Loer, Kathrin

Article

Verhaltenswissenschaftlich informierte Politik für mehr Cybersicherheit

Wirtschaftsdienst

Suggested Citation: Loer, Kathrin (2020) : Verhaltenswissenschaftlich informierte Politik für mehr Cybersicherheit, Wirtschaftsdienst, ISSN 1613-978X, Springer, Heidelberg, Vol. 100, Iss. 2, pp. 91-94, https://doi.org/10.1007/s10273-020-2574-x

DOI: 10.1007/s10273-020-2574-x

Ende des vorherigen Zeitgesprächsartikels

Kathrin Loer

Verhaltenswissenschaftlich informierte Politik für mehr Cybersicherheit

Als Medien im Januar 2020 über eine Sicherheitslücke im Betriebssystem Windows berichteten, erklärten sie, dass die „National Security Agency“ (NSA) dieses Risiko entdeckt und das Unternehmen Microsoft darüber informiert habe. In dem Zuge erhielt auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) entsprechende Hinweise, um die deutschen Windows-Nutzer zu warnen.[1]

Im Zusammenhang mit einem solchen situativen Ereignis gelangt das Thema Cybersicherheit für kurze Zeit prominent ins Bewusstsein, erfährt viel Aufmerksamkeit vor allem durch die Verbreitung in den Medien. Allerdings handelt es sich bei Cybersicherheit um ein Dauerthema, das kontinuierliches politisches Handeln dringend erforderlich macht.

1 dpa: Microsoft schließt Windows-Schwachstelle nach NSA-Hinweis, Zeit-Online, 15.1.2020, https://www.zeit.de/news/2020-01/15/microsoft-schliesst-windows-schwachstelle-nach-nsa-hinweis (15.1.2020).

Dr. Kathrin Loer ist Leiterin des Projekts „Instrumente in der Verbraucherpolitik“ an der Fakultät für Kultur- und Sozialwissenschaften der FernUniversität in Hagen.

So stellt sich generell die Frage, mit welchen politischen Maßnahmen der Staat reagieren kann, um mehr Cybersicherheit zu gewährleisten und welche Rolle die Bürger als Verbraucher und Nutzer dabei spielen. Doch nicht nur die Bürger sind gefragt, sondern letztlich geht es auch um die Anbieter digitaler Dienstleistungen, die einerseits Maßnahmen etablieren können, um dem Bürger Schutz zu bieten, andererseits gegebenenfalls selbst bestimmten Schutz durch staatliche Maßnahmen erwarten. Als verbraucherpolitische Ziele im Sinne der Cybersicherheit lässt sich im Hinblick auf die Marktakteure ausmachen, dass diese Regulierung und Schutz benötigen. Für den Verbraucher zielen staatliche Maßnahmen ebenfalls auf Schutz ab, der letztlich aber auch dadurch erreicht werden kann, dass der Verbraucher befähigt wird, sich selbst besser zu schützen. Darüber hinaus müssen staatliche Maßnahmen zur Überwachung, Kontrolle sowie zur strafrechtlichen Verfolgung von Cyberkriminalität etabliert werden.[2]

Cybersicherheit für Verbraucher

Nicht nur Sicherheitslücken in Betriebssystemen, sondern ein komplexes Spektrum an Gefahren entsteht durch die Nutzung digitaler Angebote: Dies betrifft vor allem smarte Lautsprecher, Online-Banking, Cookies, falsche Antivirensoftware, Online-Shopping, Identitätsdiebstahl, Botnetze, Schadprogramme, Spam, künstliche Intelligenz, Hacking, Phishing sowie Kostenfallen und unerwünschte Zugaben bei unterschiedlichen Internetleistungen.[3] Letztlich sorgt die Weiterentwicklung technischen Wissens und digitaler Angebote für kontinuierlichen Handlungsbedarf für alle Beteiligten – für Staat, Marktakteure und Verbraucher. Dabei müsste im Idealfall deren Informationsstand mit der technischen Entwicklung Schritt halten, müsste sich das Verhalten bei der Nutzung der Dienste anpassen, was zumeist mit Aufwand der Nutzer verbunden ist, bestimmte Sicherheitsmaßnahmen zu beachten, auf Angebote zu verzichten, auszuweichen oder technische Einstellungen anzupassen.

Aus politikwissenschaftlicher Perspektive lässt sich vor diesem Hintergrund umreißen, dass sich staatliches Handeln am Tempo der technischen Entwicklung orientieren muss, dass es auf Erwartungen der Bürger (als Verbraucher) stößt, einen gewissen Schutz zu erhalten, und dass es dabei die (unter Umständen mangelnde) Fähigkeit der Verbraucher einkalkulieren muss, wirksame Maßnahmen auch tatsächlich zu nutzen. Gleichzeitig handelt es sich um einen komplexen Adressatenkreis, der nicht nur die Verbraucher, sondern auch Unternehmen sowie internationale Partner umfasst.

Die möglichen politischen Instrumente reichen von staatlicher Regulierung über Ge- und Verbote, ökonomische und soziale Anreize, informative Maßnahmen bis zur Etablierung von Institutionen, Organisation und Bereitstellung von Infrastrukturen. Dies bedeutet konkret, dass staatlicherseits Standards vorgegeben, Informationspflichten eingeführt oder bestimmte Praktiken verboten werden könnten (Ge- und Verbote). Darüber hinaus sollten Standards und Prozesse formuliert (Organisation) und Institutionen geschaffen werden, die wiederum bestimmte Dienstleistungen zur Verfügung stellen, wie beispielsweise das BSI.

In allen Fällen hängt der Einsatz und die Entscheidung für die jeweiligen Maßnahmen davon ab, welche Ressourcen zur Verfügung stehen, welche Institutionen beteiligt sind oder etabliert werden müssen, aber auch wie sich die notwendigen Kompetenzen zwischen Bund und Ländern für die Implementation verteilen – abgesehen davon handelt es sich immer um politische Entscheidungen, auf die sich Interessen, Wertvorstellungen und Überzeugungen derjenigen auswirken, die an der Entscheidung beteiligt sind. Insbesondere wenn es um die Frage nach der Verantwortung geht, dürften politischen Interessen prägend sein: Wie weit reicht die Verantwortung des Einzelnen für seine Sicherheit als Verbraucher, der sich „im Netz“ bewegt und digitale Dienste in Anspruch nimmt? Wie umfassend müssen Marktakteure ihren Kunden ihrerseits Sicherheit bieten und Verantwortung für Schäden übernehmen? Welche Rolle kommt dem Staat zu, um Verbraucher wie Unternehmen in ihren verschiedenen Rollen (selbst als „Verbraucher“, aber auch als Anbieter) zu schützen oder aber Verantwortung zu übertragen?

Unabhängig davon, wie diese Fragen konkret beantwortet werden, spielt stets eine Rolle, wie sich der einzelne Verbraucher verhält. Dabei zeigt der Blick auf die dargestellten politischen Instrumente, dass sie in der Regel einen gut informierten, rational handelnden Akteur voraussetzen.[4] Gerade im Bereich der Instrumente, die im weitesten Sinne für Information sorgen sollen (Bildung, Aufklärung, Informationskampagnen, Label, Zeichen etc.), und auch solcher Instrumente, die eine Organisationsleistung darstellen, trifft diese Voraussetzung zu. Da jedoch in der Realität – und vermutlich erst recht bei der alltäglichen Nutzung digitaler Dienste – sorgfältig abgewogene Ent-

2 Strafrechtliche Maßnahmen gegen Cyberkriminalität bleiben in diesem Beitrag ausgeklammert.

3 Für einen Überblick siehe Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI für Bürger, https://www.bsi-fuer-buerger.de/BSIFB/DE/Home/home_node.html (15.1. 2020).

4 Vgl. auch K. Loer, A. Leipold: Varianten des Nudgings? Verhaltenswissenschaften und ihr Einfluss auf politische Instrumente, in: Vierteljahrshefte zur Wirtschaftsforschung, 1/2018, S. 41-63.

scheidungen auf der Basis umfassender Informationen unwahrscheinlich oder selten sind, müssen andere Perspektiven auf das Verbraucherverhalten eingenommen werden, wenn Instrumente tatsächlich wirksam sein sollen.[5] Der Verbraucher ist eben nicht selbstverständlich oder automatisch Befolger von Ge- und Verboten, kalkulierender, verständiger, informierter oder kooperativer Akteur. Sein Verhalten kann lethargisch, spontan, fehlkalkulierend sein, er handelt eingebettet in soziale Zusammenhänge, zuweilen emotional. Die Verhaltensforschung bietet Erkenntnisse dafür, wie sich die unterschiedlichen politischen Instrumente vor diesem Hintergrund so verändern lassen, um das wahrscheinliche Verhalten oder die verschiedenen Verhaltensdimensionen bestimmter Zielgruppen in unterschiedlichen Situationen zu berücksichtigen und somit die Wirksamkeit der Instrumente zu erhöhen. Staatliche Akteure müssen letztlich einen multidimensionalen Akteur in heterogenen Adressatengruppen berücksichtigen und brauchen dafür externe Kenntnisse.

Neue Optionen für staatliches Handeln: Umbau von Entscheidungsarchitekturen

Die lebhafte Debatte um Verhaltenspolitik lässt sich auch für das Thema Cybersicherheit führen. Letztlich dürften die meisten klug gestalteten Angebote für digitale Dienstleistungen ihrerseits auf der Basis von Erkenntnissen aus den Verhaltenswissenschaften gestaltet sein. Richtet sich der Blick auf staatliche Aktivitäten, können verhaltenswissenschaftliche Erkenntnisse (behavioural insights) zur Gestaltung von politischen Instrumenten eine Rolle spielen. Dies ist deshalb besonders attraktiv, weil durch diese Erkenntnisse der Verbraucher als multidimensionaler Akteur angemessener berücksichtigt wird (vgl. Tabelle 1).

Tabelle 1
Verhaltenswissenschaftliche Expertise in der Politik

Wie wirkt verhaltenswissenschaftliche Expertise?	
Strategien/Aktivitäten	Systematische Analyse des menschlichen Verhaltens (durch Beobachtung/Experimente) führt zu Erkenntnissen, die Instrumente (neuartig) verändern können.
Grenzen: technisch/ wissenschaftlich	Evidenz/Erkenntnisgrenzen der Verhaltenswissenschaften
Grenzen: normativ	Adressierung von System 1 (intransparente Interventionen), Werte, Einstellungen und Überzeugungen der Adressaten
Politische Kosten	Notwendigkeit von (teilweise) unsichtbaren Eingriffen in den Politikprozess

Quelle: eigene Darstellung.

Dabei geht es nicht nur um die Mechanik der Instrumente, sondern schon zuvor um Kenntnisse über die Adressatentypen und -gruppen. Sind diese identifiziert – also z. B. bestimmte Nutzergruppen von Plattformdiensten im Internet – , schließt sich eine Charakterisierung der Adressaten und ihrer Verhaltensmuster an. Erst dann lassen sich Instrumente so verändern, dass sie dem erwarteten (also besonders wahrscheinlichen) Verhalten Rechnung tragen und darauf einwirken können. Dabei kann es sich um verschiedene Formen von Information, auch um Varianten zur Aufklärung und Befähigung handeln.

Im Ergebnis kommt es durch diesen Erkenntnisprozess, also durch Identifikation und Charakterisierung von Adressatengruppen, Ermittlung von Verhaltensmustern und Analyse potenziell wirksamer Einflussfaktoren auf die unterschiedlichen Dimensionen von Verhalten (System 1 und System 2)[6], zum Umbau von Entscheidungsarchitekturen. Bezogen auf die Optionen für politisches Handeln bedeutet dies, dass Instrumente, darunter insbesondere Information und Organisation, basierend auf verhaltenswissenschaftlichen Erkenntnissen gestaltet werden. Konkret ermöglichen diese Erkenntnisse, dass Voreinstellungen verändert (default rules), Informationsdarstellungen vereinfacht, der Zugang, die Bequemlichkeit bzw. die Verbraucherfreundlichkeit systematisch verbessert werden, Transparenz hergestellt wird, besonders ansprechende, einfach zu verstehende oder auffällige Grafiken verwandt werden. Dieses Spektrum eher passiv orientierter Formen ergänzen solche Techniken, die das Verbraucherhandeln strategisch mit einbeziehen: Verhaltenswissenschaftliche Erkenntnisse können darüber informieren, wie in konkreten Situationen bestimmte Handlungsabsichten provoziert werden, wie Verbraucher sich selbst (vorab) binden, Erinnerungen eingestellt werden oder durch gezielte (gegebenenfalls personalisierte) Informationen und Aufklärung über Konsequenzen früherer Entscheidungen eine bestimmte auch emotionale Reaktion hervorgerufen wird.[7]

Eine gezielte Auswahl einer oder mehrerer Techniken aus diesem Spektrum könnte zu einer verbesserten Instrumentengestaltung beitragen, um die Cybersicherheit zu erhöhen. Vorstellbar wäre beispielsweise, dass es Vorgaben dafür gibt, wie Fragen zu individuellen Einstellungen für mehr Datensicherheit bei der Einrichtung und

5 Anschaulich am Beispiel von Informationskampagnen: M. Bada, A. M. Sasse, J. R. C. Nurse: Cyber Security Awareness Campaigns: Why do they fail to change behaviour?, 9.1.2019, https://arxiv.org/pdf/1901.02672.pdf (15.1.2020).

6 D. Kahneman: Thinking fast and slow, New York 2011.

7 Für einen Überblick siehe L. A. Reisch, M. Zhao: Behavioural economics, consumer behaviour and consumer policy: state of the art, in: Behavioural Public Policy, 1. Jg. (2017), H. 2, S. 190-206.

Nutzung von Apps auf dem Smartphone formuliert und gestaltet sein müssen, damit der Verbraucher tatsächlich eine Einstellungsvariante wählt, die seinem Sicherheitsinteresse entspricht. Letztlich kommt es darauf an, dass verhaltenswissenschaftliche Expertise sowohl zur Analyse von Adressatengruppen als auch zur Auswahl von passenden Techniken (Nudges), durch die sich vor allem informatorische Instrumente verändern lassen, in der Politik berücksichtigt werden. Die Nutzung von verhaltenswissenschaftlichen Erkenntnissen ist allerdings nicht auf informatorische Instrumente beschränkt, sie kann letztlich das gesamte Instrumentenspektrum betreffen. Ein kenntnisreicher und konstruktiver Umgang mit verhaltenswissenschaftlichen Analysen in politischen Prozessen bedarf jedoch einiger Voraussetzungen: Vor allem müssen die Erkenntnisse anschlussfähig an die jeweiligen Handlungsoptionen des Staats in konkreten Entscheidungskontexten sein. Diese sind in Bezug auf Cybersicherheit vielfältig und einem dynamischem Wandel ausgesetzt, sie betreffen häufig sowohl die Verbraucher als auch die Marktanbieter, die wiederum ihre Angebote in bestimmter Weise anpassen müssen. Letztlich gilt es, das gesamte Instrumentenportfolio adressatenbezogen auszuschöpfen und seine Wirkung unter Nutzung verhaltenswissenschaftlicher Erkenntnisse zu erhöhen. Dies gelingt dann, wenn institutionelle Voraussetzungen einen kontinuierlichen Transfer verhaltenswissenschaftlicher Erkenntnisse in politische und administrative Prozesse ermöglichen oder sogar befördern. Letztlich benötigen die jeweiligen Akteure (Behörden, Agenturen, Verwaltungen) für die Ausgestaltung von Instrumenten Handlungs- und Gestaltungsspielräume, um verhaltenswissenschaftliche Erkenntnisse sinnvoll nutzen zu können[8].

8 Feitsma erläutert an einem Beispiel, wie deliberativ Verhaltenspolitik inklusive ihrer Implementation erfolgen kann, ohne dabei technokratisch oder „psychokratisch“ zu werden: J. Feitsma: The behavioural state: critical observations on technocracy and psychocracy, in: Policy Sciences, 51. Jg. (2018), S. 387-410.