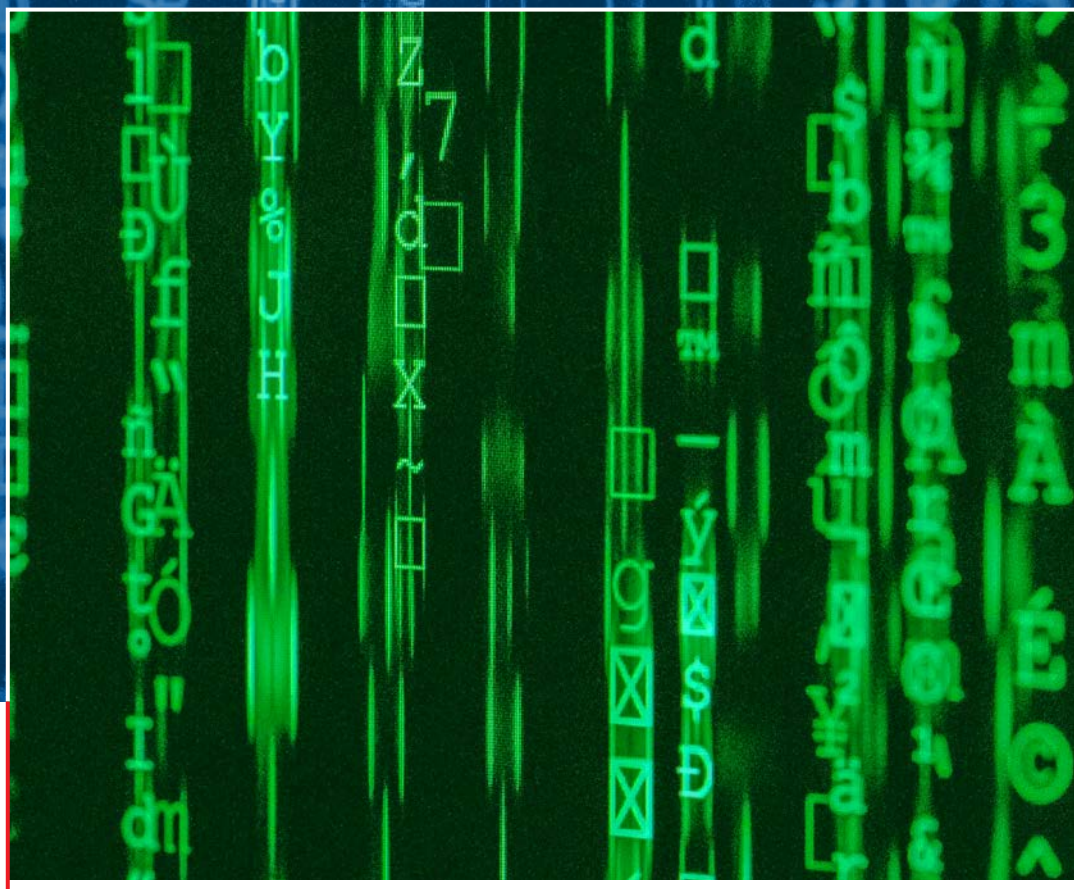


SCHRIFTENREIHE
INNERE
SICHERHEIT
3

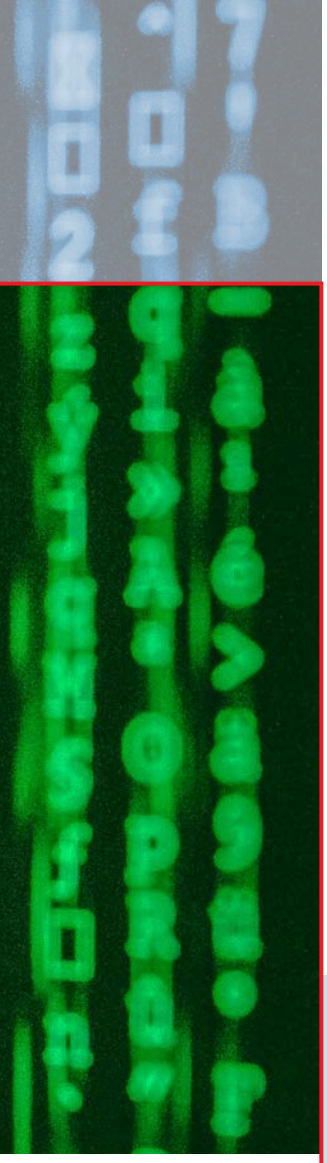
Katrin Kubica, Florian Schumacher

»Protect me from what I want«[1]

Cyber-Sicherheit gestalten – Verbraucher_innen schützen

forum INNERE SICHERHEIT

FRIEDRICH EBERT STIFTUNG
Forum Berlin



Die Schriftenreihe »Innere Sicherheit« wird in loser Folge vom Forum Berlin der Friedrich-Ebert-Stiftung herausgegeben. Expertinnen und Experten aus Politik, Zivilgesellschaft, Wissenschaft und Verwaltung beleuchten darin aktuelle Entwicklungen und Herausforderungen der inneren Sicherheit und stellen Lösungsansätze vor.

Über die Autor_innen

Katrin Kubica ist Referentin im Referat Strategien und neue Ansätze der Informationssicherheit beim Bundesamt für Sicherheit in der Informationstechnik (BSI).

Florian Schumacher ist Leiter der Projektgruppe Digitaler Verbraucherschutz beim Bundesamt für Sicherheit in der Informationstechnik (BSI).

Kernthesen auf einen Blick

Cyber-Sicherheit ist eine Bedingung für eine erfolgreiche Digitalisierung. Primäres Ziel sollte sein, den Dreiklang von IT-Sicherheit – Vertraulichkeit, Integrität und Verfügbarkeit – unter Berücksichtigung sozialer, kultureller, politischer und rechtlicher Dimensionen zu gewährleisten.

Um die Potentiale der Digitalisierung zu nutzen und den Risiken zu begegnen, besteht insbesondere auf drei Feldern Handlungsbedarf:

1. Die Investitionen in Cyber-Sicherheit müssen erhöht sowie staatliche Akteure mit den erforderlichen Befugnissen und Ressourcen ausgestattet werden.
2. Die IT-Sicherheit von Unternehmen muss gestärkt und Hersteller bzw. Dienstleister müssen in die Pflicht genommen werden, die IT-Sicherheit ihrer Produkte zu gewährleisten.
3. Das Ziel, das Bewusstsein und die Beurteilungsfähigkeit für die Risiken digitaler Anwendungen zu steigern, muss weiter verfolgt werden.

Durch die fortschreitende Digitalisierung erweitert sich der Aufgabenbereich des Verbraucherschutzes um das Thema Cyber-Sicherheit. Besondere Herausforderungen sind dabei die rasante Technologieentwicklung und die hohe Komplexität der globalisierten Märkte in diesem Bereich. Die zunehmende Vernetzung und Interaktion von Produkten erfordert dabei die Sicherheit jedes einzelnen Produktes, nicht nur im Auslieferungszustand, sondern auch über den Produktlebenszyklus hinweg. Daher werden konkrete Instrumente zur Bewertung der Sicherheit von Angeboten am Markt benötigt.

Wir leben in einer Welt, in der das Wort »smart« aus dem Alltag kaum wegzudenken ist: Smartphone, Smart Home, Smart Cities, Smart Meter. Doch ist das neue »smart« wirklich so smart, im Sinne von schlau und sicher?

Sicher ist nur: Die Digitalisierung betrifft unser Arbeitsleben und unsere Freizeitgestaltung, unsere Kommunikation und ganz generell unser Zusammenleben und Miteinander. Sie bietet ein enormes Potential, wobei vieles noch gar nicht absehbar und manches nicht einmal denkbar ist.

Das Vertrauen in die Funktionsfähigkeit etablierter Systeme und gesellschaftlicher Strukturen, der Schutz der Privatsphäre, das Verständnis von analogen und digitalen Prozessen, all das ist Funktionsvoraussetzung für das Zusammenleben in unserem Gemeinwesen auch und gerade in einem solch gewaltigen Veränderungsprozess. Um die Digitalisierung unserer Gesellschaft zukunftsfähig und sicher zu gestalten, müssen wir Informationssicherheit von Beginn an mitdenken: sei es bei der Digitalisierung unseres Verbraucheralltags, bei Prozessen in der staatlichen Verwaltung oder in der Wirtschaft.

Cyber-Sicherheit ist nicht alles – aber ohne Cyber-Sicherheit ist alles nichts

Cyber-Sicherheit ist Voraussetzung, Grundlage und Bedingung *sine qua non* für eine erfolgreiche Digitalisierung. Nicht nur in Deutschland sondern weltweit, denn: »Innere und äußere Sicherheit fallen in wenigen Bereichen so eng zusammen wie im Cyberraum.«[2]

Den Chancen der Digitalisierung stehen potentielle Gefahren gegenüber: Die Anzahl und Qualität der Cyber-Angriffe auf staatliche und zivile Ziele ist signifikant, wobei auch Kritische Infrastrukturen[3] verstärkt im Fokus der Angreifer sind. Die Weiterentwicklung von Schadprogrammen mit mehreren hunderttausend neuen Varianten pro Tag, neuen Vektoren, die steigende Betroffenheit durch ein »Smart-Everything« sowie die zunehmende Angriffsintensität verdeutlichen die Verletzlichkeit von IT-Systemen und digitalen Infrastrukturen in einer zunehmend vernetzen Welt[4].

Konkrete Herausforderungen für Staat, Wirtschaft und Gesellschaft sind beispielsweise:

- Cyber-Angriffe auf Staaten und deren Infrastrukturen
- Diebstahl und Missbrauch persönlicher Daten bis hin zu Erpressung und Lösegeldforderung
- Angriffe auf Kritische Infrastrukturen, die schwerwiegende Folgen für die Zivilbevölkerung und die Aufrechterhaltung der sozialen Ordnung haben können
- (Wirtschafts-) Spionage
- Beeinflussung der öffentlichen Meinung wie der Steuerung von Diskussionen in sozialen Netzwerken bis hin zur Manipulation von Informationen auf Nachrichtenportalen.

Die Liste der Herausforderungen und Gefahren ließe sich noch weiter fortsetzen. Jedoch ebenso die Liste der Möglichkeiten und Potentiale, die die fortschreitende Digitalisierung weltweit ermöglicht. Es darf eben nicht so sein, dass die Veränderungen, die die Digitalisierung mit sich bringt, »[…] entweder als Weltrettung gefeiert oder als Weltuntergang verdammt«[5] werden. Zwischen Schwarz und Weiß, zwischen Gut und Böse ist bekanntlich viel Luft.

Um die Potentiale der Digitalisierung zu nutzen und den Risiken zu begegnen, besteht insbesondere auf drei Feldern Handlungsbedarf: Erstens die Investitionen in Cyber-Sicherheit müssen erhöht sowie staatliche Akteure mit den erforderlichen Befugnissen und Ressourcen ausgestattet werden; zweitens die IT-Sicherheit von Unternehmen muss gestärkt und Hersteller bzw. Dienstleister müssen in die Pflicht genommen werden, die IT-Sicherheit von Produkten zu gewährleisten; und drittens muss das Ziel weiter verfolgt werden, das Bewusstsein und die Beurteilungsfähigkeit für die Risiken digitaler Anwendungen zu steigern.

Cyber-Sicherheit als gesamtgesellschaftliche Aufgabe

Kein Akteur allein kann Cyber-Sicherheit gestalten oder gewährleisten: »Die Bedrohungslage im Cyberraum erfordert eine ganzheitliche Betrachtung im Rahmen der Cyber-Sicherheitspolitik. Die Wahrung der Cyber-Sicherheit und -Verteidigung ist somit eine gesamtstaatliche Aufgabe, die gemeinsam zu bewältigen ist.«[6]

Ziel und Anspruch muss sein, den Herausforderungen der Cyber-Sicherheit auf allen Ebenen und gemeinsam zu begegnen: auf europäischer und internationaler Ebene, in Bund, Ländern und Kommunen und selbstverständlich ressortübergreifend in der Zusammenarbeit staatlicher Stellen mit Betreibern Kritischer Infrastrukturen und KMUs sowie mit zivilgesellschaftlichen Akteuren.

Um die Voraussetzungen für das Gelingen der Digitalisierung in Deutschland zu schaffen, sind unterschiedliche und gleichzeitig einander ergänzende Maßnahmen notwendig: sei es die Etablierung eines einheitlichen, qualitativ hohen IT-Sicherheitsniveaus im Bund und in den Ländern, Investitionen im Bereich der digitalen (Weiter-) Bildung, gezielte Fachkräftegewinnung auch für den öffentlichen Dienst, das Gewinnen und Teilen von Informationen z. B. im Rahmen des Nationalen Cyber-Abwehrzentrums, die Umsetzung einer zukunftsfähigen digitalen Infrastruktur sowie die Schaffung einer modernen Verwaltung.

Die immer komplexer werdende Cyber-Sicherheitsarchitektur in Deutschland ist für Außenstehende oftmals schwer zu durchschauen; etliche Ressorts, Akteure, nachgeordnete Behörden und Organisationen schützen und stärken die Cyber-Sicherheit in Deutschland.[7]

Cyber-Sicherheit ist Pflichtaufgabe von Ressorts, Parteien und vielen zivilen Akteuren geworden. Die damit einhergehenden Herausforderungen sind erheblich, angefangen beim Fachkräftemangel bis hin zum Ressourcenmangel. Jede IT-Fachkraft kann nur einmal eingestellt, jeder Euro nur einmal ausgegeben werden.

So wenig die Gestaltung der Digitalisierung eine rein nationale Aufgabe ist, so wenig können der Bund oder die Länder die Cyber-Sicherheit allein gewährleisten. Aus diesem Grund besteht für die Sicherheit der Bundesrepublik Deutschland und ihrer Länder die gemeinsame Verantwortung, durchgehend ein qualitativ hohes, einheitliches und angemessenes Cyber-Sicherheitsniveau sicherzustellen. Als herstellerunabhängiger, technisch kompetenter Dienstleister kann das Bundesamt für Sicherheit in der Informationstechnik (BSI) hierbei eine entscheidende Rolle spielen, ebenso wie bei der Gestaltung neuer Themenfelder. So kommt dem BSI bei der Entwicklung des digitalen Verbraucherschutzes als unabhängige Kompetenzstelle mit rein ziviler Ausrichtung eine wichtige Bedeutung zu.

Cyber-Sicherheit für Verbraucher_innen gestalten …

Durch die fortschreitende Digitalisierung erweitert sich der Aufgabenbereich des Verbraucherschutzes um das Thema Cyber-Sicherheit. Dies ist ein Ausdruck des Wandels in der Bedeutung von Cyber-Sicherheit für die Gesellschaft als Ganzes. Die Bundesregierung trug dem mit dem Koalitionsvertrag aus dem Jahr 2018 Rechnung und schrieb den digitalen Verbraucherschutz als neue Aufgabe dem BSI zu.[8] Nicht nur große Cyber-Sicherheitsvorfälle, wie der Doxing-Fall im Januar 2019, sondern auch das Gefahrenempfinden[9] in der Bevölkerung zeigen die Notwendigkeit des Handelns und der Beschäftigung mit dem neuartigen Feld.

Doch wen oder was gilt es überhaupt zu schützen? Ein adäquater Schutz der Verbraucher_innen erfordert Klarheit über die Zielgruppe. Im öffentlichen Diskurs werden auch in Bezug auf Cyber-Sicherheit dem »Faktor Mensch« eine Vielzahl von Erwartungen entgegengebracht, verbunden mit einem vereinfachenden, homogenen Bild des »mündigen Verbrauchers«. Dabei gilt auch für die Online-Welt, dass dieser nicht existiert und auch nicht existieren kann.[10] Vielmehr sollten Maßnahmen zum Verbraucherschutz differenziert und kontextabhängig konzipiert werden. Wissenschaftlichen Erkenntnissen zufolge verhalten sich Verbraucher_innen je nach Bereich des Konsums bzw. Lebens entweder verletzlich, vertrauend oder verantwortungsvoll.[11] Diese Verhaltensweisen können sich natürlich in Abhängigkeit von Handlungskontext und Lebenslage bei einer Person unterschiedlich ausprägen.[12]

Für eine kontextspezifische und abgestufte Gestaltung von Maßnahmen in der digitalen Welt sind u. a. Alter, Einkommen, Zugang zu digitalen Technologien und Diensten relevante Faktoren sowie bestehende Asymmetrien hinsichtlich Kompetenz und Information zwischen Herstellern, Dienstleistern und letztlich den Verbraucher_innen.[13] Darüber hinaus sind weitere Faktoren, die unser Handeln im digitalen Umfeld bestimmen, noch zu erforschen.

… heute wie morgen eine herausfordernde Aufgabe

Die Rahmenbedingungen für den Verbraucherschutz in Bezug auf Cyber-Sicherheit werden durch Charakteristika der digitalen Welt geprägt. Im Folgenden soll beispielhaft auf drei Aspekte eingegangen werden:

1. **Technologieentwicklung:**
   Neue Geschäftsmodelle und schnelle Innovationszyklen sorgen in kurzer Zeit für neue Produkte und Dienste am Markt, die wiederum die Cyber-Sicherheit und den Verbraucherschutz vor neue Aufgaben stellen. In den nächsten Jahren werden Trends wie Künstliche Intelligenz, 5G, Cloud Computing oder Internet of Things unseren Verbraucheralltag bestimmen und verändern.

2. **Komplexität:**
   Verbraucher_innen bewegen sich in entgrenzten, globalisierten Märkten. Ohne großen Aufwand ist es möglich, physische oder digitale Produkte und Dienste aus anderen Teilen der Welt zu beziehen. Diese zeichnen sich wiederum selbst durch einen hohen Grad an Komplexität aus, sowohl durch Wechselwirkungen von Komponenten und Funktionalitäten sowie einer Vielzahl von beteiligten Akteuren[14].

3. **Schutzinteresse:**
   Die zunehmende Vernetzung und Interaktion von Produkten erfordert die Sicherheit jedes einzelnen Produktes. Jedoch nicht nur im Auslieferungszustand, sondern auch über den gesamten Produktlebenszyklus hinweg. Dabei kann das individuelle Schutzinteresse und das der Gesellschaft divergieren. Steht für das Individuum die Funktionsfähigkeit beispielsweise seines vernetzten Smart Home-Geräts im Vordergrund, so ist für die Gesellschaft wichtig, dass dieses nicht Teil eines Botnetzes ist und Infrastrukturen des öffentlichen Lebens angreifen kann.

Diese drei Elemente zeigen exemplarisch die Herausforderungen für den digitalen Verbraucherschutz. Die Dynamik dieses Bereichs erfordert eine aktive Gestaltung, die Verbraucher_innen auf Risiken vorbereitet und deren Resilienz steigert. Im Sinne des Verbraucherschutzes müssen die passenden Antworten auf die Technologieentwicklungen gefunden werden. Dabei geht es nicht nur darum, den Verbraucher bzw. die Verbraucherin in den Blick zu nehmen und deren Risikobewusstsein zu stärken, sondern es gilt bereits in der Phase der Gestaltung von Technologie, Sicherheit zu einem relevanten Bestandteil zu machen. Hierzu ist der Dialog seitens etablierter Akteure des Verbraucherschutzes sowie des BSI mit Herstellern und Dienstleistern essentiell. In diesem Austausch sollten auch herausfordernde Fragen betrachtet werden, wie die Gewährleistung der Sicherheit über den vollständigen Produktlebenszyklus.

Verbraucherschutz-Akteure müssen mit ihren Kompetenzen sowohl mit der Innovationsgeschwindigkeit und den neu aufkommenden Risiken und Gefahren Schritt halten als auch den Markt überblicken können. Zu diesem Zweck ist eine aktive Beobachtung des Marktes für Verbraucherprodukte und -dienste sowie der sich daraus ergebenden Entwicklungen und Trends unerlässlich.

Weiter müssen Verbraucher_innen über Wahlmöglichkeiten verfügen und in ihrer Beurteilungskompetenz gestärkt werden. Bestehende Informations- und Kompetenzasymmetrien zwischen Verbraucher_innen müssen reduziert und neutrale, vertrauenswürdige Stellen mit ihren Informationsangeboten gestärkt werden. Ferner werden konkrete Instrumente zur Bewertung der Sicherheit von Angeboten am Markt benötigt. Um den gegebenen Aussagen als Verbraucher_in vertrauen zu können, müssen Mindestanforderungen klar definiert und deren Einhaltung überwacht werden. In Situationen der Unsicherheit benötigen Verbraucher_innen Anlaufpunkte, die ihnen mit ihrer Expertise zur Seite stehen und ihre Lösungskompetenz befördern.

Darüber hinaus muss das Bewusstsein geschärft werden, dass ein aktiver Verbraucherschutz in der digitalen Welt auch gesellschaftlichen Interessen dient und einen gesamtgesellschaftlichen Nutzen stiftet. Über den Beitrag zum individuellen Schutz kann auch die öffentliche Sicherheit gesteigert werden.

Zur aktiven Gestaltung des Verbraucherschutzes gehört allerdings auch, in einen Dialog über neue Ansätze zu treten. Auf welche Weise muss der Verbraucherschutz an die Herausforderungen der digitalen Welt angepasst werden? Welcher neuen Ansätze und Instrumente bedarf es? Welche Lernerfahrungen aus anderen Feldern kann man auf den digitalen Verbraucherschutz übertragen? Zur Beantwortung dieser Fragen müssen alle relevanten Akteure aus Staat, Wirtschaft, Wissenschaft und Zivilgesellschaft vernetzt werden. Um die neue Aufgabe des Verbraucherschutzes bewältigen zu können, ist eine konzertierte Anstrengung notwendig, in Kooperation

und Kollaboration etablierter Akteure des Verbraucherschutzes, national wie international.

Lasst uns die Digitalisierung sicher gestalten – und so wie wir sie wollen!

Die mit der Digitalisierung zunehmende Vernetzung aller Lebensbereiche eröffnet den Bürger_innen Chancen, bedeutet aus IT-Sicherheitsperspektive aber auch eine erweiterte Angriffsfläche. Hierbei ist die Gewährleistung von Cyber-Sicherheit eine Bedingung für eine erfolgreiche Digitalisierung. Primäres Ziel sollte dabei sein, den Dreiklang von IT-Sicherheit – Vertraulichkeit, Integrität und Verfügbarkeit – unter Berücksichtigung sozialer, kultureller, politischer und rechtlicher Dimensionen zu gewährleisten.

Derzeit erleben wir eine Gestaltung in geteilter Verantwortung; die Gestaltung der Cyber-Sicherheit in Deutschland sollte jedoch aus einem Guss erfolgen. Ein Nebenher oder – schlimmer – ein Gegeneinander darf es nicht geben. Für alle Beteiligten bleibt es gleichermaßen herausfordernd, in einem solch schnelllebigen Themenfeld mit den aktuellen Entwicklungen Schritt zu halten sowie den Anschluss an Know-how und dessen Anwendung nicht zu verlieren.

Cyber-Sicherheit ist eine gesamtgesellschaftliche Aufgabe und sollte dementsprechend partizipativ gestaltet werden. Dies erfordert eine gemeinsame Anstrengung, um Sicherheit zu garantieren, das Gemeinwohl zu fördern und den Wohlstand in der Bundesrepublik Deutschland zu erhalten. Schließlich sollte es im Interesse aller liegen, die Resilienz der Gesellschaft zu fördern, für Vertrauen in die Sicherheit und einen angemessenen Schutz der Verbraucher_innen zu sorgen. Nur so kann die Digitalisierung in Deutschland erfolgreich gelingen.

ANMERKUNGEN

1 Holzer, Jenny (US-Künstlerin), abgerufen am 01. 08. 2019: https://artsation.com/artists/jenny-holzer, http://artdaily.com/news/1856/-quot-Protect-Me-From-What-I-Want-quot-.

2 Weißbuch der Bundesregierung. Zur Sicherheitspolitik und zur Zukunft der Bundeswehr (2016), S. 38, abgerufen am 02. 08. 2019: https://www.bmvg.de/de/themen/weissbuch.

3 Die Bundesregierung hat Kritische Infrastrukturen wie folgt definiert: Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

4 Die Lageberichte zur IT-Sicherheit des BSI geben einen Überblick über die Bedrohungen Deutschlands im Cyber-Raum. Abgerufen am 05. 08. 2019: https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html.

5 Passig, Kathrin; Scholz, Aleks (2015), Schlamm und Brei und Bits. Warum es die Digitalisierung nicht gibt, abgerufen am 01. 08. 2019: https://www.klett-cotta.de/media/14/mr_2015_11_0075-0081_0075_01_Passig_Scholz_Schlam_Brei_Bits_Digitalisierung.pdf.

6 Weißbuch der Bundesregierung. Zur Sicherheitspolitik und zur Zukunft der Bundeswehr (2016), S. 38, abgerufen am 02. 08. 2019: https://www.bmvg.de/de/themen/weissbuch.

7 Für eine detaillierte und umfangreiche Übersicht sämtlicher Akteure bieten sich die Publikationen der Stiftung Neue Verantwortung an.
Breternitz, Tabea; Herpig, Dr. Sven (2018), Zuständigkeiten und Aufgaben in der deutschen Cyber-Sicherheitspolitik. Eine Übersicht, Stiftung Neue Verantwortung, abgerufen am 02. 08. 2019: https://www.stiftung-nv.de/sites/default/files/cybersicherheitsarchitektur_papier.pdf, https://www.stiftung-nv.de/sites/default/files/cybersicherheitsarchitektur9.pdf.

8 Koalitionsvertrag zwischen CDU, CSU und SPD. 19. Legislaturperiode, S. 44, abgerufen am 02. 08. 2019; https://www.bundesregierung.de/resource/blob/975226/847984/5b8bc23590d4cb2892b31c987ad672b7/2018-03-14-koalitionsvertrag-data.pdf?download=1.

9 82 Prozent der Bürger_innen machen sich Sorgen um die eigene Sicherheit im Internet.
Bundesamt für Sicherheit in der Informationstechnik (BSI); Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) (Hrsg.) (2019, im Erscheinen), Digitalbarometer: Bürgerbefragung zur Cyber-Sicherheit. Erstellt durch Ipsos Public Affairs.

10. Vgl. Kenning, Peter; Wobker, Inga (2013), Ist der »mündige Verbraucher« eine Fiktion?, in: Zeitschrift für Wirtschafts- und Unternehmensethik, 14/2, S. 282–300.

11. Oehler, Andreas; Reisch, Lucia. A. (2016), Verbraucherleitbild: Differenzieren, nicht diskriminieren!, in: SVRV Working Paper Nr. 1, Berlin.

12. Konkretisiert auf die digitale Welt, lässt sich zwischen fünf verschiedenen Nutzertypen unterscheiden: aktiv Kompetente, unbekümmerte Nutzer, zukunftsgläubige Nutzer, ängstliche Wenig-Nutzer, skeptische Laien.
Vgl.: Franzl, Kerstin; Tripp, Volker (2018), Digitale Gesellschaft: smart & sicher – Zusammenfassung der Studienergebnisse, IT-Sicherheit aus Sicht von Nutzer/innen und Expert/innen, Studie im Auftrag des Bundesamts für Sicherheit in der Informationstechnik, abgerufen am 02. 08. 2019: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SuSi_DigitaleGesellschaft/Zusammenfassung_Ergebnisse_SuSi.pdf?__blob=publicationFile&v=3.

13. Vgl. auch: Grugel, Christian (2017), Verbraucherpolitik statt Verbraucherschutz, in: Kenning, Peter; Oehler, Andreas; Reisch, Lucia A.; Grugel, Christian (Hrsg.), Verbraucherwissenschaften. Rahmenbedingungen, Forschungsfelder und Institutionen, Springer Gabler, Wiesbaden, S. 51–66.

14. Bspw. Betriebssystemhersteller, Softwareentwickler, Gerätehersteller

Impressum

© 2020
Friedrich-Ebert-Stiftung, Forum Berlin

VERANTWORTLICH
Jan Niklas Engels, Forum Berlin,
Friedrich-Ebert-Stiftung
Hiroshimastraße 17, 10785 Berlin

LEKTORAT
Gaby Rotthaus, Forum Berlin,
Friedrich-Ebert-Stiftung

LAYOUT/SATZ
Heike Wächter, Punkte + Striche,
Büro für Grafikdesign, Berlin

BILDMATERIAL
© Markus Spiske/unsplash.com, Symbolbild

DRUCK
Druckerei Brandt GmbH, Bonn

ISBN: 978-3-96250-492-2

FRIEDRICH EBERT STIFTUNG
Forum Berlin

Über uns

Die **Friedrich-Ebert-Stiftung** (FES) ist die älteste politische Stiftung Deutschlands. Benannt ist sie nach Friedrich Ebert, dem ersten demokratisch gewählten Reichspräsidenten. Als parteinahe Stiftung orientieren wir unsere Arbeit an den Grundwerten der Sozialen Demokratie: Freiheit, Gerechtigkeit und Solidarität. Als gemeinnützige Institution agieren wir unabhängig und möchten den pluralistischen gesellschaftlichen Dialog zu den politischen Herausforderungen der Gegenwart befördern. Mit unserer Arbeit im In- und Ausland tragen wir dazu bei, dass Menschen an der Gestaltung ihrer Gesellschaften teilhaben und für Soziale Demokratie eintreten. (www.fes.de)

Das **Forum Berlin** ist ein Arbeitsbereich im Haus der Friedrich-Ebert-Stiftung in Berlin-Tiergarten. Unsere Aufgabe besteht in der Organisation politischer Bildung und Kommunikation sowie Politikberatung in den bundespolitischen Arbeitsbereichen. Die Themen unserer Arbeitsbereiche vermitteln wir in Fachtagungen, Kolloquien, Lesungen, Gesprächskreisen, digitalen Debattenforen und Publikationen an die Öffentlichkeit. Unser Bemühen gilt dem demokratischen Diskurs und der Kommunikation zwischen Bürgerinnen und Bürgern, Politik, Wissenschaft und Praxis. (www.fes.de/forum-berlin)

Im **Forum Innere Sicherheit** beschäftigt sich die Friedrich-Ebert-Stiftung mit den aktuellen Herausforderungen und Entwicklungen im Politikbereich »Innere Sicherheit«. Sicherheit ist für alle da und gehört zur Bringschuld des Staates. Mit unseren Angeboten zur politischen Bildung leisten wir einen Beitrag zur Aufklärung und zum Diskurs in diesem komplexen Politikfeld und entwickeln gemeinsam mit Expertinnen und Experten Vorschläge für eine funktionierende und vertrauenswürdige Sicherheitsarchitektur, die den Werten der Sozialen Demokratie verbunden ist. (www.fes.de/forum-berlin/innere-sicherheit)