März 2013

Deutsches Institut für Vertrauen und Sicherheit im Internet

DIVSI magazin

DIVSI Entscheider-Studie

Digital Souveräne auf Distanz zum Staat: Läuft die Zeit für unser System in seiner jetzigen Form ab?

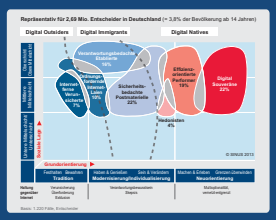
Tragen Sie zu einer neuen Computer-Ethik bei?

Hacker als Agenten des Fortschritts?

Eine Bilanz der „Enquete-Kommission Internet und Digitale Gesellschaft“

Der Anfang ist gemacht

Inhalt



Haben Sie Fragen oder wünschen Sie weitere Informationen?

So erreichen Sie das Deutsche Institut für Vertrauen und Sicherheit im Internet (DIVSI):

Web: www.divsi.de
E-Mail: info@divsi.de

Öffentlichkeitsarbeit:
E-Mail: presse@divsi.de
Tel.: + 49 40 226 369 895

Wissenschaftliche Leitung:
Joanna Schmölz
E-Mail: wissenschaft@divsi.de
Tel.: + 49 40 226 369 896

Anschrift:
DIVSI
Mittelweg 142
20148 Hamburg

Von Uhrmacher-Kunst, der Entscheider-Studie und Liebe zum Detail

Nehmen wir mal eine Uhr. Ein richtig edles Teil, das man sich nach langem Sparen gönnt und über Generationen vererben kann. Der Laie ahnt nicht einmal, wie dort im Inneren die Zahnrädchen ineinander greifen. Doch sie tun es. Und am Ende zeigt unsere Traumuhr nicht nur die Zeit. Manche Modelle faszinieren mit einem mechanisch funktionierenden ewigen Kalender, den selbst Schaltjahre nicht verwirren. Der Uhrmacher erklärt dieses Wunderwerk an Präzision schlicht so:

Ein kleines an den Monatsmechanismus gekoppeltes Planetenzahnrad vollführt in einem Zeitraum von vier Jahren eine vollständige Drehung. Im vierten Jahr zeigt der Mechanismus den 29. Februar an, bevor es direkt zum 1. März übergeht. Genau wie beim Umlauf des Mondes um die Erde dreht sich dieses kleine Planetenrad um seine eigene Achse und wird dabei von einem Schwenkrad gestützt.

Warum ich Ihnen das erzähle?

Weil die Arbeit an einer neuen Studie – wenn sie denn wissenschaftlich fundiert, belastbar und aussagekräftig sein soll – nach ähnlichen komplizierten Mechanismen abläuft wie die hohe Schule der Uhrmacher-Kunst.

Liebe zum Detail, Geduld und Fingerspitzengefühl sind entscheidend. Beim Bau wertvoller Uhren ebenso wie bei der Erstellung von Studien, deren Aussagen auch kritischen Betrachtungen Stand halten. Ein paar Zahlen mögen belegen, welch' praktisch-technischer Aufwand hinter der Entscheider-Studie steckt:

13.105 Adressen wurden in die Ausgangsstichprobe eingespielt. Auf dieser Basis waren 70.491 Kontaktversuche notwendig, um insgesamt 1.221 Interviews zu realisieren. 37 Interviewer telefonierten dafür 2.928 Stunden. Im Schnitt waren 58 Versuche erforderlich, um ein Interview mit einem Entscheider durchzuführen. Zur reinen „Feldarbeit" (2.928 Stunden) addieren sich für den zeitlichen Gesamtaufwand 190 Stunden der Fragenentwicklung sowie 970 Stunden für Auswertung, Analyse und Berichtslegung.

Um im Uhrmacher-Bild zu bleiben: Allein schon dieser Einsatz zeigt, dass DIVSI mit seiner bundesweit repräsentativen Entscheider-Studie nicht einfach nur die Zeit anzeigen will. Über wesentliche Punkte dieser Untersuchung informieren wir ausführlich in diesem Heft.

Was bietet diese erste Ausgabe des DIVSI magazins 2013 außerdem?

Die Enquete-Kommission Internet und digitale Gesellschaft hat ihre Arbeit abgeschlossen. Harald Lemke hatte den Vorsitz in der Projektgruppe „Zugang, Struktur und Sicherheit im Netz". Sein persönlicher Rückblick ist ab S. 13 zu finden.

Prof. Dr. Hans Peter Bull war der erste Bundesbeauftragte für den Datenschutz. Jetzt hat der anerkannte Hamburger Rechtswissenschaftler ein neues Buch geschrieben. „Hacker als Agenten des Fortschritts?" heißt dabei eine seiner provokanten Thesen. Wir informieren auf S. 16.

Dr. Göttrik Wewer, ehemaliger Staatssekretär im Innenministerium, hat in jüngster Zeit bundesweit viel Beachtung mit Aufsätzen rund um das Thema „Vertrauen" erfahren. Sein aktueller Ansatz: Vertrauen ist wie ein geldwerter Vorteil. Warum das so ist, steht auf S. 18.

Wie können Digital Outsiders an das Internet heran geführt werden? Zur Lösung dieser wichtigen Frage gibt es mittlerweile viele Ansätze. Eine Möglichkeit haben Andreas Dautermann und Kristoffer Braun entwickelt. Ihr Projekt heißt „Starthilfe50". Ein Interview auf S. 24.

Ich wünsche Ihnen informative Unterhaltung mit dem neuen „DIVSI magazin". Und schließe wie gewohnt auch dieses Vorwort mit einem Wunsch: Wenn unser Heft Ihnen gefällt – erzählen Sie es unbedingt weiter. Im anderen Fall sagen Sie bitte mir Bescheid.

Jürgen Selonke
Chefredakteur
DIVSI magazin

Pressekonferenz in Berlin

Große Resonanz auf die DIVSI Entscheider-Studie

Berlin – Im Tagungszentrum der Bundespressekonferenz am Schiffbauerdamm in Berlin hat Direktor Matthias Kammer zusammen mit Dr. Silke Borgstedt (SINUS) die neue, bundesweit repräsentative „DIVSI Entscheider-Studie zu Vertrauen und Sicherheit im Internet" vorgestellt. Er erinnerte eingangs an ein wesentliches Ergebnis aus der DIVSI Milieu-Studie von Anfang 2012: Demnach erwarten fast 75 Prozent der in Deutschland lebenden Bevölkerung, dass Staat und Wirtschaft aktiv für Sicherheit im Internet sorgen. Bislang war jedoch ungeklärt geblieben, wie Entscheider aus den angesprochenen Bereichen zu dieser Erwartung der Bevölkerung stehen. Die entsprechenden Antworten liegen jetzt vor. Die mit großem Interesse aufgenommenen Fakten der neuen Untersuchung belegen nämlich, dass die Entscheider mehrheitlich die Hauptverantwortung bei den Nutzern sehen. Dabei räumen die Befragten gleichzeitig ein, dass diese sich keineswegs auskennen. Matthias Kammer: „Der Nutzer hat den Schwarzen Peter."

DIVSI-Schirmherr Prof. Dr. Roman Herzog zur Entscheider-Studie

Die jetzt in Berlin vorgelegte Entscheider-Studie gibt fraglos Denk-Anstöße in verschiedene Richtungen. Sie ermuntert auch, über soziale und ethische Fragen aus gänzlich neuen Blickwinkeln nachzudenken. Erstmals und in bislang nicht gekannter Klarheit lässt sich aus den Ergebnissen ein möglicher gesellschaftspolitischer Umbruch ablesen. Für mich eine der wesentlichen Erkenntnisse dieser Entscheider-Studie.

Mich hat dieses Ergebnis der sorgfältigen Untersuchung äußerst nachdenklich gestimmt: Die Digital Souveränen unter den Entscheidern, also die nachwachsende Elite unseres Landes, hat im Vergleich zu anderen Teilnehmern der Studie das geringste Vertrauen in das politische System, ja sogar in unseren Rechtsstaat selbst. Hier könnten Entwicklungen zu einem Abrücken vom Rechtsstaat und vom Staat gegebenen Garantien im Gange sein.

Was bedeutet das für unser Land und für unser aller Zukunft? Die Gruppe der Digital Souveränen immerhin ist die Avantgarde unter den Führungskräften. Steuern wir durch diesen natürlichen Prozess womöglich einer allgemeinen Vertrauenskrise entgegen?

Ich will über diese offengelegte Tendenz nicht weiter philosophieren, sondern einfach davor warnen, sie leichtfertig zu ignorieren. Eine mögliche Entwicklung zu erkennen und zu benennen, ist immer nur der erste Schritt. Wir brauchen Vertrauen in unser politisches System, unseren Staat. Ich empfehle den Verantwortlichen, die Erkenntnisse der Studie ernst zu nehmen.

Noch etwas anderes glaube ich aus der Studie zu erkennen: Die Tonalität, der wechselseitige Umgang, das Vertrauen zueinander scheint mir zunehmend belastet. Da werden Verantwortlichkeiten und Schwarze Peter hin- und hergeschoben, da traut man – besonders den Politikern – wenig zu. Da werden Internet-Unkundige mit Neandertalern verglichen.

Ich würde mir wünschen, statt dessen das Miteinander, das Menschliche mehr in den Fokus zu rücken. Auch und gerade im Zeitalter des Internets. Um das Vertrauen ins Internet, in die mit ihm eröffneten Chancen und Möglichkeiten nicht zu verspielen, brauchen wir eine breite Diskussion darüber, welche verbindlichen Spielregeln hier gelten sollen. Wir brauchen Leitplanken, die uns auf dem richtigen Weg halten. Ein digitaler Kodex, von allen Verantwortlichen getragen, könnte ein Weg dahin sein.

Dennoch empfehlen die Entscheider den Nutzern, sich vor allem auf eigene Erfahrung und Bildung zu verlassen. Niemand könne ihnen die Verantwortung abnehmen. Am wenigsten sollte man sich auf das deutsche Rechtssystem und die Internet-Gemeinde verlassen.

Was ist angesichts dieser deutlich auseinander klaffenden Schere jetzt zu tun?

Matthias Kammer beantwortete diese Frage so: „Es gibt keine Spontan-Lösung. Gleichwohl scheint es mir wichtig, dass dieses Dilemma offen und durch wissenschaftliche Untersuchungen gestützt unübersehbar auf dem Tisch liegt. Die eine Seite wünscht sich Schutz. Die andere Seite macht dagegen kein Hehl daraus, dass sie diesem Wunsch nach Schutz wenig Interesse schenkt. Eine für alle Beteiligten gerechte Lösung im Sinne eines sichereren Umgangs mit dem Internet wird sich nur finden lassen, wenn vorurteilsfreie Gespräche in Gang kommen."

Bereits unmittelbar nach der Pressekonferenz war die bundesweite Resonanz auf die vorgelegten Fakten erheblich. Quer durch alle unterschiedlichen Medien konzentrierte sich die Presse-Reaktion auf die DIVSI Entscheider-Studie vor allem auf drei Ergebnisse der Untersuchung. Nachdrücklich wurden dabei diese Punkte herausgestellt:

- Führungskräfte haben nur geringes Vertrauen in die Sicherheit von Daten im Netz. 68 Prozent der Entscheider meinen, dass es vollständige Sicherheit im Internet nicht geben kann.
- 70 Prozent sehen die Dominanz globaler Internet-Riesen skeptisch. Dagegen spielt die Politik nach Ansicht der Entscheider nur eine untergeordnete Rolle.
- Die größte Gefahr droht den Unternehmen und Organisationen nach Ansicht ihrer Chefetagen von Hackern im Netz. Für 92 Prozent der Befragten liegen hier die größten Risiken.

Eine ausführliche Vorstellung der „DIVSI Entscheider-Studie zu Vertrauen und Sicherheit im Internet" finden Sie auf den folgenden Seiten.

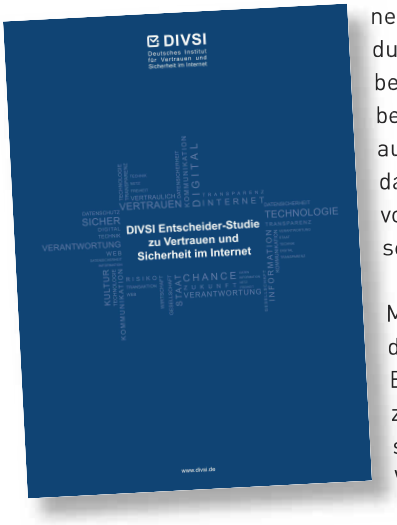
Die Studie kann kostenfrei im Internet (www.divsi.de) heruntergeladen oder in gedruckter Form bei DIVSI (Mittelweg 142, 20148 Hamburg) sowie unter info@divsi.de bestellt werden.

Die Mühen haben sich gelohnt

DIVSI Entscheider-Studie: Basis für interdisziplinäre Diskussionen

Von Matthias Kammer

Hamburg - Wer steckt hinter dem Internet? Wer sind die Entscheider, Macher und Beobachter? Welche Einflussmöglichkeiten haben diese Akteure, wie schätzen sie die Nutzer ein, was sagen sie zu Sicherheits- und Freiheitsbedürfnissen? Die aktuelle DIVSI Entscheider-Studie, bundesweit repräsentativ und wissenschaftlich untermauert, hatte einen umfangreichen Punktekatalog abzuarbeiten.



Die neue Studie von DISVSI wurde jetzt in Berlin vorgestellt. Sie ist bundesweit repräsentativ, bündelt auf 120 Seiten wissenschaftlich fundierte Aussagen.

Die Mühen haben sich gelohnt. Die neue Untersuchung, wiederum durch das renommierte Heidelberger SINUS-Institut realisiert, beantwortet nämlich nicht nur alle aufgeworfenen Fragen. Sie füllt darüber hinaus eine Lücke, die voraus gegangene Studien gelassen haben.

Motivationen und Einstellungen der in Deutschland lebenden Bevölkerung in ihrem Verhältnis zum Internet sind spätestens seit der „DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet“ bekannt. Dargelegt ist dort auch, welche Erwartungen die Menschen hinsichtlich Sicherheit und Datenschutz haben.

Aber auch unsere Untersuchung betrachtete den fortschreitenden Digitalisierungsprozess – wie fast alle ähnlich gelagerten Arbeiten zu diesem Thema – aus der Nutzer-Perspektive. Seither tauchte in Diskussionen über die Studie, die oft auch interdisziplinär geführt wurden, immer wieder die Frage nach der Verantwortung für das Internet auf, nach dem Gestaltungsmandat.

Relativ einfach ließen sich aus den verschiedenen Bereichen unserer Gesellschaft Entscheider identifizieren. Bei einem zweiten Blick zeigte sich jedoch, dass wenig bis gar nichts dazu bekannt ist, welche Einstellungen diese Gruppen zum Internet haben, was ihre Intentionen sind, wo sie Chancen und Gefahren sehen.

Diese Erkenntnis gab letztlich den Anstoß zur DIVSI Entscheider-Studie. Vorausgegangen ist ihr eine qualitative Untersuchung, deren Ergebnis wir im November 2012 vorlegen konnten.

Aus den jetzt vorliegenden Ergebnissen lassen sich fünf wesentliche Aussagen ableiten. Sie mögen nicht immer ungeteilte Zustimmung erfahren. Das wird uns jedoch nicht daran hindern, auch unwillkommene Fakten zur Diskussion zu stellen.

In Schlagzeilen gepresst lesen sich diese herausragenden Erkenntnisse so:

- Es gibt kein Offline-Leben mehr
- Sicherheit im Internet ist ein Top-Thema – aber eine Illusion
- Die Privatwirtschaft macht das Netz
- Die Hauptverantwortung liegt beim Nutzer, doch der kennt sich nicht aus
- Risikoverursacher im Netz sind Hacker, globale Internet-Dienstleister und unbedachte Nutzer

Dr. Silke Borgstedt, beim SINUS-Institut verantwortlich für die Realisierung der DIVSI Entscheider-Studie, erläutert diese Headlines im Detail (s. ab Seite 10).

Die Ergebnisse der Studie zeigen nach meiner Einschätzung auch: Die Digitalisierung wird die Entwicklung des 21. Jahrhunderts zentral prägen. Dies beinhaltet aus Sicht der Entscheider eine Veränderung von Selbstverständlichkeiten. Vieles muss neu definiert und ausgehandelt werden.

Auffällig ist weiter, dass eine Gesamtverantwortung für „das Internet“ von den Entscheidern strukturell weder als möglich erachtet wird noch gewollt ist. Ihre Lösung besteht darin, die Verantwortung zu großen Teilen an den Nutzer weiter zu reichen. Hier stehen uns sicher noch Diskussionen bevor, ob man es sich mit dieser Sichtweise nicht zu einfach macht.

Das Gebot der Stunde – so ein Ergebnis der Studie – sei Eigenverantwortung. Unter dieser Prämisse sollten sich die

Nutzer im Internet bewegen. Der Nutzer sei selbst schuld, wenn er Risiken im Internet leichtfertig übersieht.

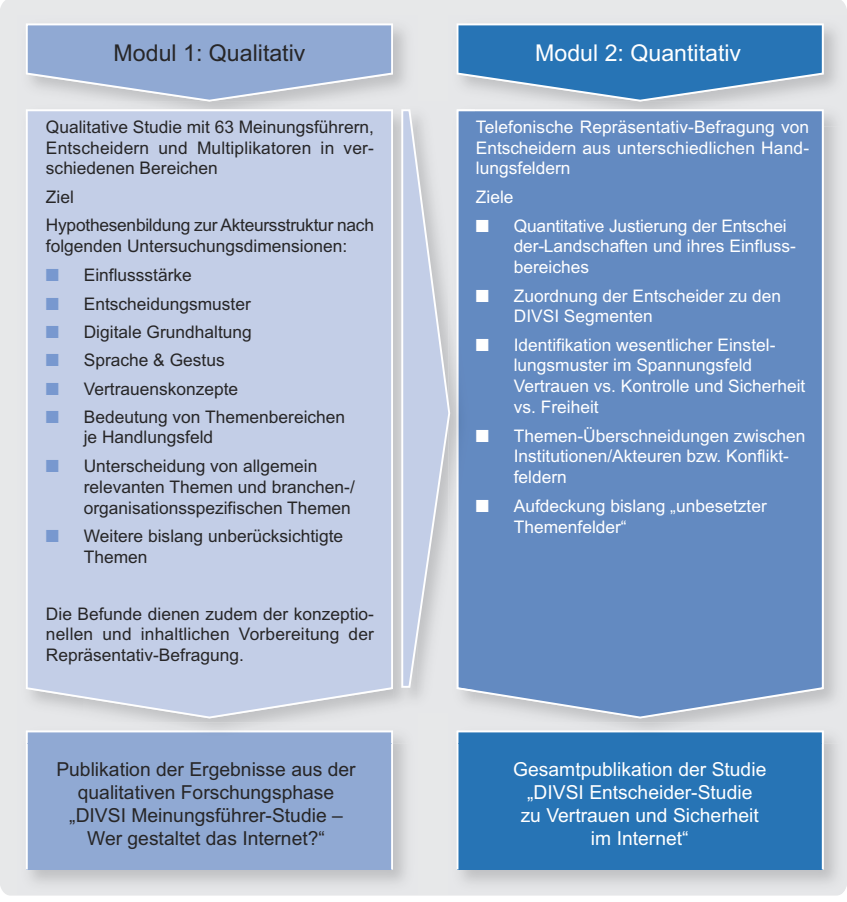
Verhält es sich tatsächlich so?

Auffällig ist auch, dass den Machern des Netzes die Formulierung eines übergeordneten Werte-Kodex geradezu utopisch erscheint. Aus Sichtweise der Entscheider wird es immer schwieriger, Rechtsgrundlagen zu schaffen, die wirksam und durchsetzbar sind. Dies auch vor dem Hintergrund, dass das Internet ein globales Phänomen ist.

Es ist gut, dass diese Ansicht nunmehr offen auf dem Tisch liegt. Es ist aber nicht gut, sie einfach zu akzeptieren. Es lohnt sich mit Sicherheit, die Diskussion um einen Werte-Kodex für das Zusammenleben in der Gesellschaft im digitalen Zeitalter aufzunehmen und voranzubringen.

Wir haben deshalb den Versuch gestartet, mit unserem Schirmherrn Prof. Dr. Roman Herzog einen solchen Kodex zu entwickeln. Die Schwierigkeiten auf diesem Weg sind uns sehr wohl bewusst. Gleichwohl liegt darin eine wichtige gesellschaftspolitische Aufgabe, die unbedingt in Angriff genommen werden sollte.

Das Stufenmodell der DIVSI Entscheider-Studie



Bereits jetzt wird es immer schwieriger, für den Verhandlungsraum Internet generell gültige Regelungen und gegenseitige Vereinbarungen zu treffen. Der Diskurs bewegt sich von einer rein technologischen Perspektive zunehmend zu einer Frage nach der „digitalen Kultur“.

Die DIVSI Entscheider-Studie macht auch deutlich, dass Hackerangriffe als das größte Risiko im Internet angesehen werden. Neun von zehn Entscheidern stimmen darin überein, dass eine Garantie gegen derlei Angriffen nicht gegeben werden kann. Interessant ist in diesem Zusammenhang die provokante These von Prof. Dr. Hans Peter Bull, der fragt: „Hacker als Agenten des Fortschritts?“ (s. ab S. 16).

Neben den reinen faktischen Erkenntnissen gibt die Entscheider-Studie Hinweise darauf, dass ein größerer

***Matthias Kammer**, Direktor des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI)*

gesellschaftlicher Umbruch im Gange ist. Im Vergleich zu allen anderen Entscheidern bekunden die Digital Souveränen das geringste Vertrauen in das politische System und unseren Rechtsstaat. Droht unserem Land angesichts dieser Antworten der Avantgarde der Führungskräfte eine allgemeine Vertrauenskrise?

Kennern unserer ersten Studie wird übrigens auffallen, dass sich die Ansichten der Entscheider teils deutlich von den im letzten Jahr ermittelten Einstellungen und Handlungsweisen der Bevölkerung unterscheiden. 39 Prozent der in Deutschland lebenden Menschen sind danach Digital Outsiders. Für die Entscheider spielt das keine Rolle. Denn aus ihrer Sicht leben auch die Digital Outsiders in einer Umgebung, die fortwährend stärker von der Online-Welt geprägt wird.

Wer ist wo verortet?

Internet-Milieus für Bevölkerung und Entscheider im Vergleich

Von Dr. Dirk Graudenz

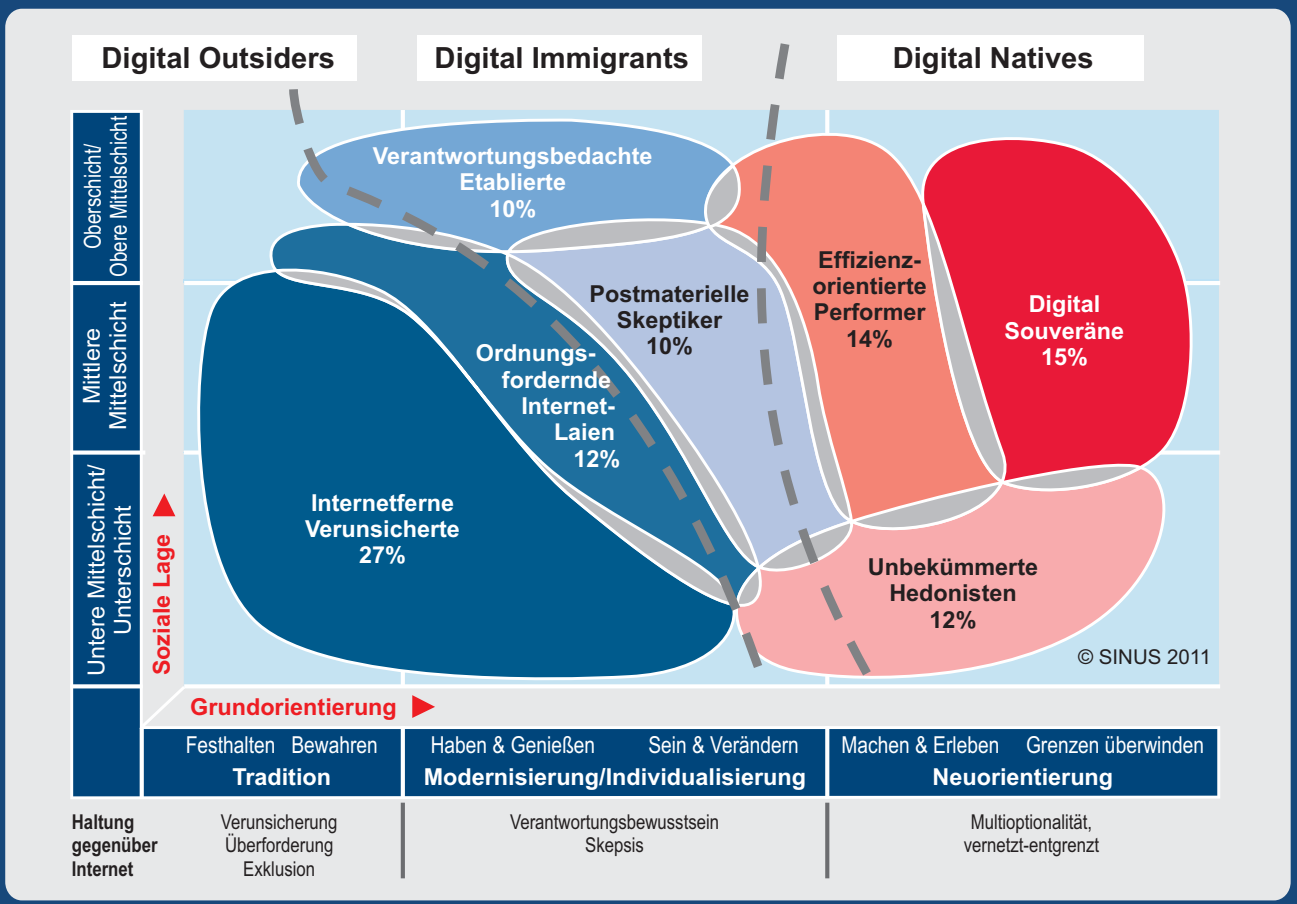
Hamburg – Im Auftrag von DIVSI hat das SINUS-Institut in zwei quantitativen Studien Bevölkerung und Entscheider zu Vertrauen und Sicherheit im Internet befragt. In beiden Studien wurden Internet-Einstellungen und die jeweiligen Lebenswelten (SINUS-Milieus), in denen das SINUS-Institut unsere Gesellschaft regelmäßig abbildet, kombiniert. Die so entstandenen DIVSI Internet-Milieus ermöglichen einen pointierten Vergleich von sozialer Lage im Sinne von Einkommen, Bildung und Berufsgruppe und soziokultureller sowie digitaler Grundorientierung dieser Gruppen.

In der Abbildung 1 (unten) sind für die Bevölkerung die sieben Internet-Milieus der Digital Souveränen, Effizienzorientierten Performer, Unbekümmerten Hedonisten, Verantwortungsbedachten Etablierten, Postmateriellen Skeptiker, Ordnungsfordernden Internetlaien und Internetfernen Verunsicherten in einem Koordinatensystem verortet. Digital Souveräne sind beispielsweise eher Mitglieder der Mittel- bzw. Oberschicht und zeichnen sich hinsichtlich ihrer Grundwerte durch eine starke Tendenz zur Neuorientierung aus (z. B. hohe Wichtigkeit von Mobilität und Globalität).

Im Gegensatz dazu sind Internetferne Verunsicherte eher Teil der sozialen Unterschicht bzw. Mittelschicht und haben in ihrer soziokulturellen Grundorientierung vielfach ein starkes Element der Tradition. Gezeigt sind in der Abbildung auch die beiden digitalen Gräben, die die Gruppen der Digital Natives, der Digital Immigrants und der Digital Outsiders voneinander trennen.

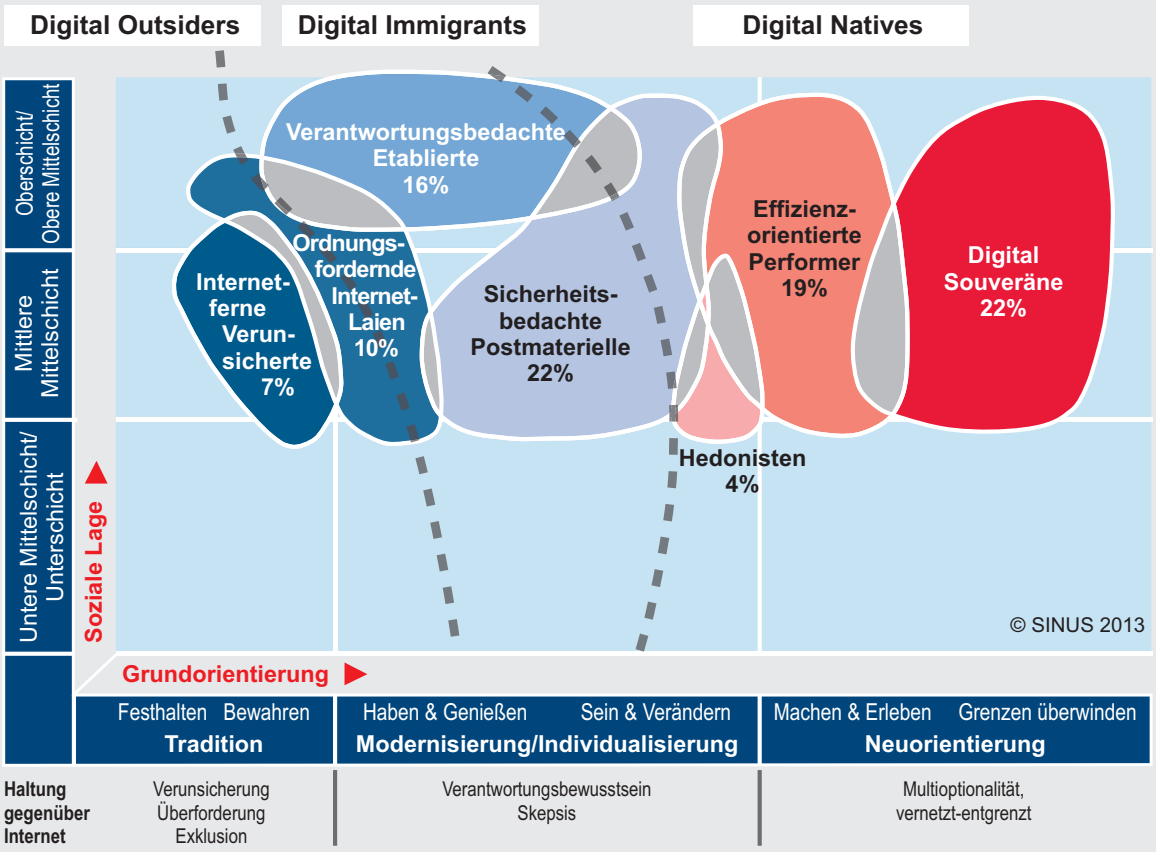
Die Entsprechung dieser Milieu-Landkarte für Entscheider ist in Abbildung 2 (rechts) gezeigt. Aufgrund leicht anderer

Internet-Milieus in der Gesamtbevölkerung zu Vertrauen und Sicherheit im Netz unterscheiden sich hinsichtlich sozialer Lage und soziokultureller Grundorientierung



In der Internet-Milieu-Struktur der Entscheider gibt es deutlich andere Schwerpunkte als in der Bevölkerung

Repräsentativ für 2,69 Mio. Entscheider in Deutschland (= 3,8% der Bevölkerung ab 14 Jahren)



Basis: 1.220 Fälle, Entscheider

Einstellungen zu Vertrauen und Sicherheit im Internet wurden zwei Milieus im Fall der Entscheider umbenannt: Postmaterielle Skeptiker werden zu Sicherheitsbedachten Postmateriellen und Unbekümmerte Hedonisten zu Hedonisten.

Zwei Charakteristika der Entscheider im Vergleich zur Bevölkerung sind offensichtlich: Entscheider sind, was ihre soziale Lage angeht, in der Regel der Mittel- und Oberschicht zuzuordnen – dies ist keine Überraschung. Wesentlich interessanter sind die klaren Schwerpunkte in der Internet-Milieu-Struktur, die eine wesentlich höhere Affinität zur digitalen Lebenswelt zeigen. Dies führt bei Entscheidern im Vergleich zur Bevölkerung zu einem hohen Anteil von Digital Natives, die sehr gut durch die Begriffe Effizienz und Souveränität im Umgang mit dem Internet charakterisiert werden können.

Deutlich geringer ist der Anteil von Digital Outsiders. Unabhängig von der Milieuzuordnung hat sich im Rahmen der Entscheider-Befragung gezeigt, dass es unter den Entscheidern fast keine „Offliner" gibt – digitale Kommunikation ist eine conditio sine qua non für ihre Rolle.

Dr. Dirk Graudenz *(*1965) ist freiberuflicher Unternehmensberater zu strategischen Themen im Schnittpunkt von Informationstechnologie und öffentlichem Sektor sowie zu Fragen der IT-Governance und IT-Organisation. Sein besonderes Interesse gilt Design Thinking-Ansätzen zur Ideenfindung und gesellschaftlichen Entwicklungen im Kontext neuer Medien (kontakt@dirkgraudenz.de).*

An den Enden der Welt schmilzt das Eis immer schneller. Forscher befürchten seit langem: An den Polen könnte die Klimaveränderung eine katastrophale Dynamik bekommen. Den meisten Entscheidern, so die DIVSI-Studie, ist Online-Sicherheit jedoch wichtiger als die Klimaveränderung.

Informationslücke geschlossen

So denken Entscheider über Vertrauen und Sicherheit im Internet

Von Dr. Silke Borgstedt

Hamburg - Wie sich die deutsche Bevölkerung im Internet bewegt und wie sie über Sicherheit im Internet denkt, ist mittlerweile grundlegend bekannt. Wer aber prägt die unterschiedlichen Einstellungen zum Internet? Wer sind die Menschen, die das öffentliche Klima in punkto Internet beeinflussen – sei es durch mediale Meinungsbildung oder durch die Formulierung von Regeln für die Internet-Nutzung am Arbeitsplatz? Und wie denken Entscheider über Chancen und Risiken im Internet und setzen dies in ihrem Einflussbereich entsprechend um?

Zu diesen Fragen fehlten bislang die Antworten. Als Fortsetzung und komplementär zur Bevölkerungsbefragung konzipiert, lässt die DIVSI Entscheider-Studie daher erstmalig Entscheider aus Wirtschaft, Politik, öffentlichem Dienst, Zivilgesellschaft, Medien sowie Wissenschaft und Forschung zu diesen Fragen zu Wort kommen.

Denn um Vertrauen im Umgang mit dem Internet zu schaffen, genügt es schließlich nicht, dass Entscheider wissen, was die Nutzer im Netz machen; die Nutzer sollten auch wissen, wie sich die Entscheider im Netz bewegen, welche Haltung sie gegenüber Chancen und Risiken einnehmen und nicht zuletzt, wie sie über die Nutzer und andere Entscheider denken und was sie von ihnen erwarten.

Im Rahmen der Untersuchung ließen sich fünf Kernthesen identifizieren, hinsichtlich derer sich die Entscheider weitgehend einig sind:

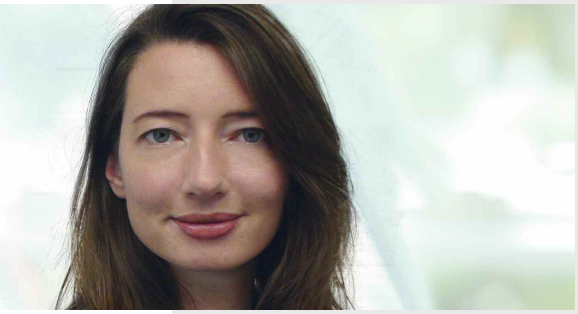
- **Sicherheit im Internet ist ein Top-Thema – aber eine Illusion**

  - Acht von zehn Entscheidern sehen Datensicherheit gleichermaßen für sich persönlich (80 Prozent) als auch für die Gesellschaft (78 Prozent) als zentrales Themenfeld. Themengebieten wie wirtschaftliche Entwicklung, Bildung, Arbeitslosigkeit, Energieversorgung und soziale Gerechtigkeit wird zwar noch etwas mehr Bedeutung zugesprochen; jedoch ist Online-Sicherheit wichtiger als Klimaveränderung oder Migration.

  - Das Netz ist schwer zu kontrollieren: Datensicherheit im Internet kann es nicht geben – 68 Prozent sind davon überzeugt. Ihnen ist bewusst, dass (technische) Systeme immer nur eine Teil-Sicherung gewährleisten können und ein Restrisiko bleibt. Folglich sind Entscheider überwiegend der Ansicht, dass wir uns an einen freieren Umgang mit Daten im Internet gewöhnen müssen (60 Prozent).

- **Es gibt kein Offline-Leben mehr**

  - Die Entscheider sind mehrheitlich überzeugt, dass die Unterscheidung von online und offline bald obsolet sein wird: 64 Prozent sind der Meinung, dass es in der Zukunft nicht mehr möglich sein wird, komplett offline zu sein. Die Technologien werden sich aus ihrer Sicht so weit vereinfachen und ausdifferenzieren, dass die Nutzung verschiedener Geräte und ihrer Funktio-



Dr. Silke Borgstedt *(*1975) ist am Sinus-Institut Direktorin für die Sozialforschung.*

nen immer weniger digitales Grundlagenwissen, generelles Technikverständnis oder Feinmotorik voraussetzen.

– Das Phänomen des real existierenden Offliners wird sich von allein „auswachsen", denn Menschen werden in Kürze nicht mehr „ins Internet gehen", weil ohnehin online immer mehr Prozesse des Alltags gesteuert werden (z. B. die Navigationstechnik im Auto, die Bestückung des Supermarktregals, das Monitoring im Krankenhaus).

– Aus Sicht der Entscheider befinden wir uns mitten in einem grundlegenden gesellschaftlichen Wandel, denn es geht längst nicht mehr um technologische Veränderungen, die sich allein auf die Effizienz von Arbeitsabläufen auswirken. Es entstehen neue erforderliche Kompetenzen zur Erfüllung eines Berufs (z. B. die schnelle Verzahnung von Wissenseinheiten, die Gestaltung bzw. Bewertung der persönlichen oder institutionellen Internet-Präsenz, das flexible Agieren in globalen Kontexten); „klassische" Kompetenzen hingegen werden immer weniger gebraucht oder haben sich wesentlich verändert (Ablage, Terminkoordination per Telefon). Zudem sind Arbeits- und Berufsleben in vielen Bereichen immer schwerer voneinander zu trennen, denn die digitalen Anwendungen ermöglichen die Abwicklung von Projekten jenseits des Bürotisches. Daraus erwachsen neue Chancen (Home-Office, „Workation"), aber auch Herausforderungen (Abgrenzung des Privatlebens, Fehler durch Informationsüberlastung).

■ **Die Privatwirtschaft macht das Netz**

- Nach Ansicht der Entscheider wird das Internet vor allem durch die Privatwirtschaft dominiert. Insbesondere die großen, global agierenden Internet-Dienste-Anbieter wie Google, Apple, Facebook, eBay und Amazon gelten als Hauptakteure, die Basis-Anwendungen in erheblichem Maße bestimmen.

- 70 Prozent der Entscheider sehen Machtkonzentrationen der globalen Player überdies als Risiken im Netz. Viele Entscheider bekunden, dass ihnen die Abhängigkeit von einzelnen Unternehmen Sorge bereitet, da es kaum alternative Angebote gibt, im Internet zu suchen, zu kaufen oder sich zu vernetzen. Mit der zunehmenden Verbreitung und Vernetzung einzelner Dienste haben sich Monopole ausgebildet, die marktbestimmend sind – auch für das eigene Arbeitsfeld.

- Der Staat wird kaum als dominanter Akteur im Internet wahrgenommen. Nur 15 Prozent sprechen der Politik und nur elf Prozent der öffentlichen Verwaltung einen großen Einfluss im Internet zu.

■ **Risikoverursacher im Netz sind Hacker, globale Internet-Dienstleister und unbedachte Nutzer**

- Die Entscheider sind sich einig, dass Hackerangriffe das größte Risiko im Internet darstellen. Eine Garantie, vor Hackerangriffen geschützt zu sein, wird als vollkommen unmöglich betrachtet. Strategien, die einen (maximal temporären) Schutz gewährleisten, müssen regelmäßig überprüft und ständig aktualisiert werden.

- Auch großen globalen Internet-Dienstleistern wird von 73 Prozent der Entscheider ein großes Risikopotenzial zugesprochen. Ein gleich hohes Risiko wird bei unbedachten Usern gesehen, welche Datensicherheit und Datenschutz gefährden bzw. auf Angebote hereinfallen, weil sie (noch) nicht gelernt haben, diese zu durchschauen.

- Vom Staat geht im Internet kein Risiko aus. Lediglich neun Prozent der Entscheider sehen ein großes Risikopotenzial bei der Bundesregierung, 18 Prozent bei staatlichen Verwaltungsorganen und 21 Prozent bei politischen Akteuren. 20 Prozent konstatieren ein Risiko im Internet durch staatliche Sicherheitsbehörden.

■ **Die Hauptverantwortung liegt beim Nutzer, doch der kennt sich nicht aus**

- Nutzer tragen die größte Verantwortung, sind jedoch überfordert. Im Vergleich der verschiedenen Netz-Akteure sehen 82 Prozent der Entscheider vor allem die Bevölkerung in der Verantwortung, nur 27 Prozent vertrauen jedoch deren Kompetenzen.

- Entscheider empfehlen dem Nutzer, sich vor allem auf Bildung und die eigene Erfahrung zu verlassen, denn die Verantwortung kann ihm niemand abnehmen. Auch Rat von unabhängigen Institutionen und Experten gilt den Entscheidern als relevant; weniger verlassen sollten sich die Menschen jedoch auf das deutsche Rechtssystem und die Internet-Gemeinde.

Der Anfang ist gemacht

Was hat die „Enquete-Kommission Internet und Digitale Gesellschaft“ gebracht?

Von Harald Lemke

Berlin - Im Mai 2010 hatte die Enquete-Kommission Internet und Digitale Gesellschaft ihre Arbeit aufgenommen. Der Anfang gestaltete sich aus vielerlei Gründen schwierig. Die unterschiedlichen Erwartungshaltungen, insbesondere von Sachverständigen und Abgeordneten, unterschiedliche Diskussionskulturen und unterschiedliche Herangehensweisen an komplexe Themen mussten zunächst in scheinbar endlosen Geschäftsordnungsdebatten auf einen Nenner gebracht werden.

Selbst die simple Frage, wie und mit welchen Systemen man die Netz-Gesellschaft als „18. Sachverständigen“ an der Diskussion beteiligen kann, artete zum Politikum aus, in der alle taktischen Register gezogen wurden. Am Ende wäre die Beteiligung der Öffentlichkeit an den formalen Entscheidungs- und Beschaffungsprozessen der Bundestagsverwaltung gescheitert, wenn nicht eine private Initiative Entwicklung und Betrieb der Beteiligungsplattform „Adhocracy“ finanziert hätte.

Endlose und zum Teil ins persönlich gehende Debatten wurden über die Unabhängigkeit der Sachverständigen geführt, als vielen klar wurde, dass eine Enquete-Kommission nach politischen Regeln funktioniert. Insbesondere das Abstimmungsverhalten der Sachverständigen führte immer

Eine Empfehlung der Projektgruppe „Zugang, Struktur und Sicherheit“ der Enquete-Kommission, getragen von einem breiten Konsens: Kritische Systeme etwa bei der Energieversorgung sollten möglichst strikt vom Internet getrennt sein.

wieder zum Streit. Die thematische Breite der Enquete-Kommission war so groß, dass eine Fokussierung auf einzelne Projektgruppen notwendig war.

Wie aber sollte man als Sachverständiger über Sachverhalte abstimmen, bei denen man nicht im Stoff war? Enthaltung oder Koalitionstreue? Am Ende hat sich meist die letztere Option durchgesetzt, was im parlamentarischen Alltag ja nicht unüblich ist.

Das alles ist nun Geschichte. Am 28. Januar fand die letzte Sitzung der Enquete-Kommission statt und in den nächsten Monaten wird die redaktionelle Arbeit abgeschlossen sein. Dann können sich Politik und Öffentlichkeit auf mehreren tausend Seiten über den Stand der Diskussion, Handlungsfelder und Handlungsempfehlungen informieren.

Wer sich die Mühe macht, den Bericht zu lesen, wird folgendes feststellen: Es gibt großes Einvernehmen, in welchen Feldern der Netzpolitik Handlungsbedarf besteht. Zwar verwiesen die Vertreter der Regierungsfraktionen gern auf das Erreichte, während die Vertreter der Oppositionsparteien lieber auf das Nichterreichte fokussierten. Hier waren jedoch meist Kompromisse möglich.

Richtig strittig wurde es regelmäßig bei den Handlungsempfehlungen. Diese unterschiedliche Perspektive drückt sich dann in einer Vielzahl von Minderheiten-Voten aus, so dass der Bericht am Ende für jede politische Couleur Lesenswertes bereithält.

Ich möchte die inhaltliche Arbeit in der Enquete-Kommission anhand der Projektgruppe „Zugang, Struktur und Sicherheit“ verdeutlichen, deren Vorsitzender ich war.

Die Projektgruppe kam insgesamt zu 17 Treffen zusammen. Der Gruppe gehörten 29 Mitglieder an, davon sieben mit Stimmrecht. Wie alle anderen Projektgruppen bestand auch diese Projektgruppe aus Sachverständigen und Abgeordneten. Größe und Zusammensetzung war sicher hinderlich, wenn es allein um eine wissenschaftliche Aufarbeitung der komplexen Materie gegangen wäre. Stichworte wie „Vorratsdatenspeicherung und Bundestrojaner“ machen aber deutlich, dass auch bei dieser Projektgruppe Grundüberzeugungen und politische Richtungskämpfe in die Kommissionsarbeit getragen wurden.

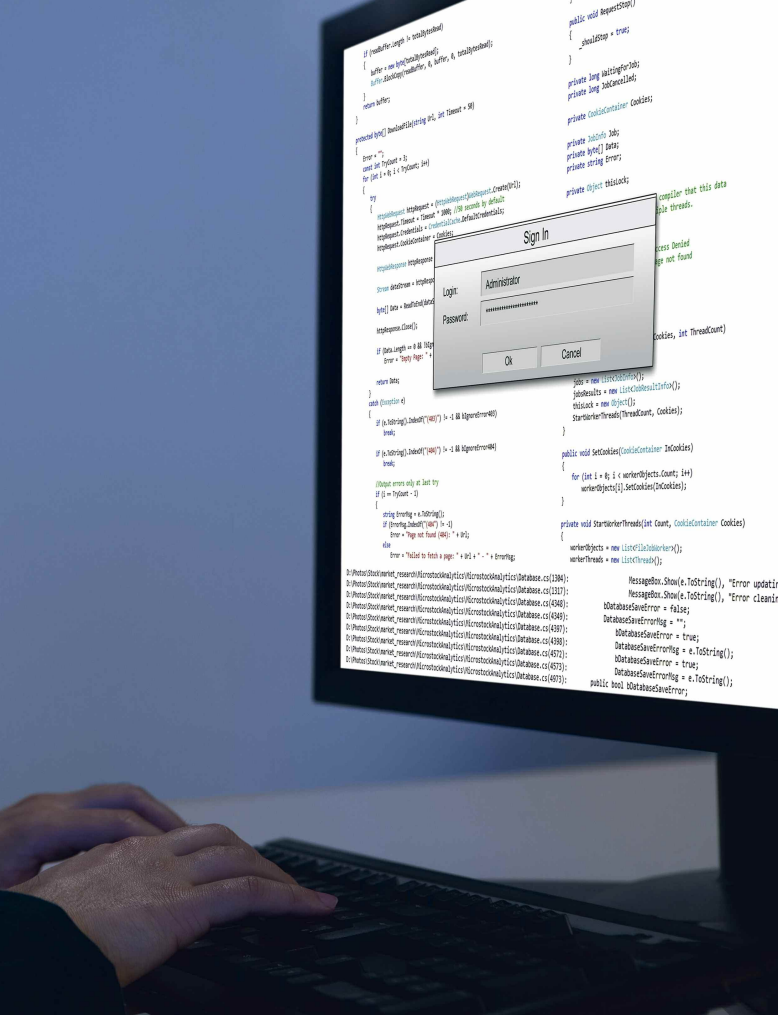
Der Bericht der Projektgruppe weist auf rund 250 Seiten sechs Themenfelder aus: Ausbau und Modernisierung der Netze, Wettbewerb, Schutz kritischer Infrastrukturen im Internet, Internet-Kriminalität, Sabotage sowie Spionage.

Nach den Erfahrungen anderer Projektgruppen waren wir sehr schnell übereingekommen, anstelle von umfassenden Zustandsbeschreibungen lieber Perspektiven aufzuzeigen:

Cybercrime boomt und wird allgemein als Riesengefahr gewertet. Allerdings brachte die Arbeit der Enquete-Kommission keine neuen, übereinstimmenden Erkenntnisse darüber, wie der Internet-Kriminalität künftig wirksam zu begegnen sei.

- Wie kann gewährleistet werden, dass der Bevölkerung dieses Landes in den nächsten Jahrzehnten ein Internet-Zugang zur Verfügung steht, der tatsächlich ihren Bedürfnissen entspricht?
- Wie können die Chancen des neuen Internet-Protokolls IPV6 genutzt werden und wie kann man dabei die datenschutzrelevanten Risiken minimieren und auch in Zukunft Anonymität im Netz sicherstellen?
- Wie können die Sicherheitsrisiken des Internets grundrechtsschonend minimiert werden?

Einig waren wir uns, dass die flächendeckende Versorgung Deutschlands mit leistungsfähigem Internet die Grundlage für wirtschaftliche Entwicklung und gesellschaftliche Teilhabe schafft. Strittig war jedoch, welche Leistungsfähigkeit ausreichend ist und welche Rolle der Staat hierbei spielen soll. Sehr intensiv wurde diskutiert, ob es hier einen Grundsicherungsauftrag des Staates gebe und welche Konsequenzen ein daraus resultierender Universaldienst für die Entwicklung des Internets hätte. Es liegt auf der Hand, dass hier sofort die grundsatzpolitischen Gräben gezogen wurden – und wer wissen will, welche Parteien welches Wirtschaftsmodell bevorzugen, kann dieses auch im Bericht der Projektgruppe nachlesen.



Bei der Frage des neuen Netzprotokolls IPV6 ist wieder einmal die Chance vertan, der Bevölkerung mit einfachen Worten zu erklären, welche Chancen und Risiken in dieser Technologie stecken. Nach langen Diskussionen darüber, ob Anonymität die Identifizierbarkeit oder die Wiedererkennbarkeit (oder beides) bedeute, haben wir sehr lange und sehr korrekte Sätze geschmiedet, die nach meiner persönlichen Einschätzung kein großes Interesse in den Redaktionsstuben hervorrufen werden.

Breiten Raum nahm die Fragestellung ein, ob das Internet bereits ein Teil unserer kritischen Infrastruktur ist, d. h., funktioniert unser Gemeinwesen noch ohne Internet oder kann unsere Grundversorgung aus dem Internet heraus bedroht werden. Es gab einen breiten Konsens darüber, dass die kritischen Systeme, z. B. bei der Energieversorgung, möglichst strikt vom Internet getrennt sein sollen. Dabei wurde jedoch auch deutlich, dass dieses Trennungsgebot nicht immer und überall umsetzbar ist und dass selbst eine vollständige Trennung keinen hundertprozentigen Schutz vor Cyber-Attacken bietet. Der Stuxnet-Virus ist ein Beispiel dafür, dass Attacken auch über einen USB-Stick funktionieren.

Die Diskussion zum Thema Internet-Kriminalität lässt sich in zwei Teile gliedern: Große Einigkeit gab es bei der Feststellung, dass die digitale Transformation auch nicht vor dem Verbrechen halt macht und dass sich zwischenzeitlich internetspezifische Kriminalitätsformen herausgebildet haben. Ebenfalls war man sich weitestgehend einig darüber, dass viele Kriminalitätsformen nur deshalb funktionieren, weil das Sicherheitsbewusstsein vieler Internet-Nutzer nur sehr schwach ausgeprägt ist und daher noch sehr viel Potenzial in eigenverantwortlicher Prävention liegt.

Bei der naheliegenden Frage, welche Werkzeuge die Strafverfolgungsbehörden zur effektiven Verbrechensbekämpfung brauchen, wechselte die Diskussion in den Debatten-Modus, in der die altbekannten Argumente pro und contra Vorratsdatenspeicherung und Quellen-TKÜ (auch „Staats-Trojaner“) ausgetauscht wurden. Hier hat die Enquete-Kommission keine neuen Erkenntnisse erbracht.

Hat sich diese Arbeit gelohnt? Ja, auf jeden Fall!

Während der Enquete-Jahre ist das Thema Internet endlich in der Bundespolitik angekommen. Viele politisch Verantwortliche haben erkannt, dass das Internet keine Angelegenheit für picklige Nerds ist, sondern dass es hier um grundsätzliche Fragen unserer Zukunft geht. Das Internet geht alle an, ob man drin ist oder nicht. Die Netz-Gesellschaft sind wir alle und nicht nur ein Verein sogenannter Netz-Aktivisten.

Wir alle müssen dafür Sorge tragen, dass dieses Zukunftsthema aktuell bleibt. Die Enquete-Kommission hat sich dafür ausgesprochen, einen ständigen Ausschuss zur Netz-Politik einzurichten und vieles spricht dafür, dass der nächste Bundestag dieser Empfehlung folgt. Der Anfang ist gemacht.

Harald Lemke *(*1956) ist seit Juli 2010 Sonderbeauftragter für E-Government und E-Justice bei der Deutschen Post. Von 2003 bis 2008 arbeitete er im Range eines Staatssekretärs als CIO für das Bundesland Hessen. Zwischenzeitlich war Lemke Berater für McKinsey&Company. 2002/ 2003 arbeitete er als IT-Direktor des BKA in Wiesbaden. Bei der Enquete-Kommission Internet und digitale Gesellschaft war er Vorsitzender der Projektgruppe „Zugang, Struktur und Sicherheit im Netz“.*

Hacker als Agenten des Fortschritts?

Gedanken darüber, ob sie wirklich zu einer neuen Computer-Ethik beitragen

Von Prof. Dr. Hans Peter Bull

Wir mögen einfache Erklärungen für komplizierte Sachverhalte. Die Risiken der Computertechnik sind schwer erklärbar, deshalb behelfen sich manche Kommentatoren mit einer pauschalen Schuldzuweisung, möglichst an „den Staat“. So lesen wir in einer Zeitung, der unsorgfältige Umgang mit Daten – die „Datenschluderei“ – habe „System“, und dieses System ziehe sich „durch die gesamte westliche Welt, weil kein Staat die verantwortungslosen Datenmanager in Unternehmen und Behörden zur Rechenschaft zieht“. Man lasse sie gewähren, „wie man früher Walfänger und Ölkonzerne gewähren ließ“. „Anders ausgedrückt: Der Staat versagt.“

Der Autor lobt das „Hacker-Netzwerk Anonymous“ dafür, dass es einen großen Datendiebstahl begangen hat. Das sei zwar ein Verstoß gegen geltendes Recht gewesen, aber weil die bestohlene Firma Kundendaten unverschlüsselt verwaltet habe und man infolge einer Schwachstelle im Computer der Firma auf diese Daten zugreifen konnte, hätten die Hacker ebenso „ehrenwert“ gehandelt wie die Greenpeace-Aktivisten, die gegen Walfang und Meeresverschmutzung gekämpft haben. Nicht die Profitgier habe die Hacker von Anonymous getrieben, sondern „die gute Sache oder das, was sie dafür halten“.

Soll denn aber jeder, der eine Sache gut findet, sie ohne Rücksicht auf geltendes Recht durchsetzen? Sind die Hacker, die andere auf den Weg der datentechnischen Tugend führen wollen, die modernen Robin Hoods, die Verteidiger der individuellen Freiheit, die Agenten des Fortschritts? Handeln Datendiebe, die auf Schwachstellen aufmerksam machen wollen, sozusagen in Ersatzvornahme für den Staat?

Die Fragen stellen, heißt sie verneinen – wenn alle so handelten, wäre gar kein Staat mehr zu machen, sondern es würde Unordnung herrschen. Man braucht gar nicht einmal zu prüfen, ob der behauptete gute Zweck des Hackens nicht vielleicht der Werbung für Sicherheitsdienstleistungen dienen sollte – jedenfalls ist die Heroisierung des Regelverstoßes kein brauchbares Rezept, um die weltweite „Datenschluderei“ zu verhindern.

Ein seriöser Experten-Verein

Der Chaos Computer Club, der vor dreißig Jahren gegründet wurde, um Hackern eine Plattform zu geben und über Aktivitäten berichten zu können, nach seiner Selbsteinschätzung „die größte europäische Hackervereinigung und seit 25 Jahren Vermittler im Spannungsfeld technischer und sozialer Entwicklungen" – dieser Club gilt gegenwärtig allgemein als seriöser Verein von Experten, die sich um die Sicherheit des Netzes verdient gemacht haben; seine Sprecher wie Frank Rieger und Constanze Kurz schreiben kultur- und politikkritische Artikel in der ‚Frankfurter Allgemeinen Zeitung' und dienen Bundestags- und Landtagsausschüssen in Anhörungen als Sachverständige für Fragen der Informatik und ihrer sozialen Risiken.

Auch der CCC hat sich durch mancherlei Hacker-Erfolge profiliert – und war manchmal auf der falschen Spur. Insgesamt aber scheinen die „Chaos"-Hacker überlegt und vorsichtig vorgegangen zu sein.

Die Hacker-Ethik, die der CCC propagiert, ist recht allgemein formuliert. Vom Eindringen in fremde Datenverarbeitung ist da gar nicht die Rede; das wird offenbar als die „normale" Aktivität eines Hackers vorausgesetzt, und die Frage nach der Rechtmäßigkeit wird in diesem Papier nicht thematisiert. Die ersten Sätze dieser Hacker-Ethik lauten: „Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein. Alle Informationen müssen frei sein."

Als spätere Hinzufügung steht am Schluss aber: „Mülle nicht in den Daten anderer Leute" und „Öffentliche Daten nützen, private Daten schützen". Dass hierin ein Widerspruch liegt – die „Daten anderer Leute" und die „privaten" Daten sind dann eben doch nicht frei –, wird nicht zum Ausdruck gebracht. Doch wird durch die Änderungen deutlich gemacht, dass man nicht mehr ohne Rücksicht auf die Folgen hacken will.

Wörtlich heißt es: „Auch Eingriffe in die Systeme fremder Betreiber wurden zunehmend als kontraproduktiv erkannt." Geradezu weise lautet es am Schluss: „Die Hacker-Ethik befindet sich – genauso wie die übrige Welt – insofern in ständiger Weiterentwicklung und Diskussion."

Als Befreier von allen „Datenschludereien" dürften die Hacker also auch nach eigener Einschätzung nicht berufen sein. Aber vielleicht tragen sie wirklich zu einer neuen Computer-Ethik bei, die nicht nur in der Leugnung traditioneller Rechtsprinzipien besteht. Damit die rechtlichen Grenzen der Datensammlung und -verwendung tatsächlich eingehalten werden, bedarf es der Datensicherung (die insofern vom Datenschutz abzugrenzen ist).

Sicherheit zu gewährleisten – im Netz und in den angeschlossenen Computern – ist eine riesige Aufgabe für die Verantwortlichen, aber primär verantwortlich für die Einzelheiten und für die Durchführung ist nicht der Gesetzgeber, sondern es sind die Betreiber und Nutzer der Datenverarbeitung – Unternehmen, Behörden und Private. Der Gesetzgeber kann insofern auf den Stand von Wissenschaft und Technik verweisen, so wie er es auch beim Umweltschutz, bei der Reaktorsicherheit und in vielen anderen Bereichen tut.

Eher kontraproduktiv als hilfreich

Zwar hat das Bundesverfassungsgericht (im Urteil über die Vorratsdatenspeicherung) dem Gesetzgeber aufgegeben, auch die Sicherung der Daten penibel zu regeln. Es ist damit aber weiter in die Details gegangen, als nötig wäre, und hat einem Misstrauen gegen alle Anwender Ausdruck verliehen, das eher kontraproduktiv als hilfreich wirken wird. Denn diejenigen, die den Datenverarbeitern nur Schlechtes zutrauen, werden sich gerade durch solche Urteile bestätigt fühlen, und die anderen werden zu grübeln beginnen, ob die Angst vor Missbrauch nicht doch etwa begründet sei, wenn schon die höchsten Richter sie ernst nehmen.

Die praktischen Schwierigkeiten bei der Sicherung sensibler Daten beruhen nicht darauf, dass die Normen ungenau und mehrdeutig sind. Viel bedrohlicher ist die „Cyber-Kriminalität" in ihren zahlreichen Varianten. Sie ist längst international organisiert und deshalb mit nationalstaatlichen Instrumenten schwer zu fassen. Von Regierung und Parlament dürfen wir erwarten, dass sie auf diesem Gebiet besonders aktiv sind. Nur aufgrund europarechtlicher Normen und internationaler Abkommen und durch supra- und internationale Behörden kann die Internet- und Computerkriminalität wirksam bekämpft werden.

***Prof. Dr. Hans Peter Bull** (*1936) wurde 1978 zum ersten Bundesbeauftragten für den Datenschutz berufen. Dieses Amt hatte er bis 1983 inne, nahm dann wieder seine Tätigkeit als Professor an der Universität Hamburg auf. 1988 bis 1995 übernahm Hans Peter Bull das Amt des Innenministers von Schleswig-Holstein. Danach wirkte er erneut als Professor an der Universität Hamburg. Seit 2002 ist er im Ruhestand. Der Text stammt aus seinem neuen Buch „Netzpolitik – Freiheit und Rechtsschutz im Internet".*

Vertrauen ist wie ein geldwerter Vorteil

Der Glücksatlas für Deutschland zeigt: Der Nordwesten und Südosten liegen vorn

Von Dr. Göttrik Wewer

Warum beschäftigen sich Ökonomen mit Glück? Weil sie gemerkt haben, dass das Sozialprodukt eines Landes allein kein hinreichender Maßstab für das Wohlbefinden der Bevölkerung ist. Es gibt Länder, wo die Menschen relativ zufrieden sind, obwohl sie ziemlich arm sind, und es gibt Länder, wo die Menschen wohlhabend, aber dennoch unzufrieden sind. „Das BIP misst alles, außer das, wofür sich das Leben lohnt" (Robert Kennedy). Aber wie misst man Glück, wie Wohlbefinden, wie Zufriedenheit?

Die Deutsche Post hat 2012 zum zweiten Mal einen „Glücksatlas" für Deutschland herausgegeben, der von renommierten Wissenschaftlern in Zusammenarbeit mit dem Bielefelder Meinungsforschungsinstitut TNS Emnid erstellt worden ist. Dieser Atlas bietet nicht nur eine Fülle von Material zu der Frage, wie glücklich die Deutschen sind, sondern auch wichtige Erkenntnisse zu den Themen, mit denen sich das Deutsche Institut für Vertrauen und Sicherheit im Internet beschäftigt. Sie machen deutlich: Geld ist längst nicht alles. Das haben auch Unternehmer verstanden: „Lieber Geld verlieren als Vertrauen" (Robert Bosch).

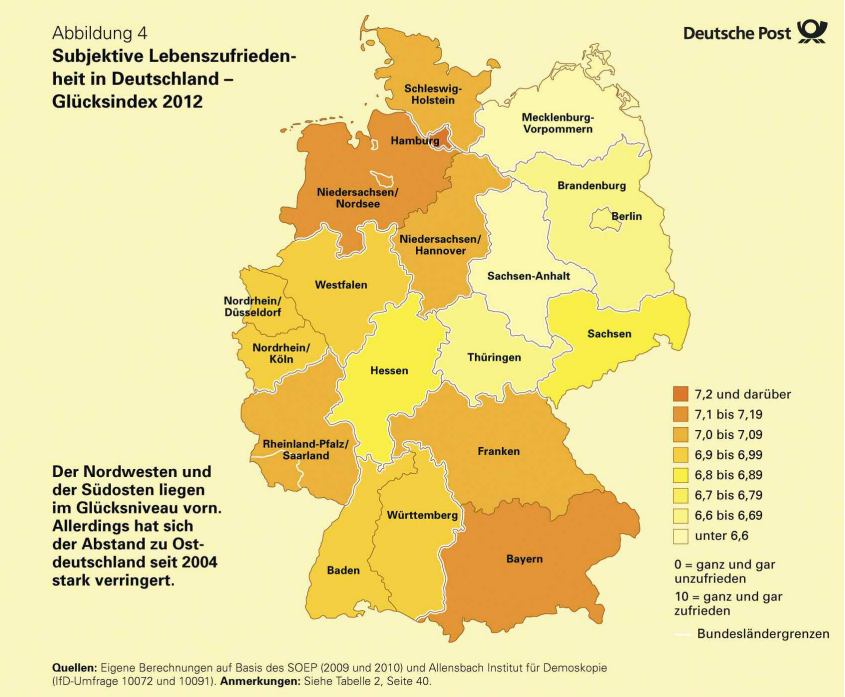
Der Atlas enthält ein eigenes Kapitel zum Thema Vertrauen. Das ist kein Zufall: Das Ausmaß an Vertrauen, das innerhalb einer Gesellschaft herrscht, ist nämlich einer der wichtigsten Indikatoren für die Zufriedenheit der Menschen, die darin leben. Anders gesagt: Wer Vertrauen zu seinen Mitmenschen hat, ist in der Regel auch deutlich zufriedener. Vertrauen ist so etwas wie ein geldwerter Vorteil: Vertrauensvoll auf seine Mitmenschen schauen zu können ist nämlich, das zeigen statistische Analysen, für den Durchschnittsbürger ähnlich kostbar wie eine Verdoppelung des Einkommens!

Vertrauen hat auch indirekte ökonomische Aspekte: Ohne Vertrauen kommt es weder zu Kreditvergaben noch zu Investitionen, und ohne Investitionen bleibt die wirtschaftliche Prosperität aus. Aber das gesellschaftliche Vertrauensniveau beeinflusst die Lebenszufriedenheit der Menschen auch direkt. Relativ hohe Werte weisen beispielsweise die skandinavischen Länder auf. Und wo stehen wir Deutschen?

Immerhin rund sechzig Prozent der Bevölkerung blicken vertrauensvoll auf ihre Mitmenschen, fünf Prozent sind dagegen sehr misstrauisch eingestellt. Diese Werte haben sich in den letzten zwanzig Jahren nicht nennenswert verändert. Man kann also weder von einer deutlichen Zunahme noch von einer wirklichen Abnahme des Vertrauens in Deutschland ausgehen. International bewegen wir uns hinsichtlich der Lebenszufriedenheit eher im Mittelfeld.

Wer seinen Mitmenschen vertraut, ist meist deutlich zufriedener. Ein vertrauensvolles Verhältnis zum sozialen Umfeld trägt dabei mehr zur individuellen Zufriedenheit bei als etwa eine eigene Immobilie. Kein Wunder, dass sich inzwischen auch Ökonomen mit der Frage beschäftigen, wie Vertrauen eigentlich entsteht und wie man es ausbauen und festigen kann.

In einer Umgebung zu leben, die als vertrauenswürdig angesehen wird, führt ebenfalls zu einer höheren Lebenszufriedenheit. In Deutschland schenken einander das größte Vertrauen die Menschen in Schleswig-Holstein und Hamburg sowie in Bayern, aber auch im nördlichen Niedersachsen und in Franken. Das geringste Vertrauen zueinander haben die Menschen in Mecklenburg-Vorpommern und in Sachsen-Anhalt.



Alles auf einen Blick: Je dunkler die Farbe, desto höher die Lebenszufriedenheit

In Westdeutschland ist das Vertrauen untereinander höher als in Ostdeutschland. Allerdings betrifft das vorwiegend die ältere Generation, unter den Jüngeren sind die Niveaus weitgehend ähnlich. Es wächst also doch zusammen, was zusammen gehört.

Das Misstrauen gegenüber Regierung und Parlament ist in der gesamten Europäischen Union relativ stark ausgeprägt. Das hat nicht nur etwas mit der aktuellen Euro-Krise zu tun, die als Banken-Krise und als Schulden-Krise begonnen hat, sondern auch damit, dass politisch umkämpfte Institutionen immer schlechter abschneiden als solche, die als „unpolitisch" oder „neutral" gelten wie die Feuerwehr, die Polizei oder die Gerichte. Das Vertrauen der Deutschen in den Rechtsstaat ist sowohl absolut als auch relativ zu anderen Ländern besonders ausgeprägt.

Was hat das alles mit dem Internet zu tun? Eine ganze Menge. Zum einen dürften Menschen, die nicht misstrauisch gegenüber allem und jedem sind, eher bereit sein, auch im Internet gewisse Risiken einzugehen. Das gesellschaftliche Vertrauensniveau müsste eigentlich, was aber noch niemand untersucht hat, positiv korrelieren mit einer intensiven, bisweilen auch riskanten Nutzung des Internets.

Zum anderen macht die Erkenntnis der Glücksforschung, dass eine wesentliche Grundlage für das Entstehen gegenseitigen Vertrauens die Kenntnis des jeweils anderen ist, deutlich, dass Vertrauen in einer Sphäre, in der man nicht immer sicher sein kann, wer der andere wirklich ist, oder in der man sich nur virtuell kennt, weitaus schwerer aufzubauen ist als in sozialen Beziehungen – wo das auch schon nicht ganz einfach ist. Zwischenmenschliche Beziehungen, aber auch das Wissen, was vorgeht, können Misstrauen vorbeugen. Von diesem Punkt aus ist es nicht mehr weit zum Thema Bildung. Aber auch Transparenz, was mit den Daten geschieht oder wie Algorithmen funktionieren, spielt eine gewisse Rolle. Je mehr ich von etwas verstehe, desto weniger muss ich einfach darauf vertrauen, dass es irgendwie funktioniert.

Und drittens zeigt der Glücksatlas, dass die Medien sowohl beim Vertrauensniveau als auch hinsichtlich der Relevanz für die Lebenszufriedenheit bloß im Mittelfeld liegen: Schlechter als die Polizei, besser als die Parteien. Das Vertrauen zur Presse weist den stärksten Zusammenhang mit der Lebenszufriedenheit auf, dem Internet wird innerhalb der Medien am misstrauischsten begegnet. Das deutet die Größe der Aufgabe an, die vor denjenigen liegt, die für mehr Vertrauen und Sicherheit im Internet sorgen wollen.

***Göttrik Wewer** (*1954) studierte Politikwissenschaft, Soziologie, Volkswirtschaftslehre, Öffentliches Recht und Neuere Geschichte in Braunschweig und Hamburg. Er war von 2001 bis 2003 Staatssekretär im niedersächsischen Kultusministerium und 2003 bis 2006 im Bundesministerium des Innern, danach Staatsrat für Bildung und Wissenschaft bzw. für Inneres und Sport in Bremen und später Geschäftsführer der Nationalen Anti-Doping-Agentur (NADA). Seit 2010 ist Wewer Vice President E-Government bei der Deutsche Post Consult GmbH.*

Privatsphäre - ein gefährdeter Wert

Machen wir uns freiwillig zum gläsernen Menschen?

Von Dominik Höch

Die Piraten-Politikerin Marina Weisband hat jüngst im Interview mit „Spiegel online" Erstaunliches preisgegeben: „Ich habe mir vorgenommen, nicht zwischen mir als Mensch und als Politikerin zu trennen. In Zukunft brauchen wir die Trennung zwischen Privat und Politik hoffentlich nicht mehr."

Das bedeutet also: Sie ist bereit, auch ihr Privatleben zum Thema und Mittel ihrer politischen Arbeit zu machen. Das Privatleben also als Teil des politischen Meinungskampfes? Was zunächst klingt wie die bloße Idee der Vertreterin einer Partei, die sich der gesellschaftlichen Transparenz verschrieben hat, ist in Wirklichkeit schon ein seit Jahren geübtes „Spiel" der Berliner Republik.

Auch Spitzenpolitiker der etablierten Parteien machen das Private öffentlich, um sich beim Wähler als besonders menschlich, glaubwürdig und damit wählbar darzustellen. Immer wieder suchen bestimmte Politiker den Weg, sich mit ihrem Privatleben zu vermarkten. Wie sollen Politiker heute auch auf sich aufmerksam machen? Die langen Bundestags-Debatten übertragen die großen TV-Sender nicht mehr – weil sie eben nicht genug Zuschauer finden.

Gleichwohl zeigt dieser Weg in der Politik beispielhaft, wie gefährdet die Privatsphäre als gesellschaftlicher Wert ist. Es gab über viele Jahrzehnte einen gesellschaftlichen Konsens, dass die Privatsphäre zu schützen ist. Niemand wollte ein „gläserner Mensch" werden.

Privatsphäre und Rückzugsmöglichkeit wurden als wichtig angesehen, um zu sich selbst zu kommen, um für das immer hektischere soziale Leben Kraft zu sammeln oder um beispielsweise bei Krankheiten zu gesunden. Doch dieser Konsens bröckelt. Während bei den Politikern das Spiel mit der Privatsphäre mit der Berliner Republik immer wichtiger wurde, ist die Aufgabe des Privatlebens bei den „Normalbürgern" sicherlich mit der Einführung des Privatfernsehens zu verorten.

Man erinnere sich nur an die Anfänge mit der Auszieh-Show „Tutti Frutti". Schließlich flimmerten auf allen möglichen Kanälen Casting-Shows und Reality-Doku-Serien über die Mattscheibe. Das war aber erst der Anfang: Das „Ausziehen" als Ausdrucksform der Selbstinszenierung nahm erst mit der ständig wachsenden Popularität des Internets und insbesondere der sozialen Netzwerke wie Facebook seinen ungehemmten Lauf.

Es ist nichts Ungewöhnliches, wenn ein Facebook-Nutzer seinen mehreren hundert „Freunden" mitteilt, dass sich seine Krebs-Metastasen weiter vergrößert haben. Wir kennen alle die pikanten „Sauf"-Bilder von wilden Parties, die weltweit in sozialen Netzwerken mit jedermann geteilt werden. Ebenso bekannt sind die eingestellten Bilder mit sexuellen Inhalten aus dem eigenen Liebesleben.

Warum machen Menschen das? Warum teilt man heute Dinge aus dem Privatleben mit häufig hunderten von gemeinsamen Facebook-„Freunden", die man früher für sich behalten hätte? Sicherlich hat es mit Neugier auf die technischen Möglichkeiten zu tun. Facebook und andere soziale Netzwerke sind bequem zu bedienen, versprechen Spaß bei der Interaktion und stellen keine Begrenzungen auf, welche Inhalte man teilt.

Ein zweiter Punkt ist die technische Naivität vieler Nutzer. Viele Menschen wissen gar nicht, wie sie beispielsweise bei Facebook die Privatsphäre-Einstellungen bedienen sollen. Die Betreiber von sozialen Netzwerken machen es den Nutzern natürlich nicht einfach. Denn sie haben ein Interesse daran, dass möglichst viele Daten gesammelt werden, die dazu für möglichst viele Menschen sichtbar sind, um die Attraktivität ihres Angebots zu steigern.

Man fragt sich schon, warum – jedenfalls auf europäischer Ebene – bisher der Datenschutz nicht derart verbessert wurde, dass den Betreibern von sozialen Netzwerken aufgegeben wurde, bei der Grundeinstellung möglichst viel Datenschutz walten zu lassen („privacy by default"), der dann durch den Nutzer „erweitert" werden kann, wenn er

selber dies wünscht. Es ist heutzutage möglich, Ansprüche gegen Möbelhäuser auf eine fehlerhafte Gebrauchsanleitung zu stützen, aber anscheinend bislang unmöglich, die Nutzer bei den komplizierten Bedienmechanismen von derartigen Internet-Seiten gesetzgeberisch zu unterstützen.

Damit ist das Kernproblem umschrieben: Niemand anderes als wir, die Nutzer selber, sind in der Lage, Datenschutz durchzusetzen – und zwar durch ein vernünftiges und „datenschonendes" Sozialverhalten in den (neuen) Medien. Vorausgesetzt: „Wir" wollen das, wollen Privatsphäre als geschütztes Gut erhalten. Der nationale Gesetzgeber ist bei weltweit agierenden Unternehmen wie Facebook überfordert. Ob im Rahmen einer EU-Datenschutzgrundverordnung möglichst „datenschonendes" Surfen für den Normalbürger einfacher wird, steht in den Sternen. Auch von Seiten der Gerichte ist nicht wirklich Hilfe zu erwarten:

Gerade die deutsche Rechtsprechung hat in den vergangen Jahren zahlreiche Entscheidungen hervorgebracht, die die Persönlichkeitsrechte und das Recht auf Privatsphäre gegenüber anderen Rechtsgütern wie der Meinungs- und Pressefreiheit in den Hintergrund gestellt haben. Die bekannteste Entscheidung ist dabei sicherlich die spickmich.de-Entscheidung des Bundesgerichtshofs. Nach dieser ist es zulässig, Lehrerbewertungen von Schülern weltweit und letztlich für jeden abrufbar ins Netz zu stellen. Früher hat man einmal die Auffassung vertreten, Schule sei ein besonders geschützter Bereich, bei der die Kommunikation vor allen Dingen intern ablaufen sollte. Der Bundesgerichtshof sieht das offenbar anders und meint, dass sich Lehrer öffentlich vorführen lassen müssen.

Es heißt also, sich „digital mündig" zu verhalten. Also: Sich immer zweimal zu überlegen, welche Sachverhalte aus der eigenen Privatsphäre man teilt und wer das alles wirklich wissen soll oder muss. Allein: „Digitale Mündigkeit" muss man lernen. In diesem Zusammenhang taucht immer wieder der Ruf nach der Schule auf, konkret auch nach Einführung eines Schulfachs „Internet" oder „Medienkommunikation". Man sollte die Hoffnungen hier nicht zu hoch hängen. Lehrer können digitale Mündigkeit nur vermitteln und lehren, wenn sie selber über das notwendige Wissen verfügen. Hier liegt noch einiges im Argen.

Dasselbe gilt selbstverständlich auch für Eltern, die ihren Kindern einen vernünftigen Umgang mit dem Internet beibringen sollen, aber selbst nicht wissen, wie die Privatsphäre-Einstellungen bei Facebook funktionieren. Also lautet der Auftrag an die Erwachsenen: Macht euch fit, um die jungen Leute fit zu machen. An den Schulen hat sich in der Vergangenheit auch die Installation von sogenannten „Medien-Scouts" bewährt, bei denen ältere, schon Internet-erfahrene Schüler den jüngeren Schülern etwas beibringen.

Privatsphäre ist ein leicht zerbrechliches Gut. Mit einen Paar Klicks sind wir heute in der Lage, diesen geschützten Raum aufzuweichen und uns gegenüber der Öffentlichkeit mit gegebenenfalls sogar intimen Dingen zu öffnen. „Zurückzuholen" sind diese „Einbrüche" in die Privatsphäre selten. Für Kulturpessimismus ist allerdings kein Raum. Zwischen den ganz jungen Kindern und Jugendlichen, die ihre Erfahrungen mit dem Netz erst machen und der Eltern-Generation (also etwa ab 40 Jahren), die in vielen Fällen mit dem Datenhunger im Netz nicht gut umgehen können, weil sie eben nicht in der digitalen Welt groß geworden sind, gibt es die Generation der etwa 20- bis 35-Jährigen.

Sie sind alt genug, um auch negative Erfahrungen mit Privatsphäre-Verletzungen und Mobbing im Netz gemacht zu haben und auf der anderen Seite immer noch die unendlichen Chancen des Netzes zu sehen und ihr Surf-Verhalten darauf einstellen. Aus dieser Altersgruppe sind nicht nur die wenigsten rechtlichen Probleme beim Autoren dieses Beitrages bekannt; Mitglieder dieser Gruppe melden sich häufig entweder gar nicht bei sozialen Netzwerken an oder haben jedenfalls die Privatsphäre-Einstellungen so gut geregelt, dass wirklich nur ein enger Freundeskreis Einblick in die private Lebensgestaltung bekommt.

Im Übrigen berichten auch beim Medium Fernsehen Verantwortliche davon, dass es immer schwieriger wird, Darsteller für Reality-Shows zu finden. „Deutschland ist durchgecastet", hat es einmal eine Casterin genannt. Insofern gibt es positive Beispiele, dass auch in Zukunft „Privatsphäre" als Wert gesehen wird.

Insofern ist die Sicht von Frau Weisband auf ihr privates Leben als Teil der Politik vielleicht kein Zukunftsmodell.

Dominik Höch *(* 1974) ist seit 2004 als Rechtsanwalt tätig und seit 2008 Partner der Kanzlei Höch & Höch. Er ist Fachanwalt für Urheber- und Medienrecht. Parallel zum Studium war er ständig als freier Journalist für Rundfunk und Print tätig und absolvierte 2001/2002 ein Volontariat bei einer großen Berliner Tageszeitung. Der Schwerpunkt seiner Tätigkeit liegt im Presse- und Äußerungsrecht. Er hält regelmäßig Seminare zum Medienrecht, unter anderem auch an der Electronic Media School (EMS), Potsdam, und als Lehrbeauftragter am Anwaltsinstitut der Humboldt-Universität Berlin. Sein besonderes Interesse gilt der Beratung von Einzelpersonen und Unternehmen in (medialen) Krisensituationen und der Verhinderung solcher Krisen.*

Die zehn Gebote für mehr Datenqualität

So leicht lassen sich die Weichen im Unternehmen auf Erfolg stellen

Von Carsten Kraus

Datenqualität wird oft vernachlässigt. Steigende Prozesskosten und Umsatzverluste sind die Folgen, was sich letztlich in Ergebniseinbußen summiert. So gut wie jeder Geschäftsprozess basiert auf Daten: Kunden- und Interessenten-Daten, Kreditoren- und Debitoren-Stammdaten, Artikel- und Material-Stammdaten. Sind diese schlecht strukturiert, laufen die Prozesse ineffizient. Sind die Daten falsch, liefern auch die Prozesse fehlerhafte Ergebnisse.

Diese hausgemachten Nachteile sind vermeidbar. Wer die Qualität seiner Daten systematisch verbessern will, kommt nicht daran vorbei, die Datenbasis zunächst einmal initial zu harmonisieren und zu konsolidieren. Das heißt: doppelte oder gar mehrfach angelegte Datensätze finden und entfernen, Schreibweisen vereinheitlichen oder Datenbank-Felder aufräumen. Wer nach einer solchen Initialbereinigung dann die folgenden zehn Gebote im Daten-Management befolgt, hat eine der wichtigsten Weichen im Unternehmen auf Erfolg gestellt:

1. Gebot: Du sollst erkennen, dass du betroffen bist!

Datenbanken sind kein statisches Gebilde, sondern unterliegen oft ständiger Veränderung. Werden sie nicht gepflegt, schleicht sich Wildwuchs ein: durch falsches oder doppeltes Ablegen von Informationen, durch unterschiedliche Schreibweisen, durch unkontrolliertes Zusammenführen von Datenbanken usw. Jedes Unternehmen ist betroffen. Dubletten-Quoten von 30 Prozent und mehr in gewachsenen Datenbanken sind keine Seltenheit.

2. Gebot: Du sollst Verantwortlichkeiten für Datenqualität festlegen!

Datenqualität entsteht nicht von allein. Daten brauchen verantwortliche Mitarbeiter, die ein Bewusstsein für die Wichtigkeit der Datenpflege entwickelt haben und sich um diese Aufgabe dauerhaft kümmern. Dazu muss ein Hauptverantwortlicher ernannt werden, der in regelmäßigen Zeiträumen einen Blick auf die Datenqualität wirft, die Reports von Data-Quality-Tools auswertet und ggf. Handlungen einleitet. Zudem sollten alle Mitarbeiter, die mit und in Datenbanken arbeiten, für das Thema sensibilisiert sein. Erfolgreiches Data-Quality-Management braucht Akzeptanz und eine nahtlose Integration in die Prozesse des Arbeitsalltags. Letztlich steht Datenqualität in der Verantwortung der gesamten Firma.

3. Gebot: Du sollst Deinen Datenschatz hüten und mehren!

Die bereinigte Datenbank muss vor neuen Verschmutzungen geschützt werden. Dabei helfen Data-Quality-Werkzeuge, die jeden neuen Datenbankeintrag prüfen: Ob er schon einmal angelegt wurde (fehlertoleranter Dubletten-Abgleich), ob z. B. Name und Adresse stimmen und die Angaben real sind (Abgleich mit Referenz-Datenbanken), ob Kunden oder Lieferanten Compliance-Bestimmungen verletzen (Abgleich mit Sanktionslisten). Datensätze lassen sich aber auch mit wertvollen Zusatzinformationen anreichern (Enrichment), beispielsweise mit Telefonnummern, Mailadressen oder, bei Sachdaten, mit internationalen Begriffen. Existiert eine zentrale bereinigte Datenbank, können alle daran angeschlossenen Systeme (z.B. ERP, CRM oder Webshop) auf die vereinheitlichten Daten („Golden Copy“) zugreifen.

4. Gebot: Du sollst deine Daten zugänglich und leicht auffindbar machen!

Auch die bestgepflegte Datenbank ist unprofitabel, wenn die in ihr schlummernden digitalen Informationen im Bedarfsfall nicht schnell gefunden werden. Um das schnelle Auffinden von Datensätzen zu gewährleisten, wenn etwa im Call Center der Name eines Anrufers richtig zugeordnet werden soll, bedarf es einer fehlertoleranten Suchfunktion, die in der Lage ist, selbst in riesigen Datenmengen die gewünschten Informationen blitzschnell aufzuspüren.

5. Gebot: Du sollst Datenqualitätsprozesse automatisieren!

Datenbanken beinhalten oft Hundertausende oder sogar Millionen von Datensätzen. Es wäre völlig ineffizient, Aufgaben der Datenbereinigung und der laufenden Qualitätspflege manuell steuern zu wollen. Viele der genannten Prozesse und Aufgaben können mit entsprechender Software in serviceorientierten Architekturen (SOA) automatisiert ablaufen. Diese Software sollte sich aber nicht nur recht bis schlecht, sprich: nachträglich an SOA anpassen lassen, sondern eigens dafür konzipiert sein. Webservices unterstützen beispielsweise beim Neuanlegen von Daten den Abgleich mit Bestands- oder Referenzdatenbanken.

6. Gebot: Du sollst Datenqualität als internationale Aufgabe begreifen!

Datenqualität wird mehr und mehr zur grenzüberschreitenden Herausforderung. Bei Fusionen und Übernahmen müssen internationale Stammdaten miteinander verheiratet werden. Darüber hinaus weiten immer mehr Unternehmen ihren Einkauf auf weltweite Märkte aus. Der Abgleich internationaler Daten stellt Unternehmen vor allem dann vor ganz besondere Herausforderungen, wenn die Daten aus verschiedenen Alphabeten und Kulturkreisen stammen und beispielsweise optische Ähnlichkeiten in chinesischen oder japanischen Schriftzeichen erkannt werden müssen.

7. Gebot: Du sollst dich auf Expertenwissen und professionelle Erfahrung stützen!

Es bringt nichts, Daten einfach durch ein Analyse-Tool laufen zu lassen. Im Umgang mit Stammdaten ist Expertise gefragt. Das betrifft die grundsätzliche Zielstellung und Herangehensweise, die Parametrierung der operativen Prozesse, die Bewertung der Ergebnisse und das Installieren von Automatismen zur nachhaltigen Qualitätspflege. Im Betrieb sollte das System allerdings selbsttätig funktionieren und einfach zu bedienen sein.

8. Gebot: Laste Dir nicht zu viel auf einmal auf, sondern verbessere die Qualität deiner Daten schrittweise!

Datenqualitäts-Prozesse werden am besten in nur einem Bereich gestartet: und zwar dort, wo es am meisten Nutzen bringt – diese Strategie hat sich in der Praxis vielfach bewährt. Denn erstens ergeben sich so schon in kurzer Zeit messbare Erfolge „im Kleinen", z. B. im CRM-System, zweitens sorgt dieser Weg der kleinen Schritte für Planungssicherheit und drittens gewährleistet solch ein „schlankes" Master Data Management (LeanMDM), dass der Aufwand und die Kosten überschaubar bleiben – im Unterschied zu klassischen MDM-Projekten, die oft langwierig und kostspielig sind, ohne dass sich am Horizont ein ROI abzeichnet. Multi Domain Capability ist der Schlüssel zum (Schritt-für-Schritt-) Erfolg.

9. Gebot: Du sollst die Ziele deiner Datenqualitäts-Aktivitäten immer vor Augen haben!

Datenqualität ist kein Selbstzweck, sondern dient letztlich dem einen großen Ziel: Alle Prozesse im Unternehmen effizienter zu gestalten, um den Gewinn zu maximieren. Damit dieses große Ziel im kleinen Datenqualitäts-Alltag nicht aus den Augen gerät, empfiehlt es sich, unternehmensspezifische Datenqualitäts-Standards (KPIs) zu definieren und deren Einhaltung kontinuierlich zu überwachen. Denn: Man kann nur verbessern, was man auch messen kann.

10. Gebot: Du sollst die Früchte hoher Datenqualität ernten!

Wer seine Kunden fehlerfrei anspricht, vermittelt Professionalität und Kompetenz, vermeidet Reklamationen oder gar Kündigungen und erzeugt keine unnötig hohen Prozesskosten. Wer saubere Kreditoren- und Material-Stammdaten hat, verringert den Verwaltungsaufwand und ist in der Lage, Einkaufsprozesse zu optimieren, etwa Mengenvorteile konsequent auszuschöpfen. Auch die Vorteile des E-Procurement können nur dann zum Tragen kommen, wenn die Prozesse auf nachhaltig sauberen Lieferanten-Stammdaten basieren. Investitionen in Data Quality amortisieren sich in der Regel rasch.

Carsten Kraus *ist Gründer und Geschäftsführer der Omikron Data Quality GmbH. Dazu gehören außerdem die Geschäftsbereiche FACT-Finder und FACT-Finder Travel. Noch vor seinem Abitur gründete Kraus das erste Unternehmen, für das er unter anderem eine neue Architektur für einen Programmiersprachen-Interpreter entwickelte und ihn an Atari Computers verkaufte.*
1993 widmete er sich dem Thema Datenqualität. Schnell wurde er zu einem Experten auf dem Gebiet und veröffentlichte kurz darauf sein erstes Buch.
Heute ist Omikron eines der führenden Unternehmen im Bereich Kunden- und Produktdatenqualität. Durch die Bereitstellung integrierter Software, Services und Beratungsleistungen können verlässlich Betrugsversuche identifiziert, Zahlungsrisiken verringert und Dubletten bereinigt werden.
2001 wurde der Unternehmensbereich FACT-Finder gegründet. Inzwischen ist FACT-Finder europäischer Marktführer für Suche und Navigation in Online-Shops. 2011 kam mit FACT-Finder Travel die erste semantische Suche für Touristik-Portale hinzu.

Erklär-Videos für Digital Outsiders

Wie „Starthilfe50.de“ Internet-Einsteigern das Leben erleichtert. Erkenntnisse aus vier Jahren Arbeit

Von Jürgen Selonke

27 Millionen der in Deutschland lebenden Menschen sind Digital Outsiders, nutzen das Internet also kaum oder gar nicht. Viele fühlen sich überfordert, sind ängstlich und verhalten sich deshalb sehr reserviert gegenüber den Möglichkeiten des Mediums. Das ist ein Ergebnis der DIVSI Milieu-Studie.

Eine wichtige, auch gesellschaftspolitische Aufgabe liegt also darin, diese meist älteren Menschen fit im Umgang mit dem Internet zu machen. Einen erfolgreichen Weg zur Lösung dieser Aufgabe geht seit rund vier Jahren „Starthilfe50.de“. Wir sprachen darüber mit Andreas Dautermann und Kristoffer Braun, den Machern und Verantwortlichen des Projekts.

Was ist das Besondere an Starthilfe50?
„Leicht verständliche Erklär-Filme helfen ungeübten Anwendern Schritt für Schritt bei der Nutzung von Computer, Internet und Programmen. Dabei wird bewusst auf englische Fachbegriffe verzichtet und didaktisch gezielt auf Menschen eingegangen, die nicht mit dem Computer aufgewachsen sind. Ein zentrales Thema der Erklär-Videos ist der sichere Umgang mit dem Computer und dem Internet.“

Warum rangiert das Thema Sicherheit weit oben in der Prioritätenliste?
„Wer mit einem Fahrzeug am Straßenverkehr teilnimmt, ist in der Regel stets bedacht, für seine eigene Sicherheit zu sorgen. Zahlreiche Maßnahmen helfen dabei. Bremsen werden genauso kontrolliert wie Ölstand und Kühlwasser. Winterreifen werden aufgezogen, und man bemüht sich, vorausschauend zu fahren. Kaum jemand würde in Frage stellen, dass jeder in erster Linie selbst für seine Sicherheit verantwortlich ist. Auch bei der Nutzung des Internets ist Sicherheit ein wichtiges Thema. Doch hier sind die erforderlichen Maßnahmen weitaus weniger selbstverständlich. Der Vergleich mag etwas hinken, da im Straßenverkehr die eigene Gesundheit gefährdet ist, während man im Internet keine körperliche Schädigung davon tragen kann. Doch durch digitale Betrügereien und unvorsichtige Internet-Nutzung können erhebliche finanzielle Schäden entstehen.“

Wer ist besonders gefährdet?
„Nach unserer Erfahrung meist ältere, noch ungeübte Computernutzer.“

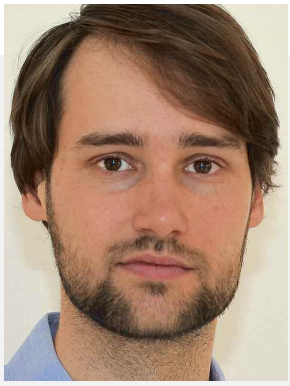
Wo liegen für Anfänger die größten Unsicherheiten und Schwierigkeiten?
„Unsere Erfahrungen zeigen, dass immer wieder die gleichen Fragen und Probleme auftauchen. Grundsätzlich stellen wir eine Ängstlichkeit bei der Internet-Nutzung fest, die sich auf Sicherheitsbedenken gründet. Gleichzeitig ist in diesem Zusammenhang allerdings ein oft erstaunliches Verhalten zu beobachten.“

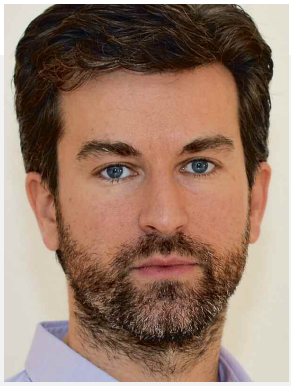
Wie äußert sich dieser Widerspruch bei den Nutzern?
„An manchen Stellen herrscht zu viel Sorge, während tatsächlichen Gefahren nur wenig Beachtung geschenkt wird. So lehnen viele Online-Banking wegen Sicherheitsbedenken ab, obwohl hier von den Banken durch standardmäßige SSL-Verschlüsselung und PIN-/TAN-Verfahren eine Menge zum Schutz der Nutzer getan wird. Gleichzeitig jedoch lässt sich ein leichtfertiger Umgang mit sozialen Netzwerken

registrieren. Hier werden sehr private Informationen öffentlich preisgegeben – oft aus Unkenntnis. Denn einschränkende Maßnahmen muss der Nutzer selbst treffen. Dazu ist er allerdings häufig nicht in der Lage. Wie die neue DIVSI Entscheider-Studie zeigt, schieben die Macher des Internets gern den Nutzern die Verantwortung zu. Wir wissen, dass zumindest Anfänger damit in der Regel überfordert sind."

Was machen Internet-Anfänger noch falsch?
„Sehr häufig wird versäumt, Programme stets auf dem aktuellen Stand zu halten, also regelmäßige Updates durchzuführen. Wir zeigen in unseren Aufklärungsfilmen, dass dies in besonderem Maße für das eigene Betriebssystem, den Virenscanner und den Internet-Browser gilt, denn Programme, die nicht auf dem neuesten Stand sind, bieten Sicherheitslücken. Beim Virenscanner ist die Notwendigkeit der Aktualisierung besonders nachvollziehbar, da dieser immer nur so gut ist wie sein letztes Update. Täglich kommen neue schädliche Anwendungen in Umlauf. Der Virenscanner kann nur diejenigen erkennen und entfernen, die ihm durch das letzte Update mitgeteilt wurden."

Auf welche Sicherheitsrisiken weisen Sie noch explizit hin?
„Kaum ein Internet-Einsteiger weiß, wie wichtig sorgfältig gewählte Passwörter sind. Das gilt besonders, um den Zugang zu privaten Daten wie E-Mail-Konto oder Online-Banking zu sichern. Im Grunde bringen wir hier das kleine 1x1 bei: Ein gutes Passwort besteht aus mindestens acht Zeichen, enthält sowohl Zahlen als auch Buchstaben, zudem werden Groß- und Kleinschreibung kombiniert. Unbedingt zu vermeiden ist das Nutzen von Wörtern des normalen Sprachgebrauchs als Passwort."





***Andreas Dautermann** (* 1980) **und Kristoffer Braun** (* 1982) sind Gründer und Geschäftsführer von Starthilfe50. Beide haben seit 2006 an der Johannes Gutenberg-Universität in Mainz Publizistik studiert und 2012 als Magister Artium abgeschlossen. In ihren wissenschaftlichen Abschlussarbeiten untersuchen sie die Interessen der älteren Computernutzer und evaluieren Methoden zur Steigerung der Medienkompetenz. Die Idee für Starthilfe50 kam ihnen bereits zu Studentenzeiten, als sie neben dem Studium älteren Computernutzern bei PC-Problemen behilflich waren. Durch diese private Auseinandersetzung mit der wissenschaftlichen Problematik der „Digital Divide" entwickelte sich zunehmend ein persönliches Engagement für die Onliner der Generation 50plus. Mittlerweile wird ihre PC-Hilfe in ganz Deutschland genutzt. Für ihre Arbeit an Starthilfe50 wurden sie vom Bundesministerium für Wirtschaft und Technologie beim Wettbewerb „Wege ins Netz" und vom Ministerium des Inneren des Landes Rheinland-Pfalz ausgezeichnet. Die Erklär-Filme können unter www.starthilfe50.de kostenfrei und werbefrei angesehen werden.*

Cybercrime boomt. Wie agiert Starthilfe50 in diesem Zusammenhang?
„Spam-E-Mails, also massenhaft versendete E-Mail-Nachrichten, sind in erster Linie ärgerlich, weil sie das Postfach verstopfen und oft unerwünschte Werbung enthalten. Hier machen wir deutlich, dass solche E-Mails auch Viren und Trojaner enthalten können oder versuchen, dem Empfänger sensible Daten wie Passwörter oder PIN-Nummern zu entlocken – das sogenannte Phishing. Häufig werden hierbei raffiniert die Internet-Auftritte seriöser Firmen visuell kopiert."

Welche konkrete Warnung geben Sie dazu Einsteigern?
„Jede E-Mail mit unbekanntem Absender genau prüfen und niemals deren Anhänge öffnen. Enthält die E-Mail Fehler in der Rechtschreibung oder wurde sie beispielsweise mitten in der Nacht versendet, so ist dies ein deutliches Indiz für eine Spam-E-Mail. Seriöse Firmen wenden sich außerdem bei sensiblen Themen nicht per E-Mail an ihre Kunden, hier sollte man also skeptisch sein."

Worin liegt ein weiterer Fehler von Internet-Neulingen?
„Wer das Internet auf einem fremden Computer oder mit mehreren Personen gemeinsam nutzt, hinterlässt oft Spuren für nachfolgende Nutzer. Häufig speichern Browser Passwörter, Suchabfragen oder den gesamten Verlauf besuchter Seiten ab. Diese Daten sind dann später auch für andere Personen einsehbar. Daher empfiehlt es sich, den privaten Modus zu aktivieren. Alle Browser bieten mittlerweile die Möglichkeit des privaten Surfens an. Ist dieser Modus aktiviert, werden keinerlei Daten in der Chronik gespeichert."

Ihr Fazit nach den ersten erfolgreichen Jahren von Starthilfe50?
„Das Unwissen ist riesengroß. Alle erwähnten Verhaltensweisen und Handlungen erschließen sich Neulingen am Computer nicht ohne kompetente Hilfe von außen. Doch anders als im Straßenverkehr gibt es weder eine Fahrschule, die wesentliche Prinzipien der Sicherheit vermittelt, noch einen TÜV, der in regelmäßigen Abständen das Fahrzeug auf seine Sicherheit hin überprüft. Bei der Internet-Nutzung liegt die Sicherheit nahezu allein in der Hand des Nutzers, dem häufig die tatsächlichen Gefahren und mögliche Gegenmaßnahmen kaum bekannt sind. Daher ist es besonders wichtig, in dieser Hinsicht aufzuklären und auch in der Erwachsenenbildung nachhaltig Medienkompetenz zu vermitteln, damit Grundvoraussetzungen zur sicheren Internet-Nutzung verstanden und angewendet werden können."

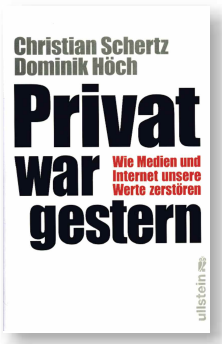
Aktuelle Bücher

Netzpolitik: Freiheit und Rechtsschutz im Internet

Autor: Prof. em. Dr. Hans Peter Bull
Wesentliche Fragen der Netzpolitik sind: Was heißt Freiheit im Internet? Was kann das Recht bewirken, um die Risiken der elektronischen Vernetzung zu minimieren und die Individualrechte zu schützen? Wie kann sich die Demokratie unter dem Einfluss neuer Techniken und der Forderung nach größerer Transparenz weiterentwickeln? Welche Bedeutung hat der Datenschutz und wie sollte er in Zukunft ausgestaltet werden? Prof. Dr. Hans Peter Bull stellt nicht nur Fragen, sondern gibt Antworten: Auf der Grundlage von Risikoanalysen behandelt er die verschiedenen Problembereiche und gibt konkrete Lösungshinweise. Er setzt sich vor allem mit den Ängsten und Sorgen derer auseinander, die den neuen Techniken und ihren Anbietern und Nutzern misstrauen, und plädiert für gezielte, effektive rechtliche Regelungen, die zum Abbau der Risiken beitragen.
Verlag: Nomos, ISBN 978-3-8487-0130-8, Preis: 39,00 €

Wir klicken uns um Freiheit und Verstand
Warum die neuen Medien unsere Demokratie bedrohen

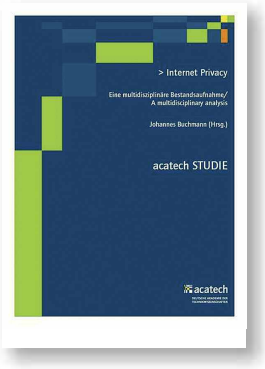
Autor: Dr. Frank Meik
Der langjährige Medienprofi Meik prangert die zunehmende Boulevardisierung und Trivialisierung der Medienlandschaft an: Die neuen Medien haben unsere Denkweise verändert und dominieren unsere Informationswelten. Seiner Einschätzung nach informiert das Internet seicht, oberflächlich und möglichst unterhaltsam. Frank Meik zeigt bei aller Kritik aber auch auf, wie wir die Hoheit über unser Denken wiedergewinnen und die drohende Entmündigung der Demokratie durch die neuen Medien abwenden können. Dafür entwickelt er konkrete Vorschläge.
Verlag: Murmann, ISBN 978-3-86774-214-6 , Preis: 16,90 €



Privat war gestern
Wie Medien und Internet unsere Werte zerstören

Autoren: Christian Schertz, Dominik Höch
Menschen ziehen sich vor der Kamera aus, lassen sich im Kreißsaal filmen und prügeln sich live im Fernsehen mit ihren Nachbarn. Jugendliche offenbaren der Weltöffentlichkeit via Facebook und Co. ihre Sex-Vorlieben. Vom Politiker bis zum C-Prominenten wird die Boulevardpresse gern für Home-Stories benutzt. Der Schutz der Persönlichkeit und der Privatsphäre zählt auf einmal nichts mehr. Medienanwalt Christian Schertz deckt gemeinsam mit seinem Kollegen Dominik

Höch auf, warum der ungewollte und unbedachte Verlust des Privaten für den Einzelnen und die Gesellschaft katastrophale Folgen haben kann – und was wir tun müssen, damit unser Leben auch in Zukunft uns selbst gehört.
Verlag Ullstein, ISBN-10 3550088620, ISBN-13 9783550088629, Preis: 19,99 €



Internet Privacy
Eine multidisziplinäre Bestandsaufnahme

Herausgeber: Johannes Buchmann
Das Buch beinhaltet eine Bestandsaufnahme der existierenden individuellen und gesellschaftlichen Vorstellungen von Privatsphäre im Internet sowie der existierenden rechtlichen, technischen, ökonomischen und ethischen Rahmenbedingungen für Privatsphäre im Internet. Es ist der erste Teil einer zweiteiligen acatech Studie zum Projekt „Internet Privacy – Eine Kultur der Privatsphäre und des Vertrauens im Internet." Johannes A. Buchmann ist Professor für Informatik und Mathematik an der Technischen Universität Darmstadt, Fachbereich Informatik.
Verlag: Springer, Berlin, ISBN-13 9783642319426 , Preis: 39,95 €

Datenschutz
Grundlagen, Entwicklungen und Kontroversen

Herausgeber: Jan-Hinrik Schmidt und Thilo Weichert
Der interdisziplinär angelegte Sammelband gibt einen allgemeinverständlichen Überblick zum aktuellen Stand von Recht, Technik und gesellschaftlichen Debatten, zu Herausforderungen, Chancen und Risiken sowie zu möglichen Szenarien der zukünftigen Entwicklung. In fünf Abschnitten enthält der Band eine Bestandsaufnahme der gegenwärtigen Datenschutz-Regelungen und ihres Anpassungsbedarfs an das digitale Zeitalter. Außerdem beleuchtet er sozialwissenschaftliche, pädagogische, politische und psychologische Aspekte. Die Schrift richtet sich vor allem an junge Leute, ist gut geeignet für die Ausbildung zum Umgang mit Datenverarbeitung. Der Band kann auch im Internet bestellt werden.

Bundeszentrale für politische Bildung Bonn, Band 1190, Gebühr 4,50 €

Impressum

Herausgeber:
Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI)
Matthias Kammer, Direktor
Mittelweg 142
20148 Hamburg

Chefredaktion:
Jürgen Selonke (V.i.S.d.P.)

Autoren:
Dr. Silke Borgstedt, Kristoffer Braun, Prof. Dr. Hans Peter Bull, Andreas Dautermann, Dr. Dirk Graudenz, Dominik Höch, Matthias Kammer, Carsten Kraus, Harald Lemke, Dr. Göttrik Wewer

Realisation:
PubliKom Kommunikationsberatung GmbH, Hamburg

Bildnachweis:
CSM Stock

Verbreitete Auflage:
ca. 7.500 Exemplare
Abgabe kostenlos


DIVSI
Deutsches Institut für Vertrauen und Sicherheit im Internet

www.divsi.de