Deutsches Institut für Vertrauen und Sicherheit im Internet

DIVSI magazin

JULI 2015

Hamburgs Bürgermeister Olaf Scholz

Lernen, mit Unsicherheiten umzugehen

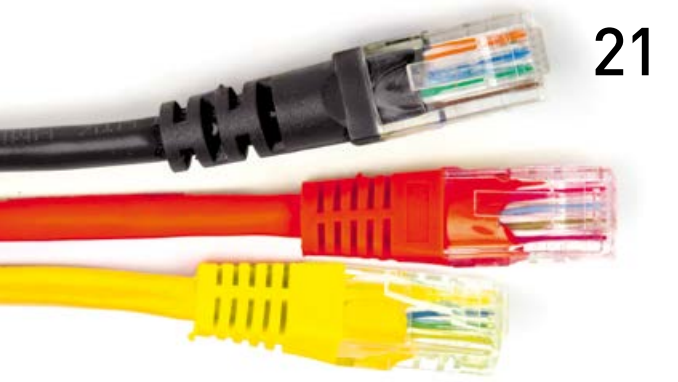
Auftakt-Rede beim Symposium „Neue Macht- und Verantwortungsstrukturen in der digitalen Welt“

Your Net

Workshops, Diskussionen und Show – über 500 junge Gäste waren dabei

Digitaler Kodex

Schwerpunktthema Big Data und Smart Mobility



Inhalt

Impressum

Herausgeber:
Deutsches Institut
für Vertrauen und
Sicherheit
im Internet (DIVSI)
Matthias Kammer,
Direktor
Mittelweg 110B
20149 Hamburg

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

Autoren: Jan Philipp Albrecht, Dr. Dirk Graudenz, Michael Hange, Holger Münch, Joanna Schmölz, Tom Solbrig

Realisierung:
Lohrengel Mediendesign
Schulterblatt 58
20357 Hamburg

Verbreitete Auflage:
ca. 7.500 Exemplare,
Abgabe kostenlos

Titel: Stefan Zeitz

Haben Sie Fragen oder wünschen weitere Informationen?

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

Anfragen DIVSI magazin:
Michael Schneider,
Leitung Kommunikation
Tel.: + 49 40 226 369 895
E-Mail: michael.schneider@divsi.de
E-Mail: presse@divsi.de

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

Emilia und das Wischen auf der Watch

Emilia erblickte vor rund 17 Monaten das Licht unserer zunehmend digitalisierten Welt. Einen Tag nach der Geburt tauchte ihr Name erstmals in einem elektronischen Medium auf. Die stolzen Eltern informierten, dass das Töchterchen um 21.14 Uhr die junge Familie vergrößert hatte.

Emilias Mama heißt Joanna. Die ist wissenschaftliche Leiterin von DIVSI. Und sie kann dank des mittlerweile höchst mobilen Krabbelflohs die Erkenntnisse der jüngsten DIVSI-Untersuchung live und am familiären Objekt überprüfen.

In der U9-Studie geht es erstmals dezidiert um „Kinder in der digitalen Welt". Dabei wurde ermittelt, ob und welche Rolle das Internet bereits im Leben der 3- bis 8-Jährigen einnimmt. Eine steigende, wie der Bericht ab Seite 14 zeigt.

Wobei Emilia sich bereits auf spezielle Weise den neuen Medien genähert hat. Und damit eine Erkenntnis der Studie nachhaltig bestätigte: Niemand muss lesen können, um Grundprinzipien der digitalen Praxis zumindest instinktiv zu erfassen. Jedenfalls griff sie mit flinken Fingern nach Mamas neuer Apple Watch, erkannte an dem Teil eine Oberfläche und wischte sofort darauf herum. Das hatte zwei Dinge zur Folge. Emilia strahlte, weil sich das Display laufend veränderte. Und Mama staunte, weil ihr leibhaftig vorgeführt wurde, was denn vielleicht ein künftiger Digital Native ist.

Lassen Sie mich beim Nachwuchs bleiben. Tom Solbrig, Abiturient des Vitzthum Gymnasiums in Dresden, ist 18 Jahre alt und damit der Jüngste, der sich in die Autorenreihe dieses Magazins eingereiht hat.

Seine Reportage über die „Your Net – DIVSI Convention 2015" beginnt auf Seite 10. Ich habe ihn ausgesucht, weil er 2014 den bundesweiten SPIEGEL-Schülerzeitungspreis in der Rubrik „Reportage" gewonnen hat. Tom beschrieb damals in „Trügerische Aussichten" den Alltag eines Fischers. Für unseren Internet-Kongress junger Menschen in Hamburg hatte er freie Hand. Es sollte gern über alles berichtet werden – lebendig, mit Hintergrund, Augenzwinkern und gerne auch kritischen Elementen.

Zum 5. Öffentlichen Diskussionsabend im Rahmen des Projekts „Braucht Deutschland einen Digitalen Kodex" hatte DIVSI in die Stuttgarter Phoenixhalle eingeladen. Es ging um Big Data & Smart Mobility. Dr. Dirk Graudenz liefert dazu einen Diskussionsbeitrag (S. 18).

Mit ein wenig Stolz möchte ich auf die Beiträge von gleich zwei Präsidenten hinweisen. Michael Hange, Präsident des BSI, informiert über die Lage der IT-Sicherheit in Deutschland (S. 21). Holger Münch, Präsident des BKA, schreibt über eine Bringschuld der Polizei: Vertrauen schaffen durch Aufklärung. Die Aufsätze eint eine Botschaft: Wir haben die Zeichen der Zeit erkannt, auf unsere Arbeit könnt ihr bauen (S. 24).

Und dann – last but not least – war da noch ein wichtiges Symposium in der Hamburger Bucerius Law School zum Thema „Neue Macht- und Verantwortungsstrukturen in der digitalen Welt". Lesen Sie dazu Wegweisendes von Bürgermeister Olaf Scholz (S. 4). Und Gedanken von Jan Philipp Albrecht (MdEP), worauf es dem Europäischen Parlament beim EU-Datenschutz ankommt (S. 8).

Ich wünsche Ihnen eine informative Lektüre.

Jürgen Selonke
Chefredakteur, DIVSI magazin

Wer trägt wo welche Verantwortung?

Hochkarätig besetzte Veranstaltung in der Bucerius Law School: Digitalisierung als Herausforderung für Staat, Politik und Gesellschaft.

Jürgen Selonke

Um „Neue Macht- und Verantwortungsstrukturen in der digitalen Welt" ging es bei einem zweitägigen Symposium in der Hamburger Bucerius Law School. „Die Digitalisierung aller Lebensbereiche hat einen Veränderungsprozess der Macht- und Verantwortungsstrukturen in Gang gesetzt und stellt eine immense Herausforderung für Staat, Politik und Gesellschaft dar. Insbesondere beim Umgang mit den wachsenden Datenmengen, die in Teilen sensibel und gleichzeitig hochrelevant und wertvoll sind, steht die Gesellschaft vor der komplexen Frage, wie eine Verantwortungsverteilung zwischen Staat, Unternehmern und Nutzern gestaltet werden kann", betonten DIVSI-Direktor Matthias Kammer und Prof. Dr. Karsten Thorn (Präsident der Bucerius Law School) in ihrer gemeinsamen Einladung.

Grundfragen. Matthias Kammer weiter: „Ich bin in einer Zeit groß geworden, in der ein demokratisches gesellschaftliches Zusammenleben in einer freien, sozialen Marktwirtschaft entwickelt wurde, in der es um den ständigen Ausgleich zwischen Starken und Schwachen geht. Die Macht- und Verantwortungsteilung zwischen Staat, Wirtschaft und Gesellschaft hat sich über die Jahre viel Grundstabilität erarbeitet und hat sie auch behalten bei allen Schwankungen, die es gab. Gilt das auch weiterhin? Entwickeln sich nicht schleichend oder schon deutlich sichtbar Verschiebungen in diesem Gefüge? Das sind Grundfragen, die wir in dieser Veranstaltung zum Thema machen wollen."

Zu der Veranstaltung hatten DIVSI, die Bucerius Law School sowie das Kieler Lorenz-von-Stein-Institut eingeladen.

Im Mittelpunkt des ersten Tages stand ein Beitrag von Jan Philipp Albrecht (Grüne, MdEP) zum „Aktuellen Stand der Diskussion um die EU-Datenschutzgrundverordnung (s. Beitrag S. 14).

Einführung. Bürgermeister Olaf Scholz sprach das Grußwort.

Technologische Innovationen fordern demokratische Systeme heraus.

Olaf Scholz

Austausch. Bürgermeister Scholz, Matthias Kammer (DIVSI).

Austausch. Prof. Dr. Spaeth (l.), Staatssekretär Dr. Kleindiek.

Fotos: Stefan Zeitz

Das Grußwort für die hochkarätig besetzte Veranstaltung in der Bucerius Law School sprach Hamburgs Erster Bürgermeister Olaf Scholz. Dabei äußerte er sich u.a. zu:

Hamburg und die Medien- und Digitalwirtschaft

„Als ein zentraler Standort der Medien- und Digitalwirtschaft haben wir mit zu den Ersten gehört, die die Folgen der Digitalisierung in Wirtschaft und Öffentlichkeit zu spüren bekamen. Um nicht dauerhaft als Getriebene der Zeitläufte durch den Wandel gehetzt zu werden, fördern wir heute die digitale Transformation mit Nachdruck – das gilt für die Hafenlogistik genauso wie für die Lehrangebote unserer Schulen und Hochschulen, für die Verkehrssteuerung ebenso wie für die staatlichen Museen. Hamburg entwickelt sich zu einer digitalen Stadt, und wenn wir es richtig angehen, dann haben wir die Möglichkeit, diese große und moderne Stadt mithilfe neuer Technologien noch lebenswerter und wirtschaftlich stärker zu machen."

Grundeinstellung zu Chancen und Risiken

„Ich will hier nicht einer naiven Technikgläubigkeit das Wort reden, aber es könnte nicht schaden, wenn wir uns von diesem Optimismus [der sogenannten ‚California Ideology'] ein wenig abgucken würden. Denn die grundsätzliche Überzeugung, dass es möglich ist, mit technischen Innovationen unser Leben zu verbessern, teile ich ausdrücklich. Der Fortschritt nicht nur der Industrie-, sondern auch der digitalen Gesellschaft ist eng verknüpft mit der technologischen Entwicklung und unserer gesellschaftlichen Fähigkeit, uns diese nutzbar zu machen. Hier können wir durchaus lernen von einer Kultur wie der US-amerikanischen, die in neuen Möglichkeiten zunächst einmal Chancen und nicht Risiken entdeckt. ➜

Neben der Transparenz öffentlicher Daten ist der Schutz individueller Daten ein weiteres wichtiges Prinzip der neuen digitalen Ordnung. **Olaf Scholz**

➔ Die moderne Gesellschaft, in der wir leben, ist geprägt davon, dass soziale und wirtschaftliche Veränderung möglich ist. Sie muss daher auch lernen, mit Unsicherheiten und Unübersichtlichkeiten umzugehen."

Zur aktuellen und künftigen Werteordnung

Zunächst einmal gilt die Werteordnung unseres Landes und unserer Gesellschaft ganz unabhängig von der Frage der technologischen Möglichkeiten. Das ist auch ein Hinweis auf die Frage nach den künftigen Machtstrukturen: Auch künftig wird es demokratisch legitimierte Machtausübung durch entsprechend ausgestattete gesellschaftliche Institutionen geben.

Technologische Innovationen fordern demokratische Systeme heraus, aber sie verändern sie nicht automatisch und an sich. Letztlich müssen sich Innovationen an den durch sie ermöglichten gesellschaftlichen und wirtschaftlichen Mehrwerten messen lassen. Den dazu nötigen politischen Diskurs müssen wir organisieren."

Geforderte Stärke

Wer den Fortschritt durch Technik will, der muss aushalten können, dass manches gut klingende Vorhaben scheitert und aus manch unscheinbarem Anfang Großes entstehen kann."

Drei Wellen der neuen Technologie

Die neuen technologischen Möglichkeiten ergreifen unsere Wirtschaft und unsere Gesellschaft seit zwei Jahrzehnten wellenweise. Zunächst hat die Digitalisierung die Informations- und Kommunikationsmöglichkeiten erfasst und insbesondere die Medien- und Kreativwirtschaft vor neue Herausforderungen gestellt.

In einer zweiten Welle haben sich die Produktions- und Logistikprozesse tief greifend verändert und tun es noch. Das Schlagwort von der Industrie 4.0 ist mittlerweile in aller Munde. Hier im Hamburger Hafen, im Smart Port, lässt sich erleben, wie weitreichend der Wandel ist.

Und in einer dritten Welle ergreift die Digitalisierung die öffentliche Infrastruktur und den öffentlichen Raum. Die Schnittstellen der technischen Systeme werden zunehmend allgegenwärtig und ermöglichen uns Formen der Zusammenarbeit und Prozesssteuerung, die noch vor wenigen Jahren undenkbar waren."

Spezielle Aufgaben für Hamburg

Wir stehen vor der Aufgabe, die Schnittstellen der Verwaltung zu den Bürgerinnen und Bürgern ebenso zu digitalisieren wie unsere öffentliche Infrastruktur. Und wir haben die Chance, dadurch Innovationsräume für Unternehmen zu öffnen, in denen neue Angebote und Technologien ausprobiert und in Piloten zur Marktreife geführt werden können. Dabei geht es letztlich immer darum, durch Technologie die Qualität unserer Services zu verbessern und Ressourcen effizienter zu nutzen."

Über eine künftige Medien- und Kommunikationsordnung

Wir diskutieren nicht die Kompetenzverteilung zwischen Ländern, Bund und Europa und propagieren auch keine völlig neue Ordnung, sondern versuchen die Schnittstellen zwischen Landes-, Bundes- und Europarecht besser zu managen. Das kann gelingen, wenn wir uns auf gemeinsame Regulierungsziele, auf Kollisionsregeln und auf Governance-Instrumente verständigen.

Gastgeber, Ehrengast. Olaf Scholz mit Matthias Kammer und Prof. Dr. Karsten Thorn (Präsident Bucerius Law School).

Schlagabtausch. Rege Diskussion über „Digitalen Fortschritt – staatenlos, uferlos, rechtlos – wo bleibt der Nutzer?“

Diesen Ansatz verfolgen wir aktuell in der Bund-Länder-Kommission, in der sich die Länder gemeinsam mit dem Bund vor allem über die Schnittstellenthemen wie Kartellrecht und Vielfaltssicherung oder Intermediär-Regulierung austauschen, um gemeinsam abgestimmte Regulierungsvorschläge zu entwickeln. Diese Herangehensweise scheint mir für Fragen des Managements der Digitalisierung ganz generell sinnvoll zu sein.

Innovationsdynamik und Vorgaben

„Angesichts der Innovationsdynamik werden wir kaum in der Lage sein, ex ante Vorgaben zu machen. Viel wichtiger ist es, dass wir abstrakte und prinzipiengeleitete Vorstellungen entwickeln, die dann entweder auf dem Wege der Co- und Selbstregulierung oder aber im Rahmen der deutschen oder europäischen Gesetzgebung angewendet werden.

Das ist keine Aufgabe für den Gesetzgeber allein, sondern hier sind Wirtschaft und Gesellschaft gleichermaßen in der Pflicht, gemeinsame Überlegungen zu entwickeln und zur Geltung zu bringen.“

Eine neue Leitstelle

„Wir haben uns in Hamburg vorgenommen, die Digitalisierung und ihre Potenziale zu verstehen und als Chancen zu begreifen. Wir wollen auf Augenhöhe sprechfähig sein. In der Stadt passiert schon unglaublich viel. Um diese Prozesse zu bündeln, aufeinander abzustimmen und Synergien zu heben, richten wir derzeit in der Senatskanzlei im Amt Medien eine Leitstelle für die Digitale Stadt ein. Sie soll dabei helfen, einen besseren Überblick über die zahlreichen Projekte und Prozesse zu erlangen. Zugleich belassen wir die Verantwortung für die einzelnen Projekte der Digitalisierung ausdrücklich bei den fachlich zuständigen Behörden.

Wir wollen nicht, dass die Transformationsthemen in irgendwelche Stäbe oder ins IT-Referat delegiert werden. Sie müssen Gegenstand des alltäglichen Verwaltungshandelns werden. Erst dann wird es uns gelingen, die Chancen der Digitalen Stadt voll zu entwickeln.“

Das Transparenzgesetz

„... ein Beispiel dafür ist das Transparenzgesetz, das wir in Hamburg in der vergangenen Legislaturperiode verabschiedet haben und das die Grundlage geschaffen hat für ein Transparenzportal, in dem alle wesentlichen Informationen über das Handeln von Senat und Verwaltung für jede Bürgerin und jeden Bürger zugänglich sind. Mit diesem Schritt haben wir die bisherige Logik des Verwaltungshandelns umgedreht.

Es ist noch gar nicht so lange her, da musste derjenige, der eine Auskunft haben wollte, begründen, warum er einen Anspruch darauf hat, sie zu bekommen. Jetzt muss der Staat begründen, warum er eine Information nicht preisgibt. Diese Umkehr der Beweislast ist eine richtige und sinnvolle Antwort auf die berechtigten Partizipationsansprüche der Bürgerinnen und Bürger.“

Datenschutzgrundverordnung

„Neben der Transparenz öffentlicher Daten ist der Schutz individueller Daten ein weiteres wichtiges Prinzip der neuen digitalen Ordnung. Hier haben wir es mit einer zentralen Bürgerrechtsfrage zu tun – vor allem, wenn es um den Schutz dieser Daten vor dem Zugriff des Staates geht.

Die Debatte über die Datenschutzgrundverordnung der EU zeigt, wie viel Arbeit wir hier noch gemeinsam zu leisten haben und wie sehr dieses Politikfeld noch in Bewegung ist. Allerdings findet die Debatte an der richtigen Stelle statt. Denn nur ein europaweites Recht hat eine Chance, relevant zu sein. Die Nationalstaaten sind für eine Regelung im weltweiten Web oft zu klein.“

Paradigmenwechsel

„Vielleicht erleben wir zurzeit ja sogar einen Paradigmenwechsel weg von der reinen Datensparsamkeit hin zur individuellen Datensouveränität, die vorrangig darauf zielt, den Einzelnen wirklich informationell selbstbestimmt sein zu lassen. Die Sensibilität dafür, dass sinnvoller Schutz nicht in übergriffigen Paternalismus ausufern darf, scheint mir jedenfalls zu wachsen.“

Politik und Spielregeln

„Wir sind hier politisch gefragt, Spielregeln zu entwickeln, die einerseits eine freie und liberale Öffentlichkeit nach wie vor ermöglichen und die andererseits Diskriminierung und Einschränkungen von Vielfalt verhindern.“

Führungsaufgaben

„Regierung und Parlamente werden sich nicht aus der Führungsaufgabe für die Gesellschaft zurückziehen. Im Gegenteil: Dort, wo allgemeinverbindliche Regeln identifiziert, formuliert und durchgesetzt werden müssen, ist Politik unerlässlich. Hier übt sie demokratisch legitimierte Macht aus.“ ⊡

Fotos: Stefan Zeitz

Transparenz – ein wichtiger Schwerpunkt

Worauf es dem Europäischen Parlament beim EU-Datenschutz ankommt.

Jan Philipp Albrecht

Datenschutz ist ein Grundrecht, das mit dem Inkrafttreten des Lissaboner Vertrages am 1. Dezember 2009 fester Bestandteil des EU-Rechts ist. Ihren neu geschaffenen Posten als Justizkommissarin nutzte die damalige EU-Kommissionsvizepräsidentin Viviane Reding dann, um mit einem Vorschlag für eine Datenschutzverordnung die bereits seit einigen Jahren diskutierte Reform der allgemeinen Datenschutzrichtlinie von 1995 anzustoßen. Das Europäische Parlament nahm dazu im Juli 2011 ausführlich und mit einer fast einstimmig verabschiedeten Resolution Stellung.

Die Abgeordneten forderten darin, dass die EU-Kommission einen mutigen Schritt hin zu einem einheitlichen Datenschutz für die gesamte Europäische Union gehen solle. Die Parlaments-Resolution sieht einen umfangreichen und bereits konkret formulierten Katalog von Anforderungen an ein zukünftiges EU-Datenschutzrecht vor. Wer den mit großer Mehrheit am 12. März 2014 beschlossenen Gesetzentwurf des Europäischen Parlaments und die anstehenden Verhandlungen zwischen Ministerrat, Kommission und Parlament verstehen will, wird um diese Ausgangsposition nicht herumkommen.

Schutz notwendig. Die wichtigste Forderung des Europäischen Parlaments ist die nach einem einheitlichen Datenschutzrecht in Europa. Die Fragmentierung der Regeln für die Verarbeitung personenbezogener Daten in der EU ist ein großes Problem für den effektiven Grundrechtsschutz. Der immer größere Anteil grenzübergreifender Dienste und Maßnahmen zur Datenverarbeitung und der zunehmend automatisch stattfindende grenzübergreifende Austausch von Daten in Sekundenschnelle erfordern einen EU-weiten Schutz für die Bürger.

Die noch bis vor wenigen Jahren angeführte Vermutung, nur ein Teil der personenbezogenen Daten würde grenzübergreifend verarbeitet, haben spätestens die Folgen des rasant wachsenden „Cloud Computing" widerlegt. Das Europäische Parlament hat diese Erkenntnis bereits früh diskutiert, nachdem bekannt wurde, dass die Anti-Terror-Behörden der Vereinigten Staaten auf die in US-Datenzentren gespeicherten Daten europäischer Unternehmen wie dem Bankdienstleister SWIFT oder dem Buchungsdienstleister Amadeus zugriffen.

Handleln geboten. In zahlreichen Debatten und Auseinandersetzungen ging es um Rechtshilfeabkommen der EU mit den USA sowie die Enthüllungen des NSA-Wistleblowers Edward Snowden. Die Forderung, das Datenschutzrecht in Europa endlich lückenlos für den EU-Binnenmarkt zu regeln und – ähnlich dem Wettbewerbsrecht – auch eine extraterritoriale Wirkung einzuführen, ist folge-

Machtzentrum in Straßburg. Vier Tage im Monat wird hier abgestimmt und debattiert.

Fotos: European Parliament/Fritz Schumann, Leonid Andronov – Shutterstock

Kämpferisch. Viviane Reding, Mitglied des Europäischen Parlaments, ist überzeugt:

„Von einem starken Datenschutz profitieren alle."

richtig und zukunftsweisend. Auch mit Blick auf die Situation von Datenverarbeitern und „Datensubjekten" im EU-Binnenmarkt ist dringend Handeln geboten. Immer deutlicher wird, dass die unterschiedliche Umsetzung und Durchsetzung der gemeinsamen Regeln aus der Richtlinie 95/46/EG zu massiven Wettbewerbsverzerrungen zwischen den Unternehmen in den unterschiedlichen Mitgliedstaaten führt. Zudem werden Bürgerinnen und Bürger immer häufiger von ihren eigenen Aufsichtsbehörden und Gerichten an Aufsichtsbehörden und Gerichte anderer Mitgliedstaaten verwiesen.

Hohes Schutzniveau. Das Europäische Parlament hat in seiner Resolution vom Juli 2011 „betont, dass die Standards und Grundsätze der Richtlinie 95/46/EG einen idealen Ausgangspunkt darstellen und als Teil eines modernen Datenschutzrechts weiterentwickelt, erweitert und gestärkt werden sollten". Des Weiteren forderte es von der EU-Kommission die volle Harmonisierung auf höchstem Niveau, die für Rechtssicherheit und ein einheitliches hohes Schutzniveau für den Einzelnen sorgt. Auf Grundlage dieser Forderungen hat die EU-Kommission mit ihrem Verordnungsvorschlag einen Harmonisierungsschritt vorgelegt, der vor allem das bestehende Rechtsniveau der 1995er-Richtlinie fortschreibt.

Darüber hinaus schlug die Kommission Erweiterungen der individuellen Rechte vor, etwa durch das dem Recht auf Löschen hinzugefügte „Recht auf Vergessenwerden" und das Recht auf Datenportabilität. Beides hatte das Europäische Parlament in seiner Resolution ausdrücklich eingefordert. Gerade im Bereich der Transparenz geht das Europäische Parlament jedoch noch über die Vorschläge der Kommission hinaus. Mit erweiterten Auskunfts- und Informationsansprüchen sowie dem Vorschlag einfacher standardisierter Symbole wird es seinem eigenen Anspruch aus der Resolution gerecht.

Das Kernstück des Kommissionsvorschlages war der „Konsistenz-Mechanismus", der in Verbindung mit dem „One-Stop-Prinzip" zu einer Win-win-Situation für „Datensubjekte" und Datenverarbeiter führen soll. Einerseits soll danach jeder Verarbeiter, der unter den Anwendungsbereich der Verordnung fällt, einen festen Ansprechpartner haben. Andererseits soll die inkonsistente Umsetzung und Anwendung des Datenschutzrechts durch eine verstärkte und verbindliche Zusammenarbeit auf EU-Ebene endlich der Geschichte angehören und den Bürgern damit ein effektiv durchsetzbares Grundrecht auf Datenschutz auch in der Praxis gewährt werden.

Durchsetzung angemahnt. In seiner ursprünglichen Resolution zur Datenschutzreform hatte das Europäische Parlament bereits die bessere Durchsetzung des EU-Datenschutzrechts im gemeinsamen Binnenmarkt angemahnt und dabei besonders auf Unternehmen abgezielt, die aus Drittstaaten heraus auf dem EU-Binnenmarkt tätig sind. Angesichts des sich stetig vergrößernden digitalen Marktes und der Öffnung des Binnenmarkts für Unternehmen aus Drittstaaten hatte sich die Durchsetzung des Datenschutzrechts für die Aufsichtsbehörden der EU-Mitgliedstaaten immer deutlicher als Problem herausgestellt: In vielen Beschwerdefällen hatten sich die Betroffenen nicht an die für die Aufsicht zuständige Behörde gewandt. Dies zog oft langwierige Abstimmungsprozesse zwischen den Aufsichtsbehörden nach sich – an deren Ende nicht selten die Feststellung stand, dass die Durchsetzungsmaßnahmen der Aufsichtsbehörden in den verschiedenen Mitgliedstaaten in der Praxis stark variierten.

Angesichts des Stellenwerts des Datenschutzes als individuelles Grundrecht erschien dies der großen Mehrheit der Parlamentarier als nicht hinnehmbar. Die Aufforderung an die EU-Kommission, ein einheitliches Datenschutzrecht vorzulegen, konnte deutlicher nicht ausfallen. Damit ist auch klar, dass das Europäische Parlament eine horizontale Regelung auf EU-Ebene fordert und Abweichungen im Rahmen der mitgliedstaatlichen Rechtsetzung zur Ausnahme machen will.

Jan Philipp Albrecht
ist stellv. Vorsitzender des Innen- und Rechtsausschusses des Europäischen Parlaments und Berichterstatter des Europäischen Parlaments für die Datenschutzgrundverordnung.

Jugend entdeckt das Internet neu

Your Net – DIVSI Convention 2015: Hamburger Kongress ein voller Erfolg. Zwei Tage lernen, diskutieren, Spaß haben.

Tom Solbrig

Ghana-Power. Einchecken, dann locker begrüßt von Nana Domena (l.).

Fotos: Stefan Zeitz

Über Nana Domenas Gesicht kullern große Schweißperlen. Er ist voller Energie. Um ihn herum Sand, Palmen und euphorische Menschen.

Der aus Ghana stammende Moderator hat soeben mit Matthias Kammer, Direktor des Deutschen Instituts für Vertrauen und Sicherheit im Internet, die erste „Your Net-Convention" im Beach Hamburg eröffnet. „Ich erhoffe mir, dass die jungen Leute im Netz vom Nutzer zum Macher werden", sagt Kammer.

Ungewöhnlich ist die Location. Aus Liegestühlen kann man die Veranstaltung verfolgen. „Man ist irgendwie vom Alltag herausgelöst", sagt Stimmungskanone Domena, der begeistert von der Idee ist, durch Sand bei einem Kongress zu laufen.

Promis vor Ort. Mit dabei sind Viviana und Lennart. Der 16-jährige Schüler interessiert sich wie auch viele andere für den Datenschutz im Internet.

Mit der Convention erhofft er sich, wichtige Fragen beantwortet zu bekommen. Wie öffentlich muss unser Leben sein? Wie schnell werden unsere Daten missbraucht? Ist ein Leben ohne Internet vorstellbar?

Dafür stehen Referenten auf Podiumsdiskussionen und in Workshops Rede und Antwort. Große der Szene wur-

Staun-Zeit. Tobias Schrödel (l.) zeigte, wie leicht er in Laptops und Co. eindringen kann.

den eingeladen. Einer der bekanntesten ist Max Schrems. Der österreichische Autor sorgt derzeit mit einer Schadensersatzklage im Millionenbereich gegen Facebook für Furore – wie auch gegen das NSA-Überwachungsprogramm „PRISM", über das in Kürze der Europäische Gerichtshof entscheiden wird.

Für die 20 Jahre junge Viviana wurde das Thema jedoch oft genug in den Medien thematisiert. „Die NSA-Affäre ist schon ausgekaut", sagt die Kommunikationsstudentin und besucht daher am Vormittag den Workshop „Berufsfeld Internet".

Datenklau-Debatte. Zeitgleich verfolgt Lennart im Plenum die Podiumsdiskussion „Privacy – Wie öffentlich möchtest du sein?". Mit dabei sind unter anderem Max Schrems und Sabine Leutheusser-Schnarrenberger. Der Datenklau wird auch debattiert. Dass man nüchtern betrachtet als Nutzer nicht viel gegen den Internetriesen Facebook und dessen Datenmissbrauch unternehmen kann, lautet im Endeffekt das Fazit.

„Man sollte am besten keine Postings machen, die nicht notwendig sind. Sonst kann man nicht viel tun, außer dass man auf alles verzichtet. Denn selbst bei der Synchronisation des Handys deines Freundes gelangen Informationen von dir ins Netz", sagt Schrems.

Draußen im Pavillon ist der Workshop zu Ende gegangen, den Viviana besuchte. In der Hoffnung, neue Impulse zu bekommen, wurde sie ein wenig enttäuscht. „Es hat mir nicht wirklich was gebracht. Das lag vielleicht auch an den jungen Teilnehmern. Die Fragen gingen teilweise echt am Thema vorbei", erzählt die →

Aktiv dabei. Staatssekretär Dr. Ralf Kleindiek begrüßte die jungen Gäste. DIVSI-Direktor Matthias Kammer mit Sabine Leutheusser-Schnarrenberger und Prof. Dr. Tobias Keber, der über „Law & Order im Netz" diskutierte (v.l.).

Spaß & Ernst. Konzentriert in den Workshops, locker in den Pausen.

> Wichtig ist, dass jeder eine tiefe Sensibilität besitzt, Informationen aus dem Internet zu hinterfragen.
>
> **Anselm Sellen, Mediendesigner**

→ Studentin. Zudem gab es Probleme mit dem WLAN, weshalb kaum Zeit für die Gruppenarbeit blieb.

Währenddessen beschäftigt man sich ein paar Pavillons weiter mit der Frage: „Liegt im Netz immer die Wahrheit?" Wie schwierig es ist, Fehlinformationen von der Wahrheit zu trennen, zeigt der „Stinkefinger-Eklat" um den griechischen Finanzminister Varoufakis. Wenn selbst die seriösen und öffentlich-rechtlichen Sender nicht die Wahrheit wissen, wie kann dann der Einzelne verlässliche Informationen aus dem Internet beziehen?

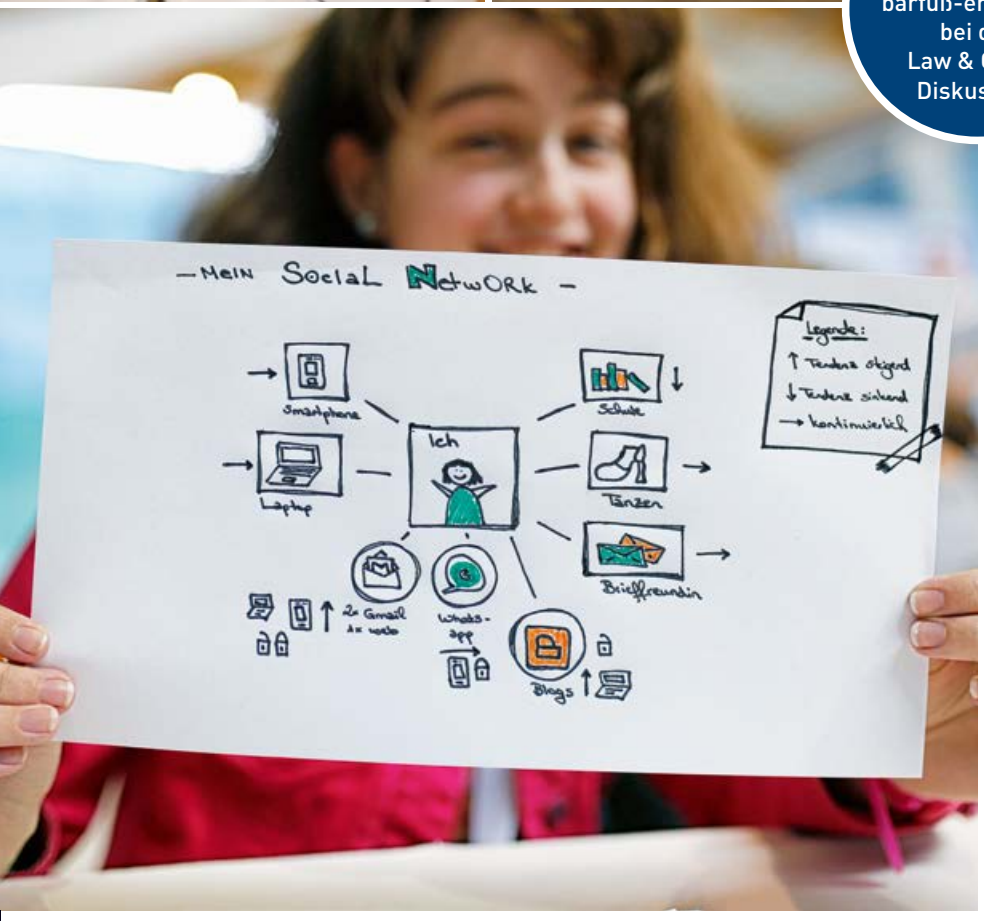
„Im Internet läuft es nicht mehr so ab, dass nur noch Medienmacher Informationen zu den Konsumenten spielen, sondern dass es auch mittlerweile umgekehrt ablaufen kann. Informationen sind somit inzwischen von jedermann manipulierbar", sagt der Mediendesigner Anselm Sellen und rät: „Wichtig ist, dass jeder eine tiefe Sensibilität besitzt, Informationen aus dem Internet aufzunehmen und diese zu hinterfragen."

Ein wenig erschöpft strömen die 500 Teilnehmer nach den ersten neun Workshops in die zwei großen Hallen, um sich am Buffet zu bedienen. Essen, Getränke, Unterkunft und Anreise sind für alle Teilnehmenden kostenlos. „Ziel war es, diese Veranstaltung jedem zu ermöglichen – also allen frei zugänglich zu machen", so Direktor Kammer.

Knack-Zeit. Auch in das Plenum strömen wieder die Massen. Anziehungspunkt ist diesmal Deutschlands erster IT-Comedian. Die Zuschauer werden beim Live-Hacker Tobias Schrödel Augenzeuge, dass es nicht lange braucht, Passwörter oder Smartphones zu knacken. Mithilfe eines ZIP-Archives kann er in nur acht Sekunden ein fünfstelliges Passwort knacken. „Zum einen sollten vernünftige Passwörter verwendet werden. Nicht zu vergessen ist ein aktueller Virenschutzscanner. Und alles, was funkt, nicht immer nur funken lassen. Sondern nur verwenden, wenn man es braucht", rät Schrödel.

In den Nachmittagsworkshops sind unter anderem Florian Thalmann, Journalist, und Alexander Bangula, YouTube-Blogger, dabei. Während Alexander Ban-

Dauer-Power. Sängerin Jean Pearl begeisterte beim Get-together am Startabend. Jana, Sarah, Simin, Johanna, Pauline und Angelika: Erst ein Gruß an alle, die nicht dabei sein konnten, dann ein Handyfoto von den Show-Events (v.l.).



Locker-flockig. Marina Weisband, barfuß-entspannt bei der Law & Order-Diskussion.

tet. Auf der Convention gibt er einen Einblick in das Business Internet und zeigt auch, wie er sein Geld verdient, etwa mit Affiliate-Marketing.

Vivianas zweiter Workshop ist mittlerweile auch vorbei. „Der Workshop jetzt war viel besser. Ich fand gut, dass sich gleich drei Professoren aus den Wissenschaftsfeldern Soziologie, Psychologie und Neurologie mit der Frage, wie uns das Internet verändert, beschäftigt haben", sagt sie. Der Kongress hat ihr sehr gefallen. „Die Auswahl an Angeboten war groß. Man hätte vielleicht noch ein, zwei Workshops mehr mitnehmen können statt nur die zwei. Location, Atmosphäre und Programm waren auch gut."

Daumen hoch. Auch Lennarts Fazit fällt positiv aus. Besonders der Live-Hacker hat ihm gefallen. „Man hört ja regelmäßig über diverse Sicherheitslücken. Aber irgendwie konnte ich mir nie richtig vorstellen, dass es jeden so einfach treffen könnte", sagte er und will bewusster umgehen: „Ich werde in nächster Zeit einige meiner Passwörter ändern und weniger Daten in meiner Cloud speichern."

Dafür, dass es die erste Veranstaltung war, fanden es beide gelungen. Auch Nana Domena ist begeistert: „Das ist wahnsinnig cool, dass die jungen Leute durch DIVSI so eine Chance bekommen."

Tom Solbrig
Abiturient des Vitzthum Gymnasiums in Dresden. Er gewann 2014 den SPIEGEL-Schülerzeitungspreis in der Rubrik „Reportage".

gula, bekannt als „Mr. Helfersyndrom", beruflich aufs Internet angewiesen ist, hat Florian Thalmann einen Selbstversuch gewagt und sich die Frage gestellt: „Ist ein Leben ohne Internet vorstellbar?" Dafür war er vier Wochen offline. „Ich hatte viele Momente, wo ich kurz vor dem Einknicken war und gemerkt habe, jetzt brauche ich das Internet", sagt Florian Thalmann und empfiehlt daher, nicht komplett auf das Internet zu verzichten: „Ich finde es wichtiger, man schafft sich kleine Oasen. Also dass man mal spazieren geht und das Handy zu Hause lässt."

Der YouTube-Blogger Alex Bangula sieht es ähnlich. Sein Smartphone schaltet er etwa abends aus oder checkt nicht mehr unterwegs die Mails. „Man muss lernen, vernünftig umzugehen", sagt er, der mit seinem Kanal mehrere Tausend Fans erreicht und Smartphones bewer-

Fotos: Stefan Zeitz

STUDIE

Digitale Teilhabe bedeutet soziale Teilhabe

Warum wir wissen sollten, wie die 3- bis 8-Jährigen mit dem Thema Internet umgehen.

Joanna Schmölz

Früh übt sich! Oder? Ungelöstes Diskussionsthema: Ab wann ist Internet für Kids gut?

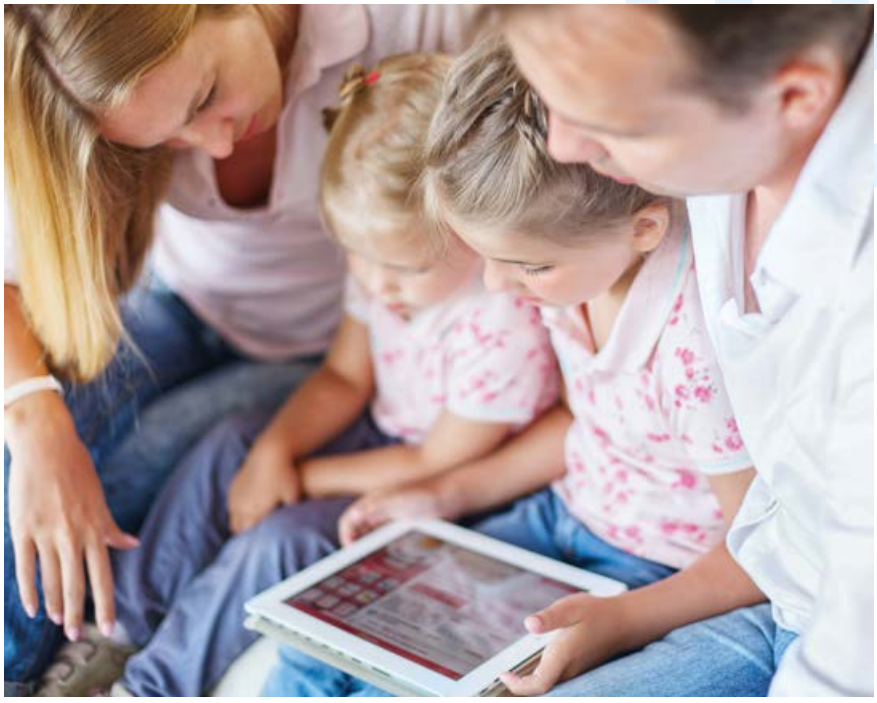
Das Thema „Kinder und Internet" ist hochaktuell. Die einen meinen, Kinder müssten so lange wie möglich von der digitalen Welt ferngehalten werden. Die anderen verlangen Tablets in der Kita und Programmieren/Coding bereits in den ersten Schuljahren. Facettenreich wird darüber diskutiert und gestritten, wie, ab wann oder ob Kinder überhaupt mit digitalen Medien in Berührung kommen sollten. Dabei sind jedoch – und das wird häufig übersehen – manche der Problemstellungen längst von der Realität überholt worden.

Zwar ist das Internet selbst ja gerade mal ein Teenager, in mancher Hinsicht steckt es noch in den Kinderschuhen. Aber es entwickelt sich rasant; die Digitalisierung verändert vieles, das sich zuvor über Jahrzehnte etabliert und bewährt hatte. Diese Entwicklung wirkt sich auf nahezu alle Bereiche unseres Lebens aus.

Kein Luxusgut. Heute ist das „Internet to go" für die meisten von uns ein ständiger Begleiter und damit auch in dem Lebensraum gegenwärtig, in dem Kinder und Jugendliche sozialisiert werden. Die jetzige junge Generation ist die erste, die in einer derart stark digitalisierten Welt aufwächst. Ich denke hier vor allem an das Zeitalter des mobilen Internets, in dem Smartphones & Co. kein Luxusgut für wenige sind, sondern zum Alltag vieler oder gar der meisten gehören. Diese Entwicklung hat erst mit der iPhone-Einführung 2007 begonnen. Was sich seitdem verändert hat, ist enorm.

Dieser kurze Blick auf die Situation beschreibt allerdings nur den verfügbaren Handlungsrahmen. Wie sich die grundsätzlichen Einstellungen und Handlungslogiken entwickeln, hängt von einer Vielzahl weiterer Faktoren ab – ganz wesentlich vom lebensweltlichen Hintergrund, vor dem die Kinder aufwachsen.

Vor fast genau einem Jahr haben wir die Ergebnisse der DIVSI U25-Studie vor-



So soll es sein. Jung probiert, Alt ist aufmerksam dabei.

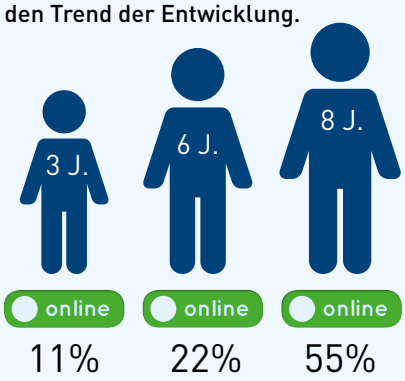
gestellt. Sie nahm Kinder, Jugendliche und junge Erwachsene zwischen 9 und 24 Jahren und ihr Leben in und mit der digitalen Welt in den Blick. Die Untersuchung zeigte, dass bei ihnen digitale Medien längst etabliert sind und dass es bereits in diesen Altersgruppen große Unterschiede in Hinblick auf Medienkompetenz, auf die subjektive Souveränität im Umgang mit dem Internet, aber auch hinsichtlich Sicherheitserwartungen gibt.

Doch längst nicht alle jungen Menschen, die in unserer digitalisierten Welt aufwachsen, sind automatisch „Digital Natives". Einige sind stark verunsichert oder wissen schlichtweg nichts mit ➜

DIVSI U9-Studie – Kinder in der digitalen Welt: Zentrale Befunde aus der jetzt vorgestellten Untersuchung

Das Internet erlangt schon bei kleinen Kindern eine relevante Alltagsbedeutung. Bereits die Kleinsten sind gelegentlich online; die Internetnutzung intensiviert sich fortan rasch. Auch Kinder ohne Lese- und Schreibfähigkeit können zum Teil – über das Erkennen von Symbolen – eigenständig Internetseiten aufrufen.

Online-Nutzung. Die Zahlen zeigen den Trend der Entwicklung.



Die Studie zeigt: Mehr als die Hälfte der 8-Jährigen (55 Prozent) ist bereits online. Von den 6-Jährigen geht fast ein Drittel ins Internet, und bei den 3-Jährigen ist es schon jedes zehnte Kind.

Mit Schuleintritt wird der Computer bzw. Laptop im Medienalltag wichtiger und löst die Spielekonsole als meistgenutztes Endgerät ab. 6- bis 8-jährige Mädchen und Jungen sind gleichermaßen interessiert an digitalen Medien und dem Internet.

Zudem gibt es keine Geschlechterunterschiede bei der Selbsteinschätzung, wie gut man sich mit dem Internet auskennt. **Interessenunterschiede zeigen sich mit Blick auf die genutzten Inhalte im Netz:** Jungen sind deutlich spieleorientierter, Mädchen recherchieren häufiger Informationen.

Die digitale Ausstattung von Kindern und ihre technischen

Interessen. Jungen sind spieleorientierter, Mädchen recherchieren häufiger.

Zugangsmöglichkeiten zu digitalen Medien und dem Internet sind – trotz enormer Einkommensunterschiede der Eltern – **keine Frage des Geldbeutels**. Kinder haben nahezu vergleichbare Möglichkeiten, auf Spielekonsolen, Smartphones und Computer/ Laptops zuzugreifen.

Gleiche technische Voraussetzungen sind nur notwendige, aber noch keine hinreichenden Bedingungen für den Zugang zu digitalen Medien und dem Internet. Ent- ➜

Fotos: Dasha Petrenko/nenetus – Shutterstock

Gaming. Wer wie oft Spiele nutzt, hängt auch von der formalen elterlicher Bildung ab.

➔ dem reichhaltigen Angebot anzufangen. Für die einen ist das Internet ein reiner Freizeitraum, andere nutzen es für Informations- und Bildungszwecke und begreifen es als Werkzeug für das persönliche und berufliche Weiterkommen.

Um zu verstehen, wann genau und unter welchen Umständen sich diese teils stark auseinanderklaffenden Entwicklungen vollziehen, haben wir mit der U9-Studie, realisiert durch das SINUS-Institut, noch etwas früher angesetzt. Wir wollten die ersten Phasen des eigenständigen Umgangs mit digitalen Medien und insbesondere mit dem Internet unter die Lupe nehmen.

Wen fragen? Denn – so eine wichtige Erkenntnis der U9-Studie: Die Kinder SIND bereits online. Rund 1,2 Millionen 3- bis 8-Jährige gehen regelmäßig ins Internet. Tendenz vermutlich steigend. Die Frage nach dem „Ob" stellt sich so also nicht mehr.

Hinsichtlich vieler anderer Fragen rund um „Kinder und Internet" gibt es aber keine oder keine ausreichenden Erfahrungswerte. Eltern können auch ihre eigenen Eltern kaum fragen: „Wie habt ihr das denn damals gemacht mit dem Internet?"

Im Kern der Debatte stehen dabei Fragen wie:

- Wie viel Internet ist gut für Kinder?
- Was können oder sollten sie dort machen (dürfen)? Was nicht?

➔ scheidend dafür, ob Kinder überhaupt online gehen (dürfen), ist die digitale Lebenswelt der Eltern, das heißt ihr Digitalisierungsgrad sowie ihre Einstellung zu digitalen Medien und zum Internet.

Über die Hälfte (53 Prozent) der 6- bis 8-Jährigen aus dem sehr internetaffinen Milieu der Digital Souveränen gehen ins Internet. Bei den Kindern der vorsichtigen und selektiven Internetnutzer aus dem Internet-Milieu der Verantwortungsbedachten Etablierten sind es 36 Prozent. **Nur 20 Prozent der Kinder aus dem Milieu der Internetfernen Verunsicherten** sind manchmal online.

Je selbstverständlicher Eltern im Internet sind und digitale Medien als festen Bestandteil in ihren Alltag integriert haben, desto mehr Selbstsicherheit zeigen auch ihre Kinder im Umgang mit digitalen Medien. Wie Kinder mit digitalen Medien konkret umgehen und was sie im Internet machen, **unterscheidet sich vor allem entlang der formalen Bildungsgrade der Eltern**.

Kinder von Eltern mit geringer formaler Bildung haben **im Kontext Spiele einen stärkeren Unterhaltungsfokus** und nutzen das Internet deutlich seltener für Informationssuche und Lernzwecke. Je geringer die formale elterliche Bildung, desto weniger engagiert sind sie, ihre Kinder in die digitale Welt aktiv zu begleiten. Sie meinen vielmehr, **man bräuchte Kinder beim Erlernen des Umgangs mit digitalen Medien nicht anzuleiten**, da sie dies von allein lernen würden.

Schutzprogramme. Bei gut der Hälfte sind Sicherungen eingebaut.

Die deutliche Mehrheit der Eltern (65 Prozent) sieht die Chancen digitaler Medien und des Internets für ihre Kinder; dies besonders dann, wenn es um die Sicherstellung der sozialen Teilhabe geht. Als solche Chancen für Kinder werden vor allem das **umfangreiche Informationsangebot des Internets** und die Motivationsleistung von Lernspielen und Lernprogrammen gesehen. 58 Prozent der Eltern glauben zudem, dass Computerspiele die Konzentrationsfähigkeit und die motorischen Fähigkeiten von Kindern verbessern können.

Allerdings überwiegen die Risiken des Internets aus Sicht der Eltern die wahrgenommenen Chancen. Insbesondere mit Blick auf das Thema „Kinder und Internet" haben sie ausgeprägte Bedenken – zwei Drittel der Eltern 3- bis 8-Jähriger **verbieten ihren Kindern, ins Internet zu gehen**.

Als größte Risiken werden nicht kindgerechte Inhalte und der mögliche Kontakt zu unbekannten Personen sowie Mobbing angesehen. Auch der Schutz

- Welche Kompetenzen benötigen sie, um die vielfältigen Chancen des Internets für sich (und ihre Zukunft) nutzen zu können?
- Welchen Gefahren/Risiken sind sie im Internet ausgesetzt, und wie können sie geschützt werden? Und zwar auch ohne dass sie bei jedem einzelnen Klick beaufsichtigt werden.

Digitale Teilhabe ist jetzt schon eine der zentralen Voraussetzungen sozialer Teilhabe. In Zukunft wird sich das eher noch verstärken. Da unsere Lebenswelt stark medialisiert ist, ist es nur logisch, dass auch die Sozialisierung der Kinder davon nicht frei bleibt. Ein Heranwachsen ohne Auseinandersetzung mit Medien ist – unabhängig von Sinn oder Unsinn – höchst unwahrscheinlich.

Weichenstellung. Die Ergebnisse der U9-Studie machen überdeutlich, wie weichenstellend bereits die ersten Jahre für die Entwicklung digitaler Kompetenz(en) sind. Welche Einstellungen junge Menschen zum Internet entwickeln, wie sie sich darin bewegen und welche Chancen und Risiken sie wahrnehmen, wird bereits in der Kindheit angelegt. Selbstsicherheit und Chancenorientierung stehen also gegen Ängste und Restriktionen.

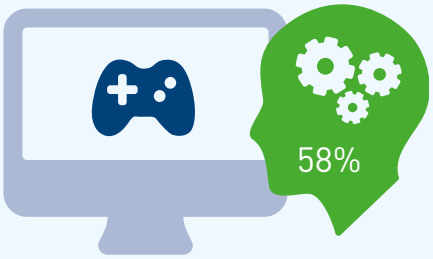
Dabei kommt der technischen Ausstattung bei Weitem nicht die größte Bedeutung zu. Weder die Verteilung von Tablets an Schulen noch „Breitband für alle" werden als Maßnahmen ausreichen, um die Chancengleichheit, die der Digitalisierung gern zugeschrieben wird, zu sichern. Es reicht nicht, dass alle dem Grunde nach Zugang zur großen bunten digitalen Welt bekommen.

Das Gegenteil scheint der Fall zu sein. Die Schere droht noch deutlich weiter auseinanderzuklaffen, wenn sich die sozialen Ungleichheiten im Netz reproduzieren. Die Erkenntnisse der U9-Studie können eine wissenschaftlich gesicherte Grundlage für sachlich fundierte Diskussionen darüber sein, welche Maßnahmen ergriffen werden könnten, um Kindern einen guten Start in einer immer stärker digitalisierten Welt zu ermöglichen.

Diskurs-Anstöße. Es geht im Kern um die Frage: Wie ebnen wir Kindern den Weg in eine chancenreiche Zukunft, und wie bereiten wir sie qualifiziert auf eine Welt vor, in der kaum noch etwas ohne Internet gehen wird? Die aktuelle Untersuchung soll dazu beitragen, einen fundierten Diskurs hierüber zu organisieren.

WEITERE INFORMATIONEN
divsi.de/publikationen

Joanna Schmölz
studierte Medienkultur und Politische Wissenschaft. Sie ist stellv. Direktorin und wissenschaftliche Leiterin des DIVSI.



Schlaumacher. Die Mehrheit glaubt, dass Computerspiele förderlich sind.

der Privatsphäre ist aus Elternsicht ein relevantes Risikofeld. Sie befürchten, dass Kinder **im Internet zu viel von sich preisgeben**.

Sicherheitsthemen spielen aus Elternsicht **mit steigendem Alter der Kinder eine immer wichtigere Rolle**. Die Anwendung konkreter Sicherheitsmaßnahmen steigt jedoch nicht proportional dazu an.

Etwas mehr als die Hälfte der Eltern hat Kinder- und Jugendschutzprogramme auf ihren Computern/Laptops installiert.

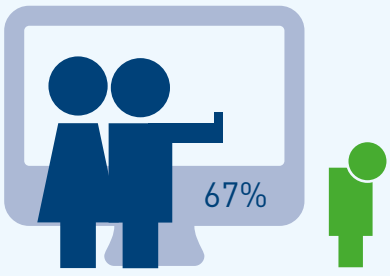
Je ausgeprägter die subjektive Internetkompetenz der Eltern, desto mehr Sicherheitsmaßnahmen werden ergriffen. Dabei nimmt trotz intensiverer Nutzung des Internets und einer zunehmenden Bedeutung von Sicherheitsfragen der Informationsbedarf der Eltern mit steigendem Alter ihrer Kinder nicht zu.

Eltern sehen sich selbst als die Hauptverantwortlichen, wenn es darum geht, Kindern einen kompetenten Umgang mit dem Internet zu vermitteln. Dennoch zeigen sie **Unsicherheiten bei konkreten Herausforderungen** und (Erziehungs-)Entscheidungen im digitalisierten Familienalltag.

Ausgerechnet für die Fähigkeiten, die Eltern als besonders wichtig für den sicheren Umgang ihrer Kinder mit dem Internet einstufen, **schreiben sie sich selbst geringe Kompetenzen zu**. So ist die Fähigkeit, gewalthaltigen und/oder pornografischen Seiten ausweichen zu können, für sie **von enormer Bedeutung**. Gleichzeitig sagt ein Drittel der Eltern, dass es vorkommt, dass ihre Kinder auf solche Inhalte im Internet treffen und durch diese eingeschüchtert werden.

Je ausgeprägter die Risikowahrnehmung der Eltern, desto häufiger wird ein Online-Verbot ausgesprochen. Die Unsicherheiten der Eltern führen vielfach nicht zu verstärkter Informationssuche nach geeigneten Sicherheitsmaßnahmen, sondern **zu einer restriktiven Haltung gegenüber der Internetnutzung**.

Nix Internet. Verbote werden vor allem für die 3-bis 8-Jährigen ausgesprochen.



Segen oder Fluch? Fitnessarmbänder zeichnen alles auf. Wollen wir das?

Digitaler Kodex: Spielregeln für den Einsatz von Big Data

Annäherung an ein komplexes Thema anhand von Smart Health und Smart Mobility.

Dr. Dirk Graudenz

Braucht Deutschland einen Digitalen Kodex?" – das ist die Frage, die DIVSI im April 2013 gestellt und am Ende der ersten Phase eines fundierten Projekts im Mai 2014 nach inhaltlichen Analysen, Expertenkonsultationen und öffentlichen Diskussionsveranstaltungen positiv beantwortet hat. Unter einem „Digitalen Kodex" werden dabei, vereinfacht gesagt, Normen verstanden, an die sich Akteure im Netz halten, ohne dass es dafür staatlicher Sanktionsmechanismen bedarf. In einer zweiten Projektphase wird die Frage nach einem „Digitalen Kodex" nun für das Thema „Big Data" konkretisiert.

Vielfach unbemerkt werden bei fast jeder digitalen Transaktion Daten nicht nur verarbeitet, sondern von großen Plattformanbietern auch gespeichert und im Rahmen ihrer Geschäftsmodelle verwertet. Oftmals lautet der unausgesprochene Deal der Plattformen mit dem Nutzer: „Meine Services kosten nichts, aber dafür überlässt du mir deine Daten." Für den Nutzer ist dabei vielfach nicht transparent, was im Hintergrund abläuft. Suchmaschinen beispielsweise nutzen Suchanfragen, um präzisere Ergebnisse zu liefern, aber auch, um detaillierte Nutzerprofile aufzubauen und dadurch beispielsweise Werbung präziser zu platzieren. Ähnliche Geschäftsmodelle gibt es bei sozialen Netzwerken und vielen anderen Diensten, die sich in den vergangenen Jahren etabliert haben.

Konsequenzen. Kennzeichnend ist für diese Services, dass es sich um „Big Data"-Anwendungen handelt, also exorbitant große Datenmengen genutzt werden. Wertvoll werden die aufgezeichneten Datenbestände insbesondere dadurch, dass die Datensätze zeitlich und nutzerübergreifend miteinander in Beziehung gesetzt werden. Dadurch lassen sich über mathematische Verfahren Erkenntnisse gewinnen, die die Dienstleistungen verbessern, aber gleichzeitig für den einzelnen Nutzer gravierende Konsequenzen haben können. Diese zwei Seiten von Big Data machen eine Regelsetzung schwer – wie sollen die Interessen von Plattformen und Nutzern ausbalanciert werden, wenn ein großer Nutzen, z.B. im Gesundheitsbereich, nur um den Preis einer potenziellen Invasion der Privatsphäre jedes Einzelnen möglich ist? Ein solches Dilemma lässt sich zufriedenstellend nur durch gesellschaftliche Aushandlungsprozesse auflösen. Dafür ist es höchste Zeit, denn Big Data ist bereits in vielen Bereichen Realität und entwickelt sich mit dem für digitale Technologien kennzeichnenden Tempo weiter fort.

Das Thema ist aus Regulierungssicht sehr komplex, weil es Charakteristika besitzt, die durch die bekannten Mechanismen nicht ausreichend eingefangen

werden. Die Herausbildung von Plattformen, die aufgrund von Netzwerkeffekten vielfach Monopole sind, erfolgt erst seit ca. zehn Jahren. In der Regel sind diese Plattformen im außereuropäischen Ausland angesiedelt, was die Einforderung von Standards, die mit europäischen Vorstellungen von Privatsphäre zu vereinbaren sind, schwierig macht. Hinzu kommt, dass sich die Vorstellungen von Privatheit im Laufe der vergangenen Dekaden gewandelt haben. Das aktuelle Datenschutzrecht ist zu Beginn der 80er-Jahre des vergangenen Jahrhunderts entstanden und basiert auf den Grundsätzen der Datenvermeidung und Datensparsamkeit. Das Verhalten der meisten Nutzer von digitalen Technologien im digitalen Raum ist allerdings konträr zu diesen Begriffen. Und Big Data ist, im Kern, die Antithese zur Idee der Datensparsamkeit.

Tracking. Im Projekt zum „Digitalen Kodex" wird Big Data anhand von zwei konkreten Themen erschlossen: Smart Health und Smart Mobility. Beiden Bereichen ist gemeinsam, dass Tracking eine wesentliche Rolle spielt – im Gesundheitsbereich z.B. durch die Aufzeichnung von Daten zu Körperfunktionen wie Bewegungsintensität und Pulsfrequenz über Fitnessarmbänder, im Verkehrsbereich durch die kontinuierliche Verfolgung des Aufenthaltsorts und Daten zur Fahrweise wie z.B. Brems- und Beschleunigungsprozesse. An beiden Beispielen lässt sich leicht dokumentieren, dass es zwischen Chancen und Risiken gesellschaftliche Konfliktlinien gibt, die noch nicht ausreichend konturiert sind.

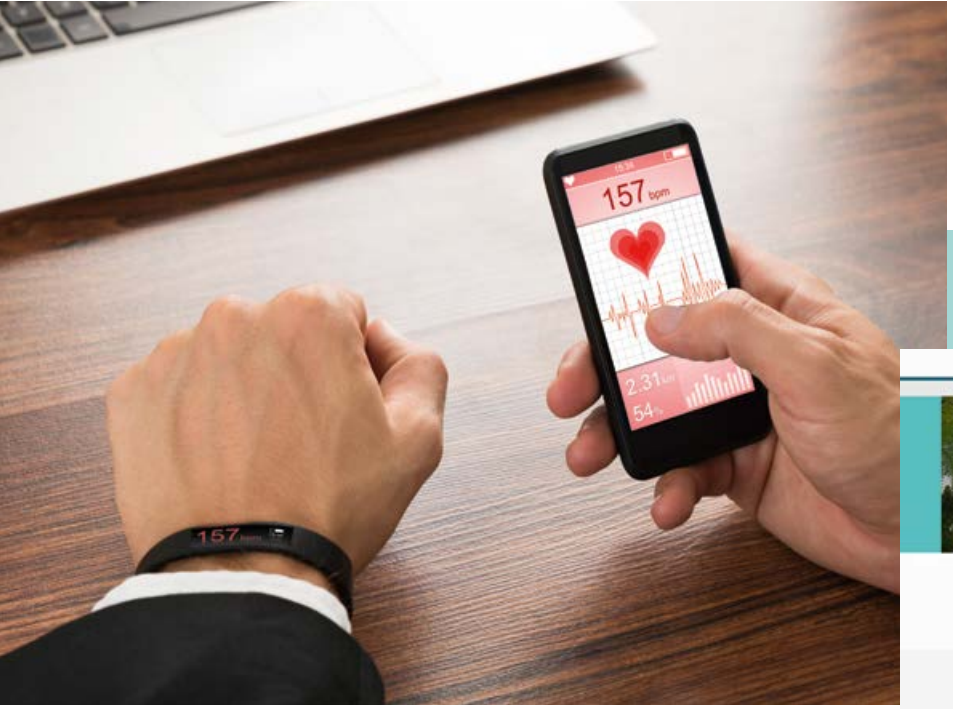
Big Data im Smart-Health-Bereich eröffnet für die Nutzer bzw. auch ihre Ärzte weitreichende Einsichten in ihren Gesundheitszustand. Viele Nutzer ➜

Mahlzeit. **Nährwerte, Kalorien, Menge: alles erfassbar.**

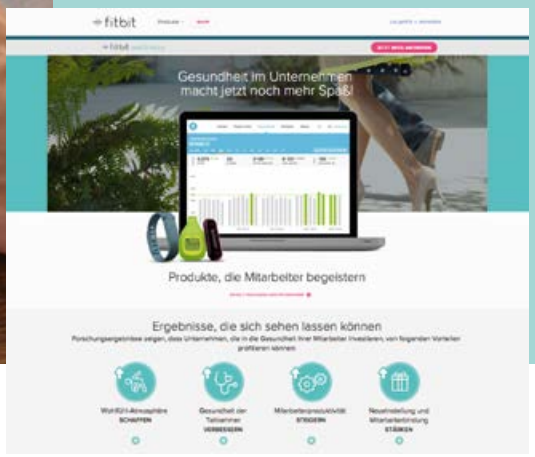
Fotos: venimo – Shutterstock, Jawbone, Anbieter-Websites

> Das aktuelle Datenschutzrecht basiert auf den Grundsätzen der Datenvermeidung und Datensparsamkeit. Big Data ist, im Kern, die Antithese dazu.

Alles im Griff. **Mobile Geräte wissen über ihre Nutzer oft mehr, als die von sich wissen.**



Mitarbeitermotivation. Unternehmen erfassen Gesundheitsinfos – das Fitnessarmband gibt es gratis dazu.



→ von Fitnessarmbändern und Pulsuhren teilen darüber hinaus ihre Errungenschaften im sportlichen Freizeitbereich auf sozialen Netzwerken mit ihren Freunden. Diese Entwicklung kulminiert in der „Quantified Self"-Bewegung, die den Einsatz digitaler Medien zur gesundheitlichen Selbstoptimierung propagiert. Versicherungsunternehmen haben diese Ideen schon weiter gedacht, und einzelne Unternehmen planen Angebote mit speziellen Tarifen, die Kunden, die Fitnessarmbänder tragen und einen gesunden Lebensstil verfolgen, mit Rabatten belohnen. Aus Sicht der Kunden, die sich darauf einlassen, ist das zunächst ein vernünftiges Angebot – ist es nicht mehr als fair, wenn gesundes Verhalten auch finanziell belohnt wird? Konsequent zu Ende gedacht könnte dies allerdings bedeuten, dass es für manche Personen schwieriger werden wird, eine bezahlbare Krankenversicherung abzuschließen – der Punkt, an dem Rabattprogramme in eine Beschädigung des Solidarprinzips übergehen, ist schwer zu bestimmen. Auch im Bereich der Arbeit gibt es Entwicklungen: Manche Unternehmen führen für ihre Mitarbeiter kostenfreie Fitnessarmbänder ein, was in vielen Fällen sicherlich als interessantes Angebot gewertet wird. Denkbar ist aber, dass der soziale Druck, sich selbst zu tracken, dadurch steigt.

Auch im Mobilitätsbereich zeigt sich Tracking von zwei Seiten. Es wird erwartet, dass die moderne urbane Verkehrsinfrastruktur stark davon profitieren würde, wenn die Informationen über die Position von Fahrzeugen zusammengeführt und ausgewertet werden könnten. Einzelne Städte wie z.B. Stockholm haben mit Big-Data-Anwendungen bereits die Verkehrsbelastung verringert, dies insbesondere auch über Verhaltensänderungen bei den Bürgern, denen Verkehrsinformationen und -alternativen auf Basis von Big-Data-Analysen z.B. zur Nutzung des öffentlichen Nahverkehrs in Echtzeit zur Verfügung gestellt werden. Auch in diesem Bereich interessieren sich Versicherungen für Tracking-Daten. Über sogenannte Telematik-Boxen werden Informationen zum Fahrverhalten aufgezeichnet und können zur Anpassung von Versicherungstarifen genutzt werden. Selbst die Uhrzeit und die Fahrstrecke können bei vergrößerter Unfallwahrscheinlichkeit (z.B. bei Nacht- und Stadtfahrten) in die Tarife eingerechnet werden. Auch hier ist der Punkt, an dem sinnvolle Anreize für vernünftiges Verhalten in eine Beschränkung der persönlichen Freiheit umschlagen, schwer zu bestimmen.

Im Projekt werden diese beiden Themen mit einem Zugang über „ausgehandelte Geschichten" verfolgt. Darunter werden konkrete Alltagssituationen verstanden, an denen sich die Konflikte für alle beteiligten Akteure herausarbeiten lassen. Das Ziel ist, zunächst einen Überblick über die gesellschaftlichen Wertentscheidungen zu gewinnen, die dann ggf. in spezifische Digitale Kodizes zu Einzelthemen einfließen könnten. Die ersten Diskussionsrunden mit Experten sind sehr vielversprechend verlaufen, und das Projekt knüpft zurzeit Kontakte zu Akteuren, die im Rahmen eines Konsultationsprozesses eingebunden werden. ⊡

Abgleich. Nichts, was nicht aufgezeichnet werden könnte. Nichts, was unbemerkt bleibt.

INFORMATIONEN ZUM PROJEKT
www.divsi.de/projekte/digitaler-kodex/big-data

Dr. Dirk Graudenz
ist Unternehmensberater zu strategischen Themen im Schnittpunkt von Informationstechnologie und öffentlichem Sektor.

Lage der IT-Sicherheit in Deutschland

Angriffe mit kriminellem Hintergrund sind eine größere Bedrohung als Angriffe mit einem nachrichtendienstlichen Hintergrund.

Michael Hange

Schwarz-Rot-Gold. Deutschland ist beliebtes Ziel von Cyberangriffen. Der Aufwand für Verbrecher ist gering.

Die millionenfachen Identitätsdiebstähle von Bürgern, Meldungen zu Cyberangriffen auf Wirtschaftsunternehmen und nicht zuletzt die Snowden-Enthüllungen haben weit über die Expertenebene hinaus das Bewusstsein der Verletzbarkeit im Cyberraum deutlich gemacht. Insbesondere ist klar geworden, dass alle Gesellschaftsgruppen hiervon betroffen sind.

Im Verständnis der besonderen Dynamik der Cybersicherheit ist es wichtig, zunächst zu beschreiben, von welchen Charakteristika die heutige Informationstechnik geprägt wird:

1. Technologische Durchdringung und Vernetzung: Alle physischen Systeme werden von IT erfasst und schrittweise mit dem Internet verbunden.
2. Komplexität: Die Komplexität der IT nimmt durch vertikale und horizontale Integration in die Wertschöpfungsprozesse erheblich zu.
3. Allgegenwärtigkeit: Jedes System ist praktisch zu jeder Zeit und von jedem Ort über das Internet erreichbar.

Unter den beschriebenen Umständen stoßen altbekannte, konventionelle IT-Sicherheitsmechanismen schnell an ihre Grenzen und vermögen es nicht, Zuverlässigkeit und Beherrschbarkeit in gewohntem Maße zu gewährleisten. Der traditionelle Perimeterschutz in der IT-Sicherheit wird überholt oder gar unwirksam.

Trotz der umfangreichen Herausforderungen für die Cybersicherheit bietet die Digitalisierung ökonomische sowie gesellschaftliche Potenziale, auf die ein hoch entwickeltes Industrieland wie Deutschland nicht verzichten kann.

Gefährdungslage. Neben dem Wissen über Technologie und Technologieentwicklung ist es unerlässlich, die Gefährdungslage zu kennen. Denn technologische Entwicklung und Gefährdungslage hängen zusammen.

Das BSI hat im Dezember 2014 den „Bericht zur Lage der IT-Sicherheit in Deutschland 2014“ herausgegeben, der Auskunft über Ursachen von Cyberangriffen, über Angriffsmittel und -methoden gibt. Eine wesentliche Schlussfolgerung ist: Das Internet ist als Plattform für Angreifer sehr attraktiv. Denn der Aufwand für einen Angriff ist gering, es reichen ein Laptop und ein Internetanschluss aus, um Angriffe zu starten. Zudem existiert ein florierender globaler Markt mit „Trojanerkoffer“ und „Malware-as-a-Service“-Angeboten, die es auch technischen Laien ermöglichen, Cyberangriffe durchzuführen. Das Entdeckungsrisiko ist gering, da das dezentral und offen gestaltete Internet für den Angreifer vielfältige Tarnmöglichkeiten bietet. Außerdem erweitert sich die Masse der möglichen Angriffsziele mit der fortlaufenden technologischen Entwicklung. Ein weiterer Grund für die Attraktivität des Internets als Angriffsplattform ist die Tatsache, dass Schwachstellen in Software systemimmanent sind. Sie sind der häufigste Ausgangspunkt für die Entwicklung von Cyberangriffsmitteln in Form von Schadprogrammen.

Neben den bekannten und weitverbreiteten Angriffsmethoden wie beispiels- →

> Altbekannte, konventionelle Sicherheitsmechanismen stoßen schnell an ihre Grenzen.

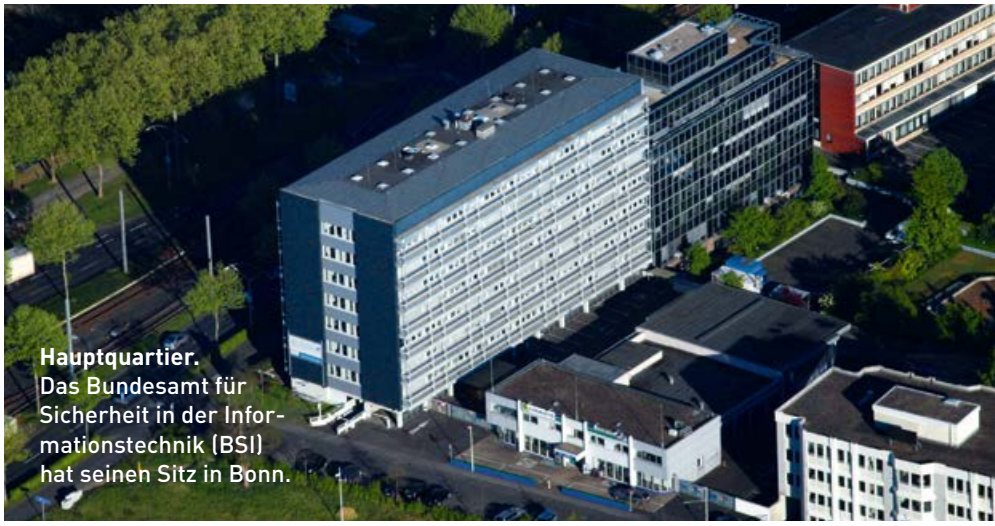
Fotos: Anbieter-Websites, Jawbone, DIVSI, venimo/Vorobyeva – Shutterstock

➜ weise Spam, Schadsoftware oder Drive-by-Exploits sind Advanced Persistent Threats (APT) von besonderer Bedeutung. Dies sind hochwertige „Premiumangriffe", die schwer detektierbar sind. APT-Angriffe zeichnen sich durch sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten aufseiten der Angreifer aus.

In der Angreifer-Typologie ist zwischen Cyberkriminellen und Cyberangriffen durch Nachrichtendienste zu differenzieren. Cyberkriminelle nutzen die gesamte Bandbreite der Cyberangriffsmethoden – meist nicht gezielt und auf den schnellen finanziellen Gewinn ausgerichtet. Nachrichtendienste arbeiten dagegen langfristiger und setzen Cyberangriffe gezielter ein, wobei hochwertigere Angriffsmethoden genutzt werden, um unter anderem das Entdeckungsrisiko zu minimieren.

Es ist festzuhalten, dass die Masse der Angriffe mit kriminellem Hintergrund heute die größere Bedrohung für Bürger und Wirtschaft darstellt als Angriffe mit nachrichtendienstlichem Hintergrund.

Man ist diesen Entwicklungen jedoch nicht schutzlos ausgeliefert. Anwender können sich relativ gut gegen gängige Breitenangriffe aus dem Bereich Cyber Crime schützen, indem sie zumindest die vom BSI empfohlenen Mindestmaßnahmen umsetzen. Ausnahmen bestehen jedoch für spionagegefährdete Bereiche wie Rüstung und potenziell auch für Betreiber kritischer Infrastrukturen.



Hauptquartier. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat seinen Sitz in Bonn.

Die Prognose sieht wie folgt aus: Es werden insbesondere der Diebstahl von digitalen Identitäten von Bürgern und APT-Angriffe auf Unternehmen und Behörden in Qualität und Quantität zunehmen.

Lösungsansätze. Grundvoraussetzungen für erfolgreiche Lösungsansätze sind folgende drei Aspekte:

1. Nationale Initiativen, die Kompetenz, Lösungsorientierung, Kooperation und Transparenz in der Cybersicherheit erhalten bzw. etablieren.
2. Sicherheitsmaßnahmen müssen skalierbar sein, da unterschiedliche Zielgruppen verschiedene Schutzbedürfnisse haben. Sicherheitsmaßnahmen werden nur in der Breite angewandt, wenn Aufwand und Nutzen angemessen in Einklang stehen.
3. Erfolgsmodelle anderer Staaten sind zu beleuchten. Politische, rechtliche und wirtschaftliche Rahmenbedingungen sind jedoch bei der Frage der Übertragbarkeit zu beachten.

Voraussetzung für die Gewährleistung von Informationssicherheit sind zudem effektive und vertrauenswürdige Sicherheitsme-

NEWS

Medienkompetenz in Schulen fördern

Berlin – So wollen Bundestagsabgeordnete künftig mithelfen.

Rund 120 Bundestagsabgeordnete wollen sich nachdrücklich für mehr Medienkompetenz in deutschen Schulen einsetzen. Sie unterstützen die Initiative „erlebe IT" des Branchenverbandes BITKOM und haben dafür jeweils eine Schirmherrschaft in ihrem Wahlkreis übernommen. Dabei wollen die Abgeordneten Schulen besuchen, um mit den Schülern sowie Eltern und Lehrern über den Umgang mit digitalen Medien zu diskutieren. Geplant sind ergänzend dazu Workshops rund um die sichere Nutzung des Internets sowie

Zukunft. IT an Schulen stärken.

verantwortungsbewusstes Verhalten in sozialen Netzwerken. Außerdem sollen auch Fragen wie Urheberrecht und Datenschutz im Netz angesprochen werden.

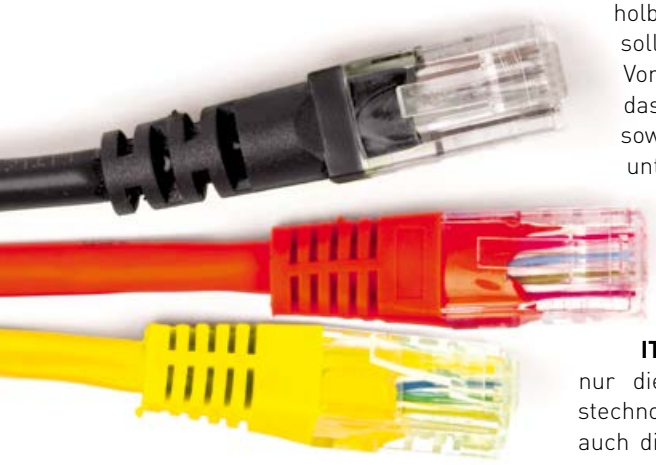
BITKOM-Vizepräsident Achim Berg zu der Aktion: „Umfragen von uns haben gezeigt, dass sich die große Mehrheit der Schüler wünscht, Themen der digitalen Welt im Unterricht ausführlicher zu behandeln. Wir wollen mit der Initiative die Schulen dabei unterstützen, diese Medienkompetenz zu vermitteln."

Deutschlandweit pflegt BITKOM die Zusammenarbeit mit rund 800 Schulen. Neben dem Angebot zur Steigerung der Medienkompetenz führt die Initiative „erlebe IT" an Schulen auch Schnupperkurse zum Programmieren sowie Informationsveranstaltungen zur Berufsorientierung durch.

chanismen auf technischer Ebene. Denn Manipulationen an IT-Komponenten können auch mit einem hohen Prüfaufwand nicht vollständig ausgeschlossen werden.

Vor dem Hintergrund der Gefährdungslage und der Grundvoraussetzungen für erfolgreiche Lösungsansätze sind die drei Bereiche Kryptosicherheit, Cybersicherheit und IT-Sicherheitsmanagement von besonderer Bedeutung.

Kryptosicherheit. Die mathematische Kryptografie ist hinsichtlich der Algorithmen stabil. Zudem gibt es in Deutschland leistungsstarke Anbieter von Kryptographie. Unsicherheitsfaktoren sind die Schlüsselversorgung und die Implementierung, die von vertrauenswürdigen Herstellern bzw. Dienstleistern erfolgen sollte.



Eine Herausforderung ist die Nachfrage und hier insbesondere die Nutzerakzeptanz von Verschlüsselungsverfahren. Auch nach den Snowden-Enthüllungen wollen ca. 75 Prozent der Nutzer ihre E-Mails nicht verschlüsseln, ca. 20 Prozent sind prinzipiell bereit, fühlen sich aber nicht kompetent genug. Lediglich 5 Prozent der Anwender nutzen Ende-zu-Ende-Verschlüsselungsverfahren.

Um mehr Verschlüsselung zu erreichen, bedarf es einer Förderung des Angebots sowohl von Ende-zu-Ende-Verschlüsselungsverfahren wie auch von Transportverschlüsselung durch Provider, aber auch durch Wirtschaft und Staat.

Cybersicherheit. In den Bereichen Cybersicherheitsprodukte und IT-Sicherheitsdienstleister besteht national Nachholbedarf. Mit der Digitalen Agenda soll diese Lücke geschlossen werden. Voraussetzung hierfür ist aber auch, dass Wissenschaft und Hersteller sowie Verwaltung und Wirtschaftsunternehmen kooperieren, sodass in Deutschland ein nachhaltiger Markt für qualifizierte Produkte und Dienstleistungen entsteht und sich weiterentwickelt.

IT-Sicherheitsmanagement. Nicht nur die Verbesserung der Sicherheitstechnologie ist von Bedeutung, sondern auch die Qualifikation und das Management von IT-Sicherheit in den Unternehmen selbst.

Fazit. Die Digitalisierung und zunehmende Vernetzung ist von Wert und bringt viele Vorteile mit sich. Die mit ihr einhergehenden Gefährdungen sind einer ständigen Bewertung zu unterziehen, und das Risikomanagement ist fortlaufend anzupassen. Zielsetzung unserer Anstrengungen muss sein, Kompetenz, Lösungsorientierung, Kooperation und Transparenz im Handeln zu schaffen.

Das Internet der 90er-Jahre als reiner virtueller Erlebnisraum existiert nicht mehr. Die Kriminalität mit geringer Aufklärungsquote und das breite Betätigungsfeld von Nachrichtendiensten mit dem Ziel der Spionage und in militärischer Perspektive der Sabotage nehmen das Internet auch für ihre Zwecke ein. Um den Mehrwert des Cyberraums zu erhalten, muss die Cybersicherheit hinreichendes Vertrauen gewährleisten können. Um zu einer leistungsfähigen Cybersicherheit zu gelangen, bedarf es der engen Zusammenarbeit zwischen Staat, Wirtschaft und Wissenschaft.

Michael Hange
ist seit 2009 Präsident des BSI. Davor war der studierte Mathematiker ab 1994 Vizepräsident der Behörde.

NEWS

Telefonaktion: DIVSI-Experten halfen weiter

Düsseldorf – Bei der „Rheinischen Post" ging es um „Sicherheit im Internet".

Für Fragen rund um das Thema Sicherheit im Internet standen Matthias Kammer und Joanna Schmölz, unterstützt von Dr. Silke Borgstedt (SINUS) sowie Social-Media-Experte Alexander Braun, in einer Telefonaktion Lesern der „Rheinischen Post" zur Verfügung.

Angesprochen wurde dabei ein weitgefächertes Themenfeld: Wie sollte ein sicheres Passwort aussehen? Wie schütze ich meinen Computer am besten vor Viren? Kann man Mails auch als Privatperson verschlüsseln? Wie verhindert

Sicherheit. Das DIVSI-Team wusste Rat.

man, dass die eigenen Kinder Opfer von Internetkriminalität oder Cybermobbing werden? Wie viele Stunden sollten Kinder generell online sein dürfen? DIVSI-Direktor Matthias Kammer: „Der Kern mancher Fragen macht bei solchen Aktionen immer wieder deutlich, wie wichtig grundlegende Aufklärungsarbeit ist. Viele Nutzer sind offensichtlich verunsichert. Wir freuen uns, insoweit Hilfe leisten zu können."

Einer der wichtigsten Tipps, der mehrfach nach entsprechender Frage gegeben wurde: „Verdächtige Mails am besten ungeöffnet löschen! Ganz wichtig dabei: Öffnen Sie keine angehängten Dateien, weil diese oft Schadprogramme oder Viren enthalten." Auch das Thema „Kinder und Jugendliche im Netz" fand reges Interesse.

Bringschuld der Polizei: Vertrauen schaffen durch Aufklärung

Hohe Erwartungshaltungen an Integrität und Korrektheit des Handelns sind berechtigt.

Holger Münch

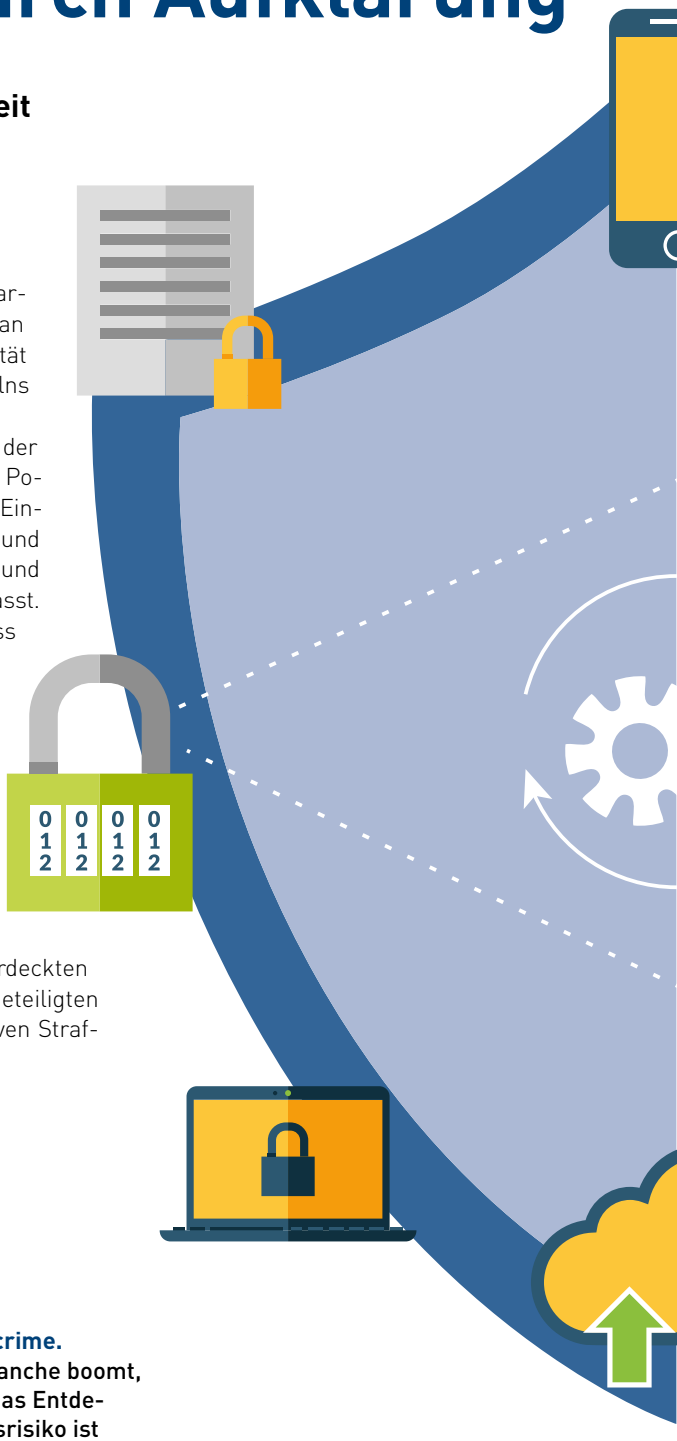
Vertrauen ist eine „Hypothese künftigen Verhaltens", die sicher genug sein muss, um darauf eigene Bewertungen und Einschätzungen aufzubauen. Vertrauen ist somit immer auch ein „Vertrauensvorschuss", der im Wesentlichen an drei Erwartungen geknüpft ist: Kompetenz, Integrität und Wohlwollen des Gegenübers. Je geringer der Einblick in das Tun des Gegenübers ist, desto höher muss das Vertrauen in seine Kompetenzen sein.

Damit die Bürger der Polizei vertrauen, muss diese als kompetent, integer und grundsätzlich gutwillig wahrgenommen werden. Vertrauen in die Polizei begründet sich in der Wahrnehmung der Professionalität und Ausgewogenheit polizeilicher Maßnahmen.

Das Besondere an der Polizeiarbeit, gegenüber den von der Bevölkerung ebenfalls als sehr vertrauenswürdig eingestuften Hilfeberufen wie Feuerwehr oder Rettungsdienst, ist, dass es sich bei der Polizeiarbeit um Eingriffsverwaltung handelt. Zu Recht sind die Erwartungshaltungen des Bürgers an polizeiliche Arbeit, an die Integrität und die Korrektheit des Handelns damit besonders hoch.

Um das hohe Vertrauen der Bevölkerung zu wahren, hat die Polizei in den letzten Jahrzehnten Einsatzstrategien verändert, Aus- und Fortbildung professionalisiert und Organisationsstrukturen angepasst. Polizeibeamte lernen heute, dass Kommunikation und Deeskalation zentrale Handlungselemente sind.

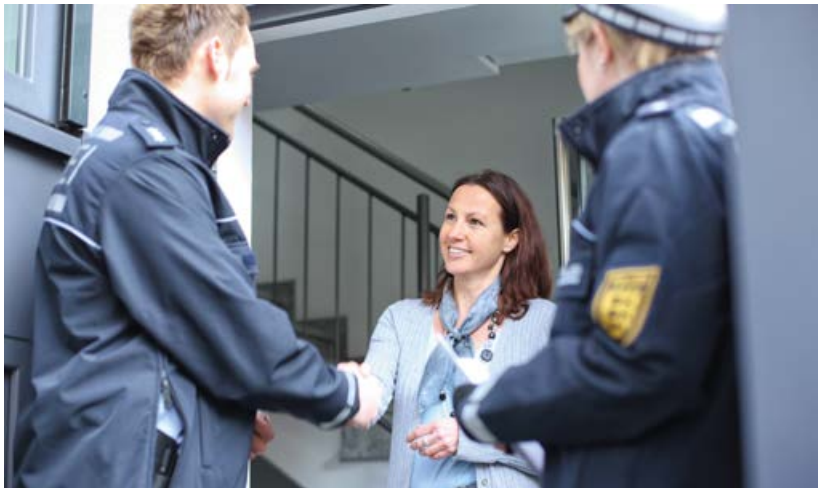
Undercover. Von besonderer Bedeutung ist das Vertrauen in die polizeiliche Arbeit, wenn polizeiliches Handeln nicht beobachtbar und nicht einschätzbar ist. Dies ist zum Beispiel bei verdeckten Maßnahmen zum Schutz der Beteiligten und zur Sicherung einer effektiven Straf-

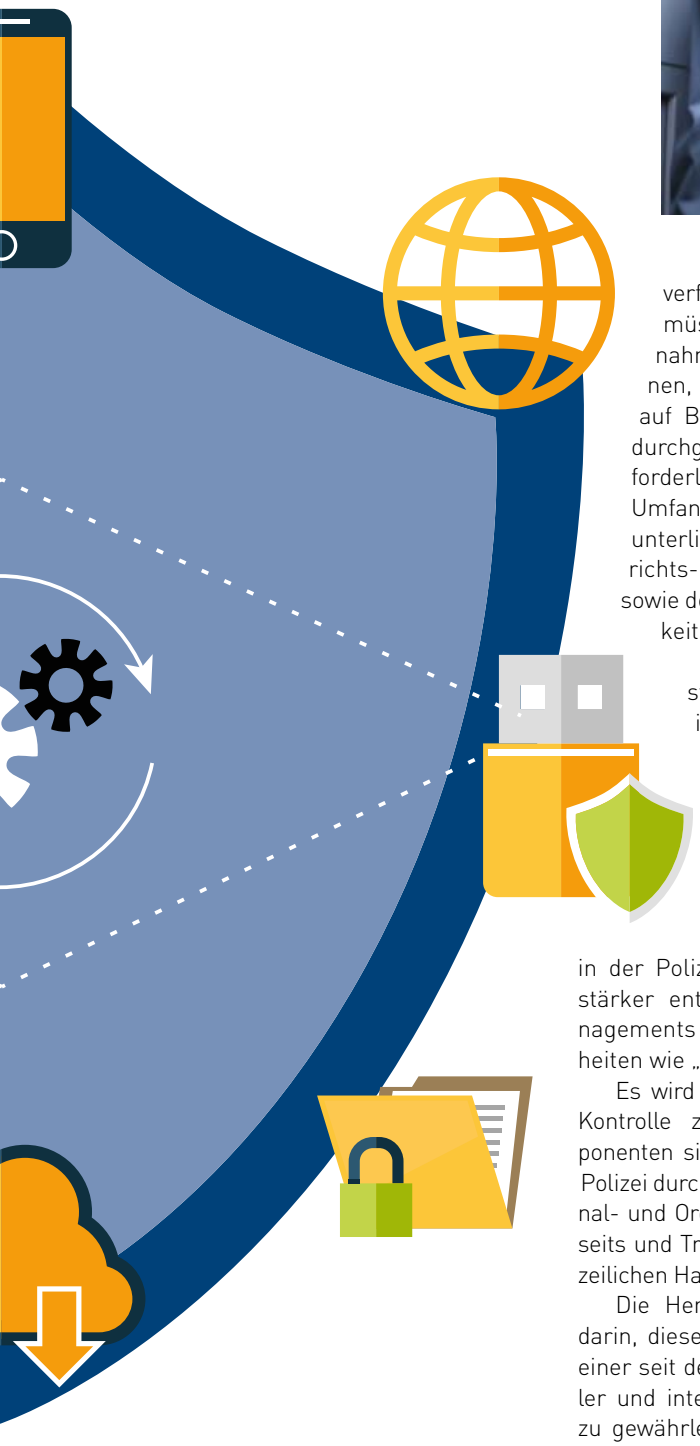


Cybercrime.
Die Branche boomt, denn das Entdeckungsrisiko ist nur gering.

Fotos: Macrovector/Smart Design/stockhits – Shutterstock, Polizeiliche Kriminalprävention der Länder und des Bundes

Kommunikation. Der direkte Kontakt mit dem Bürger gewinnt für die Polizei zunehmend größere Bedeutung.





verfolgung der Fall. Die Bürger müssen sich bei solchen Maßnahmen darauf verlassen können, dass polizeiliche Eingriffe nur auf Basis gesetzlicher Befugnisse durchgeführt werden und nur im erforderlichen und verhältnismäßigen Umfang. Polizeiliche Maßnahmen unterliegen deshalb zu Recht Berichts- und Dokumentationspflichten sowie der Kontrolle und Überprüfbarkeit durch Justiz und Parlament.

Polizeiliche Maßnahmen stehen darüber hinaus unter intensiver Beobachtung der Medien, was für das Vertrauen in die Institution Polizei ein ganz wesentlicher Baustein ist.

Balance. Ein weiteres Element ist die Selbstkontrolle in der Polizei in Form des sich immer stärker entwickelnden Beschwerdemanagements oder der Organisationseinheiten wie „interne Ermittlungen".

Es wird deutlich, dass Vertrauen und Kontrolle zwei gleichberechtigte Komponenten sind und dass Vertrauen in die Polizei durch die Balance zwischen Personal- und Organisationsentwicklung einerseits und Transparenz und Kontrolle polizeilichen Handelns andererseits entsteht.

Die Herausforderung besteht heute darin, diese Balance auch in Zukunft, in einer seit den 90er-Jahren immer digitaler und internationaler werdenden Welt, zu gewährleisten. Seit dem Fall der der Globalisierung entgegenstehenden Grenzen am 9. November 1989 ist eine vernetzte Welt mit World Wide Web und ständiger mobiler Erreichbarkeit entstanden.

Kriminelle Netze. Diese neue, vernetzte Welt bringt viele Vorteile für z.B. Wissenschaft und Wirtschaft. So können Produktions- und Steuerungsabläufe heute grenzübergreifend gestaltet werden, Forschungszentren und Computerexperten global kooperieren.

Auf der anderen Seite vernetzen sich heute aber auch Kriminelle und nutzen die digitalen Möglichkeiten, um Straftaten zu begehen. Das Entdeckungsrisiko für diese „Cyberkriminellen" ist sehr gering, was darauf zurückzuführen ist, dass die Ermittlungsfähigkeiten der Polizei in der digitalen Welt noch wenig ausgebildet sind.

Ein Problem stellt die Flüchtigkeit der Daten dar. Insbesondere dynamische IP-Adressen lassen sich nur sehr kurz zurückverfolgen, weshalb Täter und auch Opfer nur in einem kurzen Zeitfenster feststellbar sind. Eine weitere Schwierigkeit ist die zunehmende Verschlüsselung der Kommunikation. Die großen Konzerne sorgen sich um das Vertrauen ihrer Kunden und setzen immer häufiger Technik ein, die auch für die Polizei nicht zu entschlüsseln ist. Schließlich führen Datenmassen in Bereichen wie der Kinderpornografie zu hohem Arbeitsaufwand bei der Auswertung, die die Polizei an Ihre Kapazitätsgrenzen bringt.

Kommunikation zu erkennen und auszuwerten, Täter zu ermitteln und beweiskräftig zu überführen, wird damit immer aufwendiger bei gleichzeitig sinkender →

Bundestag. Werden bei den laufenden Diskussionen zur Vorratsdatenspeicherung polizeiliche Interessen sinnvoll beachtet?

→ Erfolgswahrscheinlichkeit. Der Polizei fehlt damit immer häufiger ein wichtiger Ermittlungsansatz. Zeitgleich nehmen die internationalen Bezüge stetig zu und sorgen somit für zusätzliche Komplexität in der polizeilichen Arbeit.

Diesen neuen Herausforderungen kann nur mit einem umfassenden Maßnahmenpaket begegnet werden.

Bündelung. Ein Baustein in diesem Paket ist die Vernetzung. Insofern stellt die Herausforderung gleichzeitig die Lösung dar: Kräfte im Bund und zwischen Bund und Ländern müssen weiter gebündelt werden. Zudem muss die polizeiliche Zusammenarbeit in Europa und weltweit weiter intensiviert werden.

Die Polizeiarbeit muss darüber hinaus an die neuen Gegebenheiten und Phänomene angepasst werden. Polizei muss aktiv und genauso effektiv Gefahrenabwehr und Prävention in der digitalen wie in der analogen Welt sicherstellen.

Dabei dürfen wir die bekannten und bewährten Elemente von Transparenz und Kontrolle in der digitalen Welt nicht vernachlässigen. Diskussionen wie die zu Mindestspeicherfristen geben Grund zur Sorgen, dass die Sicherheitsorgane von Teilen der Gesellschaft als Bedrohung und nicht als Verbündete zum Schutz ihrer Daten empfunden werden. Kritiker sehen die gerechte Balance zwischen Freiheit und Sicherheit, zwischen Abwehrrechten und Schutzpflichten in Gefahr. Zudem klingt aus dem verwendeten Vokabular Misstrauen. „Datensammelwut", nicht „Rückgriff auf Daten bei schwerster Kriminalität"; „Vorratsdatenspeicherung", nicht „Mindestspeicherfristen". Das Aberwitzige bei dieser Diskussion ist, dass die geäußerten Befürchtungen der Entwicklung der tatsächlichen Möglichkeiten der Polizei diametral entgegenstehen. Daher bedarf es der Überprüfung und Weiterentwicklung des Rechts und der polizeilichen Instrumente, um den digitalen und internationalen Herausforderungen mit wirksamer Gefahrenabwehr und Strafverfolgung begegnen zu können.

Hierbei ist darauf zu achten, dass die rechtsstaatlichen Prinzipien für die Bürger nachvollziehbar in der digitalen Welt angewendet werden. Zudem ist wichtig, dass sich die Polizei klar von den Methoden einiger internationaler Geheimdienste und von der Datensammelwut mancher großer internationaler Konzerne abgrenzen.

Transparenz. Die Unwissenheit und Skepsis der Bürger, die sich in Diskussionen wie der zu Mindestspeicherfristen zeigt, zieht außerdem eine Bringschuld der Polizei nach sich, polizeiliche Maßnahmen zu erläutern und so Vertrauen zu schaffen. Diese Bringschuld kann man besonders gut am Verhältnis von Transparenz und Vertrauen, welche sich komplementär zueinander verhalten, veranschaulichen.

„Vertrauen ist nicht das Ergebnis, sondern die Alternative zu Transparenz", sagt der Sozialwissenschaftler Vincent Rzepka. Und weiter: „Dabei ist Vertrauen ein risikobehaftetes Unterfangen: Wer vertraut, kann eben nicht über alles informiert sein, sondern legt seine Zukunft zu einem gewissen Grad blind in die Hand von Menschen und Mechanismen. […] Letztlich ist die Aufgabe dann aber nicht, auf Transparenz oder Vertrauen zu setzen. Vielmehr wäre es notwendig, darüber zu diskutieren, in welchem Mischungsverhältnis beide zukünftig stehen können und sollen. Bei jeder konkreten Entscheidung wäre zu hinterfragen, welche Auswirkungen das eine oder andere hat." Somit ist es Aufgabe der Polizei, Verlässlichkeit und Überprüfbarkeit in der digitalen Welt durch Kommunikation zu gewährleisten.

Lebenswirklichkeit. Zusammenfassend bleibt festzuhalten, dass das BKA und die Polizeien in Deutschland ein Programm der Personal- und Organisationsentwicklung 2.0 mit den Schwerpunkten Cyberfähigkeit, nationale und internationale Zusammenarbeit und Kompetenzbündelung umsetzen müssen. Gleichzeitig müssen die polizeilichen Instrumente an die neue Lebenswirklichkeit unter Wahrung rechtsstaatlicher Prinzipien und unter Betonung der Verlässlichkeit und Überprüfbarkeit polizeilichen Handelns angepasst werden.

Beide Entwicklungsstränge sind wichtig, damit das hohe Vertrauen in die Polizei im demokratischen Rechtsstaat erhalten bleibt, weil sie kompetent und integer ist und man sich auf die Korrektheit ihres Handelns verlassen kann. ⊡

Holger Münch
ist seit Dezember 2014 Präsident des BKA. Davor war er zuletzt Staatsrat beim Senator für Inneres und Sport der Freien und Hansestadt Bremen.

Aktuelle Bücher

Überleben in der Informationsflut

So behalten Sie die Kommunikation im Griff

Sigrid Hess

Die Menge an Informationen im Alltag wächst stetig. Kein Wunder, dass immer mehr den Überblick und die Orientierung verlieren. Die Autorin beschreibt Lösungen für dieses Dilemma. Sie erklärt, wie man die Datenflut clever filtert, mit einzelnen Office-Programmen produktiv umgeht und wie der überquellende E-Mail-Account der Vergangenheit angehört. Für alle, die unter den täglichen Informationsmengen leiden und sich den Herausforderungen rationell und professionell stellen und endlich wieder »Herr« ihrer Arbeit werden möchten.

Redline Verlag, ISBN: 978-3-86881-573-3; 19,99 €

IT-Governance in Staat und Kommunen

Vernetzung, Zusammenarbeit und Steuerung von Veränderungsprozessen in der öffentlichen Informationstechnik

Andreas Engel (Hg.)

Beleuchtet werden aus wissenschaftlicher und praktischer Perspektive die Veränderungen, die sich für IT-Governance und die Rolle des CIOs in der Verwaltung ergeben.

Edition Sigma, ISBN: 978-3-89404-846-4; 17,90 €

Abgehängt

Wo bleibt der Mensch, wenn Computer entscheiden?

Nicholas Carr

Computer übernehmen immer anspruchsvollere Aufgaben – und machen uns Menschen zu manipulierbaren Statisten. Längst verrichten Computer und computergesteuerte Maschinen nicht mehr nur stupide Arbeiten, sondern werden für hochkomplexe Tätigkeiten eingesetzt.

Hanser Verlag, ISBN: 978-3-446-44032-6; 19,90 €

Leadership in der digitalen Welt

Peter Paschek

Band 3 in der Reihe „DIVSI-Perspektiven". Es geht um das zukünftige Vertrauen in diejenigen, die den Weg in die digitale Gesellschaft maßgeblich bestimmen. Der Autor nimmt Unternehmensführung und gesellschaftliche Verantwortung unter die Lupe und beleuchtet auch, wo auf diesem Weg das Menschliche bleibt.

Nomos, ISBN:978-3-8487-2060-6; 24,- €

Wenn Träume erwachsen werden

Ein Blick auf das digitale Zeitalter

Jaron Lanier

Mit Kreativität und visionärem Blick, der sich aus dem Wissen um Chancen und Fluch der neuen Technologien speist, denkt Lanier diese in die Zukunft weiter. Seine Forschungen und Entdeckungen hat er von Beginn an mit Essays begleitet, in denen er seine Errungenschaft in ihren Implikationen für die Gesellschaft überprüft.

Hoffmann und Campe, ISBN: 978-3-455-50359-3; 25,00 €

DIVSI Veröffentlichungen

Studien

Milieu-Studie zu Vertrauen und Sicherheit im Internet, 2012
Meinungsführer-Studie: Wer gestaltet das Internet?, 2012
Entscheider-Studie zu Vertrauen und Sicherheit im Internet, 2013
Freiheit versus Regulierung im Internet, 2013
U25-Studie – Kinder, Jugendliche und junge Erwachsene in der digitalen Welt, 2014
DIVSI Studie zu Bereichen und Formen der Beteiligung im Internet, 2014
Braucht Deutschland einen Digitalen Kodex? – Verantwortung, Plattformen und soziale Normen im Internet, 2014
DIVSI Studie – Wissenswertes über den Umgang mit Smartphones, 2014
DIVSI Studie – Daten: Ware und Währung, 2014
U9-Studie: Kinder in der digitalen Welt, 2015
DIVSI Studie – Beteiligung im Internet: Wer beteiligt sich wie?, 2015

Reden

Roman Herzog: Internet und Menschenwürde, 2013
Olaf Scholz: Braucht das Internet Vertrauen?, 2013

Diskussionsbeiträge

Dominic Völz, Timm Christian Janda: Thesen zur Netzpolitik – Ein Überblick, 2013
Christina Heckersbruch, Ayten Öksüz, Nicolai Walter, Jörg Becker, Guido Hertel: Vertrauen und Risiko in einer digitalen Welt, 2013
Göttrik Wewer: Digitale Agenda 2013 – 2017 – Netzpolitik im neuen Deutschen Bundestag, 2013
Miriam Meckel, Christian Fieseler, Jan Gerlach: Der Diskurs zur Netzneutralität, 2013
Timm Christian Janda, Dominic Völz: Netzpolitik in Deutschland – Wahlprogramme, Koalitionsvereinbarung, Regierungserklärung, 2014
Manuel Schubert: Vertrauensmessung in der digitalen Welt – Überblick und Aussicht, 2014
Max-Otto Baumann: Privatsphäre als neues digitales Menschenrecht?, 2015

DIVSI
Deutsches Institut für Vertrauen und Sicherheit im Internet