DOI: 10.1007/s10273-017-2176-4

Malte Dold, Tim Krieger

Cyber-Security aus ordnungspolitischer Sicht: Verfügungsrechte, Wettbewerb und Nudges

Cyber-Security ist aus ökonomischer Sicht vor allem eine Frage fehlgeleiteter Anreize. Wenn Marktakteure nicht die vollen Kosten ihres informationstechnologischen Handelns tragen, führt dies zu ineffizienten Märkten. Ein Grund für die geringen Investitionen in Cyber-Security dürfte in fehlenden Verfügungsrechten an den eigenen Daten im Internet liegen. Darüber hinaus müsste das Wettbewerbsrecht ausgeweitet werden, um eine Machtkonzentration auf Anbieterseite zu verhindern und ein Mindestmaß an Sicherheit zu gewährleisten. Security-Nudges können dazu beitragen, die Verbraucher für Kosten und Nutzen bei der Herausgabe eigener Daten zu sensibilisieren.

Die Angriffe dubioser Hacker auf Server von Unternehmen, Krankenhäusern und staatlichen Einrichtungen haben in jüngster Vergangenheit dazu geführt, dass das Thema „Cyber-Security“[1] vermehrt ins Bewusstsein der Öffentlichkeit gerückt ist.[2] Besonders das Ausmaß des jüngsten Cyberangriffs im Mai 2017 mit dem Erpressungstrojaner „WannaCry“, der von den betroffenen Anwendern Lösegeld für den Daten- bzw. Systemzugriff verlangte, erregte großes öffentliches Aufsehen, da hierdurch Software-Schwachstellen auf über 230 000 Computern in 150 Ländern aufgezeigt wurden. Nicht nur Firmen- oder Parteigeheimnisse stehen auf dem Spiel, auch die Privatsphäre wird als gefährdet angesehen.[3] Experten betonen, dass das Internet zwar enorme ökonomische und soziale Innovationen hervorgebracht habe, dass jedoch zugleich die damit verbundenen Computersysteme, Netzwerke und digitalen Dienstleitungen in einem hohen Maße anfällig für Sicherheitslücken seien.[4] Eine Studie aus dem Jahr 2014 beziffert die weltweiten Kosten der Cyber-Kriminalität auf 445 Mrd. US-$ oder 0,6% des globalen Bruttoinlandsprodukts.[5]

Diesen Herausforderungen steht entgegen, dass Konsumentendaten für funktionierende Geschäftsmodelle im Zeitalter der Digitalisierung unerlässlich sind. Sie versprechen den Nutzern passgenaue und günstige Produkte oder Erleichterungen im Alltag (Internet der Dinge, selbstfahrende Autos). Der Reiz sozialer Netzwerke liegt in einer Beteiligung möglichst vieler Nutzer, die auf der Basis ihrer persönlichen Daten in nutzenstiftender Weise zusammengebracht werden. Regierungen sehen Big Data vor allem als Chance für die zivile Sicherheit, um organisierte Kriminalität, Terrorismus und Cyber-Kriminalität proaktiv bekämpfen zu können.

1 Cyber-Security bzw. informationstechnologische Sicherheit ist ein vielschichtiger Begriff. Allgemein versteht man unter Cyber-Security den Schutz von Computern und Servern vor Schädigung der Hardware, der Software oder der Daten bzw. Informationen, die auf diesen gespeichert sind, vgl. H. Asghari, M. van Eeten, J. M. Bauer: Economics of cybersecurity, in: J. M. Bauer, M. Latzer (Hrsg.): Handbook on the Economics of the Internet, Cheltenham, Northampton MA 2016, S. 262-287. Der Schutz personenbezogener Daten ist ein wichtiger Teilbereich der Cyber-Security; die unbefugte Nutzung bzw. Weiterverwendung von persönlichen Daten ist dementsprechend eine Verletzung der Cyber-Security. Sie umfasst damit sowohl eine Safety-Komponente (störungsfreier Betrieb von computergestützten Systemen) als auch eine Security-Dimension (Abwehr von Bedrohungen wie z.B. Hackerangriffe auf Server), vgl. S. Kaufmann: Das Themenfeld „Zivile Sicherheit“, in: C. Gusy, D. Kugelmann, T. Würtenberger (Hrsg.): Rechtshandbuch Zivile Sicherheit, Berlin, Heidelberg 2017, S. 3-22.

2 Vgl. The Economist: Incentives need to change for firms to take cyber-security more seriously, http://www.economist.com/news/leaders/21712138-software-developers-and-computer-makers-do-not-necessarily-suffer-when-their-products-go (2.1.2017).

3 Vgl. A. Acquisti, L. Brandimarte, G. Loewenstein: Privacy and human behavior in the age of information, in: Science, 347. Jg. (2015), H. 6221, S. 509-514.

4 Vgl. H. Asghari, M. van Eeten, J. M. Bauer, a.a.O.

5 Vgl. McAfee & Centre for Strategic & International Studies: Net losses: Estimating the global cost of cyber-crime, Washington DC 2014.

Malte Dold, M.A., ist wissenschaftlicher Mitarbeiter an der Albert-Ludwigs-Universität Freiburg.

Prof. Dr. Tim Krieger ist dort Inhaber der Wilfried-Guth-Stiftungsprofessur für Ordnungs- und Wettbewerbspolitik.

Ein genereller Appell zur Abstinenz im digitalen Raum bzw. zur Datensparsamkeit, wie er von Datenschützern propagiert wird, greift aus ökonomischer Sicht zu kurz, da er den Trade-off zwischen der Sicherheit einerseits und den marktlichen Anforderungen an Informationsverfügbarkeit andererseits ignoriert. Sichere Computersysteme und verschleierte Daten verursachen für alle Marktakteure Kosten (z.B. direkte Kosten der Verschlüsselungstechnologie, Opportunitätskosten in Form von entgangenen Markttransaktionen), denen ein Nutzen (z.B. Schutz der Privatheit, Vertrauen in Märkte, Aufklärung von Kriminalität) entgegensteht. Die Abwägung dieser Kosten und Nutzen bestimmt den impliziten Preis der Sicherheit für den Einzelnen. Die zentrale Frage aus gesamtwirtschaftlicher Sicht ist, wie man den impliziten Preis der Sicherheit so senken kann, dass das Niveau der Sicherheit im Cyber-Raum gesteigert wird, ohne dass dies einseitig zulasten der Effizienz auf digitalen Märkten geht.

Zentrale These aus ordnungsökonomischer Perspektive

Der Charakter eines öffentlichen Gutes der Cyber-Security, Informationsasymmetrien und Fehlanreize sind aus Sicht der ökonomischen Theorie die Haupttreiber für Sicherheitslücken bei internetfähigen Computersystemen und digitalen Dienstleistungen. Lücken in der digitalen Sicherheitsarchitektur entstehen vor allem dann, wenn Marktakteure nicht die vollen Kosten einer von ihnen zu verantwortenden Sicherheitslücke tragen müssen.

Damit einhergehende Wohlfahrtsverluste lassen sich nicht ausschließlich durch technische Innovationen beseitigen. Daher ist ein Umdenken bei der rechtlich-institutionellen Gestaltung des Datenverkehrs notwendig, damit diese Verhaltensanreize setzt, welche die Wirtschaftsakteure in Fragen der Cyber-Security zu mehr Verantwortung und Wachsamkeit anleiten. Besondere Bedeutung kommt dabei der Durchsetzung von Verfügungsrechten an (persönlichen) Daten zu.

Verfügungsrechte auf digitalen Märkten müssen zunächst ausgehandelt werden, denn eine klare Zuordnung der Rechte an Daten und die Freiheit, mit diesen handeln zu können, sind Grundvoraussetzungen für effiziente Leistungsanreize. Flankierend sollten das Wettbewerbsrecht und die Verbraucherpolitik umfassender auf den digitalen Raum ausgeweitet werden.

Ökonomische Theorie der Cyber-Security: drei Herausforderungen

Aus ökonomischer Sicht ist das Individualkalkül auf Nutzer- und Unternehmerseite hinsichtlich der Produktion und Finanzierung des Gutes Cyber-Security entscheidend, wenn man eine reine Marktlösung unter Wohlfahrtsgesichtspunkten bewerten will. Im Folgenden sollen die zentralen Herausforderungen für die Cyber-Security aus ökonomischer Perspektive herausgearbeitet werden. Hierbei wird in erster Linie auf die Nutzer- bzw. Anwenderseite abgestellt (wobei Nutzer nicht nur private, sondern auch gewerbliche Akteure sein können).

Herausforderung I: Cyber-Security und externe Effekte

Grundsätzlich führt die Bereitstellung sicherer Computersysteme aufgrund der Vernetzung zu positiven Externalitäten.[6] Wenn beispielsweise ein Server von Google in den USA mit neuester Sicherheitstechnologie ausgestattet wird, profitieren auch Nutzer in Deutschland davon. Umgekehrt profitiert Google davon, wenn private Nutzer in Deutschland in Sicherheitsvorkehrungen investieren (z.B. indem sie automatisch generierte Passwörter bei Routern individualisieren oder regelmäßig Software aktualisieren), sodass einfache Einfallstore für Hacker auf sensible Nutzer- und Firmendaten vermieden werden. Diese Interdependenz ist kennzeichnend für den Cyber-Raum.

Aufgrund der anfallenden Externalitäten klaffen private und soziale Nutzen der Bereitstellung von Cyber-Security auseinander. Die Haushalte und Unternehmen wägen private Kosten (Investitionen in Sicherheitstechnologien) und private Nutzen (z.B. in Form sicherer Internettransaktionen) gegeneinander ab und wählen ein individuell optimales Investitionsniveau. Sie ignorieren jedoch den weitergehenden sozialen Nutzen ihres Handelns. Kommt es in einem Netzwerk aufgrund einer Sicherheitslücke zu einer Cyber-Attacke (z.B. in Form von Phishing von privaten Nutzerdaten), so trägt häufig nicht der Nutzer des gehackten Computers die Kosten der Attacke, sondern andere Nutzer im Netzwerk.[7] Das bedeutet im Umkehrschluss, dass individuelle Investitionen in Sicherheitstechnologien ineffizient niedrig gewählt werden.

Die positiven Externalitäten und die Ignoranz vieler Internetnutzer befördern ein Trittbrettfahrerverhalten verbunden mit der Hoffnung, dass andere Nutzer für die systemrelevanten Technologieinvestitionen aufkommen werden.[8]

6 Potenziell können Sicherheitsinvestitionen auch negative Externalitäten auslösen, wenn die Angreifer aufgrund von Sicherheitsmaßnahmen eines Nutzers entscheiden, einen anderen, weniger geschützten Nutzer anzugreifen. Dies würde einen Investitionswettlauf im Sicherheitsbereich nach oben implizieren, der aber realiter kaum zu beobachten ist.

7 Vgl. T. Moore: The economics of cybersecurity: Principles and policy options, in: International Journal of Critical Infrastructure Protection, 3. Jg. (2010), H. 3, S. 103-117.

8 Vgl. H. Kunreuther, G. Heal: Interdependent security, in: Journal of Risk and Uncertainty, 26. Jg. (2003), H. 2-3, S. 231-249.

Die Trittbrettfahrer-Strategie wird umso wahrscheinlicher, je mehr das Sicherheitsniveau eines Netzwerks von seinem schwächsten Glied abhängt: Da der mangelnde Sicherheitsbeitrag anderer Akteure antizipiert wird, lohnt sich auch eine unilaterale Investition in Sicherheit nicht; lediglich eine kollektive Lösung würde zu mehr Sicherheit im Netzwerk führen.[9] Wegen geringer Zahlungsbereitschaften kommt es schließlich zu einer Unterbereitstellung des Gutes Sicherheit.

Herausforderung II: Informationsasymmetrien und beschränkte Rationalität der Nutzer

Cyber-Kriminalität und Hackerangriffe können am effektivsten bekämpft werden, wenn Informationen über Sicherheitslücken geteilt werden. Die Strategie einer erfolgreichen Cyber-Attacke auf einen Firmenserver kann für eine ähnliche Attacke auch auf andere Firmen angewendet werden. Jedoch ist es für einzelne Unternehmen vorteilhafter, Sicherheitslücken und Hackerangriffe zu verschweigen: Beispielsweise haben Banken einen geringen Anreiz, Online-Kreditkartenbetrug publik zu machen, da dies negative Reputationseffekte mit sich bringen oder potenzielle Nachahmer zu ähnlichen Cyber-Attacken animieren könnte.[10]

Dabei wäre es im allgemeinen Interesse, solche Sicherheitslücken öffentlich zu machen, da verlässliche Daten über Cyber-Attacken ein besseres Risikomanagement auf der Anbieter- und Nachfragerseite ermöglichen würde. Wie bei Herausforderungen im Bereich der öffentlichen Gesundheit, wenn Nachlässigkeiten einzelner Personen das Gesamtsystem gefährden (beispielsweise bei Impfungen oder Hygienestandards), so ist auch im Bereich der Cyber-Security ein kritisches Niveau individueller Sicherheitsmaßnahmen und die Dissemination von Informationen über Sicherheitslücken essenziell für ein wohlfahrtsoptimales Ergebnis.

Weiterhin ist es beim Angebot von Sicherheitstechnologien (z.B. bei Internetbrowsern oder Betriebssystemen) für den durchschnittlichen Nutzer schwierig, vor dem Kauf gute von schlechten Produkten zu unterscheiden. Es handelt sich bei Security-Produkten um Erfahrungsgüter, deren tatsächliche Qualität sich dem Nutzer erst im Laufe der Zeit offenbart. Diese Tatsache führt dazu, dass Nutzer in der Regel nicht gewillt sind, Preisaufschläge für bessere Produkte zu bezahlen. Da Anbieter die geringe Zahlungsbereitschaft auf Nutzerseite antizipieren, entsteht ein „Lemons-Markt“ und qualitativ hochwertige Sicherheitstechnologien werden aus dem Markt gedrängt.[11]

Selbst im Falle der Transparenz und Informationsverfügbarkeit reagieren viele Nutzer träge oder sind bei Fragen der Datensicherheit sehr sorglos und antizipieren die Langzeitwirkung von Daten- bzw. Informationsentäußerung kaum bis gar nicht.[12] Menschliche Fehleinschätzungen scheinen bei Fragen der IT-Sicherheit die Regel zu sein, was neben den genannten Informationsproblemen zu weiteren Verzerrungen des Marktergebnisses und zu Wohlfahrtsverlusten führt.[13]

Herausforderung III: Fehlanreize in Prinzipal-Agenten-Beziehungen

Computersysteme und Netzwerke versagen vor allem auch dann bei Sicherheitsfragen, wenn der verantwortliche Akteur nicht die vollen Kosten, die aus einer Sicherheitslücke entstehen, tragen muss. Das ist besonders bei Prinzipal-Agenten-Beziehungen der Fall. So stimmen beispielsweise die Anreize vieler Softwarehersteller und Online-Händler, die unter Kostendruck operieren und gegebenenfalls bei der IT-Sicherheit sparen, nicht notwendigerweise mit denen ihrer Kunden überein, da Letztere für den ökonomischen Schaden gestohlener Daten aufkommen müssen.

Auch Kunden haben geringe Anreize, ihr Verhalten zu ändern, da Wechselkosten sie daran hindern, auf sicherere Anbieter auszuweichen. Vor allem bei der Softwarenutzung bestehen Pfadabhängigkeiten, bei denen hohe Wechselkosten durch Gewöhnung an ein regelmäßig genutztes System – aufgrund systematischer Unterschätzung von Sicherheitsrisiken vermeintlich – niedrigen Wechselvorteilen entgegenstehen. Gleichzeitig führt die Komplexität der Systeme und die unübersichtliche Art und Zahl der Angriffe dazu, dass die Nutzer nicht mehr selbst in der Lage sind, die Sicherheitslücken zu schließen. Sie sind abhängig von den Sicherheitsmaßnahmen der Software- und Onlineanbieter, ohne in der Lage zu

9 Vgl. H. Varian: System reliability and free riding, in: L. J. Camp, S. Lewis (Hrsg.): Economics of information security, Boston 2004, S. 1-15.

10 Vgl. T. Moore, a.a.O., S. 108.

11 Vgl. G. A. Akerlof: The market for „lemons“: Quality uncertainty and the market mechanism, in: Quarterly Journal of Economics, 84. Jg. (1970), H. 3, S. 488-500.

12 Vgl. A. Acquisti, J. Grossklags: Privacy and rationality in individual decision-making, in: IEEE Security & Privacy, 3. Jg. (2005), H. 1, S. 26-33; H. Asghari, M. van Eeten, J. M. Bauer, a.a.O.; N. Steinfeld: „I Agree to the Terms and Conditions“: (How) Do Users Read Privacy Policies Online? An Eye-Tracking Experiment, in: Computers in Human Behavior, 55. Jg. (2016), S. 992-1000.

13 Verhaltensökonomisch kann beispielsweise ein „Overconfidence Bias“ vorliegen: Anwender wissen zwar häufig um das generelle Problem der Cyber-Security, jedoch überschätzen sie ihre eigenen IT-Fähigkeiten bzw. unterschätzen ihr tatsächliches Vulnerabilitätsniveau auf digitalen Märkten.

sein, deren Anstrengungen und ökonomische Kalküle beurteilen zu können.

Zwischenfazit

Eine reine Marktlösung scheint beim Thema Cyber-Security bisher nicht zu funktionieren. Nutzer können und wollen sich nicht mit Sicherheitsfragen auseinandersetzen; sie profitieren davon, wenn andere beim Thema Datensicherheit positive Externalitäten erzeugen und eigene Nachlässigkeiten verschwiegen werden können. Zwar impliziert der Trade-off zwischen Sicherheit und Effizienz, dass es ein wohlfahrtsoptimales Niveau (größer Null) an Unsicherheit in IT-Systemen gibt. Insgesamt jedoch führen die genannten ökonomischen Herausforderungen im Bereich der Cyber-Security dazu, dass das momentane Marktgleichgewicht das optimale informationstechnologische Sicherheitsniveau unterschreitet.

Ordnungspolitische Ansatzpunkte

Die genannten Herausforderungen lassen sich nur schwer direkt beseitigen. Es lässt sich jedoch ein verbindendes ökonomisches Problem ausmachen: die mangelnde Investitionsbereitschaft in Cyber-Security-Technologien in Kombination mit einer fehlenden Justiziabilität bei Transaktionen von Daten. Beides lässt sich wiederum auf die Tatsache zurückführen, dass es im Internet bisher noch keine durchsetzbaren Verfügungsrechte an Daten gibt. Dies führt zum einen zu einer Wildwestmentalität beim Umgang mit Daten und dem Glauben, dass derjenige, der als erster einer Information eines Dritten habhaft geworden ist, diese nach eigenem Gutdünken verwenden kann. Zum anderen führt der Zustand ungeklärter Verfügungsrechte dazu, dass sich (private wie geschäftliche) Nutzer nicht hinreichend mit Fragen der Daten- und Informationssicherheit auseinandersetzen, da es sich ökonomisch (und juristisch) nicht auszahlt. Um die Unterbereitstellung von Cyber-Security zu reduzieren und die Justiziabilität bei Datenmissbrauch zu erhöhen, bietet sich als erster ordnungsökonomischer Ansatzpunkt die Einführung von Verfügungsrechten an und damit eines Marktes für Daten.

Vermarktlichung von Daten schafft effiziente Anreize

Die Sicherheitstechnologien im Cyber-Raum sind untrennbar mit dem Schutz privater Informationen, die letztlich in Form von Daten vorgehalten werden, verbunden. Um effiziente Anreize zur Nutzung oder Bewirtschaftung von Informationen – und dies schließt auch den Einsatz von Sicherheitstechnologien ein – zu setzen, müssen deren Verfügungsrechte exklusiv definiert sein. Dies bedeutet, dass es eine zentrale Voraussetzung für effiziente Datenmärkte und damit auch für die Effizienz von Märkten für Sicherheitstechnologien ist, dass Daten wie private Güter gehandelt werden können. Nur dann kann eine effiziente Nutzung der Daten gegen Entgelt ermöglicht werden und nur dann kann ein hinreichend intensiver Wettbewerb um Sicherheitstechnologien entstehen.

Dabei stellt sich vor allem im Bereich der personenbezogenen Daten die fundamentale Frage, wem die relevanten Rechte idealerweise zugeordnet werden sollten. Mehrere Argumente sprechen dafür, die Rechte (zunächst) dem Schöpfer der Daten zuzuordnen, der damit selbst über die ökonomische Weiterverwendung seiner Daten entscheiden kann. *Ökonomisch* lässt sich annehmen, dass die Voraussetzungen für das Coase-Theorem nicht vollständig erfüllt sind,[14] sodass von einer allokativen Wirkung der Verfügungsrechte zugunsten des Rechteinhabers ausgegangen werden kann, die *politisch* auch von einem distributiven Effekt zugunsten dieser Person begleitet wird. Es ist unwahrscheinlich, dass eine Rechtezuordnung, die nicht den Schöpfer der Daten begünstigt, im politischen Prozess durchsetzbar wäre (außer bei einer starken Verzerrung des demokratischen Prozesses durch Lobbying- und Rent-Seeking-Aktivitäten). *Epistemisch* ist davon auszugehen, dass nur der Schöpfer der Information weiß, welche Daten für ihn vertraulich bzw. sensibel sind, und *normativ* haben Privatheit und Autonomie einen intrinsischen Wert.

Eine stärkere Vermarktlichung von privaten Daten in Form von kodifizierten und rechtlich abgesicherten Verfügungsrechten kann die Verhaltensanreize der Akteure bei Cyber-Security-Fragen positiv verändern. Zum einen werden durch eine Verrechtlichung Haftung und Kontrolle zusammengeführt. Die Verfügungsrechte ermöglichen es, dass der Inhaber der Daten(-rechte) alleine haftet, aber eben auch die alleinige Kontrolle im Sinne des alleinigen Verfügungsrechts über diese Daten zugesprochen bekommt.[15]

Zum anderen schafft diese Zusammenführung von Kontrolle bzw. Handlung und Haftung sowohl bei Individuen als auch bei Unternehmen einen Zustand der „unternehmerischen Wachsamkeit“.[16] Handelbare Verfügungsrech-

14 Aufgrund der Informationsasymmetrien in IT-Angelegenheiten und hohen privaten Transaktionskosten in digitalen Rechtsfragen muss davon ausgegangen werden, dass private Verbraucher einen systematischen Nachteil in „Daten-Verhandlungen“ haben.

15 Vgl. M. Dold, T. Krieger: Informationelle Selbstbestimmung aus ordnungsökonomischer Sicht, in: M. Friedewald, J. Lamla, A. Roßnagel (Hrsg.): Informationelle Selbstbestimmung im digitalen Wandel, Wiesbaden 2017, S. 181-198.

16 Vgl. I. M. Kirzner: Creativity and/or alertness: A reconsideration of the Schumpeterian entrepreneur, in: The Review of Austrian Economics, 11. Jg. (1999), H. 1-2, S. 5-17.

te an Daten führen dazu, dass sich Wirtschaftsakteure über deren ökonomischen Wert bewusst werden. Das hat zur Folge, dass Cyber-Security nicht mehr nur eine abstrakte Größe ist, sondern über den Aspekt der Datensicherheit zu einem konkreten Gut wird. Dadurch werden Anreize geschaffen, optimale Investitionen in Datensicherheit zu tätigen, denn bei Unternehmen steht die Reputation auf dem Spiel, bei individuellen Nutzern der ökonomische Gegenwert ihrer Privatheit.

Dies ist auch eine direkte Antwort auf das Privacy-Paradoxon: Nutzer verhalten sich bei Sicherheitsfragen im Internet relativ sorglos, äußern aber gleichzeitig eine starke Präferenz für den Schutz ihrer Privatheit.[17] Werden Anreize in Form von Verfügungsrechten eingeführt, so werden solche expressiven Präferenzen nun zu echten ökonomischen Interessen. Es ist zu erwarten, dass die Datenrechteinhaber wissen wollen, wer auf welche Weise Zugriff auf ihre Daten bekommt und welche Rechte sie im Falle des Datenmissbrauchs haben.

Auch auf Unternehmerseite ändern sich die wirtschaftlichen Anreize hinsichtlich der Investitionen in Cyber-Security, wenn eine stärkere Vermarktlichung von Daten durchgesetzt werden kann. Bisher erleiden Internetfirmen (inklusive der Software-Entwickler und Computerhersteller) kaum wirtschaftliche Einbußen bei Sicherheitslücken in ihren Systemen, da die Beweglichkeit bzw. Abwanderungstendenz der Nutzer relativ gering ist.[18] So haben massive Sicherheitsprobleme bei Kreditkarten oder Betriebssystemen nicht dazu geführt, dass Nachfrager im großen Stil den Anbieter gewechselt haben. Würden Daten jedoch mehr als Gut verstanden bzw. gehandelt und Nutzer dementsprechend sensibel auf Datenleaks bei Firmen reagieren, so würden sich auch auf unternehmerischer Seite Investitionen in Sicherheitstechnologien auszahlen. Die Opportunitätskosten von laxen Sicherheitsstandards würden für die Unternehmen ansteigen, da kurzfristig Gewinneinbußen und langfristig Reputationsverluste drohen.

Die Durchsetzung der Verfügungsrechte wird jedoch nicht alleine über den Markt gelingen. Dies liegt vor allem an den Öffentliches-Gut-Eigenschaften von privaten Informationen. Sind private Informationen erst einmal offenbart, dann lassen sie sich nicht mehr in die Privatheit zurückführen. Auch das zuletzt in der europäischen Datenschutz-Grundverordnung[19] verankerte Recht auf Vergessenwerden kann dieses Problem nicht grundsätzlich lösen, schafft aber einen Ansatzpunkt für rechtliche Rahmensetzungen. Vor allem das Delikts- und das Strafrecht können Anreize setzen, dass die Marktakteure Datenrechte aus eigenem Interesse einhalten. Ein scharfer Rechtsrahmen mit effektiver gerichtlicher Durchsetzung, eine Verankerung der Beweislast aufseiten der datennachfragenden Marktteilnehmer und gegebenenfalls eine ausreichend hohe strafrechtliche Aufdeckungswahrscheinlichkeit verändern das Kosten-Nutzen-Kalkül der Marktakteure zugunsten der Einhaltung der Verfügungsrechte der Rechteinhaber.[20] Zudem sollte darüber nachgedacht werden, inwiefern die Verwendung personenbezogener Daten durch Dritte ohne aktive Zustimmung des Daten-Emittenten rechtlich eingeschränkt werden kann.

Umgekehrt ginge mit dem Verfügungsrecht an Daten auch eine Sorgfaltspflicht bei Fragen der Sicherheit einher. Würde diese verletzt, so könnten die verantwortlichen Parteien rechtlich haftbar gemacht werden. Hierbei sollte wiederum die Sorgfaltspflicht der Partei zugeordnet werden, die das Sicherheitsrisiko am effizientesten (d.h. kostengünstigsten) beseitigen kann.[21]

Stärkung der Marktinstitutionen

Der zweite ordnungsökonomische Ansatzpunkt für die Datenmärkte bezieht sich auf die Verbesserung und Stärkung der Marktinstitutionen. Ihm unterliegt die Vorstellung, dass nur Märkte mit einem hinreichend großen Wettbewerbspotenzial über das Preissystem ihre allokative Lenkungswirkung in einer effizienten Weise ausfüllen können.[22] Ein funktionierendes Preissystem setzt wiederum voraus, dass die Marktmacht einzelner Akteure begrenzt wird.[23] Im Hinblick auf die Cyber-Security kann dies einerseits durch das Wettbewerbsrecht passieren, andererseits aber auch durch eine rechtliche Absicherung von Marktsignalen.

Wettbewerbsrechtlich ist zu beachten, dass die Marktkonzentration auf digitalen Plattformen (Amazon, Facebook etc.) durch Netzwerkeffekte zwar Nutzen für

17 Vgl. A. Acquisti, L. Brandimarte, G. Loewenstein, a.a.O., S. 510.
18 Vgl. T. Moore, a.a.O.

19 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=DE (7.6.2017).
20 Vgl. M. Dold, T. Krieger, a.a.O.
21 Vgl. R. Anderson, T. Moore: The economics of information security, in: Science, 314. Jg. (2006), H. 5799, S. 610-613.
22 Vgl. F. A. Hayek: The use of knowledge in society, in: American Economic Review, 35. Jg. (1945), H. 4, S. 519-530.
23 Vgl. W. Eucken: Grundsätze der Wirtschaftspolitik, Tübingen 1952.

die Anwender stiften kann, zugleich aber mit der Gefahr verbunden ist, dass sich ein Machtmonopol bildet. Wichtig aus ordnungspolitischer Sicht ist beim Thema Cyber-Security, dass die Nutzer nicht von einzelnen Anbietern abhängig sind, ohne die Möglichkeit zu haben, ihr Nachfrageverhalten gemäß ihren wahren Präferenzen umzusetzen. Die Abhängigkeit birgt zum einen ein hohes Sicherheitsrisiko, da ein Angriff auf einen einzelnen sehr großen Anbieter für Hacker hohe Renditen verspricht, und sich zum anderen die inhärente Trägheit von Monopolisten bei Qualitätsinnovationen durch wenig fortschrittliche Sicherheitstechnologie ausdrücken kann.

Entscheidend ist in einer solchen Situation, dass durch die wettbewerbsrechtliche Verhinderung von Machtkonzentrationen auf Anbieterseite eine höhere Beweglichkeit der Nachfrager auf digitalen Märkten ermöglicht wird. Diese führt dazu, dass die Vorteile durch eine erhöhte Reputation (z.B. im Bereich der Cyber-Security) im Vergleich zu den Anreizen, sich opportunistisch zu verhalten, gestärkt werden.[24] Anbieter werden dann seltener den kurzfristigen Gewinn durch Datenmissbrauch oder die Verletzung von Sorgfaltspflichten bei Sicherheitsstandards wählen, weil sie langfristige Reputationsverluste befürchten, die zu niedrigeren Gewinnen durch eine geringere Zahl von Wiederholungskäufen führen.

Grundsätzlich sollte den Unternehmen ein Handlungsspielraum gegeben werden, Sicherheitsstandards und technologische Mittel branchenspezifisch auszuhandeln, da diese die Sicherheitsprobleme kennen (Subsidiarität) und deren Beseitigung im eigenen Interesse (Reputation) liegt. Dabei ist das Aushandeln des richtigen Standards nicht trivial: Zu niedrige Standards führen zu Unsicherheit, zu hohe Standards zu Transaktionskosten bei der Produktnutzung und zur Hemmung wichtiger Innovationsanreize. Die Aufgabe der Politik ist es dann, die ausgehandelten Minimalstandards der Cyber-Security (z.B. bei der Markteinführung von Software-Produkten) rechtlich abzusichern, damit Verletzungen von Sorgfaltspflichten durch (hohe) Schadensersatzforderungen mit entscheidungsrelevanten impliziten Preisen versehen werden können.

Stärkung der Verbraucherposition durch „Security-Nudges“

Die Vermarktlichung der Daten und eine Ausweitung des Wettbewerbsrechts sind wichtige Säulen einer digitalen Ordnungspolitik. Sie gehen aber nicht weit genug. Verbraucher profitieren zwar über zusätzlich generiertes Einkommen aus ihren Daten und eine größere Auswahl von Anbietern bzw. Sicherheitstechnologien als Folge einer wirksamen Wettbewerbsaufsicht, jedoch sind Verfahren wegen unlauteren Wettbewerbs langwierig und scheitern oft daran, dass den Internetkonzernen nicht nachgewiesen werden kann, dass sie ihre Marktmacht für unfaire oder unachtsame Geschäftsmethoden missbrauchen. Die aktuelle Diskussion über das (mittlerweile schon dritte) Verfahren der EU-Kommission gegen Google verdeutlicht die juristische Vielschichtigkeit solcher wettbewerbsrechtlichen Auseinandersetzungen, wobei zu vermuten ist, dass es auch in diesem Verfahren nicht zu den geforderten Strafzahlungen in Höhe von 2,42 Mrd. Euro kommen wird. Zudem ist zu befürchten, dass selbst nach der Einführung von Verfügungsrechten an Daten undurchsichtige Datenschutzerklärungen und Unklarheiten über die Art der Weiterverwendung von Daten Nutzer davon abhalten, informierte Entscheidungen treffen zu können. Dies hätte zur Folge, dass es für Nutzer nach wie vor nicht möglich wäre, die Qualität von Cyber-Security-Standards valide einzuschätzen. Und selbst wenn Informationsasymmetrien beseitigt werden könnten, würden Nutzer ihre Gewohnheiten im Internet deshalb noch nicht automatisch ändern.

Für eine effektive Anwendung von Sicherheitstechnologien ist neben den genannten institutionellen Änderungen der digitalen Marktstruktur deshalb auch eine Änderung der Nutzergewohnheiten entscheidend. Erkenntnisse der Verhaltensökonomik deuten darauf hin, dass Nutzer systematisch Sicherheitsrisiken im Umgang mit computerfähigen Geräten unterschätzen und Informationen selektiv wahrnehmen, die ihre eigene Überzeugung stützen.[25] Eine Politik der reinen Verbrauchererziehung (etwa in Richtung Datensparsamkeit) ist daher aus ökonomischer Sicht nicht sinnvoll und ihre Effektivität wäre aufgrund der Komplexität des Themas ohnehin zweifelhaft.

Daher erscheint es angebracht, direkt die Verbraucherposition im Entscheidungsmoment zu stärken. Dies kann mithilfe sogenannter „Security-Nudges“ geschehen, die automatisierte Nutzergewohnheiten durch aktive Entscheidungen ersetzen. Der Gedanke dabei ist, dass kleine Änderungen in der Entscheidungsarchitektur („Nudges“, auf Deutsch: „Stupser“) den Nutzern helfen, sich situationsspezifisch der Datenschutzproblematik bewusst zu werden. Unbewusste, automatisierte System-1-Entscheidungen werden einer kognitiven Überprüfung

24 Vgl. A. O. Hirschman: Exit, voice, and loyalty, Cambridge MA 1970.

25 Vgl. A. Acquisti: Nudging privacy: The behavioral economics of personal information, in: IEEE Security & Privacy, 7. Jg. (2009), H. 6, S. 82-85; S. L. Pfleeger, D. D. Caputo: Leveraging behavioral science to mitigate cyber security risk, in: Computers & Security, 31. Jg. (2012), H. 4, S. 597-611.

unterzogen und durch System-2-Entscheidungen, die langfristige Kosten und Nutzen miteinbeziehen, ersetzt.[26]

Ein Beispiel für einen Security-Nudge wäre eine Änderung der Voreinstellungen (Defaults) bei internetfähigen Geräten, die dafür sorgen, dass eine Benutzung des Gerätes ohne eine Änderung des firmengenerierten Nutzernamens und Passwortes nicht möglich ist oder dass Aufforderungen zu Software- und Sicherheits-Updates den Nutzer dazu anregen, sich aktiv mit Fragen der IT-Sicherheit auseinanderzusetzen. Darüber hinaus wäre denkbar, dass bei der Eingabe sensibler Daten (Geburtsdatum, Kreditkartendaten) dem Nutzer übersichtliche Information darüber gegeben werden, wie viele andere Akteure auf welche Art Zugang zu den Daten bekommen.[27] Eine grafische Lösung wäre hier denkbar, ähnlich der viel diskutierten Lebensmittelampel, welche die Sicherheitsstufe der Transaktion angibt. Der rechtlichen Verpflichtung der Anbieterseite für derartige Maßnahmen kommt hier besondere Bedeutung zu. Zentral für ökonomisch fundiertes Security-Nudging ist es, dass es – anders als bei reinen „Security by default"-Ansätzen – zu einer möglichst bewussten Auseinandersetzung des Nutzers mit den Kosten und Nutzen der eigenen Auswahlentscheidung kommt.

Ausblick: supranationaler Handlungsbedarf

Cyber-Security ist ein öffentliches Gut. Ähnlich wie bei Fragen der öffentlichen Gesundheit braucht es auch hier einen geeigneten Mix aus marktlichen Lösungen und staatlicher Vorschrift sowie Kontrolle von Mindeststandards. Firmen bzw. Individuen, die diese Standards nicht einhalten, verletzen ihre Sorgfaltspflichten und müssen privatrechtlich zur Rechenschaft gezogen werden können. Erheblicher Datenmissbrauch wiederum sollte strafrechtlich belangt werden können. Nicht nur Softwarekonzerne und Internetfirmen sind dabei angesprochen, sondern auch Hersteller, die computergestützte Technologien im Rahmen des „Internet der Dinge" in ihre Produkte einbauen (z.B. Haushaltsgeräte oder Autos). Die Position der Nutzer und Informationsschöpfer sollte durch eine Ausweitung des Wettbewerbsrechts und des Verbraucherschutzes insoweit verbessert werden, dass bewusste und informierte Entscheidungen auf Anwenderseite beim Thema Cyber-Security getroffen werden können. Gleichzeitig gilt, dass auch sie ein Mindestmaß an Sorgfalt beim Umgang mit internetfähigen Produkten zeigen müssen (z.B. durch das Ändern von automatisierten Passwörtern oder Software-Updates). Verletzen sie diese, sollten auch sie durch Schadensersatzforderungen zur Rechenschaft gezogen werden können. Sicherheitsstandards und Sorgfaltspflichten dürfen gleichzeitig nicht so hoch angesetzt werden, dass sie Innovationen auf der Anbieterseite und die Nutzerfreundlichkeit der Produkte auf der Verbraucherseite hemmen.

Da die Frage nach Mindeststandards im Bereich der Cyber-Security nicht an nationalen Grenzen halt macht, ist es zentral, als ersten Schritt mindestens die EU-Datenschutz-Grundverordnung in den nationalen Gesetzgebungen zu verankern. Bisher gibt es eine Vielzahl von uneinheitlichen nationalen Vorschriften zum Datenschutz, sodass eine effektive Bekämpfung von Cyber-Risiken nicht möglich ist. Des Weiteren ist es wichtig, dass Informationen über Sicherheitsrisiken bzw. -lücken grenzüberschreitend sowohl zwischen Firmen als auch staatlichen Sicherheitsakteuren geteilt werden, denn nur so können diese effektiv bekämpft und Risiken besser eingeschätzt werden. Offenlegungspflichten und Sicherheitsstandards alleine werden jedoch nicht ausreichen. Es muss auf der EU-Ebene weiter darüber nachgedacht werden, wie Wettbewerb und Verbraucherschutz auf digitalen Märkten gestärkt werden können. Ökonomisch fundierte Security-Nudges können dabei einen wichtigen Beitrag leisten.

26 System-1-Entscheidungen wären z.B. solche, in denen man aus Gewohnheit Datenschutzerklärungen einfach wegklickt, ohne sich aktiv Gedanken über die Folgen der eigenen Handlung zu machen. Eine System-2-Entscheidung wäre es demgegenüber, wenn man sich vor dem Kauf eines Software-Produktes Test-Berichte durchliest, durch die man die eigene Kaufhandlung aktiv leiten lassen möchte. Vgl. D. Kahneman: Thinking, fast and slow, New York 2011.

27 Vgl. A. Acquisti, a.a.O.

Title: *The Constitutional Political Economy of Cyber Security – Property Rights, Competition and Security Nudges*

Abstract: *From an economic point of view, the problem of cyber security is not primarily a technological challenge but one based on misaligned incentives. When market participants do not bear the full costs of their negligent behaviour in digital transactions, the market outcome tends to be inefficient. In this article, the authors argue that one of the main reasons for a lack of investment in digital security is the lack of property rights for personal data in the internet. They argue that the right institutional environment can lead to a market for data that would spark a reputational competition for computer security technologies. Effective antitrust law and behaviourally informed policies can lead to further welfare improvements in digital markets.*

JEL Classification: *D18, P14, K24*