

Essay

Mit Netz und doppeltem Boden

Von Thomas de Maizière 8. Dezember 2009, 04:00 Uhr

Eine freiheitliche Gesellschaft braucht freie und sichere Kommunikation im Internet. Dafür muss der Staat den Ordnungsrahmen schaffen. Nicht mehr - aber auch nicht weniger

Man kennt die Szene aus Comicfilmen: Eine Figur rennt auf einen Felsen, sieht den Abgrund nicht und rennt über ihn hinaus. Sie läuft für Momente einfach in der Luft, ohne abzustürzen und ohne zu merken, dass kein fester Boden mehr da ist. Irgendwann erkennt die Comicfigur, dass etwas nicht stimmt, blickt hinab, die Gesetze der Schwerkraft gelangen wieder zur Geltung. Sie fällt nach unten. Ist das die Situation, auf die unsere Informationsgesellschaft zusteuert? Wir haben durch die digitale Revolution den Boden der altbekannten Welt verlassen und erschließen uns einen virtuellen Raum der Freiheit, in der Information und Kommunikation, Handel und Handeln sich rasant und tief greifend verändern.

In diesem Raum scheinen die Regeln, die uns bislang Halt gaben, nicht mehr vollständig zu greifen. Wir merken, dass etwas anders geworden ist, und suchen nach neuen Antworten: Was für eine Gemeinschaft entsteht im und durch das Netz? Ist es mehr als eine Erregungsgemeinschaft rund um Gerüchte, Skandale und Kuriositäten? Und ist das Internet sicher genug? Wie können wir Datenmissbrauch, Betrug und extremistischer Hetze im World Wide Web Einhalt gebieten? Befinden wir uns, wie im Comicfilm, im Augenblick des Erkennens, dem ein unsanfter Absturz folgen wird?

Nein, das tun wir nicht. Manche Gehversuche im virtuellen Raum mögen noch etwas unbeholfen wirken, und davon nehme ich die Politik nicht aus. Aber selbst Bedenkenträger werden eingestehen müssen, dass die neuen Informations- und Kommunikationsmedien riesige Chancen eröffnen, wenn wir das Laufen erst einmal gelernt haben. Die Informationsgesellschaft wird mit neuen Unsicherheiten und neuen Gefährdungen leben müssen. Dabei darf der Staat seine Hände nicht passiv in den Schoß legen. Aber wir müssen auch die Anliegen des Teils der Netzgemeinschaft ernst nehmen, der sich unverstanden und vom Staat als Gesprächspartner nicht ernst genommen fühlt.

Am 8. Dezember findet in Stuttgart der vierte Deutsche IT-Gipfel der Bundesregierung statt. Dieses Forum sollten wir nutzen, um die drängenden Fragen nach der Verantwortung für Freiheit und Schutz der Bürger im Internet zu stellen. Der IT-Gipfel kann nur ein Anstoß für diese fällige Debatte sein. Ich werde schon sehr bald Vertreter aus Zivilgesellschaft, Verbänden, Netzgemeinschaft und Wissenschaft zur Diskussion einladen. Ziel unserer Bemühungen sollte es sein, die Freiheit und Sicherheit der Bürger auch im virtuellen Raum zu

gewährleisten, das Vertrauen in das Internet zu erhalten, seine Potenziale für Gesellschaft und Demokratie zu erschließen und gute Rahmenbedingungen für Innovationen zu befördern.

Das Internet ist fester Bestandteil unseres Lebens geworden. Es hat die Wirtschaftswelt revolutioniert. Nach einer Umfrage des Branchenverbandes Bitkom wollen zum Beispiel über 14 Millionen Deutsche ihre Weihnachtseinkäufe dieses Jahr online erledigen. Die Informations- und Kommunikationstechnologie liegt, gemessen an der Bruttowertschöpfung, mit rund 90 Milliarden Euro vor dem Maschinen- und Automobilbau auf Platz eins der Industriesektoren in Deutschland.

Auch gesellschaftspolitisch hat das Internet weitreichende Entwicklungen angestoßen. Immer mehr Bürger nutzen es als erste oder sogar überwiegende Informationsquelle. Das Internet ermöglicht mehr und schnelleren Meinungs austausch. Es bietet die Plattform für mehr Teilhabe und Transparenz. Es ist für den Zusammenhalt in der Gesellschaft und für das demokratische Gemeinwesen ein entscheidender Faktor geworden. Deshalb ist die Politik gut beraten, Chancen und Risiken im Internet nicht alleine auf das Sicherheitsthema zu reduzieren. Sie sollte auch die gesellschaftspolitische Bedeutung des Themas noch besser erfassen.

Das Internet hat viele gute Seiten, aber auch Schattenseiten. Je mehr sich unser Leben ins Virtuelle verlagert, desto wichtiger wird es, sich der problematischen Entwicklungen, die es dort eben auch gibt, anzunehmen. Wir werden die Errungenschaften des digitalen Zeitalters nur dann umfassend wahrnehmen können, wenn die Nutzer keine Sorge um die Sicherheit ihrer Daten und die Integrität ihrer PCs haben müssen. Dabei halte ich es für falsch, im Staat eine bedrohende Instanz zu sehen. Er ist eine beschützende Instanz.

Kürzlich haben deutsche Banken in großer Zahl Kreditkarten ausgetauscht. Deren Daten waren bei einem Dienstleister abhanden gekommen, und ihr Missbrauch wurde befürchtet. An anderer Stelle sind offenbar gestohlene Passwörter zahlreicher E-Mail-Konten aufgetaucht. Auch in sozialen Netzwerken oder Karriereplattformen sind "Datensammler" am Werk, die es auf die dort eigentlich nur für einen kleinen Kreis hinterlegten persönlichen Daten abgesehen haben. Die Polizei registriert insgesamt eine erhebliche Zunahme von Angriffen auf persönliche Daten und digitale Identitäten.

Nicht zuletzt haben Kriminelle unter Ausnutzung von Sicherheitslücken heimlich Programme auf private PCs eingeschleust, mittels derer sie diese fernsteuern können; Schätzungen gehen von 60 bis 250 Millionen "Zombie"-PCs weltweit aus. Wir wissen spätestens seit den Vorfällen in Estland im Jahr 2007, dass Kriminelle, wenn sie eine große Zahl solcher Rechner zusammenschließen, Teile der IT-Infrastruktur eines ganzen Landes lahmlegen können. Eine aktuelle Studie hat ergeben, dass sich gut die Hälfte der privaten PC-Besitzer bei der Nutzung des Internets unsicher fühlt. 87 Prozent der Befragten können die Sicherheitsprobleme auf ihrem PC nicht ohne fremde Hilfe lösen. Der Einzelne ist angesichts der komplexen Technik immer weniger imstande, sich adäquat gegen Angriffe auf seine digitale Identität zu wehren oder sie überhaupt zu erkennen.

Hersteller von Betriebssystemen und Software haben die Sicherheit ihrer Systeme in den vergangenen Jahren deutlich gesteigert, dennoch finden Kriminelle noch genügend Lücken. Anbieter von Dienstleistungen im Internet, nicht zuletzt die Banken, befinden sich in einem steten Wettlauf, um ihre Angebote gegen kriminelle Zugriffe abzusichern. Und selbst wenn der eigene PC nicht betroffen ist: Personenbezogene Daten werden heutzutage bei unterschiedlichsten Anbietern gespeichert und verarbeitet. Die Nutzer selbst hinterlegen ihre Daten in sozialen Netzwerken wie Facebook oder StudiVZ oder veröffentlichen sie in Blogs. Gerade Zahlungsverkehrsdienstleister oder E-Mail-Provider verfügen über sensible Datensammlungen. Private Anbieter wissen überhaupt viel mehr über die Bürger als der Staat. Entsprechend groß ist die Verantwortung, die private Anbieter tragen, und entsprechend

notwendig ist es, dass sie selbst dem Thema Datensicherheit die hohe Bedeutung beimessen, die ihm zukommt.

Staatlicherseits ist Sicherheit im Internet nicht alleine mit den Mitteln des Straf- und Ordnungsrechts zu erreichen. Natürlich muss der Staat Betrug, Diebstahl, Missbrauch oder extremistische Hetze auch im Internet verfolgen. Die Verantwortung für ein sicheres Internet aber soll und kann nicht alleine der Staat übernehmen. Es ist eine gesamtgesellschaftliche Aufgabe. Einer freiheitlich verfassten Gesellschaft entspricht es, dass dabei die Freiheit und Verantwortung des Einzelnen im Vordergrund stehen. Aber um Freiheit eigenverantwortlich wahrnehmen zu können, bedarf es auch eines staatlichen Ordnungsrahmens. Sicherlich werden Unternehmen, die im oder mit dem Internet Geld verdienen, einen Teil der Verantwortung tragen müssen. Sie müssen genügend Know-how und geeignete Vorrichtungen aufbauen, um sensible Datenbestände zuverlässig zu schützen.

Provider, die den Zugang zum Internet für den Endkunden eröffnen, sind in besonderem Maß geeignet und verpflichtet, Nutzer auch bei der Sicherung ihrer persönlichen Daten und ihres PCs zu unterstützen. So bieten heutzutage die meisten E-Mail-Provider ihren Kunden Schutzmöglichkeiten vor Viren und unerwünschten Spam-Mails an. Besondere Sorgfaltspflichten können sich auch für die Anbieter digitaler Identitäten ergeben. Ob der Zugang zum Online-Banking, das Kundenkonto beim Online-Händler oder das Konto bei einem sozialen Netzwerk: Entsprechend der Sensibilität der hier erzeugten digitalen Identitäten müssen auch angemessene Vorkehrungen zu deren Schutz getroffen werden.

Auch der einzelne Nutzer kann nicht aus seiner Verantwortung entlassen werden. Angeboten zur Stärkung der Eigenverantwortlichkeit, der Aufklärung, aber auch der Transparenz der Datenverarbeitung kommt eine besondere Bedeutung zu.

Die Aufgabe des Staates besteht darin, den im gesellschaftlichen Konsens gefundenen Ordnungsrahmen abzusichern und seinen Bürgern die notwendigen rechtlichen und organisatorischen Instrumente für ihre Freiheitsausübung an die Hand zu geben. Dies kann einerseits - ganz klassisch - durch Rechtsetzung erfolgen. Der Staat kann aber auch eigene Angebote machen und Instrumente für einen freien und sicheren Gebrauch des Internets bereitstellen. Ich nenne hier nur zwei Beispiele: Mit DE-Mail wollen wir den Rechtsrahmen für eine fortschrittliche E-Mail-Kommunikation schaffen, der es Providern ermöglicht, einen nach einheitlichen Standards funktionierenden sicheren Kommunikationsweg anzubieten. Der neue Personalausweis wird die Möglichkeit beinhalten, ihn auch zur sicheren elektronischen Identifikation und Kommunikation im Internet zu nutzen. Beide Angebote sind gut und erfüllen hohe Standards.

Ein substanzieller Dialog kann nur in Gang kommen, wenn die Beteiligten bereit sind, aufeinander zuzugehen und einander zu vertrauen. Die Gräben zwischen Staat und Teilen der Netzgemeinschaft sind unübersehbar, aber nicht unüberbrückbar. Angstmachen gilt nicht: Wir [steuern](#) auf keinen Abgrund zu. Wir steuern auch nicht auf eine Welt zu, in der es dem freiheitlich verfassten Staat darum ginge, das Internet zu erobern, zu zensieren und umfassend zu kontrollieren. Unsere freiheitliche Gesellschaft braucht freie und sichere Kommunikation im Internet. Dies sicherzustellen ist eine Aufgabe des Staates. Im Dialog mit der Netzgemeinschaft will ich diese Aufgabe angehen.
