
Verantwortung zwischen Gesetzgebung und Wirtschaft

Dr. Markus Dürig

Leiter des Referats IT-Sicherheit, Bundesministerium des Innern

Zusammenfassung

Technologien und Märkte entwickeln und verändern sich. Die rasante Beschleunigung in nahezu allen Lebens- und Entscheidungsabläufen führt zu einem Wandel in der Gesellschaft, in der Politik und in der Wirtschaft. Für die Politik ergibt sich hieraus die Aufgabe, diesen digitalen Wandel aktiv zu begleiten und Rahmenbedingungen für das Leben, Lernen, Arbeiten und Wirtschaften in einer digital vernetzten Welt zu setzen.

Bei allen Veränderungen, die den Menschen umgeben und beeinflussen, ist eines geblieben: das Bedürfnis nach Sicherheit. In der so genannten „Maslowschen Bedürfnispyramide“, mit der menschliche Bedürfnisse und Motivationen in einer – wenn auch etwas grob skizzierten – hierarchischen Struktur beschrieben werden, rangiert die Sicherheit direkt nach den körperlichen Grundbedürfnissen. Gleichzeitig ist Sicherheit aber auch ein Defizitbedürfnis. Als Wert wird sie erst wahrgenommen, wenn sie fehlt. Die Frage nach der Gewährleistung von Sicherheit im Netz gerät in der öffentlichen Debatte regelmäßig in ein Spannungsfeld mit Werten wie Freiheit, Unabhängigkeit und Kreativität – mit eben jenen Werten also, die im Netz einen besonders hohen Stellenwert genießen. Wer hier Sicherheit – und damit in der Regel auch Beschränkungen – schaffen will, sieht sich besonderem Rechtfertigungsdruck ausgesetzt. Hinzu kommt, dass Sicherheit im Netz wenig greifbar ist. Schadensfälle wie Datenverluste und Betrügereien, Manipulationen und Spionage werden von den Betroffenen oft erst dann bemerkt, wenn sie sich in der realen Welt auswirken. Ein Großteil bleibt sogar unentdeckt. Gleichzeitig ist die digitale Welt in Aufbau und Funktionsweise für den Nichtspezialisten wenig durch-

dringbar. Vieles bleibt abstrakt – auch die Bedrohung. Dies mag eine der Ursachen dafür sein, dass das Streben des Staates nach mehr Sicherheit im Datenverkehr oftmals auf mehr Vorbehalte trifft als in anderen Bereichen – wie zum Beispiel im Straßenverkehr. Allerdings konnten sich die Regeln und Notwendigkeiten im Straßenverkehr auch über einen Zeitraum von mehr als einhundert Jahren entwickeln. Im Netz hatte und hat unsere Gesellschaft diese Zeit nicht. Die Gewährleistung von Sicherheit im sogenannten Cyber-Raum ist eine gemeinsame Herausforderung für Staat, Wirtschaft und Gesellschaft im nationalen und internationalen Kontext. Mit Blick auf diese verteilte Verantwortung lässt sich dieses Ziel nur dann erreichen, wenn alle Akteure gemeinsam und partnerschaftlich ihre jeweilige Aufgabe wahrnehmen.

Aufgaben des Staates

Was also sind die staatlichen Aufgaben rund um das Thema Internet? Und welche Funktionen muss der Staat wahrnehmen? Das Bundesministerium des Innern hat für sich drei Bereiche definiert:

1. Der Staat hat eine Freiheits- und Ausgleichsfunktion. Die Nutzung des Netzes und der Zugriff auf das Internet dürfen – soweit möglich – nicht begrenzt werden.
2. Der Staat hat eine Angebots- und Innovationsfunktion. Aufgabe des Staates ist es, ein Klima für Innovation zu schaffen und selbst Entwicklungen gezielt zu fördern, etwa für die Nutzung staatlicher Dienstleistungen durch die Bürgerinnen und Bürger. Beispiele hierfür sind die eID-Funktion des Personalausweises und De-Mail, mit denen wichtige Voraussetzungen für die vertrauenswürdige Kommunikation im Netz geschaffen wurden. Der Staat macht hier ein Angebot bzw. schafft die gesetzlichen Grundlagen. Das De-Mail-Gesetz etwa regelt die Mindestanforderungen an einen sicheren elektronischen Nachrichtenaustausch und sorgt für ein geregeltes Verfahren, wie diese Mindestanforderungen, die für alle privaten De-Mail-Anbieter in gleicher Weise gelten, wirksam überprüft werden. Das sind wichtige Voraussetzungen für das Entstehen von Vertrauen in die Sicherheit und für die Qualität der De-Mail-Dienste. In der Verantwortung jedes Einzelnen liegt es dann aber, darüber zu entscheiden, ob er diese Technologien auch tatsächlich zum Einsatz bringt.
3. Der Staat hat eine Schutz- und Gewährleistungsfunktion. Der Staat trägt eine Mitverantwortung für das Internet als Infrastruktur, die für alle zugänglich sein und zuverlässig funktionieren muss, und in der die in der analogen Welt über zum Teil Jahrhunderte entwickelte Rechtsordnung, insbesondere die Menschen- und Freiheitsrechte, selbstverständlich Anwendung finden.

Zu Punkt 3 gehört zunächst ein angemessener Schutz des Internets als Teil der Kritischen Infrastrukturen. Es geht darüber hinaus aber auch um den Schutz der Menschen- und Freiheitsrechte, zum Beispiel der persönlichen Daten im Netz. Meldungen über großflächige Diebstähle von Identitäten durch Kriminelle, über kaum reguliertes Sammeln, Aus- und Verwerten persönlicher Daten durch große IT-Konzerne und über die umfassende Ausspähung durch Nachrichtendienste aus der ganzen Welt haben den Blick auf das Internet und die Digitalisierung verändert. Die Themen Datenschutz und Datensicherheit haben dadurch sicherlich für alle eine ganz neue Bedeutung bekommen.

Sicherheitsgewährleistung des Staates

Im Koalitionsvertrag der Bundesregierung wird eine Vielzahl programmatischer Aussagen zu verschiedenen Aspekten der IT-Sicherheit und zum Schutz der Bürgerinnen und Bürger im Netz getroffen. Dabei geht es unter anderem um die Stärkung nationaler technologischer Kompetenzen im europäischen Verbund, die Beförderung einer vertrauenswürdigen IT- und Netzstruktur sowie auf europäischer Ebene um die Unterstützung eines europäischen Datenschutzrechts der Wirtschaft. Bei all diesen Maßnahmen geht es um die Sicherheit im Netz sowie die Sicherheit der zugrundeliegenden Netzinfrastrukturen. Dies ist zunächst wenig überraschend, gehört doch die Gewährleistung von Sicherheit seit jeher zu den vornehmsten Aufgaben des Staates. Die Prinzipien der Rechtsordnung auch im Zeitalter der Digitalisierung und Vernetzung müssen auch nicht komplett neu erfunden werden: Die Grundlagen des Rechts- und Wertesystems stammen aus der analogen Welt. Für all das, was sich dort als Interessenausgleich und Verantwortungswahrnehmung von Staat und Wirtschaft bewährt hat, ist grundsätzlich anzunehmen, dass dies auch in der digitalen Welt so ist.

IT-Sicherheitsgesetz

Zum Schutz der Bürgerinnen und Bürger in einem freien Netz sind sichere IT-Systeme notwendig. Die Sicherheit der IT-Systeme und digitalen Infrastrukturen ist Grundlage jeder Digitalisierung. Den Kern des IT-Sicherheitsgesetzes bildet das Verhältnis zwischen Risiko, Schutz und Verantwortung: Wer ein Risiko für die Menschen schafft, der trägt auch eine besondere Verantwortung für ihren Schutz. Je gravierender diese Risiken sind, desto höhere Anforderungen sind an die entsprechenden Schutzvorkehrungen zu stellen. Und desto mehr muss der für das Risiko Verantwortliche im Rahmen seiner Möglichkeiten dafür Sorge tragen, dass die zum Schutz der Personen vorgesehenen Garantien tatsächlich verwirklicht werden können. Den bestehenden Initiativen für mehr

IT-Sicherheit liegt ein freiwilliger Ansatz zugrunde. Sie sind Angebote für Bürger und Unternehmen, im Rahmen ihrer jeweiligen Eigenverantwortung selbst für mehr Sicherheit im Netz zu sorgen. Dies gilt beispielsweise für die Informationsmöglichkeiten und aktuellen Sicherheitshinweise des Bundesamtes für Sicherheit in der Informationstechnik auf der Webseite „BSI für Bürger“ und das „Bürger-CERT“. Zusätzlich leistet der Verein „Deutschland sicher im Netz“, wichtige Arbeit bei der Aufklärung von Internetnutzern über die Risiken im Netz. Speziell auf die Belange der Wirtschaft, Wissenschaft und öffentlichen Verwaltung ausgerichtet ist die vom BSI in Zusammenarbeit mit dem Branchenverband BITKOM im Jahr 2012 gegründete „Allianz für Cyber-Sicherheit“. Mehr als 1000 Institutionen aller Branchen und Größenordnungen haben sich dieser Allianz bereits angeschlossen. Sie alle profitieren von dem wechselseitigen und freiwilligen Austausch von Know-how und dem umfangreichen Informationsangebot in der Allianz. Diese Zusammenarbeit von Staat und Wirtschaft funktioniert. Die Resonanz der Beteiligten ist durchweg positiv. Wozu also ein IT-Sicherheitsgesetz?

Mit dem IT-Sicherheitsgesetz sollen in Deutschland branchenweite Standards für die IT-Sicherheit in den Bereichen der Wirtschaft eingeführt werden, die für das Wohl der Gesellschaft von elementarer Bedeutung sind. Adressaten sind somit Unternehmen aus den Bereichen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie aus dem Finanz- und Versicherungswesen. Das IT-Sicherheitsniveau ist in diesen Bereichen derzeit noch sehr unterschiedlich. Und das, obwohl Ausfälle der IT-Systeme dieser Kritischen Infrastrukturen weitreichende, teils sogar dramatische Folgen für die Gesellschaft haben würden. Es leuchtet daher unmittelbar ein, dass in diesen Bereichen höhere Anforderungen an die IT-Sicherheit gelten müssen als in anderen Bereichen des gesellschaftlichen Lebens. Auf freiwilliger Basis bestehende Angebote und Initiativen in Anspruch zu nehmen, reicht hier nicht aus. Das IT-Sicherheitsgesetz nimmt insoweit also diejenigen Aspekte von IT-Sicherheit in den Blick, deren Gewährleistung jenseits der Eigenverantwortlichkeit des Einzelnen im gesamtgesellschaftlichen Interesse liegt. Hier gibt es für den Staat eine Verantwortung, regulatorisch tätig zu werden.

Aber auch dann, wenn der Staat in einzelnen Bereichen regulatorisch tätig wird, bleibt die Gewährleistung von Sicherheit im Cyber-Raum eine gemeinsame Herausforderung für Staat, Wirtschaft und Gesellschaft. Der Gesetzgeber sollte insbesondere nicht vorgeben, bis in die kleinste Verästelung hinein alles selber regeln zu können. Es läuft auf einen kooperativen Ansatz hinaus: Die grundsätzlich betroffenen Wirtschaftszweige sind zwar gesetzt. Auch die als kritisch anzusehenden Dienstleistungen, die über das IT-Sicherheitsgesetz geschützt werden sollen. Wenn es aber im weiteren Verfahren darum gehen wird, zu bestimmen, welche Einzelsegmente der betroffenen Branchen als kritisch anzusehen und demzufolge zu regulieren sind, muss die Expertise der Wirtschaft umfassend mit einbezogen werden. Niemand kennt die Strukturen eines Unternehmens so gut wie das betreffende Unternehmen selbst. Nur im Zusammenwirken mit der Wirtschaft wird es daher möglich sein, den Adressatenkreis der Regelungen des IT-Sicherheitsgesetzes wirklich zielgenau zu bestimmen. Entsprechendes gilt für die Entwicklung

branchenweiter IT-Sicherheitsstandards: Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards vorschlagen. Das Bundesamt soll dann im Einvernehmen mit den zuständigen Aufsichtsbehörden und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe feststellen, ob diese geeignet sind, die gesetzlichen Anforderungen zu erfüllen.

IT-Sicherheitsgesetz – Meldepflicht

Das IT-Sicherheitsgesetz sieht für die Betreiber Kritischer Infrastrukturen neben der Einführung von IT-Sicherheitsstandards auch eine Pflicht zur Meldung von Cyber-Angriffen vor. Damit Bedrohungen im Cyber-Raum frühzeitig erkannt werden können und wirksame Vorsorge- und Gegenmaßnahmen ergriffen werden können, ist ein umfassendes Lagebild über die aktuelle Gefahrensituation im Netz notwendig. Dem berechtigten Bedürfnis der Unternehmen nach einem größtmöglichen Schutz ihrer Unternehmensinteressen soll dabei soweit wie möglich entsprochen werden: So sollen die entsprechenden Meldungen an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zum Beispiel auch ohne namentliche Nennung des Unternehmens möglich sein, solange es noch nicht zu einem gefährlichen Ausfall oder einer Beeinträchtigung der Kritischen Infrastruktur gekommen ist. Um den Aufwand bei den betroffenen Unternehmen möglichst gering zu halten, sieht das Gesetz außerdem vor, dass bereits etablierte Meldewege und -verfahren soweit wie möglich erhalten bleiben. Die Umsetzung dieser Meldepflicht bedeutet für die betroffenen Unternehmen einen zusätzlichen Aufwand. Sie wird den Unternehmen vor allem aber auch einen deutlichen Mehrwert bringen: Nach Auswertung der beim BSI eingehenden Informationen zu Sicherheitslücken, Schadprogrammen und Angriffen auf die IT-Systeme sowie möglichen Auswirkungen auf die Verfügbarkeit der Kritischen Infrastrukturen werden gefährdete Betreiber vom Bundesamt umgehend unterrichtet, damit dort die erforderlichen Maßnahmen zum Schutz der Infrastrukturen eingeleitet werden können. Die Unternehmen leisten also durch ihre Meldungen einen eigenen Beitrag und bekommen dafür im Gegenzug ein Mehrfaches an Informationen und Know-how zurück. Es ist in diesem Sinne also eine typische Win-win-Situation!

Die Umsetzung der genannten Maßnahmen wird mittelfristig zu einem deutlichen Gewinn an IT-Sicherheit in Deutschland Land führen, von dem der Wirtschaftsstandort insgesamt profitieren wird. Mit dem IT-Sicherheitsgesetz möchte Deutschland international Vorreiter und Vorbild für die Entwicklung in anderen Ländern sein und so nicht zuletzt auch deutschen Sicherheitsunternehmen Exportchancen eröffnen.

Datenschutz-Grundverordnung

Begleitet werden müssen diese Entwicklungen von einem modernen Datenschutzrecht, das in Bezug auf die Risiken des Internetzeitalters besseren Schutz bietet und gleichzeitig die Chancen und Freiheiten des Internets wahrt. Die geltenden Regelungen des Datenschutzrechts werden der technischen Entwicklung und Vernetzung nicht mehr gerecht. Insbesondere „Big Data“ und „Predictive Analytics“ entwickeln sich zu einem zentralen Thema, denn die hergebrachten Grundsätze des Datenschutzrechts laufen den Möglichkeiten von Big Data-Analysen teilweise diametral zuwider:

- Das betrifft zum Beispiel den Grundsatz der Datensparsamkeit: Big Data beruht auf dem Grundsatz der Datenmaximierung. Je mehr Daten vorhanden sind, desto besser die daraus gewonnenen Ergebnisse.
- Das betrifft aber beispielsweise auch den Zweckbindungsgrundsatz: Big Data kennt keine Zweckbegrenzung. Daten werden ständig de- und rekontextualisiert. Sie werden für alle denkbaren Zwecke analysiert, insbesondere auch für solche, die zum Zeitpunkt der Datenerhebung noch nicht erkennbar waren.
- Das betrifft vor allem aber auch das Einwilligungserfordernis: Aufgrund von Menge und Heterogenität der zu analysierenden Daten ist die Einholung der Einwilligung bei Big-Data-Analysen illusorisch.

Mit der Datenschutz-Grundverordnung eröffnet sich die Chance, das Datenschutzrecht in Europa so zu modernisieren, dass es den Herausforderungen des digitalen Zeitalters gerecht wird. Eine Lösung könnte ein rechtsgutsbezogener, risikobasierter Ansatz. Darunter ist zu verstehen, dass ein Datenverarbeiter je nach Risiko seiner Datenverarbeitung für einzelne Rechtsgüter bestimmte abgestufte Vorsichts- und Schutzmaßnahmen ergreifen muss. Je höher das Risiko der „Big-Data“-Analyse für das Persönlichkeitsrecht, desto schärfer die einzuhaltenden Pflichten. Die mögliche Bandbreite reicht von einer Freigabe bestimmter risikoloser „Big-Data“-Analysen bis hin zu einem Verbot besonders risikobehafteter Analysen.

Neben der Einwilligung kommen insbesondere Transparenzgebote und Informationspflichten als Schutzmaßnahmen zugunsten des Betroffenen in Betracht. Es ist mit Sorge zu betrachten, wenn im Bereich des Datenschutzes mit grundsätzlich sinnvollen Instrumenten wie der Einwilligung die Verantwortung auf die Nutzer abgewälzt werden kann. Im Internetzeitalter wird die Einwilligung oft zu einem formalisierten Akt, der beim Nutzer die Illusion der Kontrolle über „seine“ Daten erweckt und der die Illusion nährt, Einfluss auf die Datenverarbeitung zu haben. Tatsächlich hat der Nutzer nach Abgabe seiner Einwilligung kaum mehr einen Einblick in die Weiterverarbeitung seiner Daten. Dieser Intransparenz kann nur mit entsprechenden Transparenzgeboten begegnet werden! Man muss daher von Unternehmen erwarten und einfordern, dass sie ihrer Verant-

wortung im Sinne eines freien Internets, zu dem auch der Schutz der Privatsphäre, der Schutz von Persönlichkeitsrechten und der Schutz vor digitaler Diskriminierung gehört, gerecht werden.

Andererseits: Dem Datenverarbeiter zu viele Pflichten aufzuerlegen führt aber nur dazu, dass diese Pflichten in der Praxis nicht beachtet werden („Weniger-ist-mehr“-Paradoxon). Und eine strukturelle Nichtbeachtung des Datenschutzrechts führt dazu, dass die Autorität und Legitimität des Rechts untergraben wird. So gut unsere Instrumente zur Cyberabwehr und unsere Regelungen zum Datenschutz auch sein mögen: Es kommt auch hier entscheidend auf die Initiative und den Willen von Gesellschaft und Wirtschaft an. Das Bewusstsein für mehr Datenschutz und Datensicherheit im Netz muss daher weiter steigen. Zwei Zahlen sind in diesem Zusammenhang interessant:

- 80 % der Smartphone-Nutzer in Deutschland haben keinerlei Schutzsoftware auf ihrem Gerät installiert.
- 95 % der Bundesbürger verschlüsseln ihre Mails – meist mit vertraulichem Inhalt – nicht.

Hier muss sich etwas ändern! Aber das kann und soll nicht staatlich verordnet werden. Hier muss man – nicht zuletzt auch aus grundsätzlichen ordnungspolitischen Erwägungen heraus – auf die Selbstorganisation von Wirtschaft und Gesellschaft im Sinne einer Hilfe zur Selbsthilfe vertrauen. Staatliche Informationsangebote sind ja vorhanden.

Ausblick

Viele Fragen der Digitalisierung sind heute nur noch international, global zu lösen. Das findet mittlerweile auch seinen Niederschlag in der Agenda der internationalen Politik, sei es bei G7 und G8, bei der OSZE, bei OECD und APEC, in der NATO, in der EU oder bei den Vereinten Nationen. Grundlage für den Erfolg der internationalen und europäischen Initiativen ist jedoch zuallererst ein entschlossenes nationales Handeln, bei dem alle Akteure ihrer jeweiligen Verantwortung nachkommen.

Sicherheit im Wandel von Technologien und Märkten
Tagungsband zur vierten EIT ICT Labs-Konferenz zur
IT-Sicherheit

Bub, U.; Deleski, V.; Wolfenstetter, K.-D. (Hrsg.)

2015, X, 61 S. 3 Abb. in Farbe.,

ISBN: 978-3-658-11274-5