

2/2012



Deutsches Institut für Vertrauen und Sicherheit im Internet

DIVSI magazin

Digital Outsiders:

Der lange Weg ins Internet Wie sich die digitalen Gräben überwinden lassen

Erkenntnisse aus der DIVSI Milieu-Studie:

Entscheidungsträger beurteilen die Fakten

Frank Pörschmann im Interview:

Ändert sich die CeBIT?

Freie Internet-Nutzung:

Anonymität als Dilemma

Inhalt

- 4 News**
Wichtiges auf den Punkt gebracht
- 
- 6 Digital Outsiders und E-Government**
Folgerungen für die Verwaltung aus der DIVSI Milieu-Studie
- 8 Das haben wir daraus gelernt**
So beurteilen Entscheidungsträger die Studie
- 14 Interview mit Frank Pörschmann**
Zehn Fragen an den neuen Chef der CeBIT
- 
- 16 Digital Outsiders unter der Lupe**
Was sind das für Menschen, die das Netz kaum oder gar nicht nutzen?
- 18 Der lange Weg ins Internet**
So lassen sich die digitalen Gräben (vielleicht) überwinden
- 
- 20 Anonymität als Dilemma**
Freie Internet-Nutzung erfordert Schutz für die Schwächeren
- 
- 22 Gemeinsamkeiten entdeckt**
Von Internet-People und InterNOT-People
- 23 Der Altkanzler und das Netz**
Deutschlands prominentester Digital Outsider?
- 
- 24 Geheimnisverrat und Vertrauensbruch**
Was wäre eine Gesellschaft ohne Diskretion, Loyalität und Geheimnisse?
- 26 Aktuelle Bücher, Impressum**

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

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

Anschrift:
DIVSI
Mittelweg 142
20148 Hamburg



Das Meer, das Internet und die Digital Outsiders

Kleine Geschichten, liebe Leserin und lieber Leser, verdeutlichen manchmal große Dinge. Sie können helfen, dass wir uns alle besser verstehen. Vielleicht reißen sie sogar Barrieren ein oder öffnen zumindest die Augen für Sorgen, die einen selbst gar nicht quälen.

In diesem Sinne – denken Sie sich jetzt bitte ans Meer. Eine Mega-Jacht dümpelt vor Anker in der sanften Dünung. Ein Rentner-Ehepaar schaut verzückt auf den schnittigen Traum. Ihnen nähert sich der Eigner. „Schenke ich Ihnen“, sagt er und zeigt großzügig auf sein Schiff. „Gönnen Sie sich Spaß, Freude und Abwechslung. Sie müssen nur selbst durchs Wasser und an Bord gehen!“

Die beiden alten Herrschaften schlucken: „Leider wird sich diese neue Welt dann nie für uns erschließen. Wir können nicht schwimmen!“

Sagt der Eigner: „Wieso schwimmen? Es bleibt flach. Sie gehen nicht unter. Es passiert nichts.“

Nachdenken bei den Senioren. Doch: „Woher wissen wir, ob man Ihnen trauen kann? Am Ende ist alles nur ein Trick auf unsere Kosten, und wir sind die Reingelegten!“

Und die Moral von der Geschicht’?

Es ist noch viel Überzeugungsarbeit zu leisten, bevor Digital Outsiders sich ins Internet trauen werden.

Zum Glück hat die „DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet“ hierzu bundesweit eine Diskussion in Gang gesetzt. Konkrete Lösungen, wie die Outsiders sicher an Bord zu bringen sind, gibt es noch nicht. Doch ein erster Schritt ist gemacht. Denn immerhin beginnen Verantwortliche, über den Einsatz von Rettungsbooten zu grübeln.

Die zweite Ausgabe des „DIVSI magazins“ widmet sich diesem Thema ausführlich. Wir beschreiben die Outsiders

mit ihren Lebensumständen und Einstellungen (S. 16/17). Wir zeigen Wege und Einrichtungen auf, die ihnen den Weg aus dem digitalen Abseits ermöglichen können (S. 18/19). Sogar Sascha Lobo bricht eine Lanze für die, die er „Inter-NOT-People“ nennt (S. 22).

Konkrete Hilfe für Digital Outsiders ist für unsere gesamte Gesellschaft wichtig. E-Government wird nur funktionieren, wenn es gelingt, alle anzusprechen (S. 6/7). Auch das lässt sich aus der Studie ableiten. Welche Lehren und Erkenntnisse sich außerdem aus der Untersuchung ergeben, dazu haben wir Meinungsbildner aus Politik und Wirtschaft befragt. Die Antworten (ab S. 8) werden weiteren Stoff für Diskussionen liefern.

Ans Herz legen möchte ich Ihnen auch das erste große Interview mit dem neuen CeBIT-Chef (S. 14/15): Frank Pörschmann macht neugierig mit seinem Hinweis auf das Schwerpunktthema der CeBIT 2013. Er wertet Vergangenes und stellt ganz präzise Thesen für die Zukunft auf.

Zum Nachdenken regen die wissenschaftlich-philosophischen Betrachtungen unserer Autoren Prof. Dr. Dirk Heckmann und Dr. Göttrik Wewer an. Ihre Themen sind das „Dilemma einer anonymen Internetnutzung“, sowie „Geheimnisverrat und Vertrauensbruch“ mit dieser These: Eine Gesellschaft ohne Diskretion, Loyalität und Geheimnisse wäre eine andere Gesellschaft.

Viel Spaß und informative Unterhaltung mit dem neuen „DIVSI magazin“. Wenn es Ihnen gefällt – erzählen Sie es gern weiter. Und im anderen Fall sagen Sie mir bitte Bescheid.

Jürgen Selonke
Chefredakteur DIVSI magazin

DIVSI-Stiftungslehrstuhl Berufung vermutlich nach der Sommerpause



München – Nach Abschluss der Vorbereitungen soll der Lehrstuhl für Cyber-Trust an der TU München, eine DIVSI-Stiftung, jetzt ausgeschrieben werden. Den Vorsitz der Berufungskommission hat Prof. Dr. Johann Schlichter. Mitglied der Kommission ist auch Prof. Dr. Claudia Eckert. Die DIVSI-Stiftung ergänzt ihre bereits bestehende Professur für Sicherheit in der Informatik. DIVSI-Direktor Matthias Kammer wird in diesem Gremium als Gast ohne Stimmrecht mitwirken.

Laut Plan ist die Anhörung der Bewerber im Juli geplant. Weiteres Ziel ist, bis nach der Sommerpause zu einem Berufungsvorschlag zu kommen. Gemäß der Ausschreibung sollen mit der Stiftungsprofessur „Brücken zwischen den ingenieurwissenschaftlichen Ansätzen, den betriebswirtschaftlichen Ansätzen (Risikomanagement) und den gesellschaftlichen Ansätzen zum Umgang mit Risiken geschlagen werden“.

Jürgen Gerdes, Vorstand Brief der Deutschen Post, hatte im Beisein von Bundesinnenminister Dr. Hans-Peter Friedrich, Staatssekretär Franz Josef Pschierer, dem Beauftragten der bayerischen Staatsregierung für IT, sowie Prof. Dr. Helmut Krcmar, Dekan der Fakultät Informatik, am Rande des Münchner IT-Gipfels die Stiftungsurkunde überreicht. Der Umfang der Förderung beläuft sich auf 3,5 Millionen Euro.

Selbsterkenntnis Experte ja, Digital Native nein

Leipzig - Der 13. Kongress „Neue Verwaltung“ der dbb-Akademie stand in Leipzig unter dem Motto „Innovation ist Wandel“. Bei zwei Veranstaltungen ging es dabei speziell um die „DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet“. Auf Bitte von Moderator Michael Klöcker stuften sich die Teilnehmer einer Diskussionsrunde im Plenum dabei zu Beginn selbst nach den bekannten SINUS-Milieus ein. Keiner der Experten sah sich als „Digital Native“.

So outete sich die Runde:



Peter Schaar, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit: „Auch wenn man sich das vielleicht nicht vorstellen kann – früher war ich digitaler Hedonist. Heute ordne ich mich zwischen einem souveränen Skeptiker und Performer ein.“

Dr. Marianne Wulff (Geschäftsführerin VITAKO) sah sich als Digital Immigrant aber auch als „effizienzorientierten Performer“.

Thomas Fischermann (Die ZEIT und Co-Autor des Buches „Zeitbombe Internet“: „Digital Immigrant mit Assimilationsabsichten“.

DIVSI-Direktor Matthias Kammer: „Ich werde Immigrant bleiben.“

Und Dr. Silke Borgstedt (Direktorin Sozialforschung des SINUS Institut) gab ehrlich zu: „Vor der Studie habe ich mich mehr Native gefühlt, als ich tatsächlich bin.“

Web 2.0 im Bundestag Interaktion mit Bürgern ausbaufähig

Hamburg – Die ersten Ergebnisse des neuen ISPRAT-Projekts „Politiker im Netz: Der Social Media Activity Index 2011 des 17. Deutschen Bundestags“ liegen jetzt vor. Demnach nutzen nur wenige Bundestagsabgeordnete Social-Media-Plattformen für einen Dialog mit Bürgerinnen und Bürgern. Eine kleine Gruppe sehr aktiver Web-2.0-Champions steht einer Mehrheit von nur selten im Bereich Social Media aktiven Abgeordneten gegenüber. Zwar hat die Mehrzahl der Volksvertreter Accounts bei Facebook, Twitter & Co. Die Chancen einer regelmäßigen Interaktion via Social Media schöpfen aber bislang nur wenige Abgeordnete aus. Junge Volksvertreter urbaner Wahlkreise zeigen sich besonders offen für das Web-2.0. Durchgeführt wurde das aktuelle ISPRAT-Projekt vom Institut für Medien und Kommunikationsmanagement (MCM) der Universität St. Gallen.

Mit diesem eigens entwickelten Index wird eine neue Qualität in die Diskussion um die Social-Media-Nutzung der Politik eingeführt. Analysiert wird die tatsächliche Nutzung der Web-2.0-Plattformen über ein gesamtes Jahr hinweg. Neben der Anzahl der Kontakte und der medialen Vernetzung werden erstmals die verschiedenen Kommunikationsaktivitäten gemessen. Ziel ist, zu analysieren, wie sich die Kommunikation der Bundestagsabgeordneten mit den Bürgern durch soziale Medien verändert und was Treiber dieser Veränderung sind.

Prof. Dr. Miriam Meckel, Direktorin des MCM Instituts der Universität St. Gallen: „Web 2.0 ist zwar bei vielen Abgeordneten business as usual. Entscheidend für den Erfolg in sozialen



Prof. Dr. Miriam Meckel, Direktorin des MCM Instituts der Universität St. Gallen

Netzwerken ist aber Authentizität, Frequenz und Intensität der Präsenz. Für den Dialog zwischen Bürger und Politik in diesen Netzwerken gilt heute: Das ist noch ausbaufähig.“

Die Messung der Social-Media-Aktivitäten der Volksvertreter ergab: 2010 waren 34 Prozent der MdBs auf keiner Social-Media-Plattform präsent. 57 Prozent nutzten sie gelegentlich, acht Prozent waren dort häufig aktiv. Nur ein Prozent der 620 MdBs konnten als Social Media-Champions bezeichnet werden: Sie zeichnen sich durch hohe Kommunikationsfrequenz aus, verknüpfen Plattformen, interagieren direkt mit „Freunden“ oder „Followers“.

Dem vorliegenden Zwischenbericht wird eine qualitative Analyse der Social-Media-Aktivitäten durch eine Befragung der MdBs folgen. Der komplette Zwischenbericht steht zum kostenlosen Download bereit: <http://isprat.net>

Innovationskultur unterstützen Unternehmen sollten aus Unternehmern bestehen

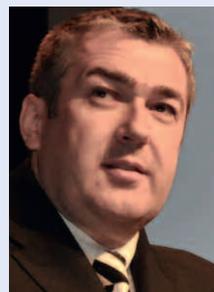
Leipzig – Welche Rolle spielen die Mitarbeiter, wenn es um den nachhaltigen Erfolg eines Unternehmens geht? Dazu äußerte sich Postvorstand Jürgen Gerdes beim dbb-Kongress in Leipzig:

„Neue Ideen fallen nicht vom Himmel. Neue Ideen kommen von Menschen. Jede Innovation beginnt mit der Idee einer Mitarbeiterin oder eines Mitarbeiters! Diese Ideen sind unsere wert-

vollste Zukunftsressource! Wir müssen die Rahmenbedingungen so gestalten, dass Mitarbeiter mit Talent und Potenzial die Möglichkeit haben, gute Ideen für die Entwicklung unserer Geschäfte zu generieren, zu prüfen und wenn möglich zu realisieren. Denn Unternehmen sollten eigentlich aus Unternehmern bestehen.

Hierbei ist unsere Rolle als Arbeitgeber im Fokus.

- *Wie ist das Arbeitsklima? Arbeiten unsere Mitarbeiter gern für uns? Sind sie motiviert?*
- *Sind die Mitarbeiter eher „Opfer“ des Wandels im Unternehmen oder können sie selbst eine wertvolle Rolle bei Veränderungen spielen?*
- *Und welches Image haben wir extern als Arbeitgeber, als Treiber von Innovation? Kommen die besten und kreativsten Leute zu uns?*



Postvorstand Jürgen Gerdes

Insbesondere in Großunternehmen wie unserem ist „anders denken“ für viele Mitarbeiter und für viele Manager eine große Herausforderung – sie waren mit bewährten Methoden, Produkten und Prozessen immer sehr erfolgreich.

Sie wollen sicher sein, dass sie alles richtig machen – und das Neue, das Unbekannte, das Ungeprobte ist alles andere als sicher. Deshalb muss eine Innovationskultur auf allen Ebenen im Unternehmen aktiv unterstützt werden.“

Entscheider im Blickpunkt Neue DIVSI-Studie in Vorbereitung

Hamburg – Die zum Jahresbeginn vorgelegte DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet hat bundesweit für Aufsehen gesorgt und eine breite Diskussion in Gang gesetzt. Jetzt hat DIVSI, das Deutsche Institut für Vertrauen und Sicherheit im Internet, die Vorbereitungen für eine Folgestudie abgeschlossen. Im Mittelpunkt stehen diesmal Entscheider, Gestalter und Multiplikatoren aus Politik, Verwaltung, Wirtschaft und Medien. In der bewährten Zusammenarbeit mit dem renommierten SINUS-Institut sollen diesmal die folgenden Grundfragen detailliert untersucht werden:

- *Wie beurteilen Meinungsbildner und Multiplikatoren die Entwicklung des Internets in Deutschland?*
- *Welche Gestaltungs- und Einflussmöglichkeiten sehen sie im Internet für die von ihnen vertretenen Institutionen?*

Das Sinus-Institut wird dazu bundesweit Führungskräfte aus den genannten Bereichen befragen. Die Ergebnisse der qualitativen Explorationsphase sollen nach jetziger Planung Anfang November vorgestellt werden. Daran anschließend ist eine quantitative Repräsentativerhebung vorgesehen. Joanna Schmölz, verantwortlich für das Wissenschaftsmanagement bei DIVSI: „Die kompletten Fakten wollen wir zur CeBIT 2013 präsentieren. Uns geht es nicht um rasche Ergebnisse. Mit SINUS zusammen wollen wir wissenschaftlich fundierte, stichhaltige Erkenntnisse aufzeigen.“



Gesucht: Der richtige Weg, um die große Kluft zu überwinden

Digital Outsiders und E-Government

Welche Folgerungen kann speziell die Verwaltung aus der DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet ableiten?

Von Matthias Kammer, DIVSI-Direktor

Kostensenkungen für die Verwaltung bei gleichzeitiger Service-Steigerung für die Bürger: Das ist eines der hohen Ziele von E-Government. Natürlich wird das Leben für jeden von uns einfacher, wenn man rund um die Uhr sein Anliegen an die Verwaltung herantragen kann. Erforderliche Daten für die Verwaltung werden gleichsam im Wohnzimmer erfasst. Das ist für uns bequem und erspart gleichzeitig der Behörde Aufwand, was eine Kostensenkung ermöglicht. Nicht zuletzt deshalb, weil sich auf Seiten der Verwaltung die Servicestellen für persönliche Kontakte deutlich reduzieren ließen.

Allerdings hat die bevölkerungsrepräsentative DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet gezeigt: 39 Prozent der bei uns lebenden Bevölkerung nutzen das Netz kaum oder gar nicht. Schon deshalb ist die genannte und richtige Zielsetzung des E-Governments

bis auf Weiteres nicht umfassend umzusetzen. Der Slogan „WLAN für alle“ reicht nicht, um eine soziale Teilhabe an der digitalen Gesellschaft zu fördern.

Es stellt sich daher die Frage, mit welchen Aktivitäten Digital Outsiders überzeugt und für die Nutzung des Internets gewonnen werden können (siehe auch Beiträge in diesem DIVSI magazin auf den Seiten 16 bis 19). Zur Beantwortung dieser Frage sollte sich zunächst vorrangig auf die kommunale Ebene konzentriert werden. Dort gibt es - neben dem staatlichen Finanzamt - die meisten Kontakte zwischen Bürgern und Verwaltung. Wo sind die Konzepte für E-Government, die diese Rahmenbedingung berücksichtigen? Mit der Milieu-Studie wollte DIVSI insoweit einen wichtigen Anstoß für den gesellschaftlichen Diskurs geben.

Unabhängig davon lohnt vielleicht auch ein Blick über unsere Landesgrenzen hinaus. Am Beispiel Schweden lässt sich erkennen, welche positive Rolle E-Government spielen kann. Bis zum Beweis, dass etwas nicht in Ordnung ist, lässt sich bei unseren nördlichen Nachbarn praktisch alles per E-Mail lösen. Dadurch werden viele Prozesse zwischen Bürger und Verwaltung natürlich einfach und leichtgängig.

Bei einem Hauskauf fungiert zum Beispiel der Makler als Schnittstelle zwischen Bürger (Kunde), Gericht und Verwaltung. Der Makler greift online auf das Grundbuch zu. Finanzielle Transaktionen sind ebenfalls einfach geregelt. Anfallende Steuern werden per Online-Bank-Account gezahlt oder die Steuerbehörde schickt dem Bürger eine Einmalkennung und eine TAN direkt zu. Und wer die elektronischen Möglichkeiten nicht nutzen möchte, kann natürlich weiterhin einen Papiervordruck ausfüllen.

Von diesen wie selbstverständlich landesweit genutzten Möglichkeiten des E-Governments ist Deutschland immer noch weit entfernt. Eine Ursache für die bislang geringe Nutzung elektronischer Verwaltungsangebote könnte hierzulande darin liegen, dass für gleiche Aufgaben viele unterschiedliche Lösungen angeboten werden. So fehlt in Deutschland bislang eine einheitliche technische Grundlage für eine sichere Kommunikation im E-Government.

Die Zielsetzung des E-Governments ist bis auf Weiteres nicht umfassend umzusetzen. Der Slogan „WLAN für alle“ reicht nicht, um eine soziale Teilhabe an der digitalen Gesellschaft zu fördern.

Dies mag der Grund dafür sein, dass auch die rund 41 Prozent Digital Natives, die unsere Studie ermittelt hat, dem E-Government oft abwartend gegenüber stehen. Dabei sind Digital Natives Menschen, die mit dem Internet groß geworden sind, es voll in ihr Leben integriert haben – und E-Government eigentlich gegenüber dem umständlichen Behördengang favorisieren sollten.

Doch diese Onliner sind höchst anspruchsvoll. Effizienz, Nutzen und Bedienerfreundlichkeit sind für sie entscheidend. Erfüllt das eher verwaltungszentrierte E-Government diese Ansprüche? Bislang kaum! Dabei wäre es so wichtig, eben jene Internet-affine Nutzergruppe zu überzeugen. Denn diese Gruppe – auch das eine Erkenntnis aus der DIVSI Milieu-Studie – bestimmt mit ihrem Verhalten maßgeblich, was sich im Netz durchsetzt und was nicht.

Ein weiteres Problem lässt sich aus den Ergebnissen der DIVSI Milieu-Studie mit Blick auf Verantwortungskonzepte in Bezug auf die Internet-Nutzung ableiten.

Fast drei Viertel der Deutschen (74 Prozent) erwarten, dass Staat und Wirtschaft aktiv für Sicherheit im Internet sorgen. Die Mehrzahl der Digital Natives dagegen sieht hier den Nutzer selbst in der Pflicht und lehnt jede Einmischung ab.

Hier steht die Politik vor der schwierigen Herausforderung, diametrale Sicherheitsbedürfnisse befriedigen zu müssen. Erfolg oder Misserfolg bei der Lösung dieser Aufgabe wird auch Einfluss auf die weitere Entwicklung und Akzeptanz von E-Government haben. Die Herausforderung für alle Verantwortlichen besteht darin, Angebote und Maßnahmen zu entwickeln, die an die unterschiedlichen Kompetenzen, Motive und Anforderungen in den verschiedenen digitalen Lebenswelten anschließen.



Matthias Kammer ist seit November 2011 Direktor des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI).

Gerade noch rechtzeitig

Von Horst Westerfeld

Die DIVSI-Studie zeigt sehr deutlich den gesellschaftlichen Umgang mit dem Internet auf. Die Studie kommt vielleicht gerade noch rechtzeitig, um die Verantwortlichen in Politik und Gesellschaft auf die „Spaltung“ der Gesellschaft aufmerksam zu machen. Für mich persönlich wird die Aufgabe im IT-Planungsrat sein, die Erkenntnisse der Studie in konkrete Handlungen für Deutschland umzusetzen.

Nach den Befragungsergebnissen der DIVSI-Studie gehören etwa 40 Prozent der Gesellschaft zu sogenannten Digital Outsiders, die das Internet gar nicht oder nur sehr eingeschränkt nutzen und eine sehr kritische bzw. ablehnende Haltung gegenüber der Nutzung des Internets haben. Wobei auch deutlich wird, dass die anderen 60 Prozent gemäß ihrer Zuordnung zu Milieus und bei der Nutzung des Internets sehr stark in Bewegung sind.

Die ermittelten Fakten müssen noch stärker in die Diskussion über Themen wie E-Partizipation, Online-Behörden oder im Kontext des E-Government-Gesetzes mit einfließen. Ein guter Ansatz für beide Gruppen liegt dabei in der flächendeckenden Umsetzung des Bürger-Services 115 als Multikanal-Angebot, der es sowohl über das Telefon als auch das Internet erlauben sollte, alle Services der Behörden zu nutzen. Für Hessen werden wir darauf hinarbeiten, dass alle gesellschaftlichen Gruppen von neuen Technologien profitieren. DIVSI kann ich nur empfehlen, den gestarteten Weg mit der Diskussion der Studie fortzuführen.



Horst Westerfeld ist CIO des Landes Hessen

Die Dialektik von Unsicherheit und Sicherheit in der technischen Innovation

Von Gerold Reichenbach, MdB

Das Internet und alle mit ihm verknüpften Innovationen und Dienstleistungen stehen heute meines Erachtens an einem Scheideweg. Dies macht die DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet implizit deutlich.

Zunehmend wird den Menschen bewusst, dass die Sicherheit ihrer Daten und die Sicherheit vor dem unbemerkten und ungewollten Ausspähen der eigenen Privatsphäre unabdingbar sind, um nicht hilflos Opfer krimineller Machenschaften oder auch ökonomischer Manipulationen zu werden.

Die Frage, ob man sich und wesentliche Teile der eigenen Lebensführung, der eigenen sozialen und ökonomischen Tätigkeiten, einem neuen, technisch nicht durchschaubaren Medium anvertraut, ist letztlich die Frage nach dem Vertrauen in die Sicherheit des Produkts und nach der Zuversicht, diese Sicherheit „in der eigenen Hand zu haben“.

Dieses Grundvertrauen lässt täglich Millionen Menschen in ein Automobil steigen, obwohl sie, im Gegensatz zu den Chauffeuren der Anfangszeit, die technische Komplexität des Produkts in keinsten Weise mehr durchschauen oder gar beherrschen könnten. Die Frage, ob die technische Innovation und das immer weitere Eindringen in immer größere Lebensbereiche - man denke nur an die Zukunftsvision für das Internet der Dinge - weiter voranschreitet oder durch die eigenen Sicherheitsmängel ausgebremst wird, ist davon abhängig, diese Form des Vertrauens herzustellen und zu erhalten.

Genau aus diesem Grunde sind alle Versuche von Teilen der Industrie und der Dienste-Anbieter, den Faktor Sicherheit und Datenschutz als Kostenfaktor oder Beschränkung der Verwertungsmöglichkeiten kleinzuhalten, schon auf mittlere Sicht völlig kontraproduktiv.

Vielmehr sollte jede Chance ergriffen werden, Sicherheitsstandards nach oben hin anzupassen und zu harmonisieren. Letztendlich ist nur dies, neben der Wettbewerbsgleichheit, zentrale Voraussetzung für die Festigung des Vertrauens „in die Gesamtproduktpalette“.

Die jetzt von der Europäischen Kommission vorgeschlagene Verordnung für eine europäische Harmonisierung des Datenschutzes bietet eine solche Chance und sollte nicht aus kurzfristigen, ökonomischen Überlegungen heraus kleingemacht werden.

Bereits heute haben wir die Situation, dass das Image von Marken durch Applikationen leidet, die die persönlichen Daten von Nutzern ohne deren Kenntnis abziehen. Der mittelfristige Imageschaden, der durch die Häufung von „Sicherheits- und Datenschutzvorfällen“ in letzter Zeit der gesamten Branche gerade im Hinblick auf die Entwicklung der Märkte für die nicht Internet-affinen Gruppen entstanden ist, ist bereits jetzt beträchtlich. Die Hemmnisse und Widerstände, die sich der Branche zur Zeit bei der Etablierung des Cloud Computings entgegen stellen, sind auch dem Umstand geschuldet, dass in vielen Bereichen des Internets, aber auch des Datenschutzes, dieses Grundvertrauen bislang nicht hergestellt werden konnte.

Die Hinnahme von Risiken und Unsicherheiten ist eben nicht dauerhaft ein Innovationsfaktor, sondern wird zum Hemmnis, wenn sie in breite Lebensbereiche eindringt, und dieses Eindringen wiederum Voraussetzung für neue Innovationschübe ist.

Für den Automobilisten des späten 19. oder frühen 20. Jahrhunderts, für den das Auto noch Freizeitbeschäftigung und technisches Abenteuer war, mögen die Risiken der unvollkommenen Sicherheitsstandards hinnehmbar gewesen sein. Für die Bürger des Automobilzeitalters, die in weiten Teilen ihrer alltäglichen Lebensführung auf diese neue Mobilität angewiesen sind, sind sie es nicht mehr.

Für den Nutzer von Google und Facebook mag es ebenso noch hinnehmbar sein, dass er nicht unter Kontrolle hat, welche seiner eingestellten persönlichen Daten wo landen, weil er zur Not dem Rat von Mark Zuckerberg folgen kann, der da lautet: „Stay out!“

Für die weitere Etablierung von mobilen Diensten sowie für die Etablierung des Internets der Dinge, bei der Geräte-nutzung, beim Facility Management, beim Ver- und Entsorgungsmanagement oder auch beim alltäglichen Lebensmitteleinkauf gilt diese Devise nicht mehr.

Niemand wird sich in die Hände einer Kommunikations- und Informationstechnologie begeben, zu der er kein Sicherheitsvertrauen hat. Der zynische Rat von Mark Zuckerberg, der in einer solchen Welt „Don't heat, don't buy, don't travel“ lauten müsste, würde sehr schnell zum Ende dieser Technologie führen.



Gerold Reichenbach (SPD) ist u.a. Mitglied im Innenausschuss sowie Mitglied der Enquete-Kommission "Internet und digitale Gesellschaft"

Werthaltungen zur Kenntnis nehmen

Von Jörn Riedel

Die DIVSI-Studie ist ein wichtiger – und der bisher einzige empirische – Beitrag für eine Diskussion um die meines Erachtens nach zwingende Neuausrichtung von öffentlichen Online-Angeboten.

Diese Neuausrichtung ist zwingend notwendig, weil

- *die bisherige Angebotsstrategie an Grenzen gestoßen ist, was das Erschließen neuer Kundengruppen angeht, und*
- *die Reorganisation der Geschäftsprozesse unausweichliche Konsequenz von Schuldenbremse, gesellschaftlicher Digitalisierung und Arbeitskräftemangel ist.*

Die Studie zeigt das Dilemma öffentlicher Online-Angebote:

- *Die Digital Outsiders nutzen sie nicht, weil sie dem Medium nicht trauen und/oder wir Sicherheitsprozesse aufsetzen, die nur IT-Profis bedienen können.*
- *Die Digital Natives nutzen sie nicht, weil sie die Sicherheitsprozesse als schikanös und als Bevormundung erleben.*
- *Allenfalls die Digital Immigrants gewinnen wir – aber nur, wenn und soweit wir ihnen trotz komplizierter Sicherheitsprozesse einen für sie messbaren Nutzen bieten.*

Die in dieser Studie belegte Lebenswirklichkeit ist bisher nicht Gegenstand der politischen Debatte rund um attraktive Online-Angebote der öffentlichen Hand. Die Debatte um das neue E-Government-Gesetz zeigt, wie es weiter in die falsche (weil vom Kunden nicht akzeptierte) Richtung geht. Die eigentlich gute Idee der zertifizierten Qualitätsmail (DE-Mail) wird totreguliert. Allen Ernstes wird diskutiert, das Senden einer DE-Mail durch einen Verwaltungskunden bedeute nicht, dass er auch eine Antwort haben will. Sondern man darf ihm nur eine DE-Mail senden, damit er – bitte sehr – auf einer bestimmte Webseite einen Zugang zu sich eröffnet, und zwar nur für den jeweiligen Verwaltungszweck.

Jedes Unternehmen, das so mit seinen Kunden verfahren würde, wäre pleite.

Wenn öffentliche Verwaltung und die sie führenden Politiker die in dieser Studie deutlich werdenden Werthaltungen nicht zur Kenntnis nehmen, wird es zu einer weiteren Entfremdung zwischen Staat und den Bürgern bzw. Unternehmen kommen.

Nach meiner Überzeugung gibt es eine Reihe von Strategien, mit denen man akzeptierte Online-Angebote der öffentlichen Verwaltung schaffen kann. Dies gelingt aber nur, wenn Regulierung auf ein vertretbares Maß zurückgefahren wird und wenn man rechtlich/politisch und im praktischen Handeln Zielgruppenorientierung zulässt. Wenn die Studie dazu einen Beitrag leistet, war sie jede Mühe wert.



*Jörn Riedel ist CIO
der Freien und
Hansestadt Hamburg*

Politik muss mit werteorientierten Entscheidungen vorangehen

von Dr. Konstantin von Notz, MdB

Die DIVSI Milieu-Studie liefert einen interessanten Blick auf unsere zunehmend heterogene Gesellschaft. Gleichzeitig wird einem bei der Lektüre bewusst, wie abstrakt die für derartige Umfragen verwendeten Begriffe sind (und wohl sein müssen) und wie unterschiedlich dementsprechend die Antworten ausfallen. Gleichwohl gibt sie praktische Hinweise darauf, dass Maßnahmen zur Steigerung des Vertrauens und der Sicherheit womöglich wirksamer ausfallen könnten, wenn sie entsprechend milieu-abgestuft erfolgen.

Es erscheint sinnvoll, die generelle Blickrichtung der Studie einzuordnen. Mit den Nutzerinnen und Nutzern stehen einerseits diejenigen im Mittelpunkt, um die es bei der Frage der Sicherheit und des Vertrauens in erster Linie gehen sollte. Das ist zu begrüßen und man vermag mit dem erlangten Wissen zum Beispiel bei Maßnahmen zur Stärkung der Medienkompetenz sehr konkret ansetzen zu können.

Allerdings gilt auch: Vertrauen und Sicherheit im Internet sind äußerst anspruchsvolle Ziele, die einen mehrdimensionalen Steuerungsansatz verlangen. Erfasst werden müssen insbesondere die großen Akteure wie Wirtschaftsunternehmen und Verwaltung, weil ansonsten keine Breitenwirkungen zu erreichen sind. Und: Die Ziele der Schaffung von mehr Vertrauen und Sicherheit müssen stets an den großen Drei unserer Rechtsordnung – an Rechtsstaat, Demokratie und den Grundrechten – Maß nehmen. Völlig zu Recht betont deshalb der Bundespräsident die Notwendigkeit, im Kontext des Internets vorrangig den Erhalt von Freiheit zu diskutieren.

Für den Erhalt von Freiheit und Selbstbestimmung muss der Gesetzgeber aktiv werden. Verkürzende Vorstellungen von „natürlicher Freiheit“ als einem (bloß) reaktiven Abwehrrecht werden den Freiheitsfragen der digitalen Gesellschaft nicht gerecht. Weder Netzneutralität noch Freiheit vor unverhältnismäßiger Verfolgung, sei es durch private Abmahnungsgesellschaften oder staatliche Sicherheitsbehörden, werden sich von selbst einstellen. Sie bedürfen anspruchsvoller Regulationsanstrengungen mit innovativen Konzepten.

Gerade der Erhalt des Datenschutzes im Internet als ganz zentrale Grundlage von Vertrauen und Sicherheit lässt sich nicht allein den überforderten Nutzern aufbürden. Hier ist die Politik gefordert, die Faktizität der Milieu-Welten zu übersteigen und Lösungen mit Blick auf die ganze Gesellschaft anzubieten.



*Dr. Konstantin von Notz
(Bündnis 90/Die Grünen) ist
u. a. Mitglied im Innenausschuss
sowie Mitglied der
Enquete-Kommission
„Internet und
digitale Gesellschaft“*

Wir brauchen ein Recht auf schnelles Netz und digitale Selbstständigkeit

Von Lars Klingbeil, MdB

„Rund 27 Millionen Menschen in Deutschland leben komplett oder nahezu komplett ohne Internet. Damit sind hierzulande fast doppelt so viele Personen offline wie bislang angenommen.“ Das ist das zentrale und irritierende Ergebnis der „DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet“. Die Studie kommt zu dem Ergebnis, dass fast 40 Prozent der Menschen in Deutschland „Digital Outsiders“ sind. Gemeint sind damit nicht allein Menschen, die keinen technischen Zugang zum Netz haben, sondern auch diejenigen, die das Netz – aus den unterschiedlichsten Gründen – nicht nutzen. Auf der anderen Seite bezeichnet die Studie 41 Prozent (28 Millionen Menschen) als „Digital Natives“. Als dritte Gruppe schließlich identifiziert die Studie 20 Prozent (rund 14 Millionen Menschen) als „Digital Immigrants“. Gemeint sind damit diejenigen, die auf der einen Seite die kommunikationstechnischen Innovationen und das Internet gezielt für ihre Zwecke nutzen, gleichzeitig aber auch die negativen Folgen des Digitalisierungsprozesses wahrnehmen und daher eher defensiv damit umgehen. Angeführt wird hier oft das Thema Datenschutz und die Offenlegung der Privatsphäre in sozialen Netzwerken.

Natürlich kann man über solche Kategorisierungen trefflich streiten. Die Zahlen zeigen jedoch, dass die oft befürchtete digitale Spaltung der Gesellschaft noch längst nicht überwunden ist und dass die signifikanten Gräben, die unsere digitale Gesellschaft spalten, weitaus größer sind, als bislang angenommen. Während man in der Diskussion um die digitale Spaltung oft zwischen „Onlinern“ und „Offlinern“ unterschieden hat – also denen, die Zugang zum Netz haben, und denen, die davon ausgeschlossen sind –, belegt die Studie, dass es viel entscheidender ist, wie die Menschen das Netz tatsächlich nutzen und wo sie diesem vielleicht auch mit Misstrauen oder Sorgen begegnen.

Im Vorwort der Studie schreibt der heutige Bundespräsident Joachim Gauck: „Das weltweite Internet bietet alle Voraussetzungen, um die in den ersten zehn Artikeln unserer Verfassung verankerten Grundrechte aller Bürger in diesem Land auszuhöhlen. Dies gilt insbesondere für das Recht auf freie Meinungsäußerung und Pressefreiheit in Artikel Fünf – eine wesentliche Grundlage unserer funktionierenden Demokratie – und es gilt letztlich auch für den Kernsatz unserer Verfassung, den Artikel Eins des Grundgesetzes: Die Würde des Menschen ist unantastbar.“ Natürlich sind mit der Digitalisierung der Gesellschaft und der weltweiten Vernetzung, wie bei vielen technologischen Innovationen, auch diese negativen Potenziale denkbar, und es muss uns darum gehen, genau diese Entwicklungen zu verhindern. Leider wurde aber diese Aussage in der öffentlichen Debatte aus dem Kontext gerissen und so der Eindruck erweckt, als ob es nahezu zwangsläufig eine solche Entwicklung geben müsse. Dem ist nicht so, denn das Internet bietet auch alle Voraussetzungen, um die verfassungsrechtlich garantierten Grundrechte aller Bürgerinnen und Bürger in unserem Land zu stärken und in vielen anderen Ländern vergleichbare Grundrechte erst zu eröffnen. Dies gilt zuallererst für das Recht auf freie Meinungsäußerung und die Pressefreiheit: Die Ereignisse in Tunesien, Ägypten oder in Libyen haben auf der einen Seite die Gefährdungen aufgezeigt, denen die freie Meinungsäußerung und die unbeobachtete Kommunikation, unabhängige Medien und ein freies Internet immer aufs Neue ausgesetzt sind. Sie zeigen aber zugleich, dass das Internet und auch die Sozialen Netzwerke einen enormen Beitrag für die Freiheitsbewegungen in diesen Ländern geleistet haben.

All dies setzt jedoch den Zugang zum Netz und den kompetenten Umgang mit dem Netz voraus. Deswegen brauchen wir das Recht auf ein schnelles Internet, und deswegen setzen wir auf die digitale Selbstständigkeit. Damit ist das Ziel gemeint, dass jeder Bürger und jede Bürgerin in der Lage sein soll, alle Möglichkeiten der „Digitalen Gesellschaft“ möglichst selbstständig zu nutzen und – anders herum – sich vor allen damit verbundenen Risiken möglichst gut schützen zu können. Und, hierfür liefert die Studie zahlreiche Belege, dies setzt Vertrauen in die neuen Kommunikationsmöglichkeiten voraus. Datenschutz und Datensicherheit sind daher zentrale Akzeptanzvoraussetzungen in der digitalen Welt.

Was schlussfolgern wir aus der Studie? Wir brauchen endlich das Recht auf Netz und auf einen schnellen Internet-Zugang, um die digitale Spaltung zu überwinden. Noch immer gibt es zahlreiche Regionen, in denen es keinen breitbandigen Zugang zum Netz gibt. Viele Menschen sind daher von den Möglichkeiten und Chancen des Netzes abgekoppelt und damit in ihren Teilhabemöglichkeiten begrenzt. Zugleich müssen wir die Menschen in die Lage versetzen, digital selbstständig und kompetent diese neuen Möglichkeiten der Information und Kommunikation zu nutzen. Ein kompetenter, gestaltender Umgang mit Medien und dem Netz ist eine Voraussetzung zur Beteiligung des Einzelnen am gesellschaftlichen Diskurs und wird damit zum Schlüssel zur gesellschaftlichen Teilhabe in Bildung und Ausbildung, Arbeit, Gemeinwesen und auch in der Politik. Wenn wir das schaffen, wird es uns auch gelingen, die Potenziale des Netzes für mehr Grundrechte und für die Stärkung der Demokratie zu stärken. Wir müssen Netzpolitik endlich als Gesellschaftspolitik verstehen.



Lars Klingbeil (SPD) ist u.a. Mitglied im Verteidigungsausschuss sowie Mitglied der Enquete-Kommission „Internet und digitale Gesellschaft“

Den digitalen Graben überwinden

Von Thomas Jarzombek MdB

Nachdem das SINUS-Institut für seine Milieu-Studien schon eine gewisse Berühmtheit erlangt hat, birgt die Studie des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI) einige unerwartete Erkenntnisse. Die Engagierten in der Netzpolitik kennen das Problem der Digitalen Spaltung spätestens aus verschiedenen Diskussionen insbesondere um den Zugang zum Internet, die dargestellten Milieus unterscheiden sich aber in ihrem Verhalten im und ihrem Umgang mit dem Internet. Deutlich zeigt sich vor allem: Die eine digitale Gesellschaft gibt es nicht, und wir müssen aufpassen, dass die Gruppe der Digitalen Souveränen nicht den Blick auf die freiwilligen oder unfreiwilligen Nichtnutzer verdeckt.

Große Sorgen bereiten mir persönlich die Ängste derjenigen, die das Internet tatsächlich nutzen. Auf die Frage nach den Gefahren der Internet-Nutzung werden die Infizierung des Computers mit Schadprogrammen (47 Prozent), die unerwünschte Weitergabe von persönlichen Daten an Dritte

(46 Prozent) und die Belästigung durch unerwünschte E-Mails genannt (43 Prozent). Ähnlich häufig wird die Angst vor dem Ausspähen von Daten aber auch die Angst vor dem Löschen von Daten genannt. Persönlich erlebt haben diese Gefahren weniger als die Hälfte der Bevölkerung. Dazu passt dann auch, dass gleichzeitig der IT-Branchenverband BITKOM in einer neuen Studie zu dem Ergebnis kommt, jeder fünfte Internet-Nutzer in Deutschland verzichte immer noch auf Virenschutz oder eine Firewall. Wie kann man diese Brücke zwischen der subjektiven Angst und den persönlichen Vorteilen durch die Nutzung des Internets abbauen?

Für mich bedeuten diese widersprüchlichen Erkenntnisse, dass der Nachholbedarf bei der technischen Medienkompetenz auch im Jahr 2012 weiterhin besteht. Gleichzeitig müssen die Ängste sowohl vor finanziellen Schäden durch Betrug oder Ausspähen im eCommerce und Online-Banking als auch vor immateriellem Schaden durch Datenverlust von den Anbietern ernst genommen werden. Um diffuse Ängste abzubauen, sollten sie ihre Kunden besser über die Verwendung ihrer Daten aufklären und aufzeigen, wie sie für den Schutz sorgen wollen. Gerade bei den oben aufgeführten, subjektiven Ängsten können wenige große Skandale viel Vertrauen zerstören, obwohl es keine persönliche Betroffenheit gibt.



Thomas Jarzombek (CDU) ist u.a. Mitglied des Ausschusses für Familie, Senioren, Frauen und Jugend sowie Mitglied der Enquete-Kommission "Internet und digitale Gesellschaft"

Daten von grundlegender Bedeutung

Von Dr. Johann Bizer

So eine Studie war längst überfällig: Eine umfassende und repräsentative Bestandsaufnahme, die die bundesrepublikanische Internet-Gesellschaft objektiv und nicht interessegeleitet darstellt. Nur so ist eine faktenbasierte Politik überhaupt erst möglich.

Für Dataport sind die Daten, die die elektronische Kommunikation zwischen Bürger und Verwaltung beschreiben, von grundlegender Bedeutung. Was machen wir aus der Erkenntnis, dass wir Anbieter die einen 40 Prozent der Nutzer erst gar nicht erreichen, aber den anderen 40 Prozent nicht „hip“ genug sind?

Mit dieser Frage kann die Gestaltung von Online-Geschäftsmodellen für den Public Sector nur in eine umfassende Multikanal-Strategie münden. Die Erkenntnis, dass sich von Online-Angeboten bestenfalls 60 Prozent der Menschen angesprochen fühlen, führt zwingend zu der Verpflichtung der Verwaltung, auch andere Kanäle des Verwaltungszuganges noch für eine lange Zeit geöffnet zu halten. Die einheitliche Behördenrufnummer 115 führt in die richtige Richtung.

Und was machen wir aus der nachgerade dramatischen Erkenntnis, dass unser staatliches Regulierungsmodell, mit dem wir die Risiken des Internets zu begrenzen gedenken, sich an einer Nutzergruppe von 20 Prozent Digital Immigrants orientiert? Bedeutet das womöglich Datenschutz von Immigrants nur für Immigrants – und damit an 80 Prozent der Nutzer vorbei? Kein Wunder, dass laut BITKOM 2011 nur jeder dritte deutsche Wahlberechtigte die Internet-Kenntnisse der Politiker für ausreichend hält.

Grundrechte sind kein Wunschkonzert, sondern basale Werte unserer Gesellschaft. Sie müssen sich durch einen wirklichkeitsbezogenen Geltungsanspruch in Rechtsordnung und Gesellschaft bewähren – und zwar offline wie online. Gewährleistungen wie Selbstbestimmung und Informationsfreiheit gewinnen oder verlieren durch die Wahl des Mediums nicht an Wert. Und das ist dann in der Tat auch die wirkliche gesellschaftliche Herausforderung, vor der wir stehen: Wir brauchen einen gesellschaftlichen Diskurs, wie wir den Spagat zwischen Datenschutz und Informationsfreiheit, zwischen Kontrolle und Selbstbestimmung für Offliner wie Onliner gleichermaßen zufriedenstellend gestalten können und wollen.



Dr. Johann Bizer ist seit November 2011 Vorsitzender des Dataport-Vorstands und verantwortlich für den Bereich Lösungen.

„Unseren Erfolg bemessen wir am Erfolg unserer Kunden“

Jürgen Selonke sprach mit dem neuen Chef der weltweit wichtigsten Veranstaltung für die ITK-Industrie

Managing Trust war das Schwerpunktthema der CeBIT 2012. Wo soll der Fokus 2013 liegen?

Mit „Managing Trust“ haben wir zur CeBIT 2012 das richtige Thema zum richtigen Zeitpunkt adressiert. Gerade in Zeiten von Cloud Computing rücken die Diskussionen rund um die Sicherheit und Vertrauenswürdigkeit von Technologien immer stärker in den Mittelpunkt. Das war in diesem Jahr auf der gesamten Veranstaltung spürbar. Auch in Zukunft werden Sicherheit und Vertrauen zu den zentralen Herausforderungen unserer Branche zählen – das ist keine Überraschung. Was hingegen eine Überraschung sein wird, ist das Motto der kommenden CeBIT. Im Spätsommer werden wir das Geheimnis lüften. Aktuell sprechen wir intensiv mit Vertretern der Anbieter- und Anwenderindustrien sowie unseren strategischen Partnern und Analysten. Dabei nehmen wir von allen Seiten Impulse auf. Unser Ziel ist es, ein Thema zu definieren, das die internationale ITK-Branche nachhaltig prägen wird und wirtschaftlich wie gesellschaftlich von hoher Relevanz ist.

Welches ist für Sie die wichtigste Erkenntnis der letzten CeBIT?

Unseren Erfolg bemessen wir am Erfolg unserer Kunden. An den fünf Messetagen im März in Hannover wurden mehr als sieben Millionen Geschäftskontakte generiert. Damit ist die CeBIT Maßstab für Geschäftsanbahnung weltweit. Um

dies zu erreichen, bauen wir unser Leistungsportfolio kontinuierlich aus und entwickeln immer neue Beteiligungsmodelle und Dienstleistungen, die individuelle Vermarktungsbedürfnisse abdecken.

Was sich ebenfalls bewährt hat, ist der kontinuierliche Ausbau der kommunikativen Reichweite der CeBIT über alle Kanäle. Die beteiligten Unternehmen konnten durch ihren Auftritt in Hannover eine deutlich höhere Aufmerksamkeit in der internationalen Berichterstattung erzielen. Selbst als Apple das neue iPad in den USA vorstellte, konzentrierten sich die Diskussionen der Netzgemeinde innerhalb kürzester Zeit auf die weiteren Tablet- und Smartphone-Anbieter, die in Hannover vertreten waren. Das war vermutlich der schnellste und intensivste Produkt- und Leistungsvergleich der CE-Branche.

Wo sehen Sie die CeBIT 2020 und behält sie ihre weltweite Anziehungskraft?

CeBIT steht einerseits für das weltweit wichtigste Ereignis der ITK-Industrie. Darüber hinaus ist die CeBIT eine Marke mit dem Leistungsversprechen, Innovationen zu fördern und Geschäft anzubahnen. Unabhängig davon, wie die ITK-Welt im Jahr 2020 aussehen mag, wer digitale Innovationen und sein Geschäft vorantreiben möchte, wird sich fragen „Wie kann die CeBIT mich dabei unterstützen?“

Schon heute ist die CeBIT viel mehr als nur eine Messe. Sie bietet Ausstellung, Foren und Kongresse, Services zur Lead-Generierung und eine einzigartige Möglichkeit zur Markenpositionierung, Pressekommunikation sowie zur Netzwerk- und Community-Pflege. Damit schafft die CeBIT ein Alleinstellungsmerkmal, das sich in seiner Wertigkeit deutlich von dem anderer Veranstaltungen abhebt. Unsere Kunden – egal



Frank Pörschmann ist seit dem 1. April 2012 Mitglied im Vorstand der Deutschen Messe AG. In dem Gremium trägt er die Gesamtverantwortung für die CeBIT als weltweit wichtigste Veranstaltung der digitalen Wirtschaft. Zudem verantwortet er die Bereiche Technik und Gelände, Protokoll und Events sowie Messe-Gastronomie. Pörschmann kam 2010 vom IT-Konzern IBM zur Deutschen Messe AG und übernahm dort zunächst als Bereichsleiter die operativen Geschäfte der CeBIT. Bei IBM war er mehr als zehn Jahre in unterschiedlichen internationalen Beratungs-, Vertriebs- und Management-Funktionen tätig. Zuvor war Pörschmann für Vertriebs-, Redaktions- und Projektarbeit in Unternehmen der Telekommunikation, Medien und Unterhaltungselektronik zuständig. Pörschmann ist Diplom-Ingenieur für Nachrichtentechnik, studierte zusätzlich Medienwirtschaft und hält einen britischen MBA.

ob Nischen-Anbieter oder internationaler Großkonzern – werden von uns individuell bei der Erreichung ihrer Ziele unterstützt. Das gilt sowohl vor und während als auch nach der Veranstaltung. Diesen Service werden wir weiter ausbauen. Denn er ist der Schlüssel in eine erfolgreiche Zukunft.

Ein Blick zurück: Was hat Sie bei der Internet-Entwicklung der letzten Jahre am meisten beeindruckt?

Am nachhaltigsten beeindruckt hat mich die Veränderung der Lebens- und Arbeitswelten. Ich selbst gehöre ja noch einer Generation an, die vor Jahren ohne mobiles Internet und Smartphone auskommen musste. Damals fanden Informationsbeschaffung, Meinungsbildung, Kommunikation und Beziehungspflege noch in einem anderen Rahmen statt. Mein heutiges Leben wäre unter den damaligen Umständen gar nicht denkbar. Heute genieße ich die vielfältigen digitalen Möglichkeiten, die mein Leben unabhängiger, mobiler und facettenreicher machen. Gleichzeitig können Innovationen auch Schattenseiten mit sich bringen, das Internet hat einige davon. Deshalb müssen wir aufmerksam und kritisch mit dem Internet umgehen und den Mut zur selbstbestimmten Lebensführung haben – dazu zählt auch ein mutiges „Nein“ zur Dauererreichbarkeit.

Ein Blick voraus: Was erwarten Sie von der Internet-Entwicklung der nächsten Jahre?

Die mobile, vernetzte Kommunikation wird unsere Gesellschaft weiterhin spürbar beeinflussen. Ich gehe davon aus, dass beispielsweise die aktive Bürgerbeteiligung durch den Einsatz von Internet und Social-Media-Instrumenten in der Verwaltung zunehmen wird.

Im geschäftlichen Umfeld sind ebenfalls große strukturelle Umbrüche zu erwarten. Denn das Internet verändert nicht nur die Art und Weise, wie wir extern kommunizieren, sondern auch die Kommunikation innerhalb von Unternehmen. Hierarchien und Strukturen werden sich an das veränderte Kommunikationsverhalten anpassen müssen. Dieser Prozess hat gerade erst begonnen und ist höchst spannend mitzuerleben.

Laut DIVSI-Studie sind 39 Prozent der Deutschen Digital Outsiders, also online kaum oder gar nicht aktiv. Erstaunt Sie diese hohe Zahl?

Es gibt auch andere Studien, die diese Zahl deutlich geringer sehen. Dennoch denke ich, dass die Branche und auch wir als CeBIT gefordert sind, Hilfestellungen zu geben, um jedem einen einfachen und schnellen Einstieg in das digitale Leben zu ermöglichen.

Wir dürfen in dieser Diskussion allerdings nicht dazu tendieren, die Digital Outsiders auszugrenzen. Wer bewusst und gewollt Abstand zu digitalen Instrumenten sucht, muss auch mit dieser Entscheidung akzeptiert werden und kann möglicherweise aus dieser neutralen Sicht gute Anregungen für zukünftige Entwicklungen geben.

Sehen Sie Möglichkeiten, diese Digital Outsiders ans Netz zu führen? Vielleicht mit einer speziellen Einrichtung im Rahmen einer CeBIT?

Schon seit Jahren ist dies eines der Anliegen, das die CeBIT sehr ernsthaft verfolgt. Mit Aktionen wie „Bürger trifft Behörde“, Informationsveranstaltungen zu speziellen Themen oder geführten Touren über das Messegelände versuchen wir, Menschen aller Altersklassen, Berufsstände und Gruppenzugehörigkeiten für digitale Technologien zu begeistern. Im Übrigen sehen wir bei der CeBIT einen erfreulichen Trend der Senioren-Generation, deren Teilnahme jetzt wieder zugenommen hat. Sie alle kommen, um sich auf der CeBIT über die digitalen Möglichkeiten zu informieren.

Eine der Kernfragen beim Umgang mit dem Netz ist die Sicherheits-Problematik. Um für mehr Schutz zu sorgen: Ist jeder Nutzer selbst gefordert oder sollte der Staat mehr eingreifen?

Der Staat kann dazu beitragen, die erforderlichen Normen und einen verlässlichen Rechtsrahmen zu definieren. Grundsätzlich ist es allerdings wichtig, dass sich jeder seiner eigenen Verantwortung bewusst ist. Verantwortung schließt dabei auch die Pflicht ein, informiert zu sein und sich etwa vor Angriffen aus dem Netz zu schützen. Die CeBIT bietet allen Besuchern vielfältige Möglichkeiten, sich über die neuesten digitalen Lösungen und deren Sicherheit und Beherrschbarkeit zu informieren.

Wie sehen Sie die Entwicklung des E-Government?

E-Government ist eines der Megathemen der Zukunft und sollte gerade vor dem Hintergrund der zunehmenden Urbanisierung als dauerhafte strategische Aufgabe verstanden werden. Die CeBIT trägt dieser Entwicklung Rechnung und fördert gezielt den Austausch zwischen ITK-Anbietern und der öffentlichen Hand. Im Rahmen von CeBIT gov können sich Vertreter der EU, des Bundes sowie der Länder und Kommunen über aktuelle Entwicklungen austauschen. In den vergangenen Jahren haben wir die erfolgreiche Plattform kontinuierlich ausgebaut. Auch international hat CeBIT gov spürbar an Bedeutung gewonnen.

Was bedeutet Cloud Computing für Sie? Ein notwendiger Schritt in die richtige Richtung oder eine riskante Weiterentwicklung?

Die zunehmende Nachfrage nach Cloud Computing wird zu einer grundlegenden Neustrukturierung der internationalen ITK-Welt führen. Hohe Bandbreiten, steigende Rechengeschwindigkeiten und ein immer einfacherer Zugang zum Internet über mobile Endgeräte sind wesentliche Treiber dieser Entwicklung. Für Unternehmen und Organisationen bietet die Cloud entscheidende Vorteile. Auch Privatpersonen profitieren davon. Sicherheit und Vertrauen sind dabei derzeit die wesentlichen Erfolgsfaktoren. Welche Maßnahmen für einen sicheren und vertrauensvollen Umgang mit den Daten im Netz erforderlich sind, hat die CeBIT in diesem Jahr eindrucksvoll gezeigt.

Digital Outsiders unter der Lupe

39 Prozent der Deutschen nutzen das Netz kaum oder gar nicht. Was sind das für Menschen?

Die DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet kennzeichnet insgesamt sieben Milieus. Mit der Verortung der Typen entstehen ganzheitliche, empirisch fundierte Zielgruppen. Sie können nicht nur hinsichtlich ihrer Einstellung zu Vertrauen und Sicherheit im Internet beschrieben werden, sondern auch entsprechend ihrem lebensweltlichen Hintergrund und ihrer Stellung in der Gesellschaft. Das ist Voraussetzung für eine milieu-sensible Zielgruppenansprache.

Zwei dieser Milieus werden als „Digital Outsiders“ eingestuft. Diese beiden Gruppen umfassen 39 Prozent der bei uns lebenden Bevölkerung. Gemeinsam ist ihnen, dass sie das Netz kaum oder gar nicht nutzen.

Ordnungsfordernde Internet-Laien

Sie gehören zur konventionellen Mitte mit starkem Streben nach Harmonie und Geborgenheit in einfacher bis mittlerer sozialer Lage. Sie haben ein grundsätzliches Misstrauen gegenüber dem Medium Internet, insbesondere in puncto Datensicherheit und Datenschutz. Die Verantwortung hierfür delegieren sie an den Staat und Unternehmen.

Für sie ist das World Wide Web unbekanntes Terrain. Aus Furcht vor Fehlern besteht die Annäherung an dieses Medium vornehmlich in Form von Vermeidungsstrategien – „nur das machen, was gefahrlos ist“. Das Internet nutzen sie entsprechend defensiv und formulieren keine profilierten Ansprüche, da sie überwiegend Basisfunktionen nutzen (möchten). Aufgrund ihrer geringen Selbstsicherheit im Umgang mit dem Internet nehmen sie gern Hilfe in Anspruch.

Ordnungsfordernde Internet-Laien haben ein zwiespältiges Verhältnis zu moderner Informationstechnik. Einerseits zeigen sie sich aufgrund fehlender Kompetenz im Umgang verunsichert. Andererseits ist ihnen bewusst, dass sie sich dem fortschreitenden Digitalisierungsprozess nicht verschließen dürfen, wenn sie berufliche Chancen und sozialen Anschluss nicht aufs Spiel setzen möchten. Als preisbewusstes und serviceorientiertes Gesellschaftssegment erkennt diese Gruppe zunehmend die Convenience-Vorteile, die ihnen das Netz bieten kann.

Das „Mithalten-Wollen“ ist für sie zentraler Motivator, sich mit Computer und Internet auseinanderzusetzen. Dies ist jedoch beschwerlich und gilt weniger als Freizeitvergnügen. Kaum hat man eine Funktion verstanden und in das eigene Handeln integriert, wird man mit Zusatzfunktionen konfrontiert. Da bleibt kaum Raum, sich zu erfreuen, eine Herausforderung gemeistert zu haben.

Aufgrund ihrer geringen Internet- und IT-Kompetenz haben sie ein starkes Bedürfnis nach mehr Sicherheit im Internet. Dementsprechend wünschen sie sich ein „überschaubares Internet“, das verbindliche und verlässliche Rahmenbedingungen bietet und so eine gefahrlose Nutzung gewährleistet. Dabei bestehen keine profilierten Ansprüche an das Medium, vielmehr muss die Basis stimmen: Die „einfachen Seiten“, die fast alle verwenden, sollen funktionieren und



besonders gut gegen Sicherheitsrisiken gewappnet sein. Sowohl Datenschutz (im Sinne des unberechtigten Zugriffs Dritter auf persönliche Daten) als auch Datensicherheit (im Sinne des Datenverlusts und/oder der Datenmanipulation) lösen bei ihnen ein latentes Gefühl des Unbehagens aus.

Größte Vorbehalte haben sie, wenn es um das eigene Geld geht, wie etwa bei Online-Bestellungen. Hier können sie die Risiken nur schwer abschätzen und sind sich unsicher, was sie in einem Betrugsfall unternehmen können. Um solche unangenehmen Situationen zu vermeiden, bestellen sie – wenn überhaupt – vorzugsweise nur bei Anbietern, die ihnen bereits persönlich empfohlen wurden. Vertrauenserweckend erscheint es ihnen, auf Rechnung oder Nachnahme zu bezahlen.

Privatsphäre ist den Ordnungsfordernden Internet-Laien sehr wichtig. Nur Verwandte und enge Freunde möchte man eingeweiht wissen bei dem, was man persönlich macht. Die Vorstellung, dass Details aus dem Privatleben an die Öffentlichkeit gelangen und für jedermann zugänglich sein könnten, ist ihnen unangenehm. Daher stellen sie nur sehr selten persönliche Daten wie Fotos, elektronische Dokumente oder persönliche Informationen ins Netz. Diese Abneigung zeigt sich auch in Vorbehalten gegenüber sozialen Netzwerken.

Internetferne Verunsicherte

Zwei Drittel von ihnen sind Offliner. Der Rest dieser Gruppe ist Gelegenheitsnutzer mit sehr geringem Internet-Wissen und nur geringen Berührungspunkten mit digitalen Medien im Alltag. Das Internet ist für sie eine fremde Welt, die verunsichernd und bedrohlich wirkt. Sie nutzen nur wenige Basisfunktionen und sind auf fremde Hilfe angewiesen.

Der Weg ins Netz wird als mühsam und weit empfunden. Konfrontiert mit intertypischen Abkürzungen und Zeichen fühlen sie sich einem Gerät ausgesetzt, das eine fremde Sprache spricht und ihr Anliegen nicht versteht. Das Internet erscheint ihnen als ein gänzlich fremder Kosmos.

Der persönliche Gewinn durch das Internet wird von ihnen kaum erkannt. Nach wie vor reichen ihnen Telefon, Brief und vor allem der persönliche Kontakt, um mit Mitmenschen zu kommunizieren. Auch Shopping-Angebote auf Ebay oder Amazon finden die Internetfernen Verunsicherten nicht attraktiv.

Nicht selten haben Internetferne Verunsicherte bereits schlechte Erfahrungen mit Computer oder Internet gemacht. Schrift und Symbole sind oft zu klein und es tauchen Wörter auf dem Bildschirm auf, von denen man gar nicht weiß, was sie bedeuten.

Da das Netz in ihrem Leben keinen großen Raum einnimmt, sind sie für die Themen Sicherheit und Datenschutz im Internet vergleichsweise wenig sensibilisiert. Hier dominieren andere Sorgen wie etwa soziale Gerechtigkeit und die Rentensicherheit. Wenn diese Gruppe jedoch an das Internet denkt, wird schnell die Scheu vor diesem Medium mit den Risiken des Datenmissbrauchs begründet. Der Argwohn gegenüber Sicherheit im Internet wird somit schnell zum zentralen Hemmfaktor, der ihre Ablehnung verstärkt.

Die primäre Perspektive ist Gefahr: Das Internet erscheint ihnen als Spielwiese für Verbrecher, Trickser und Betrüger. Entsprechend groß ist die Sorge, durch eigenes Verschulden Opfer von Datenmissbrauch zu werden. Allerdings hat man nur eine vage Vorstellung, was Datenmissbrauch bedeutet.

Da die Sicherheit im Internet in ihren Augen bisher nicht gegeben ist, fühlen sie sich größtenteils den Gefahren hilflos ausgesetzt. Deswegen wenden sie eine klare Vermeidungstaktik an. Sie hegen eine große Scheu, Daten aller Art im Internet preis zu geben. Am ehesten kann dieser Typus noch Institutionen oder Personen vertrauen, die man bereits lange kennt oder denen ein ehrenhafter und vertrauenswürdiger Ruf voraussetzt.



*Dr. Silke Borgstedt ist am Sinus-Institut
Direktorin für Sozialforschung.*

Jedoch ist für die Internetfernen Verunsicherten wenig relevant, ob Mitteilungen im Internet einen rechtsverbindlichen Charakter haben. Rechtsverbindliche Handlungen – und prinzipiell alle Tätigkeiten im Bereich Kauf und Verkauf – möchte man sowieso nicht ohne direkten Kontakt durchführen. Die klare Vermeidungstaktik gilt als sicherer Garant, Problemen auf diesem Feld aus dem Weg zu gehen. Vor diesem Hintergrund überwiegt hier fast schon ein prinzipieller Argwohn bei Aktivitäten im Internet. 84 Prozent halten persönliche Daten im Internet nicht für sicher.

Die Internetfernen Verunsicherten begegnen Personen, die ihr Privatleben ins Netz stellen, mit großem Unverständnis. Heute sind sie jedoch damit konfrontiert, dass ihre Enkel persönliche Angaben bei Facebook präsentieren. Zum Schutz der Jugend erwarten die Internetfernen Verunsicherten Altersgrenzen im Netz. Ferner sehen sie die Verantwortung bei den Eltern, ihre Kinder nicht den Risiken im Internet auszusetzen und sie durch klare Regeln und Verbote zu schützen.

Der lange Weg ins Internet

So lassen sich die digitalen Gräben (vielleicht) überwinden

Von Nicole Schmitt

Walter Kessler ist ein Digital Outsider. Einer von rund 27 Millionen Menschen in Deutschland, die das Internet nie oder kaum nutzen. Der 67-Jährige lebt in einer kleinen Zweizimmerwohnung im fränkischen Nürnberg. Auf dem Tisch in der hintersten Ecke des Wohnzimmers steht ein Computer.

„Wann ich den zuletzt benutzt habe? Lassen Sie mich mal überlegen...“ Dann antwortet der Rentner: „Ich glaube vor ein paar Tagen. Da habe ich eine E-Mail geschrieben. Das ist recht praktisch. Den Zugang hat mir mein Sohn eingerichtet. Ansonsten aber benutze ich das Ding kaum. Höchstens mal, um bei Google etwas nachzuschauen. Da spart man sich das Lexikon. Die Zeitung aber lese ich dann doch lieber in Papierform.“ Typische Aussagen eines typischen digitalen Außenseiters.

Angst, das Internet zu löschen

Beim Digital Outsider überwiegt eine distanzierte Einstellung gegenüber dem Internet. Immer wiederkehrende Medienberichte über Viren, Würmer und Trojaner, Phishing und Datenklau im Netz verstärken diese Haltung noch. Hinzu kommen Unkenntnis in der Handhabung und eine geringe Internet-Erfahrung. „Diese Menschen haben Angst, das Internet zu löschen, wenn sie die falsche Taste drücken“, kommen-

tiert DIVSI-Direktor Matthias Kammer den Gemütszustand der Digital Outsiders.

Die digitale Barriere – für einen digitalen Außenseiter scheint sie schier unüberwindbar. Besonders riskant im Auge des Digital Outsiders sind soziale Netzwerke wie Facebook, Twitter oder Stayfriends und auch das Online-Banking: „Ich vertraue bei einer Überweisung den Geräten in der Bank, wo ich das eintippen kann“, sagt Walter Kessler. „Da bekomme ich einen Beleg, der dort ausgedruckt wird und habe den Beweis, ich war an dem Tag um die Zeit in der Bank. Das ist mir lieber, als wenn ich zuhause am Rechner sitze.“

Rückgriff auf traditionelle Massenmedien

Unkenntnis generiert Unsicherheit. Die führt bei den digitalen Außenseitern zu immens großen Sicherheitsbedenken. Sie scheuen sich davor, überhaupt ins Netz zu gehen. Im Bereich der Erwachsenenbildung hat man sich diesem Problem angenommen. Volkshochschulkurse mit Titeln wie „Rund um PC & Internet“ und „Der PC – eine neue Herausforderung“ sind in Deutschland seit Jahren fest installiert.

Am Bildungszentrum (BZ) in Nürnberg, der größten kommunalen Weiterbildungseinrichtung Nordbayerns, wurde bereits 1997 ein eigener Fachbereich für Multimedia und Internet geschaffen. Aktuell bietet das Bildungszentrum 43 unterschiedliche Internet-Kurse an, von denen sich 18 an Digital Outsiders wenden: „Vor allem Seniorinnen und Senioren fühlen sich oftmals unsicher im Umgang mit dem Internet. Für diese Zielgruppe haben wir spezielle Kurse rund um das Thema Internet, die aufeinander aufbauen. Außerdem bieten wir gesonderte Kurse zum Thema Internet-Sicherheit an. Aufklärungskurse zum Thema Tauschbörsen und Musikdownload richten sich ebenfalls an diesen Personenkreis“, berichtet Barbara Müller vom BZ Nürnberg.

So weit, so gut. Nur für das Erreichen der Zielgruppe, die eben nicht oder nur kaum im Internet präsent ist, müsste man sich etwas überlegen. Das BZ wandte sich deshalb alt-hergebrachten Informationskanälen zu. Um das Kursangebot zu verbreiten, wird das konventionelle Programmheft in

gedruckter Version an öffentlichen Plätzen ausgelegt. Zusätzlich werden Flyer verteilt und Zeitungsanzeigen geschaltet.

Der Rückgriff auf traditionelle Massenmedien wie Zeitung, Radio und Fernsehen gibt demnach eine wertvolle Hilfestellung. So werden selbst diejenigen erreicht, die bisher nicht mittelbar an der Nutzung des Internets interessiert sind. Auch das Kompetenzzentrum Technik-Diversity-Chancengleichheit hat mit dieser Art der Zielgruppenansprache gute Erfahrungen gemacht. Für Geschäftsführerin Birgit Kampmann ist es unabdingbar, an der Erfahrungswelt der Menschen anzuknüpfen. „Die Leute sind am Anfang natürlich unsicher“, erläutert Kampmann. „Viele hatten früher keinen Büroberuf und somit auch keinen Computer. Der PC ist zunächst etwas völlig Neues.“

Umso wichtiger ist demnach, dass die digitalen Außenseiter unterstützend an das Medium Internet herangeführt werden: „Wenn ich zu meiner Bank gehe und die erklären mir, wie Online-Banking funktioniert, dann hat das für mich persönlich einen viel stärkeren Impuls“, so Kampmann weiter. „Worum es uns geht, ist die direkte Ansprache verbunden mit der direkten Unterstützung und dem daraus resultierenden direkten Nutzen.“

Digitale Integration mittels praktischer Maßnahmen

Unterstützung erfährt das Kompetenzzentrum Technik-Diversity-Chancengleichheit dabei von diversen Partnern. Das Bundesministerium für Wirtschaft und Technologie beispielsweise förderte bis vor Kurzem die Initiative „Internet erfahren – gemeinsam durchs Netz“. Ministeriumssprecher Stefan Rouenhoff resümiert: „Die beteiligten Partner der Initiative, die Bundesarbeitsgemeinschaft der Senioren-Organisationen, das Kompetenzzentrum Technik-Diversity-Chancengleichheit und die Stiftung Digitale Chancen haben mit Hilfe dieser Anschubfinanzierung vielfältige Maßnahmen durchgeführt und ein breites Aktionsnetz aufgebaut, um Interessierte an das Internet heranzuführen und bei der kompetenten Nutzung des Internets zu unterstützen.“

Im gesamten Bundesgebiet wurden Mitarbeiter der sozialen Arbeit und informellen Bildung dafür qualifiziert, Menschen an das Internet heranzuführen und sie mit der sicheren und verantwortungsbewussten Nutzung vertraut zu machen. Die Aktionsorte waren vielfältig: Seniorenwohnheime, Mehrgenerationenhäuser, Stadtbibliotheken, Vereine und Verbände – überall dort fanden Personalschulungen statt. Im Folgeschritt gaben diese nun qualifizierten Multiplikatoren ihr Wissen an ungeübte User weiter. Pflegebegleiter beispielsweise stattete man mit Laptops aus. So konnten sie den Angehörigen von Pflegebedürftigen ganz praktisch zeigen, wie ihnen das Internet das Leben erleichtert – sei es, dass Behördengänge online erledigt wurden oder man sich plötzlich ganz einfach über Behandlungsmöglichkeiten informieren konnte.

„Ich muss die Leute immer da erwischen, wo es ihnen wirklich hilft. Dann ist auch die technische Herausforderung nicht mehr das große Thema.“

„Das war ein unglaublich großer Erfolg“, erinnert sich Birgit Kampmann. „Das ist der entscheidende Punkt. Ich muss die Leute immer da erwischen, wo es ihnen wirklich hilft. Dann ist auch die technische Herausforderung nicht mehr das große Thema.“ Zwar endete die Finanzierung des Bundesministeriums Ende letzten Jahres. Aufgrund des großen Erfolges laufen die Projekte jedoch in Arbeitsgemeinschaften weiter – zumindest so lange es die finanziellen Mittel der Organisationen erlauben.



Nicole Schmitt ist Redakteurin und Videojournalistin. Seit 2001 arbeitet sie hauptberuflich für die Nachrichten- und Magazinformate von Sat.1 und N24 im Landesstudio Franken in Nürnberg. Daneben ist sie freiberuflich für diverse Fachverlage tätig. Um ihr Leistungsspektrum auszubauen, studierte die Journalistin in Münster Public Relations und absolvierte 2009 am Zentrum für Angewandte Kommunikation der Universität Münster die Prüfung zur PR-Managerin. Seitdem ist sie neben ihrer Haupttätigkeit als Redakteurin auch als freie PR-Beraterin für mittelständische Unternehmen tätig. Ihre thematischen Schwerpunkte sind: Politik & Gesellschaft, Schule & Bildung sowie Internet & Social Networking.

Neue Vorhaben sind schon in Planung: „Wir sitzen an einem Konzept zu einer Studie, wie sinnvoll Tablet-PCs eingesetzt werden können“, erzählt Kampmann. Sie fordert, die Technikbildung und das lebenslange Lernen stärker in den Fokus der Gesellschaft zu rücken. „Es ist dringend erforderlich, dass ein Umdenken stattfindet. Wir müssen bereit sein, die digitalen Außenseiter zu integrieren. Wir müssen sie mitnehmen.“ Derzeit aber mangle es in Deutschland noch an ausreichenden Konzepten und eben auch am nötigen Geld für langfristige Maßnahmen.

Anonymität als Dilemma

Freie Internet-Nutzung erfordert Schutz für die Schwächeren

Von Prof. Dr. Dirk Heckmann

In seiner Osterbotschaft 2012 kritisierte der Vorsitzende der deutschen Bischofskonferenz, Erzbischof Robert Zollitsch, die Gefahren des Internets, das wie die Sucht nach Alkohol, Medikamenten oder Drogen zu den „verklavenden Götzen unserer Zeit“ zähle. Zitat: „Es muss uns nachdenklich stimmen, wenn manche Zeitgenossen im Schutz der Anonymität Meinungsfreiheit im Internet als Freibrief für Hetze, Diffamierung und Mobbing missverstehen.“

Gemeint sind damit Fälle des sogenannten Cybermobbing, also Beleidigungen, Verleumdungen und Stalking im Internet. Es geht also um Straftaten jenseits der Fälle erlaubter Meinungsäußerung. Cybermobbing hat nicht nur eine große praktische und gesellschaftliche Relevanz. Es ist geradezu – leider – Alltag, auch und besonders im Internet mit seiner interaktiven Ausprägung des Web 2.0.

Inwieweit hier die Anonymität der Internet-Nutzung eine Schlüsselrolle spielt, ist noch nicht ganz geklärt. Es gibt noch zu wenige, wissenschaftlich vertiefte empirische Erkenntnisse, insbesondere zur Frage der Enthemmung und Senkung der Hemmschwellen durch Verbergung der Identität. Die erste groß angelegte Studie durch die Universität Hohenheim startete erst in diesem Jahr. Die im März 2012 veröffentlichte Sinus Milieu-Studie des Deutschen Instituts für Vertrauen und Sicherheit im Internet befasst sich nur mittelbar mit diesem Thema.

aber davon ausgehen, dass es nicht wenige Fälle gibt, in denen die zumindest vermeintliche Anonymität tatentschlussfördernd ist. Die Schaffung einer IT-Infrastruktur mit ihren technischen, sozialen und rechtlichen Bedingungen zum Schutz der Anonymität ist zumindest mitursächlich für diese Form der Alltagskriminalität. Allemal spielt die Wirkung einer erschwerten Strafverfolgung bei Zulassung von Anonymität eine wichtige Rolle.

Dilemma einer anonymen Internet-Nutzung

Wenn man genau hinsieht, dann befindet sich der Staat, insbesondere der Gesetzgeber, in einem Dilemma. Egal wie viel oder wie wenig er die Internet-Nutzung im Hinblick auf die Zurechenbarkeit des Nutzerverhaltens regelt: Er kann eigentlich nur verlieren. Gewährleistet er die Anonymität der Internet-Nutzung, verletzt er möglicherweise die Pflicht zum Schutz der Bürger vor kriminellen Übergriffen. Sorgt er hingegen für wirksame Kontrollmechanismen, dann verletzt er möglicherweise das Grundrecht auf Anonymität.

Die Möglichkeit zu anonymem Handeln (nicht nur, aber auch im Internet) gehört zur grundrechtlich geschützten Persönlichkeitsentfaltung und ist Teil informationeller Selbstbestimmung, Meinungsfreiheit und Gewährleistung von Privatheit. Das Grundrecht auf Anonymität kann hergeleitet werden aus Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 sowie Art. 5 Abs. 1, 10 und 13 GG. Dieses korrespondiert mit der informationellen Selbstbestimmung, wonach jeder selbst entscheidet, wer erfährt, welches Handeln von ihm stammt.

Auch für das Grundrecht auf Anonymität gibt es – wie für jedes andere Grundrecht – verfassungsrechtliche Schranken. Das zeigen besonders Art. 2 Abs. 1 GG, wo von den Rechten Dritter die Rede ist, und Art. 5 Abs. 2 GG, der das Recht der persönlichen Ehre betont. So wird Anonymität beschränkt durch die Schutzpflicht des Staates, für die Zurechenbarkeit menschlichen Handelns zu sorgen, wenn dies zum Schutz höherrangiger Schutzgüter erforderlich und verhältnismäßig ist. Auch in seiner Ausprägung als Recht auf anonymes Handeln berechtigt das Recht zur freien Entfaltung der Persönlichkeit nicht dazu, andere Menschen zu beleidigen, zu verleumden oder anderweitig zu verletzen. Im Gegenteil: Wenn und soweit Anonymität solchen Rechtsverletzungen Vorschub leistet oder ihre Verhinderung bzw. Verfolgung erschwert, bedarf es staatlicher Schutzmaßnahmen.

Und genau hier besteht das Dilemma, dass Schutzmaßnahmen, die zur Identifizierung von Personen führen, das Prinzip anonymer Internet-Nutzung konterkarieren. Es kann keine Anonymität geben, die nur die Guten schützt. Behält man sich selbst eine nachträgliche Identifizierung vor, entstehen automatisch Schutzlücken. Das Dilemma ist bereits im Recht angelegt.

Internet-Kriminalität als Spiegelbild unserer Gesellschaft

Letztlich sind Schutzgutverletzungen, die unter dem Deckmantel anonymer Internet-Nutzung geschehen, auch ein Spiegelbild unserer Gesellschaft. Rücksichtslosigkeit und Egoismus äußern sich täglich in unterschiedlichen Kontexten, nicht nur im Internet. Eine freiheitliche Gesellschaft muss lernen, damit umzugehen.

Als durch das Grundgesetz freiheitlich konzipierte und ebenso denkende und handelnde Gesellschaft lassen wir täglich eine Vielzahl von Rechtsverletzungen, Gefährdungen und Risiken zu – und zwar für alle Rechtsgüter (Leben, Gesundheit, Eigentum, persönliche Ehre etc.): in komplexen Infrastrukturen wie dem Straßenverkehr oder der Lebensmittelversorgung, aber auch bei technischen Anlagen.

Diese Risiken werden nicht per se gutgeheißen, aber eben doch nicht mit allen denkbaren Mitteln „um jeden Preis“ bekämpft. Denn sonst hätten wir Tempo 80 auf den Autobahnen, eine Vervielfachung der Verkehrskontrollen, permanente Hygienekontrollen, dazu Betriebsverbote für viele technische Anlagen. Dass dies nicht geschieht, liegt keineswegs an den fehlenden Ressourcen staatlicher Kontrollinstanzen, sondern vielmehr an der Grundeinstellung, Freiheit und Sicherheit in eine verträgliche Balance zu bringen.

Soweit aber staatliche Gefahrenvorsorge und Kriminalitätsbekämpfung per Mausclick mit überschaubarem Aufwand möglich erscheinen, wird schnell vergessen, dass solch eine Sicherheitsverwaltung mit einer erheblichen, in anderen Fällen nicht gewollten Einschränkung grundrechtlich verbürgter Freiheit einhergeht.

Was auch leicht übersehen wird: Bei der Güterabwägung sind neben den individuellen Schutzpositionen auch schädliche Neben- und Fernwirkungen einer umfassenden Speicherung von Zurechnungsdaten zu berücksichtigen. Das in technischen Innovationen enthaltene permanente Überwachungs- und Kontrollpotenzial muss vor dem Hintergrund des Persönlichkeits- und Privatsphärenschutzes kritisch hinterfragt werden; ein abstrakter Sicherheitszugewinn rechtfertigt keine konkreten Freiheitsbeschränkungen.

Was aber sind die Alternativen? Was sagen wir den Opfern jener Freiheitsverwirklichung wie Cybermobbing, die nur unvollkommen unterbunden werden, wenn man die technischen Kontrollmöglichkeiten nicht ausschöpft? Man kann nicht einerseits eine freie Internet-Nutzung fordern, und andererseits die Opfer des Missbrauchs solcher Freiheit gewissermaßen als „Kollateralschaden“ schutz- und hilflos zurücklassen.

Anonymitätsfolgenausgleich als Lösung?

Was wir brauchen, ist eine Art Anonymitätsfolgenausgleich. Und das ist etwas ganz anderes als die plumpe Aufhebung der Anonymität, denn die bringt uns nur zurück ins Dilemma. Wenn eine Gesellschaft die Freiheit der Internet-Nutzung in den Vordergrund stellt und damit missbilligend, aber eben doch in Kauf nimmt, dass es Fälle des Mobbing etc. gibt, dann muss sie für einen Ausgleich sorgen. An dieser Stelle können die Eckpunkte einer solchen Kompensation nur skizziert werden. Ohne Anspruch auf Vollständigkeit seien genannt:

- *Stärkung des Gedankens von Fairness, Rücksichtnahme und Verantwortung durch konzertierte Aktionen, nicht zuletzt in den Schulen und im Internet selbst*
- *Vermittlung von adäquaten Hilfsangeboten*
- *Stärkung des Selbstschutzes, auch und besonders in Form von "Medienkompetenz"*
- *Stärkung der Wächterfunktion der (Internet-)Gemeinschaft, besonders durch Solidarisierung mit Opfern*
- *Gezielte Hilfsangebote durch Erweiterung und Übertragung der Mittel des klassischen Opferschutzes*
- *Hilfe durch korrigierendes Verhalten der Provider*
- *Entwicklung vertrauenswürdiger Umgebungen im Internet*
- *Schaffung von Ombudsleuten bei kritischen Internet-Diensten*

Auf diese Weise braucht anonyme Internet-Nutzung nicht generell in Frage gestellt werden. Deren Vorteile, besonders im Hinblick auf Meinungsfreiheit und Persönlichkeitsschutz, bleiben aufrechterhalten.



Prof. Dr. Dirk Heckmann studierte an der Universität Trier von 1978 bis 1983 Rechtswissenschaften. Nach seiner mit dem Carl-von-Rotteck-Preis ausgezeichneten Promotion (1991) an der rechtswissenschaftlichen Fakultät der Universität Freiburg und seiner Habilitation im Jahr 1995 erhielt er einen Ruf an die Universität Passau. Seit dem Sommersemester 1996 ist Heckmann dort ordentlicher Professor für Öffentliches Recht, Sicherheitsrecht und Internetrecht; seit 2009 lehrt er auch an der Zeppelin Universität Friedrichshafen. 2003 wählte ihn der Bayerische Landtag zum nebenamtlichen Richter am Bayerischen Verfassungsgerichtshof. Seit 2005 leitet Prof. Heckmann die Forschungsstelle für Rechtsfragen der Hochschul- und Verwaltungsmodernisierung, die 2011 in Forschungsstelle für IT-Recht und Netzpolitik umbenannt wurde. Seit 2006 ist er auch stellvertretender Sprecher des Instituts für IT-Sicherheit und Sicherheitsrecht. 2007 wurde der Internet-Rechtler in den Vorstand der Deutschen Gesellschaft für Recht und Informatik, 2010 in den Vorstand des Deutschen EDV-Gerichtstag e.V. gewählt. Als Sachverständiger wirkt Heckmann seit 2007 auf dem Nationalen IT-Gipfel der Bundesregierung und seit 2010 im CSU-Netzrat.



Sascha Lobo und die DIVSI Milieu-Studie

Gemeinsamkeiten entdeckt



Joanna Schmölz studierte Medienkultur und Politische Wissenschaft an der Universität Hamburg und arbeitete zeitweise als freie Journalistin. Seit 1998 ist sie in der IT-Branche tätig. In der Stabsstelle Vorstand eines länderübergreifenden öffentlich-rechtlichen IT-Dienstleisters in Norddeutschland leitete sie das Vorstandsbüro und war zuletzt Referentin Strategisches Marketing. Im November 2011 kam Schmölz zum DIVSI. Sie verantwortet dort das Wissensmanagement. Aktuell leitet sie das an die kürzlich veröffentlichte "DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet" anknüpfende Folgeprojekt, in dem Entscheider, Meinungsbildner und Multiplikatoren in einer repräsentativen, wissenschaftlichen Studie befragt werden.

Von Internet-People und InterNOT-People

Von Joanna Schmölz

Blogger, Aktivisten und Forscher trafen sich bei der re:publica in Berlin. Thema dieses zentralen Jahres-Events der Netzgemeinde: die Schubkraft sozialer Medien für politische Bewegungen. Einer der Hauptredner bei der Internet-Konferenz war Sascha Lobo, für viele eine Art Guru des Netzes. Er bezog Stellung zum Stand des Internet im Jahr 2012.

Grundsätzlich unterscheidet Lobo zwischen Internet-People und InterNOT-People. Er sieht in diesem Auseinanderklaffen eine Gefahr: „Wir müssen dieses Problem erkennen und lösen.“ Es gehe darum, die 30 Millionen Menschen, die nicht ins Internet gehen, und jene, die glauben, sie würden ins Internet gehen, nicht aus dem Blickfeld zu verlieren.

Gleichzeitig präsentierte Lobo bei der re:publica dazu seine speziellen Thesen:

- * *Das Urheberrecht interessiert deine Mutter. Nicht. Das größte Problem sind die 30 Millionen Nicht-Internet-Nutzer, die bei politischen Entscheidungen zum Thema Internet (ACTA, Internetsperren etc.) auch abstimmen und deren Stimmen entscheidend sein können.*
- * *Wir müssen einen Weg finden, dauerhaft mit diesen 30 Millionen Nicht-Internet-Nutzern klarzukommen. Es existieren im öffentlichen Diskurs negative Narrative über das Internet, die zwar nicht unbedingt wahr, aber auch nicht vom Einzelnen überprüfbar sind (zum Beispiel „Internet-Surfen verkürzt die Aufmerksamkeitsspanne“ oder „Klarnamen garantieren Wohlverhalten im Social Web“).*
- * *Wir brauchen neue, positive Narrative, die aus der Internet-Szene kommen müssen, um sie den Negativ-Narrativen in der Öffentlichkeit entgegenzusetzen.*

Beobachter der re:publica stellten fest, dass Sascha Lobo offenbar Handlungsempfehlungen aufgenommen hat, die sich durchaus aus der „DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet“ ableiten lassen. So geht es auch ihm darum, dass die Internet-People überlegen sollten, wie sich der „digitale Graben zuschütten“ lässt. Lobo mit Blick auf die InterNOT-People: „Wir müssen das nächste Projekt für diese Menschen denken.“

Dabei scheint die DIVSI-Studie bereits einen Schritt weiter zu sein. Lobo skizziert nur einen Graben: zwischen Internet- und InterNOT-People (bei DIVSI sind das die „Digital Natives“ und die „Digital Outsiders“). Die Studie dagegen macht zusätzlich einen zweiten Graben aus. Demnach liegt eine trennende Problematik darin, dass die Digital Natives das Internet als alltäglichen Lebensraum begreifen und nicht nachempfinden können, dass sich Andere im Internet nicht ebenso zuhause fühlen.

Allerdings deutet auch Sascha Lobo in seinem Vortrag diese Problematik an: „90 Prozent der Themen, die die Netzgemeinde interessieren, interessieren die Leute da draußen nicht die Bohne.“ Das Problem liege darin, dass Menschen, die das Internet gar nicht nutzen, entscheidend sein werden – politisch und demokratisch.

Zu der Gruppe der Nicht-Nutzer zählt Lobo auch Menschen, die in der DIVSI-Studie als „Digital Immigrants“ eingestuft werden. Menschen also, die das Netz ganz gezielt nur dann verwenden, wenn sie sich einen direkten Vorteil davon versprechen. Etwa beim Shopping oder beim Buchen einer Reise. Lobo: „Das sind Leute, die glauben, sie würden ins Internet gehen.“

Wichtig sei nun die Lösung der Frage, wie und wann man in den Diskurs einsteigen solle. 2012 sei allerdings noch nicht so entscheidend und ein Vorgeplänkel. Lobo: „2013 wird es wichtig.“

Deutschlands prominentester Digital Outsider?

Der Altkanzler und das Netz

„Ich habe immer die briefliche Schriftform bevorzugt“

Die Facebook-Seite »Helmut Schmidt« gefällt mehr als 40.000 Mitgliedern des Sozialen Netzwerks. Der Altkanzler hat sie sich allerdings noch nie auch nur zeigen lassen. Das erklärte er in einem Gespräch mit ZEIT-Chefredakteur Giovanni di Lorenzo. Im ZEITmagazin beantwortete Helmut Schmidt Fragen rund ums Internet. Auszüge aus dem Interview.

Allgemein zum Internet:

„Drei Dinge fallen mir dazu ein. Erstens: Das Internet gehört kaum zu meiner Welt. Zweitens: Ich empfinde es als bedrohlich. Und drittens: Es hat Zukunft.“

Stichwort „bedrohlich“:

„Das Bedrohliche ist der Umstand, dass die elektronischen Medien, die sich ja ständig weiterentwickeln, eine tiefgreifende kulturelle Veränderung mit sich bringen. Das betrifft nicht nur die westliche Kultur, sondern auch andere Kulturen auf der ganzen Welt. Wenn Sie zum Beispiel im Mittleren Osten oder im Maghreb, in Tunesien, Algerien, Ägypten oder Libyen junge Leute mit einem Handy ausstatten, dann wird das im Laufe einer einzigen Generation dazu führen, dass die Frauen sich nicht mehr zwangsverheiraten lassen und die Mädchen nicht mehr beschnitten werden. Das gilt jedenfalls für die Städte; in den Dörfern liefere dieser Prozess vermutlich langsamer ab.“

Positiv, negativ:

„Unbestreitbar führt das Internet auch zu positiven Veränderungen. Das Negative besteht meiner Meinung nach darin, dass das Internet zu Oberfläch-

lichkeit verleitet, zu spontanen Reaktionen, hinter denen kein langes Nachdenken steckt: Ich habe etwas gelesen, und sofort twitterte ich dagegen oder darüber, und dann womöglich auch noch in falscher Grammatik. Die elektronischen Medien führen unter anderem dazu, dass die Qualität der Mitteilung abnimmt.“



Kommunikationsstil im Netz:

„Er wird sich zwangsläufig weiterentwickeln.“

In welche Richtung?

„Die Kommunikation im Internet wird sowohl kultivierter als auch noch oberflächlicher werden.“

Handy

„Ich habe kein Handy, und wenn ich eins hätte, würde ich es nicht benutzen. Ich telefoniere überhaupt nur noch selten. Wahrscheinlich habe ich das auch früher nie wirklich gern getan. Ich habe immer die Schriftform bevorzugt, und zwar die briefliche Schriftform.“

Geheimnisverrat und Vertrauensbruch

Eine Gesellschaft ohne Diskretion, Loyalität und Geheimnisse wäre eine andere Gesellschaft

Von Dr. Göttrik Wewer



Dr. Göttrik Wewer studierte Politikwissenschaft, Soziologie, Volkswirtschaftslehre, Öffentliches Recht und Neuere Geschichte in Braunschweig und Hamburg. Anschließend Tätigkeiten an der Universität Hamburg und als Geschäftsführer der Deutschen Vereinigung für Politische Wissenschaft (DVPW) und ab 1991 in der öffentlichen Verwaltung, u.a. in der Staatskanzlei des Landes Schleswig-Holstein und als Direktor der dortigen Verwaltungsfachhochschule. Von 2001 bis 2003 Staatssekretär im niedersächsischen Kultusministerium und von 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 Vice President E-Government bei der Deutsche Post Consult GmbH.

Vertrauen aufzubauen, ist nicht so einfach. Das gilt schon in der realen Welt, aber erst recht in der virtuellen Welt. Denn da können wir nicht immer sicher sein, dass derjenige, mit dem wir kommunizieren, auch wirklich der ist, für den er sich ausgibt. Wir kennen ihn nicht und wir sehen ihn nicht von Angesicht zu Angesicht. Wir wissen nicht, ob er gute oder böse Absichten hat. Leute, denen wir persönlich begegnen, können wir versuchen einzuschätzen: Macht die Person einen seriösen Eindruck, wie redet sie, wie benimmt sie sich?

Natürlich kann man sich dabei irren. Wenn Mörder wie Mörder aussehen würden und Betrüger wie Betrüger, dann wäre vieles leichter. Aber im Internet haben wir noch weitaus weniger Anhaltspunkte. Im Rechner sehen wir nur bestimmte Abfolgen von Buchstaben und Zahlen und selbst Fotos müssen nicht bedeuten, dass der andere, mit dem ich mich verabrede, wirklich so aussieht.

Noch aus einem zweiten Grund ist es im Internet noch schwieriger als im täglichen Leben, Vertrauen aufzubauen: weil es noch so neu ist und weil es sich ständig rasant verändert. Viele Firmen, die inzwischen alle kennen, sind erst wenige Jahre alt. Viele Angebote gibt es erst seit ein paar Jahren oder Monaten. Und ständig kommen neue Angebote hinzu. Uns fehlt also die Erfahrung, ob man diesen Anbietern wirklich vertrauen kann. Nicht nur uns selbst, sondern auch unseren Freunden und Bekannten.

Was Facebook, Google & Co. am Ende des Tages mit unseren Daten alles machen, wissen wir heute noch nicht. „Die Menschen müssen darauf vertrauen dürfen, dass die Technologie ihnen nutzt“, heißt es in der zweiten von sieben Thesen, auf deren Grundlage das Deutsche Institut für Vertrauen und Sicherheit im Internet (DIVSI) arbeitet. Dazu gehört auch die Erwartung, dass vertraulich bleibt, was vertraulich bleiben soll.

Wir alle haben unsere größeren und kleineren Geheimnisse, von denen wir nicht möchten, dass andere sie erfahren. Das gilt für den einzelnen Menschen, für soziale Beziehungen, für Organisationen und für Institutionen, für Unternehmen wie für Ministerien. Die Welt ist voller Geheimnisse und noch immer voller Rätsel. Bei Geheimnissen handelt es sich um sensible Informationen, die für andere durchaus von Interesse sein könnten, die ihnen aber nicht bekannt sind.

Wenn Menschen, denen wir ein Geheimnis anvertraut haben, dieses verraten, dann können wir ihnen die Freundschaft kündigen oder die Scheidung einreichen. Wer Betriebsinterna ausplaudert oder Staatsgeheimnisse verrät, muss mit härteren Strafen rechnen. Unter das Betriebsgeheimnis fallen technische Aspekte der Produktion, unter das Geschäftsgeheimnis kaufmännische Aspekte. Beim Verrat von Geschäfts- und Betriebsgeheimnissen droht eine Freiheitsstrafe bis zu drei Jahren oder eine Geldstrafe, in besonders schweren Fällen sogar eine Freiheitsstrafe bis zu fünf Jahren. Verrat ist ein besonders schwerer Vertrauensbruch, der die angenommene Loyalität verletzt.

Für staatliche Geheimnisse gibt es unterschiedliche Geheimhaltungsstufen. Über das „normale“ Amts- und Dienstgeheimnis hinaus – dass man nicht mit Dritten über dienstliche Angelegenheiten redet – sind das die Stufen: Vertraulich, Geheim, Streng Geheim („Verschlussache – Nur für den Dienstgebrauch“). Wer solche Geheimnisse offenbart, muss ebenfalls mit Strafe rechnen. Die Aufgabe des strafrechtlichen Staatsschutzes (§§ 80 – 92 b StGB) besteht darin, den Bestand des Staates, seine Sicherheit und die verfassungsmäßige Ordnung zu schützen. Dabei unterscheidet man traditionell zwischen Hochverrat und Landesverrat: Hochverrat meint alle Straftaten, die sich gegen den inneren Bestand des Staates, also gegen die Staatsverfassung, die Staatsgewalt oder das Staatsoberhaupt richten, während Landesverrat alle kriegerischen und nichtkriegerischen Handlungen umfasst, die die äußere Sicherheit des Staates berühren.

Dass Verrat sich nicht gehört und geahndet werden muss, war bisher nicht strittig. Sonst gäbe es die Gesetze ja nicht, die Geheimnisse schützen sollen. Dass Unternehmen ihre Planungen, Entwicklungen und Innovationen schützen, und auch der Staat gewisse Informationen vertraulich behandelt, liegt eigentlich auf der Hand. Ohne den Informanten Vertraulichkeit zuzusichern, würde er bestimmte Informationen gar nicht erst bekommen. Ohne vertrauliche Gespräche, diskrete Sondierungen und verdeckte „back channels“ – zwischen West und Ost, zwischen Palästinensern und Israelis, zwischen NATO und Taliban – würden weder Politik noch Diplomatie funktionieren. Offenheit ist die Schwester der Vertraulichkeit. Und dass jeder von uns das eine oder andere private Geheimnis mit sich herumträgt, ist eigentlich auch bekannt: Der Mensch braucht, wenn er Mensch bleiben will, eine gewisse Privatsphäre, in die er sich zurückziehen kann. Hier kann er seinen Gefühlen – wie Angst, Scham oder Ärger – freien Lauf lassen, ohne sich rechtfertigen zu müssen. Hier kann er seine Bedürfnisse ausleben. Zur Würde des Menschen gehört das Recht, frei darüber befinden zu können, ob und wie er in der Öffentlichkeit stattfinden will.

Inzwischen wird offensiv dafür geworben, Staatsgeheimnisse und Betriebsinterna auszuplaudern. Julian Assange, der Gründer von WikiLeaks, versteht seine Plattform als eine soziale Bewegung zur Aufdeckung von Geheimnissen, bevorzugt von Regierungen, von westlichen Regierungen, aber auch von Unternehmen. „Kollateralschäden“, also Gefahren für Leib und Leben betroffener Menschen, werden bei dem Streben nach totaler Transparenz in Kauf genommen.

Daniel Domscheit-Berg, Mitbegründer von WikiLeaks, aber dann im Streit geschieden und jetzt auf dem Weg, eine ähnliche Plattform („OpenLeaks“) aufzubauen, gesteht Individuen ein Recht auf Geheimnisse zu, nicht aber Firmen, Militärs und Regierungen. Diese würden Macht ausüben und deshalb müsse man sie anders betrachten. Hier werde „Geheimnisverrat zur Notwendigkeit“. Was „schlechte“ und was „gute“ Geheimnisse sind, soll offenbar jeder für sich selbst festlegen und nicht etwa an klaren Kriterien orientiert, gesetzlich geregelt oder demokratisch entschieden werden. Dass der Einzelne, wenn er sich nicht auf Recht und Gesetz berufen kann, auch das volle Risiko seiner Handlungen trägt, ist hoffentlich jedem klar. Immerhin plädiert er für „stärkere Gesetze“, um jene Geheimnisverräter, die Whistleblower, „vor Repressalien zu schützen“.

Das wollen auch die Piraten. Auch sie sehen im Whistleblowing eine Form von Zivilcourage, die unbedingt unterstützt und geschützt werden müsse. In diesem Sinne wenden sie sich gegen eine Einteilung in gute und in schlechte Geheimnisverräter und plädieren für einen „generellen und umfassenden Schutz für Whistleblower mit notwendigen Ausnahmen“ – was immer das heißen mag.

Früher gab es im Einzelfall ein gewisses Verständnis, bestimmte Interna öffentlich gemacht zu haben („Pentagon-Papiere“, Watergate), aber keine generelle

Befürwortung von Indiskretionen, Illoyalität und Verrat. In jenen Fällen handelte es sich um eine bewusste Irreführung der Öffentlichkeit durch Amtsträger oder eindeutig um Machtmissbrauch. Für Illoyalität und Verrat gab es jedenfalls bisher – jenseits strafrechtlicher Normen – hohe moralische Hürden.

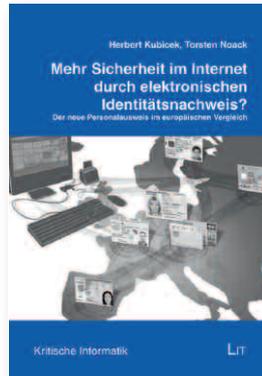
Eine Gesellschaft ohne Diskretion, Loyalität und Geheimnisse wäre eine andere Gesellschaft. Während die Piraten die Privatsphäre des Menschen noch verteidigen und nur für den Staat eine nahezu totale Transparenz wollen („Akteneinsicht für jedermann“), sind andere da schon weiter. „The age of privacy is over“, verkündet zum Beispiel kurz und bündig Facebook-Gründer Mark Zuckerberg. Es lohne sich nicht, die Privatsphäre zu verteidigen, schreibt der Blogger Christian Heller, denn dieser Kampf sei längst verloren.

Dass die Wortführer dieser Bewegung alles daran setzen, sich selbst möglichst wenig in die Karten gucken zu lassen, und dass Gruppierungen wie WikiLeaks oder Anonymus ihre eigenen Anhänger sicher nicht zu Indiskretionen, Illoyalität und Verrat aufrufen, obwohl sie gewiss auch Macht ausüben, gehört zur Ironie der Geschichte. Man meint, man gehöre zu den Guten. Und für die gilt natürlich nicht, was man von den anderen fordert.

Eine „Kultur des Misstrauens“, weil man stets damit rechnen muss, dass alles, was man sagt, schreibt und macht, öffentlich gemacht wird, wäre nicht geeignet, im digitalen Zeitalter Vertrauen und Sicherheit zu fördern. Und wer das „Ende der Privatheit“ und damit aller Geheimnisse als unausweichlich darstellt, versucht sich im Grunde einer öffentlichen Diskussion und demokratischer Entscheidung zu entziehen. Diesen Gefallen sollten wir ihm nicht tun.

Es bleibt dabei: „Verrat ist Vertrauensbruch“ (Margret Boveri).

Aktuelle Bücher

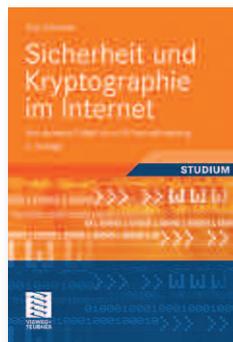


Mehr Sicherheit im Internet durch elektronischen Identitätsnachweis? Der neue Personalausweis im europäischen Vergleich

Autoren: Herbert Kubicek, Torsten Noack
Über Sinn und Zweck, Chancen und Risiken sowie Akzeptanz des elektronischen Identitätsnachweises auf dem neuen deutschen Personalausweis wird heftig diskutiert. Dieses Buch liefert empirische Befunde aus einem Vergleich mit nationalen Identity-Management-Systemen in sieben anderen europäischen Ländern.

Die Studie kommt zu überraschenden Ergebnissen: Alle bereits eingeführten und analysierten Systeme erreichen trotz erheblicher Unterschiede in Inhalt und Form nicht das Ziel, durch eine sicherere Authentisierung die Sicherheitsbedenken der Nutzer bei Online-Transaktionen zu zerstreuen und damit deren Anteil am E-Government zu steigern. Dem neuen Personalausweis dürfte dies kaum besser gelingen.

Lit Verlag, ISBN-10: 3643109164, ISBN-13: 9783643109163, Preis: 29,90 Euro



Sicherheit und Kryptographie im Internet

Von sicherer E-Mail bis zu IP-Verschlüsselung

Autor: Jörg Schwenk

Eine strukturierte, gut lesbare Einführung in das dynamische Thema Internet-Sicherheit. Ausgehend von den bekannten Diensten E-Mail und WWW wird der Leser stufenweise tiefer in die Welt des Internets eingeführt. Besonderen Wert legt das Buch auf die Darstellung, wie bekannte kryptographische Verfahren an die jeweiligen

Erfordernisse der Internet-Dienste angepasst wurden. Der Text wurde für die dritte Auflage umfassend überarbeitet. Neu hinzugekommen sind insbesondere der Bleichenbacher-Angriff auf den SSL-Handshake, eine Beschreibung von IKEv2, die neue DNSSEC-Terminologie und SAML als neuer, wichtiger Standard im Bereich Webservices.

Verlag Vieweg+Teubner, ISBN-10: 3834808148, ISBN-13: 9783834808141, Preis: 29,95 Euro



Die Internetfalle

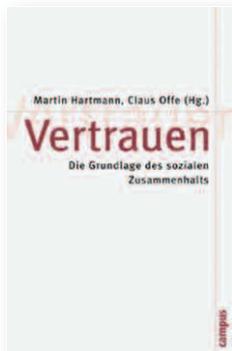
Google+, Facebook, Staatstrojaner – Was Sie für Ihren sicheren Umgang mit dem Netz wissen müssen

Autor: Thomas R. Köhler

Mehr als 40 Millionen Menschen nutzen allein in Deutschland soziale Netzwerke wie Facebook, Google+ oder XING im Internet. Dabei sind die meisten Dienstangebote im Netz nur vermeintlich kostenlos. Der Nutzer zahlt mit der Preisgabe persönlicher Daten – mit teils

erschreckenden Folgen für Privatleben und Beruf. „Die Internetfalle“ liefert einen Blick hinter die Kulissen der Webwirtschaft. Konkrete Tipps für den Umgang mit den eigenen Daten im Internet helfen nicht nur, Risiken zu beherrschen und typische Fallen zu vermeiden, sondern auch, Chancen zu erkennen und für sich zu nutzen. Erfahren Sie alles über die Chancen, aber auch Gefahren von Internet und Sozialen Netzwerken. Vollständig überarbeitete und erweiterte Neuauflage des ersten Buches zum Thema Datenspuren im Internet.

Frankfurter Allgemeine Buch, ISBN-10: 3899812808, ISBN-13: 9783899812800, Preis: 19,90 Euro



Vertrauen

Die Grundlage des sozialen Zusammenhalts

Herausgeber: Martin Hartmann, Claus Offe

Was ist Vertrauen? Wie entsteht es und wie schlägt es in Misstrauen um? Gibt es ein moralisch fragwürdiges Vertrauen oder ist Vertrauen immer gut? Die Texte dieses Bandes ermöglichen aus philosophischer, soziologischer und politikwissenschaftlicher Sicht den Einstieg in ein unübersichtliches Diskussionsfeld, das darauf verweist, mit welchen labilen Voraussetzungen es politische Regime zu tun haben, die den Namen der „Demokratie“ beanspruchen. Eine Beschäftigung mit den Voraussetzungen einer intakten demokratischen Kultur muss Vertrauen zum Thema haben.

Campus Verlag, ISBN-10: 3593367351, ISBN-13: 9783593367354, Preis: 29,90 Euro



Anonym im Netz

Wie Sie sich und Ihre Daten schützen

Autor: Jens Kubiexiel

Anonyme Kommunikation ist im täglichen Leben Normalität: Wer ein Buch in der Buchhandlung kauft, muss nicht seine Anschrift hinterlegen. Auch ein Gespräch an der Bushaltestelle setzt nicht voraus, dass Sie den Personalausweis vorzeigen. Im Internet hingegen haben Sie kaum noch Kontrolle über Ihre persönlichen Daten. Aufzeichnung und langfristige Speicherung Ihres Online-Verhaltens bis hin zur Erstellung von Persönlichkeitsprofilen sind an der Tagesordnung. Abhilfe schaffen nur Anonymisierungswerkzeuge für Browser, E-Mail, Chat und andere Dienste. In diesem Buch wird verständlich gezeigt, welche frei verfügbaren Lösungen es zum Schutz persönlicher Daten gibt und wie Sie diese einsetzen. Der Einstieg erfolgt mit einfachen Anwendungen,

die Sie als eigene Programme oder Erweiterung Ihres Lieblingsbrowsers nutzen, um anonym im Internet zu surfen.

Verlag Open Source Press, 2. Auflage, ISBN 978-3-937514-95-6, Preis: 19,90 Euro

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)

Öffentlichkeitsarbeit:

Till Martin Ritter
Mittelweg 142
20148 Hamburg
E-Mail: presse@divsi.de

Autoren:

Dr. Johann Bizer, Dr. Silke Borgstedt, Prof. Dr. Dirk Heckmann, Thomas Jarzombek, Matthias Kammer, Lars Klingbeil, Dr. Konstantin von Notz, Frank Pörschmann, Gerold Reichenbach, Jörn Riedel, Nicole Schmitt, Joanna Schmölz, Horst Westerfeld, Dr. Göttrik Wewer, Dr. Marianne Wulff

Realisation:

PubliKom Kommunikationsberatung
GmbH, Hamburg

Bildnachweis:

dpa, CSM Stock, private Archive, BfDI

Verbreitete Auflage:

ca. 7.500 Exemplare
Abgabe kostenlos



www.divsi.de