenweise erreichbare Ziele spielen eine Rolle, genauso wie mittelschwere, an die Kompetenz des Lernenden optimal angepasste Aufgabenschwierigkeiten. Hinzu kommen das Erleben von Autonomie und Selbstbestimmtheit, kooperative Lehr-/Lerndesigns und informelles Lernen, auch in formellen Lernsettings.

Durch Interaktivität und Individualisierung können diese motivationssteigernden Effekte

AKTIONSRAT BILDUNG

Aktionsrat Bildung

Der Aktionsrat Bildung ist ein politisch unabhängiges Expertengremium renommierter Bildungswissenschaftler, das sich 2005 auf Initiative der vbw – Vereinigung der Bayerischen Wirtschaft e. V. konstituiert hat. Das gemeinsame Interesse liegt vor allem darin, die gegenwärtige Situation im deutschen Bildungssystem zu bewerten und zentrale Herausforderungen zu identifizieren. In seinem Gutachten „Digitale Souveränität und Bildung“ (2018) beschreibt der Aktionsrat Bildung die Auswirkungen der Digitalisierung auf alle Bildungsphasen, die Implikationen für das Bildungssystem sowie die digitale Souveränität als übergreifendes Ziel digitaler Bildung. Als zentrales Element benennt er allgemeine sowie bildungsphasenspezifische Handlungsempfehlungen und richtet diese an politische Entscheidungsträger.

Kontakt

aktionsratbildung@hbw.de
www.aktionsrat-bildung.de

Individuen müssen über Kompetenzen zum kritischen Umgang mit Medien verfügen.

erzielt werden. Es sind diese Merkmale, die sicher mit dafür verantwortlich sind, dass digitale Medien von Menschen gerne und viel genutzt werden. Diese Prinzipien sollten noch stärker bei der Gestaltung z. B. von Lernsoftware oder von Lehr-/Lernarrangements in Bildungssettings berücksichtigt werden.

Der Aktionsrat Bildung schlägt eine Vielzahl übergreifender Maßnahmen vor, die zur Steigerung von Digital- und Medienkompetenz hilfreich sind:

Überprüfung der Lehrinhalte und systematischere Erarbeitung und Verankerung digitaler Lehr-/Lernkonzepte

Folgende Aspekte sind hierbei vor allem zu beachten:

- Für alle Bildungsbereiche gilt es, darüber nachzudenken, welche Auswirkungen der Einsatz digitaler Medien und die allgegenwärtige Verfügbarkeit von Informationen auf die zu vermittelnden Lehrinhalte haben sollten: Welche Inhalte sind so grundlegend, dass die Lernenden sie als Grundlagen- und Orientierungswissen beherrschen müssen? Welche Inhalte müssen mittels übergeordneter Medienkompetenzen und entsprechender inhaltsbezogener Kompetenzziele (z. B. die Fähigkeit, zu ausgewählten Themen selbständig zu recherchieren, Inhalte einzuordnen und kritisch zu hinterfragen etc.) Eingang in die Curricula finden?
- Da digitale Kompetenzen als vierte Kulturtechnik gelten, sollte ihre Förderung analog zum Rechnen, Schreiben und Lesen Eingang in die Gesamtkonzepte der Bildungseinrichtungen finden. Neben informationstechnischem Grundlagenwissen sind auch alle übrigen Komponenten von „ICT Literacy“ zu berücksichtigen, d. h. sowohl speziellere technische Bedien- und Anwendungskompetenzen als auch übergeordnete Medienkompetenzen („Prozesskomponenten“, z. B. Medienkritik, Medienverständnis, Kommunikationskompetenzen etc.), die für einen ziel- und problemorientierten Umgang mit digitalen Medien notwendig sind.
- Über diese überfachlichen Medienkompetenzen hinaus müssen auch für die einzelnen Inhaltsbereiche gesondert digitalgestützte fachdidaktische Lehr-/Lernkonzepte entwickelt und ausdifferenziert werden. Denn der sinnvolle Einsatz digitaler

oder herkömmlicher Medien kann sich je nach zu vermittelndem Lerninhalt sehr unterschiedlich gestalten.

- Bei der Entwicklung von mediendidaktischen Konzepten sollten herkömmliche und digitale Medien komplementär berücksichtigt werden. Ziel muss es sein, die Stärken des jeweiligen Mediums – unter Berücksichtigung vorliegender empirischer Erkenntnisse – nach Fach und Inhalt optimal zu nutzen.
- Besondere Aufmerksamkeit verdient auch die Gestaltung der Übergänge zwischen den Bildungsetappen: Es sollten jeweils die Kompetenzziele und -voraussetzungen jeder Etappe definiert und in ein phasenübergreifendes Gesamtkonzept integriert werden.

Flächendeckende und systematische Aus- und Weiterbildung des Personals in Bildungseinrichtungen

Folgende Aspekte sind hierbei vor allem zu beachten:

- Für Lehrende aller Bildungsetappen sollten ein Angebot berufsbegleitender weiterbildender Module und Masterstudiengänge (z. B. für die Ausbildung zum „Digitalisierungsbeauftragten“, s.o.) sowie ein übergreifendes Gesamtkonzept zur Förderung digitaler Kompetenzen geschaffen werden.
- Lehrkräfte sollten dafür qualifiziert werden, für die eigenen Unterrichtsziele fachdidaktisch und pädagogisch sinnvolle Unterrichtskonzepte mit digitalen Medien zu entwickeln. Darüber hinaus muss – mit dem Ziel der Nutzung von Synergieeffekten – in der Aus- und Weiterbildung der Lehrkräfte die Grundlage für einen kollegialen Austausch im Bereich der digitalen Medien und die Kooperation zwischen den Bildungseinrichtungen geschaffen werden.
- Für das Bildungs- und Verwaltungspersonal in den staatlichen Bildungseinrichtungen von der frühen Bildung bis zur Sekundarstufe sollte eine Anzahl an verpflichtenden Weiterbildungstagen für den Themenbereich Digitalisierung festgelegt werden.
- Da den Führungskräften eine bedeutsame Rolle bei der Digitalisierung der Bildungseinrichtungen zukommt, muss ein besonderes Augenmerk auf Qualifizierungsangebote für diese Zielgruppe liegen. Neben der Vermittlung der technischen und

	Wissen	Kompetenz	Bildung
Technische Souveränität (passiv-rezeptive Kompetenz + aktiv gestaltende Kompetenz)	Kenntnisse über Hard-/Software: <ul style="list-style-type: none"> ▪ Herstellung ▪ Revision ▪ etc. 	<ul style="list-style-type: none"> ▪ Computernutzung ▪ Computerprogrammierung ▪ Weiterentwicklung der technischen Mittel 	Digitales Wissen und Kompetenz als Voraussetzung für digitale Souveränität
Ethisch-reflexive Souveränität (zulässige/unzulässige Rezeption und Produktion)	Geschichte, Theorie und Implikationen von (digitaler) Information und Kommunikation	<ul style="list-style-type: none"> ▪ Hinterfragen von Quellen, „falschen“ Tatsachen ▪ Unterscheidung von Fakten und Meinungen ▪ Verantwortungsvolle Formulierung und Platzierung eigener Beiträge 	Persönliche Souveränität als individuell und gesellschaftlich verantwortungsvoller Umgang mit der Rezeption, Erstellung und Umsetzung von digitaler Information und Kommunikation

Abbildung 1: Wissen, Kompetenz und Bildung für digitale Souveränität.

didaktischen Kompetenzen sollten Angebote geschaffen werden, die zu Fragen der Mitarbeiterführung und -motivation im digitalen Wandel qualifizieren. Ziel der Einrichtungsleitungen muss es sein, dem Lehrpersonal eine offene Haltung gegenüber dem Lehren mit digitalen Medien zu vermitteln und auch speziell auf die Bedürfnisse diesbezüglich sehr zurückhaltender und skeptischer Personen einzugehen.

Förderung der wissenschaftlichen Forschung in allen Bereichen der Digitalisierung von Bildungseinrichtungen

Folgende Aspekte sind hierbei vor allem zu beachten:

- Die Wirksamkeit und der Mehrwert digitaler Unterrichts- und Prüfungsformen sollten für alle Bildungsbereiche und -etappen fortlaufend wissenschaftlich begleitet und evaluiert werden.
- Dies ist Voraussetzung, damit ein evidenzorientierter Einsatz digitaler Medien möglich wird und digitale Medien zur Individualisierung und Qualitätssteigerung von Prüfungen genutzt werden können.
- Für alle Altersstufen sollten qualitätsvolle Unterrichtsmaterialien und Lernprogramme entwickelt werden. Bildungstechnologien sollten in enger Abstimmung mit den Bedürfnissen der Praxis vorangetrieben und weiterentwickelt werden.
- Bei der Einführung von digital angereicherten Lehr-/Lern- und Prüfungsformaten sind die Vorstellungen und Bedürfnisse der Lehrenden sowie die heterogenen Voraussetzungen im Zugang zu ICT und

in der digitalen Grundbildung der Lernenden zu berücksichtigen.

- Für alle Bildungsetappen sollten die Aus- und Weiterbildungsangebote des pädagogischen Personals zum Themenbereich Digitalisierung fortlaufend evaluiert und wissenschaftlich begleitet werden.
- Die medienpädagogischen und IT-Kompetenzen der Lehrenden an Schulen, Universitäten und Weiterbildungseinrichtungen sind ein zentrales Nadelöhr für einen effektiven medienunterstützten Unterricht. Darum müssen Modelle für die Kompetenzen der Lehrkräfte entwickelt und empirisch validiert werden.
- Großer Forschungsbedarf besteht zur Frage des informellen Lernens: Über welche Kanäle werden außerhalb formaler Bildungskontexte für die Arbeitswelt und die Gesellschaft relevante Kompetenzen erworben (z. B. Diskussionen in sozialen Netzwerken, selbstgesteuerte Informations- und Meinungsrecherche zu beruflichen und privaten Themen)? ■

Kurz und Bündig

In dem Gutachten „Digitale Souveränität und Bildung“ (2018) beschreibt der Aktionsrat Bildung die Auswirkungen der Digitalisierung auf alle Bildungsphasen – von der frühen Kindheit bis zur Weiterbildung –, die Implikationen für das Bildungssystem und hebt die digitale Souveränität als übergreifendes Ziel von Bildungsprozessen hervor.



Dem Dreigestirn der Innovation begegnen

Digitale Souveränität beginnt im Kopf

Tomas Herzberger, Schaffensgeist

Was ist digitale Souveränität? Kommt darauf an, wen man fragt. Häufig wird der Begriff im Umfeld von digitaler Infrastruktur (z.B. Glasfasernetzwerk oder 5G) von Staaten oder Regionen genannt. Das ist ein Aspekt, aber etwas oberflächlich gedacht. Digitale Souveränität findet nicht nur auf kontinentaler oder nationaler Ebene statt, auch Unternehmen und sogar Einzelpersonen können digital souverän sein – oder eben nicht.

Wann ist man "digital souverän"? Wann ist man endlich dieses ungute Gefühl los, neuen Trends und dem Wettbewerb hinterherzulaufen? Wann schöpft man sein ganzes Potenzial aus? Die kurze Antwort: nie. Dazu ist der technologische Wandel zu schnell. Sofern Sie nicht selbst bei einem Innovationsführer arbeiten, wird es immer Raum für Verbesserungen geben (und selbst dann gibt es bestimmt noch Unternehmensbereiche, die hinterherhinken). Die gute Nachricht? Das ist vollkommen in Ordnung! Wenn Sie der digitalen Transformation mit dem richtigen Mindset begegnen, werden Sie von der Welle nicht hilflos überrollt, sondern können den Wandel aktiv gestalten.

Kennen Sie das deutsche "Dreigestirn der Innovation"?

- "Das haben wir schon immer so gemacht!"
- "Das haben wir noch nie so gemacht!"
- "Wo kommen wir denn da hin?!"

Wenn Sie diese Sätze von Kollegen (oder noch schlimmer: Vorgesetzten) häufiger hören, nehmen Sie die Beine in die Hand und laufen! Denn als innovationsbegeisterter Leser dieses Magazins werden Sie dort sicherlich nicht glücklich werden. Digitale Souveränität beginnt im Kopf, das heißt, es beginnt mit der richtigen Einstellung der Menschen, die für die digitale Transformation verantwortlich sind oder sie umsetzen sollen. Ironischerweise steigt mit der technischen Komplexität auch der Anspruch an den Menschen. Denn je komplexer das System, das implementiert werden soll, desto wichtiger sind die Kommunikationsfähigkeiten der beteiligten Mitarbeiter. Für die meisten Projekte brauchen Sie keinen MIT-Absolventen. Sie brauchen Menschen, die neugierig sind und gerne mit Menschen aus anderen Fachbereichen arbeiten.

In unserer Arbeit mit Start-ups, Mittelständlern und Konzernen haben sich neun Aspekte herauskristallisiert, die für digitale Souveränität kritisch sind.

Digitale Souveränität bedeutet:

1. Mut zur Sichtbarkeit: Gut sein alleine reicht nicht aus – andere müssen es auch sehen! Nur wer sein Wissen mit anderen teilt, wird als Experte in seinem Gebiet wahrgenommen. Sowohl im eigenen Unternehmen als auch auf dem Markt. Das

Mit dem richtigen Mindset können Sie den Wandel aktiv mitgestalten.

gilt ebenso für Unternehmen als Ganzes: Wer sich unnahbar zeigt, wer seine Produkte vor Launch im dunklen Kämmerlein statt gemeinsam mit Kunden produziert, hat ein viel höheres Risiko zu scheitern.

- 2. Bereitschaft:** Ob es nun ein neuer Prozess, ein neues soziales Netzwerk oder eine neue Technologie wie Kryptowährungen oder NFT ist: Seien Sie Neuem gegenüber aufgeschlossen, und testen Sie es aus! Wachstum beginnt außerhalb der Komfortzone, und nur wer Neues lernt, kann auch wachsen. Dies gilt für Unternehmen ebenso wie für Menschen. Verschließen Sie sich nicht neuesten Trends oder Technologien gegenüber, bleiben Sie aufgeschlossen, und geben Sie allem eine Chance – in einem gesunden Rahmen. In der Praxis können Sie mit neugierigen Kollegen ein Team aufbauen, dessen Aufgabe es ist, neue Technologien zu analysieren, zu bewerten und gegebenenfalls auszutesten.
- 3. Fokus:** Auf der einen Seite sollte man die Bereitschaft und Kompetenz entwickeln, neue Kanäle auszuprobieren. Auf der anderen Seite darf man sich nicht der Versuchung hingeben, überall präsent sein zu müssen. Sie wollen jeden Social-Media-Kanal bespielen, jeden Design-Trend aufgreifen oder jede New-Work-Methode einsetzen? Vielleicht kennen Sie das Gefühl vom Einkaufen an einem Black Friday: Es nennt sich Fear of missing out - die Angst etwas zu verpassen. Ganz ruhig: Sie müssen keinesfalls zwanghaft auf allen Plattformen präsent sein, nur weil das "alle anderen" machen. Ja, sie sollten neugierig und bereit sein, neue Dinge zu testen. Aber das Ergebnis dieses Tests kann auch die Entscheidung sein: "Wir machen das jetzt nicht." Fokussieren Sie sich auf die Kanäle, die wirklich relevant sind und nutzen Sie diese zielführend! Wie Sie das machen? Machen Sie niemals etwas zum Selbstzweck! Definieren Sie eine einzige Metrik, die sowohl



Tomas Herzberger

Tomas Herzberger ist gemeinsam mit Marina Zayats Co-Founder der Beratung "Schaffensgeist" und bereits seit 2006 im Digital Marketing tätig. Er hat sowohl strategisches als auch praktisches Wissen über alle Marketing-Disziplinen bei Unternehmen wie der Deutschen Bahn, paydirekt, der VTB Bank oder der Messe Frankfurt zum Einsatz bringen können. Sein Wissen vermittelt er auch als Trainer (u.a. für 121Watt, Haufe und Tomorrow Academy) sowie als Speaker. Tomas ist Co-Autor des Bestsellers "Growth Hacking" und des anstehenden Buches "Branding mit LinkedIn". Junge Startups unterstützt er als Mentor (u.a. bei Plug & Play) und bietet mit den Growth Hacking Meetups regelmäßig die Möglichkeit zum Wissensaustausch und Networking.

Kontakt

tomas@schaffensgeist.com
www.schaffensgeist.com

Unternehmenswachstum als auch Kundenzufriedenheit widerspiegelt (sog. “North-Star-Metric”), und relevante KPI, an denen Sie und Ihr Team sich orientieren können. Das gilt insbesondere für Maßnahmen wie Content- oder Social-Media-Marketing. Das sorgt für weniger Ablenkung in der Umsetzung und für mehr Transparenz und Vertrauen im Team.

4. **Begeisterung durch Geschichten:** Jeder Mensch ist ein Geschichtenerzähler – es steckt in unseren Genen. Seitdem der Mensch Sprache entwickelt hat, erzählt er sich Geschichten, um konkrete Informationen über Nahrungsquellen auszutauschen, abstrakte Konzepte wie Jahreszeiten zu erklären und als sozialer “Kleber”, als Kitt in der Gruppe. Trotzdem nutzen viele sogenannte “Kommunikationsexperten” diese Methode nicht. Warum? Weil es oftmals leichter ist, auf etablierte Fachbegriffe zurückzugreifen, statt neue Metaphern zu finden. Das Problem dabei: Gerade Experten können der Versuchung oft nicht widerstehen, ihr Wissen so anspruchsvoll zu formulieren, dass sie nur von anderen Experten verstanden werden kann. Auf Augenhöhe. Für diese Experten gilt: “lose the fancy hat!” Machen Sie ihr Wissen dank guter Geschichten anschaulich und leichter zugänglich. Die echte Expertin erkennt man daran, dass sie ihr Wissen soweit vereinfachen kann, dass es praktisch jeder Zuhörer versteht. Und nur, wenn die Nachricht auch verstanden wird, können Ihre Kollegen mitziehen und das anspruchsvolle Projekt realisieren. Gutes Storytelling wirkt nach innen und außen. Es schafft Vertrauen bei Mitarbeitern und Kunden, Abgrenzung gegenüber Wettbewerbern und beim Aufbau einer starken, einzigartigen Marke.
5. **Vertrauen:** Klingt banal, aber Unternehmen müssen lernen, den eigenen Mitarbeitern zu vertrauen. Dazu gehört insbesondere, sie im Namen des Unternehmens kommunizieren zu lassen – auch auf Social Media. Der Grundsatz “One Company, one voice” ist nicht mehr länger gültig. Stattdessen ist der Chor der Stimmen das, was die Kunden wahrnehmen. Sei es der Vertriebler am Messestand, der Marketer bei einer Keynote oder der Fachexperte über sein LinkedIn-Profil: Ihre Mitarbeiter beeinflussen maßgeblich das Image Ihres Unternehmens! Nicht nur das, sie beeinflussen natürlich auch die Unternehmenskultur und damit die Innovationsbereitschaft. Grundlage für all das ist Vertrauen. Also: Schluss mit dem Micro-Management! Informieren Sie Ihre Mitarbeiter über die Leitplanken der Kommunikation nach außen, aber lassen Sie Ihnen Spielraum. Wie Sie damit starten können? Überprüfen Sie Ihre Social Media Guidelines, ob sie auf “Beschränkung” oder auf “Unterstützung” ausgerichtet sind. Letzteres sollte das Ziel sein.
6. **Neugier:** Bleiben Sie stets neugierig! Sowohl auf neue Technologien wie auch Prozesse und Ideen. Nur weil Sie selbst nicht TikTok oder Twitch nutzen, heißt das nicht, dass es keine Relevanz hat. Millionen von Menschen (darunter vielleicht auch zukünftige Kunden oder Kollegen) würden vehement widersprechen. Gehen Sie auf Meetups, Konferenzen und Lesungen, um neue Ideen kennenzulernen – oder laden Sie Experten gleich zu sich ins Unternehmen ein, damit das gesamte Team von neuen Themen profitieren kann!
7. **Ein Vorbild zu sein:** Es beginnt bei Ihnen! Erwarten Sie keinen Wandel bei Ihren Kollegen, wenn Sie nicht vorangehen und andere Menschen inspirieren. Egal, ob Sie Geschäftsführer, Bereichsleiter oder Fachexperte sind: Ihr Unternehmen braucht “Leuchttürme”, die sich gut sichtbar ins Abenteuer stürzen. Das gilt insbesondere für die Nutzung von Social-Media-Plattformen wie Xing und LinkedIn, denn oftmals trauen sich die Menschen aus Mangel an Vorbildern gar nicht erst zu, die Plattformen zu testen. Nur als Vorbild können Sie den Wandel in Ihrem Unternehmen positiv beeinflussen. Zeigen Sie nicht nur Erfolge, sondern auch Fehlschläge und schmerzhaft Erfahrungen, um Ihren Kollegen die Furcht vor Neuem zu nehmen. Gewähren Sie auch Einblicke in Ihr Innenleben und geben zu, wenn Sie etwas nicht wissen, Hilfe brauchen oder unsicher sind.
8. **Unabhängigkeit:** Verlassen Sie sich niemals auf eine einzige Plattform oder einen einzigen Kanal – schon gar nicht, wenn Sie ihn nicht beeinflussen können. Ob Sie Salesforce oder SAP, AWS oder Oracle, Typo3 oder Drupal, Facebook oder LinkedIn nutzen: Machen Sie sich niemals abhängig von einer Plattform, einem

Anbieter oder einer Agentur. Sorgen Sie dafür, dass Sie stets die Datenhoheit haben und gegebenenfalls das System wechseln können. Lassen Sie immer ausführliche Dokumentationen anfertigen, um sich nicht von einzelnen Programmierern abhängig zu machen. Und verlassen Sie sich niemals auf eine einzige Social-Media-Plattform, sondern behalten Sie die Hoheit über Ihre Website, Ihren Blog und Ihren E-Mail-Verteiler.

- 9. Verantwortungsbewusstsein:** Digitale Souveränität ist der Mut, Verantwortung zu übernehmen und auch über einen Fehler öffentlich zu sprechen, wenn es notwendig ist. Ein Kunde beschwert sich auf Social Media über einen Produktfehler oder das Fehlverhalten eines Mitarbeiters? Zeigen Sie Größe, indem Sie den Fehler anerkennen, sich entschuldigen, und tun Sie ihr Möglichstes, um das Problem des Kunden zu lösen! Ach so, das Problem fällt nicht in Ihren Verantwortungsbereich? Das ist dem Kunden sehr egal! Wie Sie das Problem intern weiter delegieren, spielt keine Rolle. Zunächst möchte jeder Mensch gehört werden. Wir verlangen nach Anerkennung, wenn wir ein Problem gelöst haben. Diese Anerkennung, gepaart mit einer schnellen, aufrichtigen Entschuldigung, macht mehr als die halbe Miete aus. Wenn Sie in der Lage sind, das Problem so einfach, schnell und pragmatisch im Sinne des Kunden zu lösen, noch besser! War die Kundenbeschwerde öffentlich, beispielsweise via Social Media, sollten Sie so schnell wie möglich den Kanal wechseln und sich mit dem Kunden per E-Mail, Chat oder Telefon auszutauschen. Denn Social Media ist ein Zuschauersport. Nicht nur Ihr Kunde, sondern auch Ihre Wettbewerber, Partner, Dienstleister und schlimmstenfalls die Medien können auf die öffentliche Konversation aufmerksam werden und zuschauen. Ihre Reaktion auf Kundenanliegen ist deswegen ein nicht zu unterschätzender Faktor für Ihr Marken-Image.

Digitale Souveränität beginnt im Kopf des einzelnen. Erst wenn Menschen aus dem Schatten treten, Neues ausprobieren und transparent kommunizieren, können sie Mitstreiter inspirieren und somit auch einen Beitrag für eine bessere Unternehmenskultur leisten. Aber

steigt damit nicht auch das Risiko, Fehler zu machen? Natürlich! Können Sie Skifahren? Sehr wahrscheinlich haben Sie sich das eine oder andere Mal in den Schnee gesetzt, als sie es gelernt haben, richtig?

Fehler machen gehört zum Lernen dazu. Und wer keine Toleranz gegenüber Fehlern hat, der wird nicht lernen können und dessen Unternehmen wird nie innovativ oder digital souverän sein können. Es geht nicht darum, Fehler machen zu müssen. Es geht darum, zu tolerieren, dass Fehler passieren, wenn man Neues ausprobiert. Nicht nur beim Skifahren, auch im Business.

Das Gute? Wenn Sie häufig kleine Experimente und Tests machen, verlieren Sie schnell die Furcht vor Fehlern. Denn diese kleinen Tests bewahren Sie davor, große Fehler zu machen. Wenn Sie beispielsweise ein neues Produkt nutzerorientiert und agil entwickeln, anstatt jahrelang viel Zeit und Geld in die perfekte Umsetzung einer vermeintlich guten Idee zu investieren, dann ist das unternehmerische Risiko deutlich geringer.

Was Sie konkret umsetzen können: Gehen Sie "Vor die Tür", und sprechen Sie mit Ihren Kunden! Warum sind Sie Ihre Kunden, was schätzen Sie an der Zusammenarbeit, welche Probleme und Herausforderungen beschäftigen Sie? Bauen Sie keine Lösungen, und suchen dann Menschen mit dem passenden Problem, sondern erforschen Sie die Probleme der Menschen, um anschließend eine passende Lösung zu produzieren. ■

Kurz und Bündig

Digitale Souveränität findet nicht nur auf kontinentaler oder nationaler Ebene statt, auch Unternehmen und sogar Einzelpersonen können digital souverän sein. Dafür muss die Bereitschaft vorhanden sein, der digitalen Transformation aktiv und mit dem richtigen Mindest zu begegnen.

Connecting All of Europe With a Single Crossroad

The secure data-exchange layer X-Road®

Ville Sirviö, Nordic Institute for Interoperability Solutions (NIIS)

X-Road was initially developed in Estonia in 2001 and is now used by different countries and organisations as a system to exchange data securely. Together with Finland and Iceland, the Nordic Institute of Interoperability Solutions (NIIS) is responsible for the continuous development of the system. The Institute's CEO, Ville Sirviö, explained in an interview with the IM+io magazine how such a high-security data exchange system for the public sector was built and the risks and benefits of having information systems connected to the Internet.

IM+io Unlike Estonia, digitalisation in Germany's public sector has been lagging behind. Could you explain what X-Road is and what it does?

VS: X-Road is a software solution with roots in Estonia which has been implemented by numerous countries around the world. Today Estonia, Finland and Iceland are working together on the continuous development of this solution. X-Road is a centrally managed, distributed data exchange layer that transfers data between information systems in the public and private sectors. It provides a standardised way to produce and consume services while at the same time placing a high value on security. The security features include machine-level authentication, transport-level encryption, timestamping, digital signatures of messages and logging of messages.

IM+io How was the idea of this system born? What is your success story?

VS: Estonia faced a few challenges around the millennium. One of the challenges was information security and how to build a safe data exchange system. But that was only one part of the dilemma. Another question that had to be answered was how to even exchange data.

Today we do not think of the risks to our data when using the internet.

For many years governments in Europe have been using closed private networks to exchange official data between authorities. These networks usually are fully private and are not connected to the public Internet. A network of that type did not exist.

The solution the X-Road inventors in Estonia came up with was to set up a software-based system that uses the public Internet. This does not seem very innovative at first, but we have to remember that during that time, in 2001, the Internet was still a relatively new thing. Today we usually do not think of the risks to our data when using the Internet. We feel safe. The Internet is part of our daily life, which makes us forget about the dangers that come with it. I think this information security issue was the motivation to build a secure network solution that can be operated over the Internet without having to build additional infrastructure, like a new private network. That is what led to the development of X-Road.

IM+io Were there any trust issues or political discussions about data security concerning X-Road?

VS: When I think about the beginning when Estonia was proposing the use of X-Road to Finland, we had political and technical discussions between the experts on each side. Despite that, trust between the two countries was necessary to establish a cooperation like this. The fact that X-Road is used in over 20 countries today shows high confidence in the solution and in the countries that are developing it. Estonia, Finland and Iceland are countries that others can see as trustworthy partners in technology.



Ville Sirviö

Ville Sirviö is the CEO of the Nordic Institute for Interoperability Solutions (NIIS), a non-profit developing digital government infrastructure, best known for the X-Road® software. Having international experience in leading businesses ranging from start-ups to Nasdaq listed companies, he is also a board professional, advisor and keynote speaker on cross-border digital cooperation.

Kontakt

ville.sirvio@niis.org
www.niis.org

For many years governments in Europe have been using closed private networks.

IM+io What are the advantages of X-Road?

VS: The main advantage of X-Road is the ability to build a national ecosystem that can be utilised by public authorities and private companies. Through one access point, X-Road allows every organisation to access and consume data and services that are already part of the ecosystem, while at the same time making their data available to others who might need it. Having the connection in place means that we do not have to spend additional time building point-to-point integrations or connecting services by using different solutions, platforms or technologies. Once the organisation is part of the ecosystem, it can make its data available to others and vice versa.

In addition, the single ecosystem approach allows for higher security standards and enforcing certain security policies. For example, the message exchange in X-Road can be fully logged. X-Road allows the national operator to decide whether to only use metadata logs or logs including the entire message. The metadata logs only show the metadata regarding the

message exchange between the information systems and the exact time when certain data exchanges took place, but it does not include the actual business data of the messages.

Yet X-Road can also be configured to include full messages in the logging. In that case, the logs contain the full content of the message and could be even used as evidence in court. I think this is an area that has not yet been tested very thoroughly in European jurisdictions. I am curious to see if there will be cases in the future where someone will dispute that the message used before court only has metadata logs and therefore only proves that the message was exchanged but not what the content of the message was. This is one area where X-Road may have an advantage. The logs are comprehensive and provide the entire message if desired.

IM+io Does this mean that users of X-Road do not have to worry about data security anymore?

VS: Unfortunately not. Having logs that include the entire message means that there are additional challenges for information security. Nevertheless, that is a problem that every information system faces. You always have system administrators who have access to the data, this cannot be avoided. In addition to that, everything is also related to the information systems connected to X-Road. Even if we use logging, digital signing, time stamping and different authentication and rights management mechanisms, the backend-information systems have their own information security measures. X-Road is not a magic bullet



that will solve all the information security issues. Still, it can be an essential step forward in building a unified ecosystem in countries when all organisations utilise a unified security model.

I've been talking to some CIO's who said that one major problem is that they do not have anything like an ecosystem. Instead, they have a bunch of information systems based on different technologies, maintained by various organisations and having nonidentical criteria for information security. Due to the large number of information systems, it is difficult to understand and keep track of how those information systems were built and maintained. Having one ecosystem like X-Road with unified security measures makes it much easier to maintain, control and audit data exchange.

IM+io A few weeks ago, platforms like Facebook or Instagram were offline for several hours. What are key factors that need to be considered, so that something like this does not happen to systems like X-Road?

VS: As I mentioned before, the Internet is part of our everyday life, and we do not believe that more significant technical problems, like this incident with Facebook, could occur. I think this was a perfect wake up call for everyone to understand what can happen when a technical problem arises.

As long as the core internet infrastructure is working, X-Road has multiple built-in methods to protect against the failure of key components. X-Road is based on a distributed architecture that makes it extremely fault tolerant. It has been designed to support simultaneous failures of its key components without affecting the ecosystem.

The key points we must consider when building critical infrastructure are:

1. What is the role of the Internet?
2. Which services can we run on Internet?
3. What are the critical, essential services that cannot be operated via Internet?

IM+io Could X-Road also be used in the private sector?

VS: Yes, it can be used by private companies. In a recent case study from Germany, X-Road has been implemented as part of a larger project in digital health. It has also been implemented as a corporate solution by some of the largest companies in Japan.

A system like X-Road makes it easier to maintain, control and audit data exchange.

IM+io What does the future hold? Are there any current projects you are working on to improve X-Road?

VS: First of all, we just finished a study on the environmental impacts of X-Road. It is our goal to make X-Road the most sustainable data exchange solution of its kind. We analysed in which areas we can do more to cut CO2 emissions, and we found out how we can make the system more sustainable. When we now make future decisions on the technical development of X-Road, we simultaneously want to evaluate the environmental impact.

Another area of our activity is analysing the general development in Europe, trying to forecast what will happen in the future. At the moment, Europe is working on projects like Gaia X and the Single Digital Gateway. Projects like these also are interesting for us and the further development of X-Road.

Furthermore, we are currently looking into CEF eDelivery systems. We are just about to release our new product: Harmony eDelivery Access; an eDelivery access point solution. The main reasons for its development were to provide a good product for our member countries and research purposes. We will assess the results of this new product and also consider if we want to embed eDelivery into X-Road. This means that X-Road could be compatible with eDelivery in the future, which would be a huge step forward in its development. ■

In Short

X-Road® is a open-source software and ecosystem solution that provides unified and secure data exchange between organisations. The basic idea of X-Road is that members of an ecosystem exchange data through access points (Security Servers) that implement the same technical specifications. X-Road is a digital public good, available free of charge.



641.52



641.52



Der Wald als digitales Ökosystem

Wie GAIA-X neue Datenräume eröffnet

Ingo Lück, Thomas Feld, Materna



219.98



193.94

993.28



206.36



Mehr ist mehr, wenn es um die Nutzung von Daten für digitale Geschäftsmodelle geht: In der Data Economy sind mehr Datenschutz, mehr verfügbare Daten und mehr zweckgebundene Möglichkeiten zur Auswertung von Daten gefragt. Basis dafür ist eine souveräne Dateninfrastruktur als Grundlage. Die Idee leuchtet ein: Daten teilen, ohne die Datenhoheit aufzugeben, bringt mehr Nutzen für alle Beteiligten. Doch wie kann das funktionieren?

Wie können aus Daten erfolgreiche Geschäftsprozesse in digitalen Ökosystemen werden? Diese Frage bewegt derzeit die Entscheider in Wirtschaft, Wissenschaft, Politik und Verwaltung. Die gute Nachricht: Mit souveränen Dateninfrastrukturen, wie sie derzeit im Rahmen des GAIA-X-Projekts entwickelt und aufgebaut werden, ist ein wichtiger Teil der Antwort bereits gefunden. Datensouveränität bedeutet in diesem Zusammenhang, dass die Beteiligten die Hoheit über ihre eigenen, beziehungsweise die von ihnen generierten Daten behalten. So können sie beispielsweise entscheiden, mit wem sie welche Daten teilen, für welchen Zweck und zu welchen Konditionen.

Erst umdenken, dann profitieren

Um so souverän mit Daten umgehen zu können, erfordert es ein radikales Umdenken: Wo heute noch unterschiedliche Organisationseinheiten getrennte Datensilos betreiben, müssen sie künftig untereinander und mit Dritten außerhalb der eigenen Organisation mehr Datenaustausch ermöglichen. Nur dann können sie ihren Kunden den Service bieten, den diese erwarten – und selbst davon profitieren.

Zum Beispiel in der Automobilbranche: Ein Navigationssystem, das nicht nur in einem Fahrzeugtyp verbaut ist, sondern in möglichst vielen unterschiedlichen, ermöglicht eine beliebige Zahl von wirtschaftlichen Zusatzservices. Beispielsweise kann es je nach Verkehrssituation und Wetterlage Hinweise auf Alternativrouten, freie Parkplätze im Zielbereich, Verfügbarkeiten von E-Bikes und vieles andere melden. Gesammelt werden die Daten von der Gesamtheit der Verkehrsteilnehmer, die dem Austausch ihrer Daten mit dem jeweiligen System zugestimmt haben – und dafür automatisch eine Gratifikation erhalten.

Für alle Player in der Data Economy gilt: Je stärker sie vernetzt sind, desto mehr Datenpunkte für hochqualitative Prognosen und bedarfsgerechte Leistungsangebote für Nutzer entstehen. Zu den größten Hindernissen bei der Umsetzung gehört die Frage: Wie können zum Beispiel die Automobilhersteller oder Mietwagenanbieter Daten teilen, um Mehrwerte zu generieren, ohne dass sie die Datensouveränität verlieren?

Auf dem Weg zu europäischen Datenräumen

Gute Nachrichten kommen dazu aus der technologischen Entwicklung im Umfeld von GAIA-X, einem Projekt zum Aufbau einer leistungsfähigen, sicheren und vertrauenswürdigen Dateninfrastruktur für Europa. Hier entstehen derzeit durch das Zusammenwirken vieler Beteiligter aus Wirtschaft, Wissenschaft, Verwaltung und Politik in zahlreichen Einzelprojekten Lösungen für unterschiedliche Branchen und Anwendungsfälle.

In dem aktuellen Projekt „Datenraum Wald und Holz 4.0“ (DWH 4.0) wird Materna gemeinsam mit Projektpartnern den Wald als digitalen Zwilling abbilden. Die Projektpartner werden den digitalen Datenraum Wald mithilfe der Leitprinzipien der europäischen GAIA-X-Initiative zu einem föderalen, offenen und interoperablen Ökosystem weiterentwickeln. Es wird eine Föderationsdienste-Plattform entwickelt, die die bislang geschlossenen Datensilos aller Beteiligten öffnet und für die Nutzung smarter Services verfügbar macht.

Hierzu wird das Förderprojekt DWH 4.0 den gesamten Prozess von der Bepflanzung über die Bewirtschaftung der Wälder über die Holzernte und die Holzlogistik bis zur



Ingo Lück

Dr. Ingo Lück ist Projektkoordinator Forschungsprojekte bei Materna und seit 1998 im Unternehmen tätig. Seine Schwerpunkte sind Cloud Computing, IoT, Web Services und GAIA-X. Zu den aktuell betreuten Forschungsprojekten gehören InnoPortAR (Innovative Einsatzfelder für Augmented Reality in Binnen- und Seehäfen), I2PANEMA (Intelligent, IoT-based Port Artefacts Communication, Administration and Maintenance) und Mobility Data Space.

Kontakt

ingo.lueck@materna.de
www.materna.de

Verarbeitung des Holzes abbilden. In jedem Projekt oder Datenraum sind spezielle Herausforderungen zu bewältigen, je nach Art der Daten. Doch es gibt auch viele Gemeinsamkeiten, was den grundlegenden Aufbau einer souveränen Dateninfrastruktur für die verschiedenen Anwendungsszenarien betrifft.

Experten sprechen von einer föderativen Schicht, in der die Daten je nach Bedarf und Nutzungsrechten der Beteiligten anonymisiert, aggregiert und bereitgestellt werden. Das erfordert einen Architekturwechsel, weg von der Silo-Struktur hin zu so genannten Federation Services. Hier wird katalogisiert: Welche Daten hat eine Organisation? Welche Daten gibt sie heraus? Wie findet der Datenaustausch statt? Und was geschieht danach?

Ein wichtiger Aspekt in diesem Zusammenhang ist die Frage, wo die Daten geografisch gespeichert werden. Die Datenhoheitsrechte der EU lassen sich nur im Rechtsraum Europa durchsetzen. Bislang verlassen viele Daten jedoch diesen Rechtsraum. Damit sind sie faktisch nicht so geschützt, wie die EU das vorschreibt. Gleichwohl stehen Unternehmen und andere Organisationen vor der Anforderung des Marktes, dass sie Daten austauschen müssen, um Kunden zu halten und neue zu gewinnen. Denn diese, zumal die jüngeren Generationen, fordern neue digitale Services. Freilich ohne dabei ihre Datensouveränität aufzugeben. Das haben inzwischen auch Politik und Behörden erkannt – und reagieren entsprechend.

Digitale Bürgerassistenten für mehr und besseren Service

Ein Beispiel: Das Onlinezugangsgesetz (OZG) bewirkt, dass Behörden derzeit ständig mehr Services elektronisch bereitstellen. Doch dahinter liegen oftmals noch die alten Prozesse und Verwaltungsabläufe. Wer beispielsweise einen Bauantrag stellen will, weiß häufig erst einmal gar nicht, wann und wo in welchem Kontext welche Informationen zu liefern sind. Bürger

Es braucht Datenaustausch statt viele eigenständige Datensilos.

brauchen Hilfestellung. Dabei werden immer wieder die gleichen Fragen gestellt und beantwortet. Das ist eine ideale Aufgabe für Chatbots – die digitalen Assistenten lotsen die Nutzer durch das digitale Angebot einer Verwaltung.

Von dieser Art digitaler Bürgerassistenten profitieren beide Seiten. Bürger, weil ihre Anliegen schneller erledigt werden, und die Behörden, weil sie den Aufwand für Rückfragen und die Korrektur fehlerhafter Eingaben sparen. Künstliche Intelligenz (KI) sorgt dafür, dass die Systeme mit der Zeit immer besser erkennen, wo genau der Bedarf der Benutzer liegt. Lernfähige Kommunikationssysteme, die nicht nur den Wortlaut einer Eingabe, sondern auch den Gesprächsverlauf berücksichtigen, können beispielsweise Verständnisprobleme erkennen, und mit Informationen in schriftlicher Form durch Übersetzung oder Weiterleitung an menschliche Mitarbeiter den Prozessfortschritt fördern.

Bewegung im Mobility Data Space

Innovative Verkehrskonzepte wie etwa Autonomes Fahren benötigen eine Vielzahl von Daten aus unterschiedlichsten Quellen. Damit die verschiedenen Akteure vom Bundesverkehrsministerium über Landesbehörden, Kommunen und private Verbände bis hin zu Bahnbetreibern, Logistikunternehmen und Automobilwirtschaft ihre Daten zum gegenseitigen Nutzen austauschen können, entsteht bereits seit mehr als zehn Jahren ein so genannter Mobilitätsdaten Marktplatz. Denn nur mit autonom fahrenden Automobilen wird sich der Verkehrsinfarkt in den Städten auf Dauer nicht vermeiden lassen. Ebenso wenig werden E-Scooter allein die Mobilität der Landbevölkerung sichern.

Damit das Zusammenspiel aller Verkehrswege und Beförderungsmittel funktioniert, müssen sowohl die Anbieter als auch die Nutzer von Intermodaler Mobilität jederzeit über aktuelle Verkehrsdaten in Echtzeit verfügen. Dazu wird es erforderlich sein, den Mobilitätsdatenmarkt zu einem Mobility Data Space auszubauen, der die Daten nicht nur als solche bereit hält, sondern sie wertsteigernd miteinander vernetzt.

Digitales Gesundheitswesen: mehr als Apps auf Rezept

E-Health oder Digital Healthcare haben nicht zuletzt durch die Pandemie an Bedeutung

gewonnen. Doch schon länger bieten gesetzliche und private Krankenversicherungen die Möglichkeit, Informationen und Bescheinigungen online abzurufen und Anträge digital einzureichen. Inzwischen bieten sie sogar Smartphone-Apps, die ein gesundes Essverhalten oder regelmäßige Bewegung fördern – und damit die Gesundheit der Versicherten. Einen Schritt weiter gehen Projekte, bei denen KI-gestützte Systeme Sensordaten zu Körperfunktionen wie Atmung, Puls, Blutdruck, Insulinproduktion oder auch Augeninnendruck überwachen und Anomalien erkennen.

Je nach Art und Konfiguration können sie darüber hinaus einen Arztbesuch vorschlagen, gleich einen Termin vereinbaren oder einen Notarzt rufen. Die Diagnosen stellen weiterhin die Ärztinnen und Ärzte. Doch die digitale Unterstützung der frühzeitigen Erkennung von Anomalien kann Medizinern helfen, mehr Leben zu retten.

Dass die dazu benötigten Daten besonderen Schutz benötigen, ist klar. Wichtig in diesem Zusammenhang: Auch medizinische Daten in anonymisierter Form könnten die medizinische Forschung in Zukunft deutlich schneller voranbringen. Während heute für jede Studie separat Daten generiert werden müssen, was viel Zeit und Geld kostet, könnten künftig bereits vorliegende aktuelle Daten aus dem ambulanten und stationären Medizinbetrieb automatisch anonymisiert bereitgestellt werden. So entsteht viel schneller eine belastbare Datenbasis, wie man sie etwa für eine Impfempfehlung benötigt.

Predictive Maintenance sichert Lieferketten im Hafen

Mehr als vier Millionen Standardcontainer wurden 2020 im Duisburger Hafen verladen. Die dafür eingesetzten Kräne sind mit massiven Bremsen ausgestattet, damit die Anlagen auch unter Last immer punktgenau und sicher arbeiten. Die Wartung der Bremsen erfolgt bislang rein zeitbasiert. Mit dem Effekt, dass so mancher Bremsbelag ausgetauscht wird, obwohl man ihn noch weiter nutzen könnte.

Um künftig die Ressourcen noch besser zu nutzen, Standzeiten für Wartungszwecke zu reduzieren und gleichzeitig höchste Sicherheitsstandards zu wahren, erhält die nächste Generation Bremsen eine Sensorik, die unter anderem meldet, welche Teile wie verschleifen. Das macht Reparaturen und Wartungstermine nach tatsächlichem Bedarf planbar und sichert die

Unternehmen müssen Daten austauschen, um Kunden zu halten und neue dazu zu gewinnen.

Leistungsfähigkeit der Lieferketten. Denkbar ist, dass die Sensordaten künftig mit Hilfe eines Datenraums verarbeitet werden, sodass Hersteller, Benutzer und Wartungspartner des Herstellers ihre Aufgaben besser erfüllen können.

Grenzüberschreitender Nutzen im International Data Space

Dahinter steht das Konzept des Industrial Data Space. Dies legt unter anderem fest, dass der Hersteller einer Maschine Daten von ihrer Nutzung bekommen sollte, damit er zum Beispiel rechtzeitig auf Wartungsbedarf hinweisen kann. In der Praxis bestimmt immer das Ökosystem, in dem eine Anlage eingesetzt wird, über den Umgang mit den Daten, die dabei generiert werden. Dazu braucht es so genannte International Data Spaces – nicht nur im Industriebereich, sondern auch in der Medizin, in der Mobilität und überall dort, wo Daten anfallen und als Rohstoff genutzt werden. Wie diese Datenräume gestaltet werden, ist immer Sache der Beteiligten und somit schwer allgemein zu beantworten. Sicher ist jedoch, dass es sich auf Dauer wohl keine Organisation leisten kann, auf den wirtschaftlichen Nutzen des Austauschs von Daten zu verzichten. ■



Thomas Feld

Thomas Feld ist Vice President Data Economics bei Materna. Als Innovator und Architekt für datengetriebene Geschäftsmodelle, Prozesse und Dienstleistungen auf Basis von KI und Big Data entwickelt sein Bereich neue Lösungen für alle Bereiche des öffentlichen Sektors.

Kontakt

thomas.feld@materna.de
www.materna.de

Kurz und Bündig

Datengetriebene Anwendungen für souveräne Datenökosysteme sind bereits heute in verschiedenen Bereichen realisierbar, beispielsweise in den Bereichen öffentliche Verwaltung, Gesundheitswesen, Logistik und Mobilität. In der Perspektive schafft GAIA-X die Möglichkeit der sektorübergreifenden Entwicklung von Advanced Smart Services im Sinne einer Daseinsvorsorge 4.0. Organisationen sollten den Einstieg in die Datenökonomie der Zukunft nicht verpassen.

Feierliche Eröffnung des Center for Digital GreenTech

Lisa Christl, August-Wilhelm Scheer Institut

Das neue Center for Digital GreenTech des August-Wilhelm Scheer Instituts am Standort der Technischen Universität (TU) Clausthal ist am 15.11.2021 feierlich eröffnet worden. Das Innovationszentrum arbeitet an den Herausforderungen einer digitalen Kreislaufwirtschaft (Circular Economy). Der Klimawandel, der Rohstoffmangel und der Rückgang der Biodiversität sind klare Argumente für die Notwendigkeit einer Kreislaufwirtschaft. Gerade digitale Innovationen können dabei Nachhaltigkeit maßgeblich fördern. Das niedersächsische Ministerium für Wissenschaft und Kultur unterstützt das Vorhaben mit einem Fördervolumen von 2 Mio. EUR.

Das gemeinnützige August-Wilhelm Scheer Institut für digitale Produkte und Prozesse mit Sitz in Saarbrücken hat am Montag, dem 15. November 2021, erstmalig einen neuen Standort, das Center for Digital GreenTech, in Niedersachsen eröffnet. Schwerpunkte des neuen Innovationszentrums sind Digitalisierungsvorhaben, die Nachhaltigkeit und ökologischen Wandel ermöglichen. Zusammen mit der TU Clausthal wird künftig fächer- und branchenübergreifend an systemischen Ansätzen für die Schwerpunktthemen Smart Circular Economy, Smart Energy und Smart Water Cycles gearbeitet. Beide Partner verfolgen dabei einen interdisziplinären Ansatz. Bei dem Vorhaben kommt der Digitalisierung eine besondere Bedeutung zu, denn die Transformation industrieller Prozesse von einer linearen hin zu einer zirkularen Wirtschaft kann nur mit der Digitalisierung gelingen.

„Fraglos gehört es zu den großen gesellschaftlichen Herausforderungen, unsere Wirtschaft nachhaltig zu gestalten. Hierzu zählt unter anderem der sparsame Umgang mit endlichen Ressourcen und deren intelligente Wiederverwendung. Aktuell erleben wir, welche wirtschaftlichen Auswirkungen Rohstoffknappheit haben kann. Daher ist es im Interesse unseres Landes, gemeinsam mit dem August-Wilhelm Scheer Institut und aufbauend auf den Forschungsstärken der TU Clausthal hier Innovationsimpulse zu setzen, die unserer Wirtschaft und Gesellschaft zu Gute kommen“, so

Björn Thümmler, Wissenschaftsminister des Landes Niedersachsen.

Ein wichtiger Ansatz ist in diesem Zusammenhang die Kreislaufwirtschaft. „Wir brauchen einen grundsätzlichen Paradigmenwechsel: vom Rohstoffende zur Rohstoffwende. Nur so können auf ökologischen, ökonomischen und sozialen Erfolgen die Grundsteine für eine nachhaltige Gesellschaft gelegt werden. Möglich wird das durch eine umfassende digitale Transformation“, sagt Prof. Dr. August-Wilhelm Scheer, Gründer und Geschäftsführer des August-Wilhelm Scheer Instituts.

Dr. Dirk Werth, Geschäftsführer und wissenschaftlicher Direktor des August-Wilhelm Scheer Instituts, beschreibt: „Das Ziel des August-Wilhelm Scheer Instituts ist es, Forschung auf die Straße zu bringen. Damit das gelingt, schlagen wir die Brücke zwischen Wissenschaft und Wirtschaft. Mit unseren interdisziplinären Arbeiten an digitalen Innovationen verfolgen wir einen verwertungsorientierten Forschungsansatz, der den Mittelstand und auch Start-ups in die Lage versetzt, neue Produkte und Dienstleistungen zu entwickeln und marktfähig zu machen. Unsere Erfahrungen und Erkenntnisse in der Kombination von Digitalisierung und Nachhaltigkeit werden wir in Niedersachsen im Center for Digital GreenTech fokussiert nutzen und in enger Kooperation mit der TU Clausthal vertiefen.“

„Die TU Clausthal hat sich zum Ziel gesetzt, im Jahr 2025 weltweit für interdisziplinäre



Abbildung 1: Enthüllung des Logos des Center for Digital GreenTech. Von links nach rechts: Prof. Dr. Andreas Rausch (TU Clausthal), Prof. Dr. Joachim Schachtner (TU Clausthal), Björn Thümler (Wissenschaftsminister Niedersachsen), Prof. Dr. August-Wilhelm Scheer, Dr. Dirk Werth (August-Wilhelm Scheer Institut)



Lisa Christl

Lisa Christl ist seit Januar 2020 Communication Professional am August-Wilhelm Scheer Institut. Sie ist verantwortlich für die Redaktion und Produktion der IM+io und Pressesprecherin des Instituts.

Kontakt

www.aws-institut.de

Forschung und Lehre sowie für fachübergreifenden Transfer im Feld der Circular Economy zu stehen. Prof. Dr. Joachim Schachtner, Präsident der Technischen Universität Clausthal, unterstreicht die Dimension des Leitthemas: „Im wissenschaftlichen Profil unserer Universität umfasst die Circular Economy neben der klassischen Kreislaufwirtschaft (Circular Materials) die erneuerbaren Energien (Circular Energy) und – ganz wichtig – die digitale Steuerung des Gesamtsystems (Digital Transformation of Circular Economy). Gemeinsam mit dem August-Wilhelm Scheer Institut werden wir die Circular Economy durch Forschungsprojekte auf dem Gebiet der digitalen Transformation und durch ein innovatives Reallabor sichtbar nach vorne bringen. Wir wollen damit in Zeiten des Klimawandels zu einem Umdenken in Wirtschaft, Politik und Bevölkerung beitragen und helfen, eine nachhaltige Gesellschaft von morgen zu entwickeln.“

Damit die ambitionierten und zukunftsweisenden Vorhaben möglichst schnell umgesetzt werden können, soll gleich zu Beginn ein tatkräftiges und interdisziplinäres Team für das Center for Digital GreenTech gebildet werden. Dieses soll dann heute schon an den Herausforderungen von morgen arbeiten.

Die in der Aula Academica der TU Clausthal unter Corona-Auflagen (2-G) stattfindende

Eröffnungsveranstaltung wurde von 70 Personen aus Wissenschaft und Wirtschaft sowie der Politik besucht. Neben Reden der Geschäftsführer des August-Wilhelm Scheer Instituts, des Präsidenten der TU Clausthal und des Wissenschaftsministers, wurden in einer Podiumsdiskussion Ziele des und Ansprüche an das Center for Digital GreenTech diskutiert. Neben je zwei Vertretern der TU und des Digitalisierungsinstituts nahmen an der Diskussion Tristan Niewisch und Eva-Christin Ronkainen-Kolb, zwei Unternehmer aus der Region, teil. ■

Kurz und Bündig

Das August-Wilhelm Scheer Institut hat seinen ersten neuen Standort, – das neue „Center for Digital Green Tech“ – eröffnet. Das neue Innovationszentrum wird sich ab sofort mit den Herausforderungen einer digitalen Kreislaufwirtschaft beschäftigen. Bei der feierlichen Eröffnung am 15.11.2021 waren neben dem Gründer und Geschäftsführer Prof. Dr. August-Wilhelm Scheer auch der niedersächsische Minister für Wissenschaft und Kultur Björn Thümler, Regional- und Bundespolitiker sowie Vertreter aus Wissenschaft und Wirtschaft vor Ort.

East Side Fab

Wo Innovationen beschleunigt werden

Luisa Margies, East Side Fab e.V.



Abbildung 1: Der erste Cybersecurity Day mit Anna Lawera (East Side Fab), Stephan Neumann (SaarLB), Mana Mojaddar (htw saar) und Sabine Betzholtz-Schlüter (saaris) (v.l.). © Cuvée – Die Werbewinzer

„Innovation ist der mehrstufige Prozess, bei dem Organisationen Ideen in neue Produkte, Dienstleistungen oder Prozesse umwandeln, um voranzukommen, im Wettbewerb zu bestehen und sich erfolgreich auf ihrem Markt zu differenzieren“ – dies ist eine von vielen Definitionen von Innovation, die den Auftrag des East Side Fab passend beschreibt.

Das als Verein organisierte East Side Fab mit Sitz im Saarbrücker Osten führt Unternehmen aus den unterschiedlichsten Branchen mit Beratern und Wirtschaftsförderern sowie Vertretern aus Hochschulen, universitätsnahen Forschungseinrichtungen und Banken zusammen. „Wir wollen Brücken bauen und praxisorientiert an interdisziplinären Projekten, neuartigen Produkten und vor allem an Lösungen für die Zukunft arbeiten“, sagt der Vereinsvorsitzende Johannes Hauck, im Hauptberuf Strategie des Blieskasteler Elektrotechnik-Konzerns Hager.

Er weiß, dass viele saarländische Unternehmen aus diversen Branchen darüber nachdenken, die kommenden Herausforderungen – wie zum Beispiel die Digitalisierung der Geschäftsprozesse oder den Fachkräftemangel – „nicht mehr allein und mit Bordmitteln zu bewältigen, sondern die Probleme zusammen mit anderen Akteuren anzugehen.“ Mit einem lebendigen Netzwerk aus Wirtschaft und Wissenschaft sowie mittels der konsequent

eingesetzten Methoden „Open Innovation“ und „Co-Creation“ und digitalen Formaten fördert das East Side Fab den offenen Gedankenaustausch und die Projektbegleitung. Die Initiative kam von den Unternehmen. „Uns eint die Neugier, gemeinsam Neues auszuprobieren“, sagt Hauck. Als Starthilfe steuert das saarländische Wirtschaftsministerium 1,6 Millionen Euro für die ersten drei Jahre bei. Darüber hinaus finanziert sich der Verein aus den Beiträgen seiner Mitglieder. Deren Zahl ist seit der Gründung des Vereins im Oktober 2019 von sieben auf 31 angewachsen.

Beteiligt sind unter anderen Forschungseinrichtungen wie das August-Wilhelm Scheer Institut für digitale Produkte und Prozesse, das CISPA – Helmholtz-Zentrum für Informationssicherheit und das DFKI. Namhafte saarländische Industriebetriebe wie Hager, thyssenkrupp Automotive Body Solutions, Villeroy & Boch und die Baugruppe OBG oder der Messgeräte-Hersteller ZENNER International und auch die Landeshauptstadt Saarbrücken sind ebenfalls mit dabei. Auch Startups und Mittelständler wie der Gleitschirmhersteller Paratec, die Planbar Ingenieurgesellschaft, die Werbeagentur m&r Kreativ und YUNIQ aus Luxemburg, die UX-Entwickler Shapefield oder die Firmenholding inter.services haben die Vorteile des gemeinsamen Arbeitens und Denkens entdeckt.

Der Strom- und Energiesektor wird repräsentiert durch co.met, Elektro Bartruff, die Landesinnung der Elektrohandwerke, Netzwerke Saarlouis und VSE.

Aus dem Hochschulbereich sind die htw saar mit dem FITT – Institut für Technologietransfer an der Hochschule für Technik und Wirtschaft des Saarlandes sowie das K8 Institut mit von der Partie, aber auch Dock 11, die Plattform der Kreativbranche. Die Weiterbildungssparte ist vertreten durch das Festo Lernzentrum Saar, das Unternehmen b+p Beratung und Personal, die Startups SaKoWa, Knowledge Symphony und KRS Solutions im Bereich Simulationstechnologie sowie die Rechtskanzleien DURY und reuschlaw, die sich – am Puls der Zeit – u.a. im Kontext des Vereins mit Themen wie Datenschutz und Cybersicherheit befassen. Den Bankensektor repräsentiert die Finanzgruppe Sparkassenverband Saar.

Gemeinsam mit dem August-Wilhelm Scheer Institut für digitale Produkte und Prozesse sind schon einige Workshops und Events durchgeführt worden. Durch die Kollaboration ist weiterhin ein konkretes Projekt entstanden: Die Entwicklung einer virtuellen Plattform im Themenfeld digitaler Zwillinge. Dahinter verbirgt sich ein 3D-Modell, das ein reales Objekt virtuell bis ins letzte Detail abbildet. Das kann beispielsweise die Karosserie eines neuen Automodells sein, aber auch ein Bürohaus, das zwar schon geplant, aber noch nicht gebaut wurde. Alle technischen Informationen werden bei digitalen Zwillingen auf einer Datenbank detailliert hinterlegt und von den Projektbeteiligten ständig aktualisiert. Doch was unterscheidet den digitalen Zwilling einer Autokarosserie von dem eines komplexen Gebäudes, das voller Technik steckt? Und können beide Branchen voneinander lernen? Bei diesem Projekt wirken die Hochschule für Technik und Wirtschaft des Saarlandes, der Auto-Prototypenentwickler thyssenkrupp Automotive Body Solutions und weitere Beteiligte wie KRS Solutions mit.

Ein weiteres Innovationsprojekt, welches bereits gestartet ist, ist ieMETaS (intelligent e-Mobility, Energy & IoT aus dem Saarland). In einer Zeit, in der die Elektromobilität immer mehr an Relevanz gewinnt, müssen die Rahmenbedingungen für die wachsende Anzahl an Elektrofahrzeugen geschaffen werden. Die Unternehmen co.met, GP Joule Connect, Hager, IZES und ZENNER International sowie die htw saar haben sich deshalb in einem Projekt

zusammengefunden. Das Projektteam macht sich die Umsetzung des Last- und Energiemanagements für Ladeinfrastrukturen und der dezentralen Energieerzeugung zur Aufgabe. Hierbei werden insbesondere aktuelle energiewirtschaftliche und regulatorische Einflüsse berücksichtigt. Die zukünftigen Kommunikations- und Wertschöpfungsketten im Prozess werden hier ebenfalls demonstriert und getestet. Das Projektziel: Die exemplarische Realisierung einer zukunftskonformen Ladeinfrastruktur mit der angeschlossenen Back-End-Struktur für den halb-öffentlichen Raum.

„Unsere Tür steht jedem offen, der aktiv einen Kulturwandel in der eigenen Organisation vorantreiben und Innovationen zu nachhaltigen Erfolgen machen möchte“, sagt die Geschäftsführerin des East Side Fab Anna Lawera. „Jeder kann bei uns Mitglied werden und seine eigenen Bedarfe einbringen. Wir sind ein Ort von Unternehmen für Unternehmen und setzen auf die Zusammenarbeit mit Forschung und Wissenschaft – auch außerhalb des Saarlands, so wie auch viele unserer Mitglieder auf der ganzen Welt unterwegs sind.“ Torsten Schunk, Head of Competence Center bei thyssenkrupp Automotive Body Solutions, Vertreter des Vorstands und Schatzmeister des Vereins, betont dabei vor allem, dass „die Idee des East Side Fab als Innovationsbeschleuniger für Unternehmen aufgeht und Kooperationen zwischen Wirtschaft und Wissenschaft deutlich an Interesse gewinnen“. ■



Luisa Margies

Luisa Margies ist verantwortlich für Marketing und Kommunikation im East Side Fab e.V. Sie bringt praktische Expertise aus unterschiedlichen Branchen wie IT, Handel und Eventmanagement mit und setzt dabei den Fokus auf den Transfer in die digitale Welt. Studiert hat sie an der htw saar Marketing Science. Ihr weiteren Aufgabenschwerpunkte sind unter anderem Diversity und Nachhaltigkeit.

Kontakt

info@eastsidefab.de
www.eastsidefab.de

Kurz und Bündig

Das East Side Fab ist eine Initiative von Unternehmen für Unternehmen, die sich vorgenommen haben, „aus Unterschieden, gemeinsam Innovation zu machen“. Gefördert durch das saarländische Ministerium für Wirtschaft, Arbeit, Energie und Verkehr wurden ein Open Space und eine Innovation Community geschaffen.

Hier finden regelmäßig Workshops und andere Events statt, bei denen sich Gründerteams, Konzernchefs, Forschung und Mittelständler austauschen und voneinander lernen können.

Vorschau auf Heft 1 | März 2022

Digital GreenTech Vom drohenden Rohstoffende zur wichtigen Rohstoffwende



Impressum

IM+io – Best & Next Practices aus Digitalisierung, Management und Wissenschaft
36. Jahrgang, Heft 4, 2021
ISSN: 1616-1017

Herausgeber

Prof. Dr. Dr. h.c. mult. August-Wilhelm Scheer
Universität des Saarlandes, Scheer Group, Saarbrücken
Prof. Dr. Paul Schönsleben, ETH Zürich (Stellvertreter)

Verlag

August-Wilhelm Scheer Institut für digitale Produkte und Prozesse gGmbH
Uni-Campus Nord
66123 Saarbrücken/Germany
Tel.: +49 681 96777-0
info@aws-institut.de
www.aws-institut.de

Geschäftsführung

Prof. Dr. Dr. h.c. mult. August-Wilhelm Scheer, Dr. Dirk Werth

Herausgeberbeirat der IM+io

Vertreter Wissenschaft
Prof. Dr. Michael Backes, Backes SRT/Universität des Saarlandes, Saarbrücken | Prof. Dr. Dr. h.c. mult. Péter Horváth, Horváth AG/Universität Stuttgart | Prof. Dr. Christoph Igel, DFKI, Berlin | Prof. Dr. Helmut Krcmar, TU München | Prof. Dr. Georg von Krogh, ETH Zürich | Prof. Dr. Peter Loos, Universität des Saarlandes/DFKI,

Saarbrücken | Prof. Dr. Wolfgang Maaß, Universität des Saarlandes | Prof. Dr. Dr. h.c. Dieter Rombach, Fraunhofer-Institut IESE, Kaiserslautern | Prof. Dr. Günther Schuh, RWTH Aachen | Prof. Dr. Hans-Gerd Servatius, Universität Stuttgart | Prof. Dr. Wilfried Sihm, Fraunhofer Austria Research GmbH, Wien | Prof. Dr. Oliver Thomas, Universität Osnabrück | Prof. Dr. Dr. Hugo Tschirky, ETH Zürich | Prof. Dr. Florian von Wangenheim, ETH Zürich | Prof. Dr. Dr. h.c. Walther Ch. Zimmerli, BTU Cottbus

Vertreter Wirtschaft

Mario Baldi, Scheer Group, Saarbrücken | Dr. Fabian Dömer, Arthur D. Little Int. Inc., Wiesbaden | Dr. Thomas M. Fischer, avantum consult AG, Düsseldorf | Dr. Gerd Große, GFFT e.V., Bad Vilbel | Britta Hilt, IS Predict GmbH, Saarbrücken | Dr. Rainer Minz, The Boston Consulting Group GmbH, Köln | Rolf Scheuch, OPITZ CONSULTING GmbH, Gummersbach

Chefredaktion (verantwortlich)

Dr. Dirk Werth
dirk.werth@im-io.de

Redaktion

Lisa Christl (Chefin vom Dienst)
lisa.christl@aws-institut.de
Irmhild Plaetrich
(Redaktion - Innovation Review)
irmhild.plaetrich@im-io.de
Sarah Materna
(Redaktion Schwerpunkt)
sarah.materna@im-io.de

Norbert Eder

(Redaktion Schwerpunkt)
norbert.eder@im-io.de

Laura Geßner (Redaktions- und Produktionsassistentz)
laura.gessner@aws-institut.de

Fabian Buß (Redaktions- und Produktionsassistentz)
fabian.buss@aws-institut.de

Vincent Meakins (Reaktions- und Produktionsassistentz)
vincent.meakins@aws-institut.de

Erscheinungsweise

vierteljährlich, plus ggf. eine kostenpflichtige Sonderausgabe

Abonnement

Jahresabonnement Deutschland und Österreich €39,- | für Studierende gegen Vorlage einer Bescheinigung € 29,- (D) jeweils inkl. MwSt. und Versandkosten. Einzelheft €9,80 zzgl. Versandkosten und Nachnahmegebühr. Eine kostenpflichtige Sonderausgabe wird Abonnenten gegen gesonderte Rechnung automatisch geliefert. Eine Abnahmeverpflichtung besteht nicht. Eine Rücksendung der Sonderausgaben an den Verlag ist erforderlich. Das Abonnement kann innerhalb von 14 Tagen nach Erhalt des ersten Heftes schriftlich widerrufen werden. Die Vertragslaufzeit beträgt 12 Monate. Das Abonnement verlängert sich automatisch um ein weiteres Jahr, wenn 4 Wochen vor Ende der 12-Monats-Laufzeit keine schriftliche Kündigung

seitens des Abonnenten erfolgt. Im Falle höherer Gewalt besteht kein Anspruch auf Lieferung oder auf Rückerstattung der Abonnementgebühr. Abo-Bestellungen nimmt das AWS-Institut schriftlich oder via Website www.im-io.de oder über den Buchhandel entgegen.

Anzeigen

Es gilt die Anzeigenpreisliste von 2018.

Lisa Christl (Chefin vom Dienst)
lisa.christl@aws-institut.de
Tel.: +49 162 2677745

Layout/Satz

August-Wilhelm Scheer Institut
Lisa Christl

Druck

reha GmbH
Dudweilerstraße 72
66111 Saarbrücken

Lektorat

Sonja Colling-Bost
Jürgen Bost

Rechte

Namentlich gekennzeichnete Beiträge stellen nicht unbedingt die Meinung der Redaktion dar. Für unverlangt eingesendete Manuskripte wird keine Gewähr übernommen. Die Zeitschrift und alle in ihr enthaltenen Beiträge und Abbildungen sind urheberrechtlich geschützt. Kein Teil dieser Publikationen darf ohne ausdrückliche Genehmigung des Verlags in

irgendeiner Form reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden. Der Autor ist damit einverstanden, dass sein Beitrag in der Printversion der Zeitschrift IM+io erscheinen darf. Der Verlag ist darüber hinaus berechtigt, den Beitrag komplett oder in Teilen im Original oder in Übersetzung, insbesondere auch zu Werbezwecken, online (z.B. im Internet) oder offline (z.B. in Jahressbänden) zu verbreiten bzw. durch Lizenznehmer verbreiten zu lassen.



www.rehagmbh.de