Deutsches Institut für Vertrauen und Sicherheit im Internet

DIVSI magazin

MÄRZ 2014

Kinder, Jugendliche und junge Erwachsene in der digitalen Welt

DIVSI U25-Studie sorgt für neue Blickwinkel

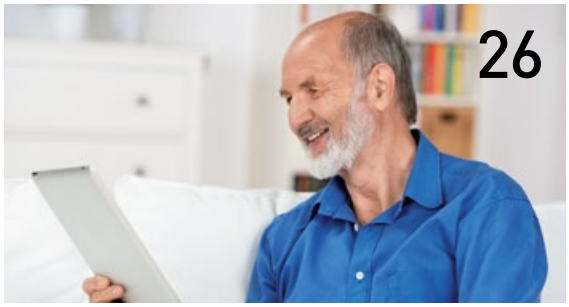
Online ist Normalität, Offline ein Ausnahmezustand

Aktuelles Projekt angelaufen

Digitale Souveränität – Wo steht Deutschland, wo wollen wir hin?

Fortentwicklung der Thesen

Basis der DIVSI-Arbeit – Keine Änderungen am Mission Statement



Inhalt

3 Editorial

4 Fünf Thesen: Basis der DIVSI-Arbeit
Keine Änderungen am Mission Statement des Instituts

6 DIVSI U25-Studie – Mit Express-Tempo in die digitale Welt
Untersuchung zeigt: 98 Prozent der 14- bis 24-Jährigen sind online

SCHWERPUNKT „DIGITALE SOUVERÄNITÄT“

12 Bedroht und bereits verletzt
Der Blick auf den Status quo. Eine Bestandsaufnahme

16 Ich bin ein Amerikaner
Das Internet ist eine US-Einrichtung

20 Welche Spielregeln sollen künftig gelten?
Wir brauchen internationale Vereinbarungen, um die Netz-Möglichkeiten besser ausbalancieren zu können

24 Staat 4.0 – Revolution von innen als Weg in die Zukunft
Akteure der Konsumgesellschaft haben die „Herrschaft“ übernommen

26 Senioren ins Internet!
Erfolgreiche Initiative der Stiftung Digitale Chancen

27 Aktuelle Bücher
Hauptvorschlag: Die Berechnung der Welt (Klaus Mainzer)

Impressum

Herausgeber:
Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI)
Matthias Kammer, Direktor
Mittelweg 14
20148 Hamburg

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

Autoren:
Meike Demattio, Lutz Diwell, Dr. Dirk Graudenz, Matthias Kammer, Harald Lemke, Dr. Göttrik Wewer

Realisierung:
Lohrengel Mediendesign
Schulterblatt 58
20357 Hamburg

Verbreitete Auflage:
ca. 7.000 Exemplare, Abgabe kostenlos

Titel: ra2studio – Shutterstock

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

Im Fokus: Wort des Jahres 2014, Neun- bis 24-Jährige und aufpolierte Thesen

Die Groko (Wort des Jahres 2013) steht im Stresstest (Wort des Jahres 2011). Rettungsroutine (Wort des Jahres 2012) wird kaum reichen, um das Schlagwort Digitale Souveränität (Wort des Jahres 2014?) so mit Inhalt zu erfüllen, dass die Bürger nicht zum Wutbürger (Wort des Jahres 2010) werden. Man sieht: Altbekannte Begriffe lassen sich durchaus mit brandaktuellen Eisen verquicken. Das DIVSImagazin hat den Komplex „Digitale Souveränität" bereits thematisiert. Diskutiert wird darüber mittlerweile vielerorts. Leider keineswegs immer der Sache dienlich.

Getreu seinem „Mission Statement" (s. S. 4/5) versucht DIVSI, die Zeit der Plattitüden auf diesem Feld zu beenden. In Expertenrunden wird ausgelotet, 1) wo Deutschland steht, 2) warum unser Land steht, wo es steht, und 3) ob es sinnvoll ist, dort zu stehen (ab S. 12).

Während die Auslotungen zur Digitalen Souveränität gerade richtig angelaufen sind, ist eine andere Aktion abgeschlossen. Die „DIVSI U25-Studie – Kinder, Jugendliche und junge Erwachsene in der digitalen Welt" wurde offiziell vorgestellt. Bislang fehlte es an einer fundierten Untersuchung mit Neun- bis 24-Jährigen im Fokus. Die Studien von DIVSI genießen mittlerweile in der Öffentlichkeit und in der Fachwelt hohen Stellenwert. Internetaffine Fragen werden hier auf wissenschaftlicher Basis untersucht und seriös präsentiert. Mit oft überraschenden Detail-Ergebnissen. Die U25-Studie setzt ein weiteres Ausrufungszeichen (ab S. 6).

Anders als bei der jüngeren Generation sind bei den Senioren wenige mit den Möglichkeiten des Netzes vertraut. Die Stiftung Digitale Chancen ist mit einer beachtenswerten Aktion dabei, dieses zu ändern. Wir sagen, wer ab wann und wie dabei einsteigen kann (S. 26).

Zum Start vor rund drei Jahren hat sich DIVSI Thesen gegeben, die als felsenfeste Basis für die gesamte Arbeit gedient haben. Schwierige Frage: Darf man an solchen Pfeilern rütteln? Die Diskussionen über das Für und Wider sind jetzt abgeschlossen. Sie münden in fünf Thesen – nicht grundlegend neu und doch im Detail leicht anders. DIVSI-Schirmherr Prof. Dr. Roman Herzog war eng in die jeweiligen Abstimmungsschleifen involviert (ab S. 4).

So viel zu den aktuellen Themen. Abschließend ganz was anderes. Die Auffrischung eines Magazins ist für Redaktion und Grafik ein schmaler Pfad. Subjektiv zu bewertende Geschmacksfragen lassen sich nämlich unter keinem Blickwinkel einfach nach richtig oder falsch einsortieren. Fest steht nur, was am Ende das Ergebnis sein muss: Der Leser soll möglichst wenig merken. Oder eben doch. Dann aber nur unterschwellig: Irgendwie ist was passiert – oder nicht? Wir haben es riskiert. Mit Beginn 2014 wurde das DIVSImagazin aufgepeppt. Ein paar Glättungen hier, eine Handvoll neuer Feinheiten dort. Wenn Ihnen am Ende – auf der ebenfalls umgestalteten Bücherseite – trotzdem alles vorkommt wie immer – nur frischer –, hat die Grafik einen hervorragenden Job abgeliefert.

Ich wünsche Ihnen informative Unterhaltung mit unseren Themen, erstmals präsentiert im neuen Gewand.

Jürgen Selonke
Chefredakteur, DIVSImagazin

Fünf Thesen: Basis der DIVSI-Arbeit

Keine Änderungen am Mission Statement des Instituts.

Matthias Kammer

Kann man Thesen, die einmal festgeschrieben und unabdingbare Arbeitsgrundlage sind, ändern? Darf man das überhaupt? Oder kann es Anlässe geben, in denen dies vielleicht sogar notwendig wird?

DIVSI-Schirmherr Prof. Dr. Roman Herzog, der Beirat – Prof. Dr. Claudia Eckert (TU München und Fraunhofer AISEC München, als Vorsitzende), Prof. Dr. Miriam Meckel (Universität St. Gallen), Thomas Götzfried (Vorsitzender des Aufsichtsrats Götzfried AG), Harald Lemke (Sonderbeauftragter für E-Government und E-Justice bei der Deutschen Post) sowie Dr. Bernhard Rohleder (Hauptgeschäftsführer BITKOM) – und alle anderen Verantwortlichen des Instituts haben sich in der jüngsten Vergangenheit mit Fragen dieser Art intensiv und durchaus kontrovers beschäftigt. Dabei war der frühere Bundespräsident eng in die notwendigen Abstimmungsschleifen eingebunden.

Der letztlich gefundene und verabschiedete Konsens hat nicht zu neuen Thesen geführt, wohl aber zu einer Fortentwicklung der bisherigen Richtlinien. Damit trägt das Deutsche Institut für Vertrauen und Sicherheit im Internet rund drei Jahre nach der Gründung in der Formulierung seiner Thesen einer fortgeschrittenen gesellschaftlichen und technischen Entwicklung Rechnung.

Besonders auch die Aktualisierung der vierten These macht deutlich, dass vorsichtige Anpassungen allein schon durch laufende Arbeiten notwendig werden können. Die Rede ist dort von auszuhandelnden „Grundregeln für den Umgang miteinander im Internet". Auf Anregung seines Schirmherrn ist DIVSI dabei, die Frage nach einem solchen „digitalen Kodex" zu beantworten. Roman Herzog glaubt, dass wir „digitale Leitplanken" benötigen, um in der weiten Welt des Netzes nicht unterzugehen. Hier könnte ein solcher digitaler Kodex helfen.

Das in den aktualisierten Thesen genannte Zusammenwirken von Nutzer, Wirtschaft und Staat war bereits Joachim Gauck, bis zur Wahl zum Bundespräsidenten erster DIVSI-Schirmherr, ein Anliegen. Er formulierte, dass diese drei

Mission Statement

Das Deutsche Institut für Vertrauen und Sicherheit im Internet ...

- bietet als unabhängige und gemeinnützige Einrichtung eine Plattform für einen offenen und transparenten Dialog zu Vertrauen und Sicherheit im Internet – über Parteien und Interessengruppen hinweg und national wie international.
- arbeitet interdisziplinär und fördert den Austausch zwischen Wissenschaft und Praxis, Wirtschaft und Politik, Anbietern und Nutzern.
- unterstützt Wissenschaft und Forschung und will so mithelfen, Chancen und potenzielle Risiken im Netz zu untersuchen und zu analysieren.
- sorgt durch Aufklärungsarbeit für eine Sensibilisierung der Nutzer zur Steigerung von Vertrauen und Sicherheit im Internet.
- stellt seine Arbeitsergebnisse öffentlich und zugänglich für alle zur Verfügung.

Jürgen Gerdes informierte 2011 über die DIVSI-Gründung.

Gruppierungen gemeinsam „verantwortlich für Schutz und Gestaltung unserer Zukunft mit dem Internet" seien.

Das ist der DIVSI-Auftrag. Auch der eigentliche Anlass für die Gründung des DIVSI ist unverändert geblieben, seit Jürgen Gerdes, Vorstand Brief der Deutsche Post AG, das Institut im Rahmen der CeBIT 2011 vorgestellt hat. Er formulierte bereits bei der Vorstellung unserer ersten Studie so: „Um zu beurteilen, was tatsächlich im Netz passiert, (...) dazu braucht es mehr an Zahlen, Daten und Fakten. Was wir brauchen, ist eine Art Landkarte der Strukturen im Netz, damit wir künftig zeigen können, welche Pfade sicher sind. Solche Landkarten im Web zu erstellen, die Wege darin zu erforschen und daraus neue Erkenntnisse über das Netz zu erzielen, (...) das ist der Auftrag (...) für DIVSI."

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

WEITERE INFORMATIONEN
divsi.de/ueber-uns/das-institut

Experten-Know-how. Bundespräsident a.D. Prof. Dr. Roman Herzog bringt seit November 2012 sein Wissen und seine Erfahrung in die DIVSI-Arbeit ein. Parallel zur Übernahme seiner Schirmherrschaft wurde auch der Beirat institutionalisiert. Vorsitzende ist Prof. Dr. Claudia Eckert (linke Seite, Mitte). Weiter gehören diesem Gremium an: Prof. Dr. Miriam Meckel sowie Thomas Götzfried, Harald Lemke und Dr. Bernhard Rohleder (unten, v.l.n.r.).

Die 5 DIVSI-Thesen in ihrer neuen Form

1 Das Internet ist eine Kulturleistung der Menschheit von historischer Bedeutung. Es revolutioniert unsere Arbeit und die Freizeit, unser Denken und die Kommunikation. Deshalb geht das Internet uns alle an – ob wir es schon nutzen oder (noch) nicht.

2 Sicherheit und Stabilität der Internet-Infrastruktur – beides ist unabdingbar. Sie ist zu einem elementaren Bestandteil des gesamten Wirtschafts- und Sozialraums geworden.

3 Das Internet bietet Möglichkeiten zur Beteiligung an der Gestaltung von Staat und Gesellschaft. Es fördert Wohlstand, Bildung, Chancengerechtigkeit und Informationsfreiheit. Seine enorme gestalterische Kraft braucht jedoch das Vertrauen der Menschen, damit sie sich entfalten kann.

4 Nutzer, Wirtschaft und Staat haben eine gemeinsame Pflicht, Grundregeln für den Umgang miteinander im Internet auszuhandeln und für deren Verbindlichkeit zu sorgen. Dabei sind Wirtschaft und Staat gefordert, die Nutzer in die Lage zu versetzen, dieser Verantwortung gerecht zu werden.

5 Freiheit und Sicherheit sind Grundbedürfnisse – auch im Internet. Voraussetzung dafür ist das Vertrauen darauf, dass der Staat und alle anderen Internet-Akteure diese Grundbedürfnisse mit geeigneten Maßnahmen angemessen ausbalancieren.

Fotos: DPDHL, DIVSI

Mit Express-Tempo in die digitale Welt

- **98 Prozent der 14- bis 24-Jährigen sind online**
- **Schluss mit dem Mythos von Freundesinflation**
- **Neue Definition schützenswerter privater Daten**

Meike Demattio

Welche Rolle spielt das Internet im Alltag junger Menschen? Wer ist im Internet ein „Freund"? Was bedeutet Vertrauen im Internet für sie? Die „DIVSI U25-Studie – Kinder, Jugendliche und junge Erwachsene in der digitalen Welt" gibt erstmals umfassende Antworten in den relevanten Themenkomplexen. Eine wichtige Untersuchung, denn in den nächsten Jahren werden vor allem die heute Neun- bis 24-Jährigen wesentlich mitbestimmen, was im Hinblick auf Handeln im Internet zum Allgemeingut wird.

Die DIVSI Milieu-Studie zu „Vertrauen und Sicherheit im Internet" zeigte digitale Gräben in der deutschen Gesellschaft auf: Für manche Menschen ist das Internet eine fremde Welt, manche tasten sich gerade vorsichtig in sie hinein, und eine dritte Gruppe ist so selbstverständlich online, dass sie sich kaum vorstellen kann, wie jemand ohne Internet leben kann.

Wird innerhalb der Gesamtbevölkerung nun nur die Gruppe der 14- bis 24-Jährigen betrachtet, wird deutlich: Digitale Gräben sind kaum mehr auszumachen. Nur zwei Prozent nutzen das Internet gar nicht. In der Gesamtbevölkerung finden sich zum Vergleich 19 Prozent Offliner.

Dennoch bedeutet „online sein" nicht für alle der jungen Befragten das Gleiche. Vielmehr existiert eine Vielzahl unterschiedlicher Einstellungen nebeneinander. Die Differenzierungen zeigen sich weniger in der Breite der genutzten Online-Angebote, in der Dauer des täglichen Online-Seins oder der Art und Weise des Zugangs zum Internet. Sie werden vielmehr in einer Positionierung zu netzrelevanten Themen und Fragen deutlich. Bedeutsam sind auch Unterschiede in der subjektiven Souveränität bei der Nutzung verschiedener Netzangebote. Es sind also zwar (fast) alle online, dieser Status sagt jedoch kaum etwas über die Haltung und Beziehung zum Internet aus.

Die aktivsten „Onliner" mit einer selbstverständlichen und intensiven Internet-Nutzung finden sich in den Milieus der Souveränen, Pragmatischen und Unbekümmerten. Zusammengenommen stellen diese drei U25-Internet-Milieus die deutliche Mehrheit dar. Diejenigen →

#INTERNET UND ZUKUNFT

„Internet muss jeder!"

♀ 18- bis 24-jährig

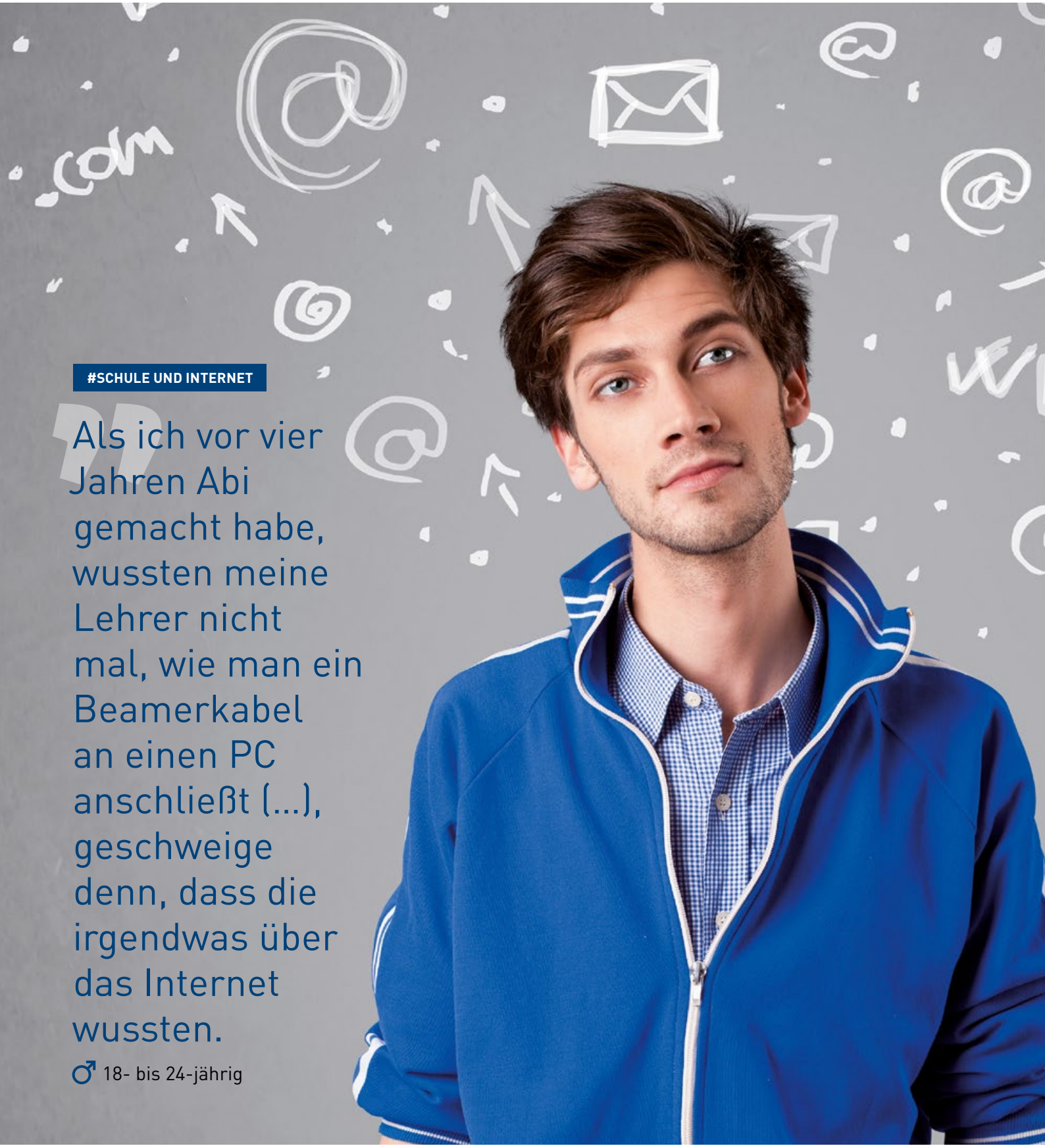
Gesagt ist gesagt. Bestandteil der Studie sind auch Zitate aus den verschiedenen Altersgruppen. Eine subjektive Auswahl finden Sie hier und auf den folgenden Seiten.

Foto: ra2studio – Shutterstock

#FREUNDE

„Ein Freund bei Facebook ist noch lang' nicht ein echter Freund…

♀ 14- bis 17-jährig



#SCHULE UND INTERNET

„Als ich vor vier Jahren Abi gemacht habe, wussten meine Lehrer nicht mal, wie man ein Beamerkabel an einen PC anschließt (...), geschweige denn, dass die irgendwas über das Internet wussten.

♂ 18- bis 24-jährig

Die sieben Milieus auf einen Blick

Die Grafik zeigt eine Projektion der Typen auf das Bezugssystem der Sinus-Milieus mit den beiden Hauptachsen Grundorientierung (horizontal) und Bildung (vertikal). Die sieben Typen sind entsprechend ihrem jeweiligen dominanten Milieu-Hintergrund positioniert. Je höher eine Gruppe in der Grafik angesiedelt ist, desto gehobener ist die Bildung; je weiter rechts sie sich erstreckt, desto moderner im soziokulturellen Sinn ist die Grundorientierung.

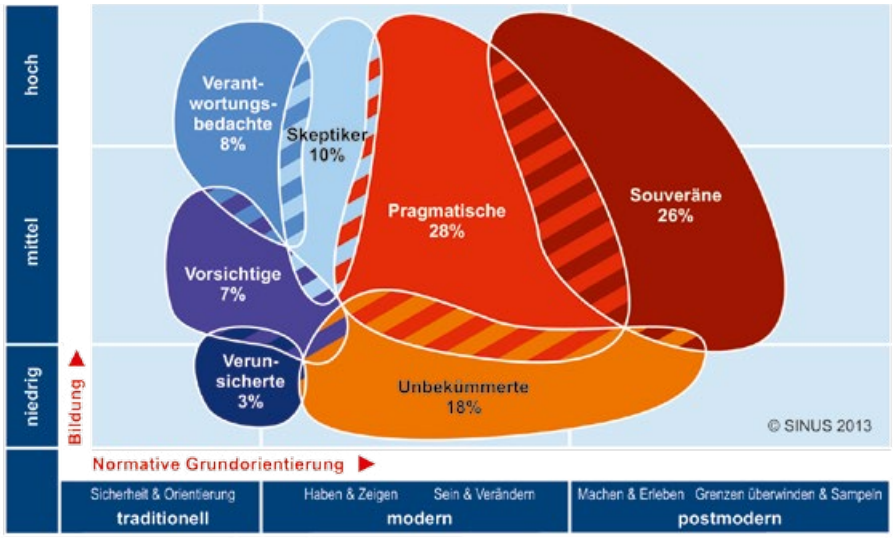


Foto: ra2studio – Shutterstock

→ Jugendlichen und jungen Erwachsenen, die eher selektiv und bewusst bis hin zu zurückhaltend oder auch verunsichert mit dem Internet umgehen, bilden die Milieus der Skeptiker, der Verantwortungsbedachten, der Vorsichtigen und der Verunsicherten.

Die DIVSI U25-Studie liefert neben einer differenzierten Landschaft der jungen Netzkulturen auch darüber hinaus gehende wertvolle Erkenntnisse zu verschiedenen Schlagworten.

Beispiel „Freundschaft". Seit Facebook wird das Wort „Freund" inflationär genutzt. Als Ergebnis der Studie ist jedoch zu erkennen, dass die Befragten in dieser Hinsicht fein unterscheiden: Facebook-Freunde, Bekannte, enge Freunde. Die Bezeichnung „Freund" ist zu einem multidimensionalen Begriff geworden, mit dessen unterschiedlichen Bedeutungen sicher hantiert wird. Unverändert macht Freundschaft mehr aus als gegenseitig gezeigte Profile in Online-Communitys. Auch heute geht es um geteilte Werte, Ansichten und Interessen und die Sicherheit, sich aufeinander verlassen zu können. Bei der Betrachtung der Anzahl von „Freunden" im Netz gegenüber engen Freunden zeigen sich klare Abstufungen:

- In der Gruppe zwischen neun und 13 Jahren werden durchschnittlich 57 Online-Freundschaften genannt. Etwa jeder Sechste gehört dabei zum tatsächlichen, engsten Freundeskreis.
- Die zweite Phase (ab 14 Jahren) ist gekennzeichnet durch offensives Netzwerken und ein Gefundenwerden-Wollen. Die Zahl der Freunde gilt als Indikator für Beliebtheit. Bei im Schnitt 163 Online-Freundschaften zählen aber nur etwa elf als enge Freunde. →

#KOMMUNIKATION

Ganz schlimm! Ich finde das so krass im Internet, wie sich da die Menschen auf einmal trauen, Dinge zu sagen, die sie sonst einem nie persönlich ins Gesicht sagen würden.

♀ 14- bis 17-jährig

#DOWNLOADS

Diese Tauschportale nutze ich gar nicht. Da habe ich Angst vor, dass die Polizei mich damit irgendwie verfolgt.

♂ 18- bis 24-jährig

#FACEBOOK

> Wenn ich Schluss habe, gehe ich nach Hause, geh' erst einmal auf Facebook, zocke eine Runde, danach treffe ich mich mit Freunden, und am Abend gucke ich, was ich für die Schule aufhabe, dann guck' ich fern und geh' pennen.
>
> ♂ 9- bis 13-jährig

- Phase drei (nach Schulzeit-Ende/ Beginn des Studiums) bedeutet moderates Netzwerken. Die Zahl der Facebook-Freunde vergrößert sich vor allem durch neue Bezugsgruppen mit Eintritt in ein neues Umfeld und neue Lebensabschnitte. Bei durchschnittlich 175 Online-Freunden bezeichnen junge Erwachsene jedoch nur etwa neun als enge Freunde.

Beispiel „Privatsphäre". Erkennbar ist ein neues Verständnis von Privatsphäre. Als schützenswert gelten vor allem Informationen, welche die soziale Reputation potenziell gefährden können. Klassische personenbezogene Daten dagegen werden als weniger schützenswert betrachtet.

Ein gewisses Maß an Offenheit in Online-Communitys wird als Muss angesehen. Für 50 Prozent der Jugendlichen hat bei Facebook nichts verloren, wer nichts von sich preisgibt. Gleichzeitig werden dort selten intime Gespräche geführt oder ernste Themen besprochen. Über 90 Prozent sprechen über private Dinge lieber persönlich.

Online und offline verschwimmen. Das Internet wird mit zunehmendem Alter immer unentbehrlicher. Während 22 Prozent der neun- bis 13-Jährigen täglich das Internet nutzen, sind es bei den 14- bis 17-Jährigen bereits 67 Prozent und bei den 18- bis 24-Jährigen 72 Prozent.

Das Aufkommen von mobilen internetfähigen Geräten hat dabei das Online-Sein vollkommen neu in den Alltag der Nutzer integriert. Das Smartphone ist zum ständigen Begleiter geworden. Es ist Weg-Navigator, Organisationswerkzeug, Unterhaltungsmedium und Kommunikationsstandleitung zu den Freunden in einem. Dagegen wird deutlich weniger Zeit an Laptops oder stationären Computern verbracht.

Im subjektiven Empfinden der Befragten sind die Grenzen zwischen Online- und Offline-Zeiten fließend. Offline zu sein ist vielmehr ein Ausnahmezustand – eine Notsituation.

Die Untersuchung zeigt: Digitale Medien und „Online-Sein" sind heute im Alltag von Kindern, Jugendlichen und jungen Erwachsenen fest verankert. Wird im öffentlichen Diskurs jedoch pauschal von „der" Internet-Nutzung „der" jungen Menschen gesprochen, verschleiert dies den Blick auf die unterschiedlichen digitalen Lebenswelten und Denkmuster. Es gilt, die unterschiedlichen Einstellungen, Nutzungsweisen und Bedürfnisse der jungen Menschen im Internet in den Blick zu nehmen, um mit Ihnen in eine aussichtsreiche digitale Zukunft zu gehen.

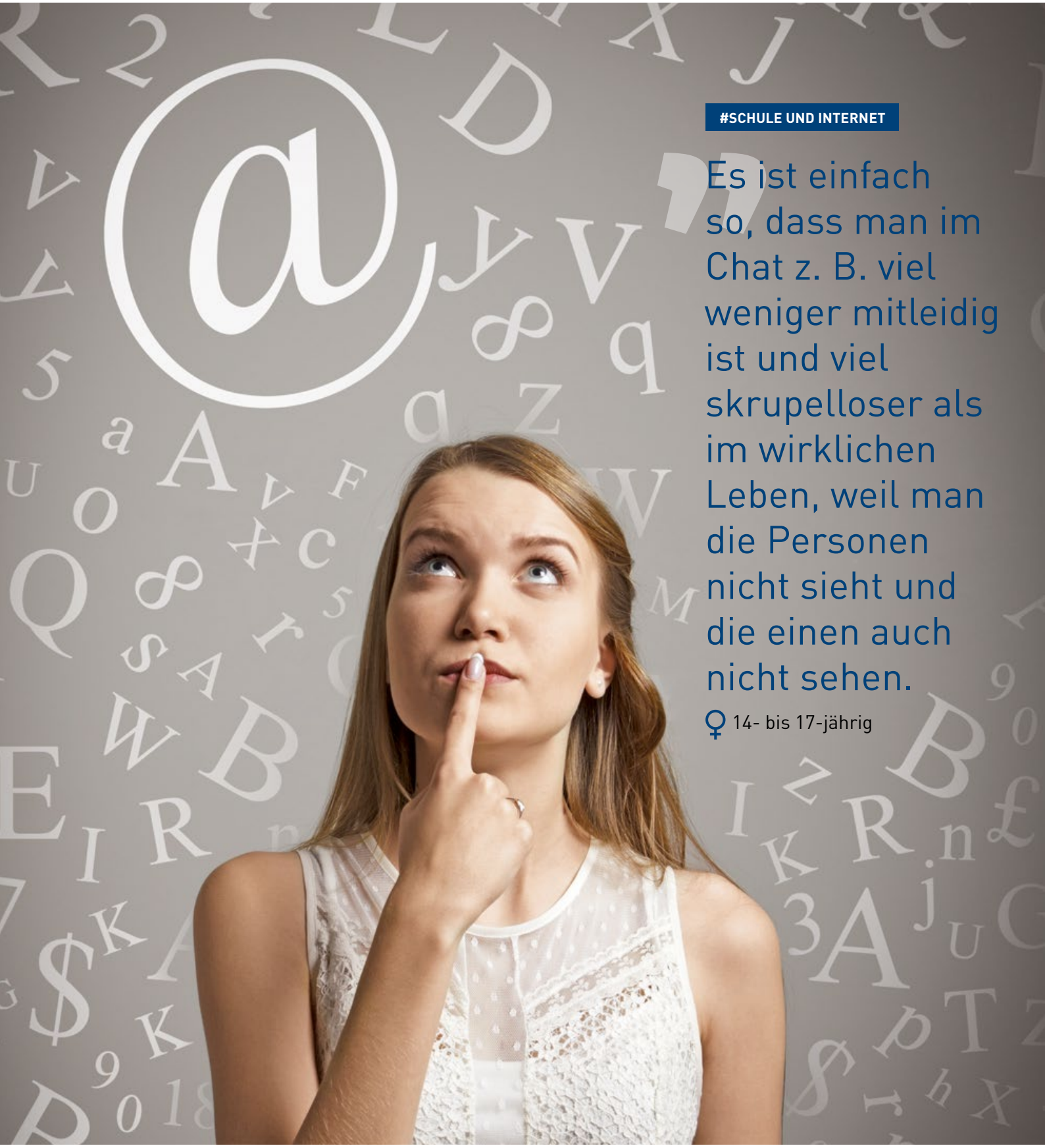
Meike Demattio
ist Projektleiterin bei DIVSI, verantwortet diverse Studienprojekte des Instituts.

WEITERE INFORMATIONEN
divsi.de/publikationen/studien

#INTERNET UND FAMILIENROUTINE

> Wir haben neuerdings ein Smiley-System angefangen. Das heißt, wenn ich irgendwas Haushaltsmäßiges mache, kriege ich einen Smiley. Und diesen Smiley kann ich dann für andere Aktionen eintauschen wie Computer oder Fernsehen.
>
> ♂ 9- bis 13-jährig

Foto: Marijus Auruskevicius – Shutterstock



#SCHULE UND INTERNET

„Es ist einfach so, dass man im Chat z. B. viel weniger mitleidig ist und viel skrupelloser als im wirklichen Leben, weil man die Personen nicht sieht und die einen auch nicht sehen.“

♀ 14- bis 17-jährig

Bedroht und bereits verletzt

Der Blick auf den Status quo. Zehn Punkte, die uns alle zum Nachdenken anregen sollten. Das Fazit: Es wird höchste Zeit, Lösungen zu finden.

Dr. Dirk Graudenz

Kampfzeit. Knipsen neue Größen der alten Welt die digitalen Lichter aus?

Digitale Kommunikation besitzt eine hohe gesellschaftliche, wirtschaftliche und staatliche Bedeutung, und digitale Kommunikationsnetze sind in einigen Bereichen bereits eine kritische Infrastruktur geworden. Von dieser Infrastruktur hängt die vertrauliche Kommunikation in Politik und Verwaltung ab. Ganze Wertschöpfungsketten und Geschäftsmodelle der Wirtschaft beruhen auf ihr, und für private Nutzer ist das Internet ein Raum, in dem sie persönliche Informationen mit Freunden und Familie teilen.

Der langfristige Nutzen der digitalen Infrastruktur und der darauf etablierten Dienste und Plattformen wie E-Mail, soziale Netzwerke und Onlinehandel beruht auf ihrer technischen Zuverlässigkeit und Sicherheit sowie auf dem Vertrauen, das man ihr entgegenbringt. Ein erheblicher Anteil der übertragenen Informationen ist vertraulich, weil sie z.B. aus personenbezogenen oder aus aus wirtschaftlichen Gründen geheim zu haltenden Daten bestehen.

Unbestreitbar ist digitale Kommunikation in entwickelten Industriegesellschaften einer der wichtigsten und nicht mehr wegzudenkenden Treiber für wirtschaftlichen Wohlstand, gesellschaftliche Entwicklung und politische Partizipation. Das Internet ist, als Ganzes gedacht, in seiner Gesamtheit von Netzwerkinfrastrukturen, Kommunikationsprotokollen, Governance-Verflechtungen, Plattformen, Geschäftsmodellen und wirtschaftlichen, politischen und persönlichen Diskursen vermutlich die komplexeste und ökonomisch wertvollste Kulturleistung der Menschheit.

> Im Kern bedeutet Souveränität für einen Akteur, dass er Alternativen hat und sich frei entscheiden kann.

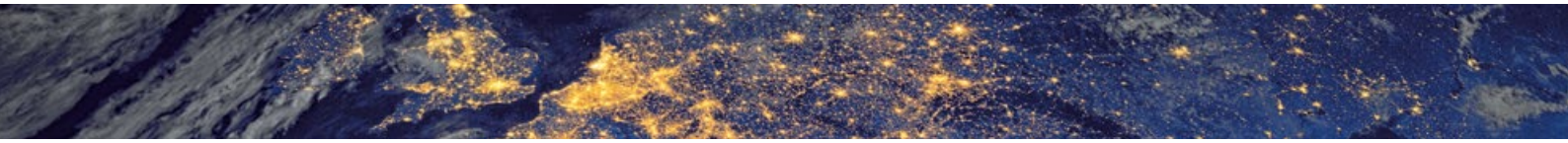
Digitale Kommunikation ist aber nur ein Beispiel für Informationstechnik, die als Schlüsselindustrie des 21. Jahrhunderts gilt. Begriffe wie das „Internet der Dinge" und „Industrie 4.0" deuten an, dass Information den virtuellen Raum verlässt und die physische Welt erobern wird. Fast kein Bereich des modernen Lebens wird sich der Durchdringung mit IT entziehen können.

Es ist also geboten, dass Deutschland und die EU auf diesem Gebiet souverän sind. Souveränität ist ein vielschichtiger Begriff. Mit „Digitaler Souveränität" ist hier die Fähigkeit zur Selbstbestimmung im digitalen Raum gemeint – dies schließt jede Form von digitaler Kommunikation und Datenverarbeitung ein, von digitalen Kommunikationsnetzwerken über zentrale und dezentrale IT-Systeme bis hin zu industriellen IT-basierten Steuerungen und eingebetteten Systemen. Im Kern bedeutet Souveränität für einen Akteur, dass er Alternativen hat und sich frei entscheiden kann. Souveränität hat eine hohe Bedeutung, da sie eine Voraussetzung für einen handlungsfähigen Staat, eine starke Volkswirtschaft und die Demokratie ist, die zusammen wiederum Freiheit, Wohlstand und eine funktionierende Bürgergesellschaft begründen.

In Deutschland und in der EU ist die Digitale Souveränität bedroht und in einigen wichtigen Bereichen bereits verletzt. Was bedeutet dies im Einzelnen?

1 | Vertrauliche Informationen, durch Geheimdienste beschafft, können staatliche Positionen schwächen und dadurch Abhängigkeiten schaffen. In Verhandlungssituationen (Beispiel: die aktuellen Verhandlungen zum Freihandelsabkommen zwischen den USA und der EU) kann eine Kenntnis von Standpunkten, Verhandlungspositionen und -strategien erhebliche Konsequenzen haben. Auch das Handeln der eigenen Geheimdienste kann so kompromittiert werden. →

Foto: MarcelClemens – Shutterstock



2 Das Fehlen von inländischen oder europäischen Anbietern kritischer Technik (z.B. Netzwerk-Hardware und Server-/Storage-Komponenten) schafft für den Staat Abhängigkeiten – wer stellt sicher, dass in importierten und in Rechenzentren des öffentlichen Sektors eingesetzten IT-Systemen oder IT-Komponenten keine „Backdoors" vorhanden sind?

Auch für die Hightech-Industrie ist dies eine Gefahr. Durch die Abhängigkeit von ausländischen, insbesondere außereuropäischen Zulieferern können Risiken entstehen bzw. sind diese bereits entstanden. Im Nicht-IT-Bereich ist eine ähnliche Gefahr bereits deutlich geworden, als China den Export der für Hochtechnologie notwendigen Seltenen Erden eingeschränkt hat.

3 Unternehmen sind durch Wirtschaftsspionage verletzbar, sowohl von staatlicher Seite als auch durch kriminelle Hacker, wodurch direkte Konsequenzen für den Unternehmenserfolg drohen. Dies ist insbesondere für solche Unternehmen relevant, die einen hohen Innovationsgrad besitzen und im globalen Wettbewerb stehen.

4 Von ausländischen, oft monopolistischen Internetunternehmen geht eine vielfache Bedrohung der Digitalen Souveränität aus. Durch eine geschickte Wahl des Ortes des Firmensitzes in der EU können über „regulatorische Arbitrage" unterschiedliche fiskalische und rechtliche Regime gegeneinander ausgespielt werden, um den steuerlichen Gestaltungsspielraum zu vergrößern und Datenschutz nur auf geringem Niveau erfüllen zu müssen. Für Internet-Nutzer ist der Umgang dieser Unternehmen mit persönlichen Daten potenziell hochgradig kritisch, da sie in vielen Fällen die Kontrolle über ihre Daten verlieren.

In einigen Nutzungsszenarien gelangen sogar persönliche Daten von Personen, die den Service gar nicht nutzen, in die Hand dieser Unternehmen, da die digitalen Adressbücher anderer Nutzer in toto auf diese Plattformen hochgeladen werden.

Im Umkehrschluss können inländische Unternehmen aufgrund des regulatorischen Umfelds gegenüber der globalen Konkurrenz benachteiligt sein – sowohl fiskalisch und datenschutzrechtlich, aber insbesondere auch kartellrechtlich. Unternehmen, die aus kartellrechtlichen Gründen in ihrem Heimatmarkt beschränkt sind, haben u.U. nicht die ausreichende Größe, um global wettbewerbsfähig zu sein.

5 Da es sich bei Internet-Plattformen um privatrechtlich organisierte und nicht öffentliche Räume handelt, können beispielsweise auch Inhalte zensiert werden. Die entsprechenden Regeln orientieren sich häufig an der Kultur des Landes, in dem der jeweilige Anbieter der Plattform seinen Sitz bzw. seinen Ursprung hat – Fälle bei den einschlägigen sozialen Netzwerken sind wohlbekannt.

6 Das Wissen um ständige Überwachung kann zur Folge haben, dass Internet-Nutzer im vorauseilenden Gehorsam ihr Verhalten ändern. In Bezug auf das Internet wird dieses Phänomen auch das Panopticon-Prinzip genannt.

Das Panopticon, eine Erfindung von Jeremy Bentham, ist eine Konstruktion für ein Gefängnis, bei dem die Wärter von einem zentralen Turm aus alle Zellen und Trakte im Blick haben. Auf die Gefangenen wird so ein ständiger Überwachungsdruck ausgeübt, der zu regelkonformem Verhalten führt, auch wenn die Gefangenen nicht dauerhaft überwacht werden – die Ungewissheit darüber genügt. Im Vergleich zu einem Panopticon ist die Überwachung im Internet aber u.U. tatsächlich dauerhaft.

7 Bürger vertrauen auf den Staat, dass er sie gegen Bedrohungen von innen und von außen schützt, im Gegenzug besitzt der Staat das Gewaltmonopol. Die Akzeptanz des Gewaltmonopols ist nur bei Einhaltung dieser Verpflichtung denkbar. Nichthandeln des Staates kann so zu einer Vertrauenskrise in Bezug auf staatliche Institutionen führen.

8 Deutschland und die EU haben nur wenig Einfluss bei der Internet-Governance. Eine wesentliche Ressource, das Domain Name System (DNS), steht über die ICANN („Internet Corporation for Assigned Names and Numbers") unter

Wirtschaftsspionage. Die Hightech-Industrie ist durch Abhängigkeit von außereuropäischen Zulieferern hoch gefährdet.

der Kontrolle des US-amerikanischen Department of Commerce. Damit sind beispielsweise Änderungen, die Top Level Domains betreffen, nur mit amerikanischer Zustimmung möglich.

9 Auch Cyberterroristen bedrohen die staatliche Souveränität, da sie kritische Infrastrukturen der Daseinsvorsorge, z.B. Elektrizitäts- und Kommunikationsnetze, angreifen und sabotieren könnten. Diese Bedrohung gilt auch für Infrastrukturen und Produktionsanlagen der Wirtschaft, beispielsweise durch Eingriffe in SCADA-Systeme*.

10 Schließlich bedrohen Internet-Kriminelle die Wirtschaft und Verbraucher durch Datendiebstähle sowie einzelne Unternehmen durch Erpressung beispielsweise auf Basis von „Denial of Service"-Angriffen.

Insgesamt sind die Bedrohungen der Digitalen Souveränität vielfältig und betreffen sowohl den Staat als auch die Wirtschaft und die Bürger.

*SCADA-Systeme („Supervisory Control And Data Acquisition") sind Systeme, die computergestützt beispielsweise Produktionsprozesse in der produzierenden Industrie überwachen.

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

NEWS

Neue Wege gegen Cyberkriminalität

Stuttgart – Spezieller Ausbildungsweg für IT-Spezialisten angelaufen. Sie werden im gehobenen Polizeivollzugsdienst eingegliedert.

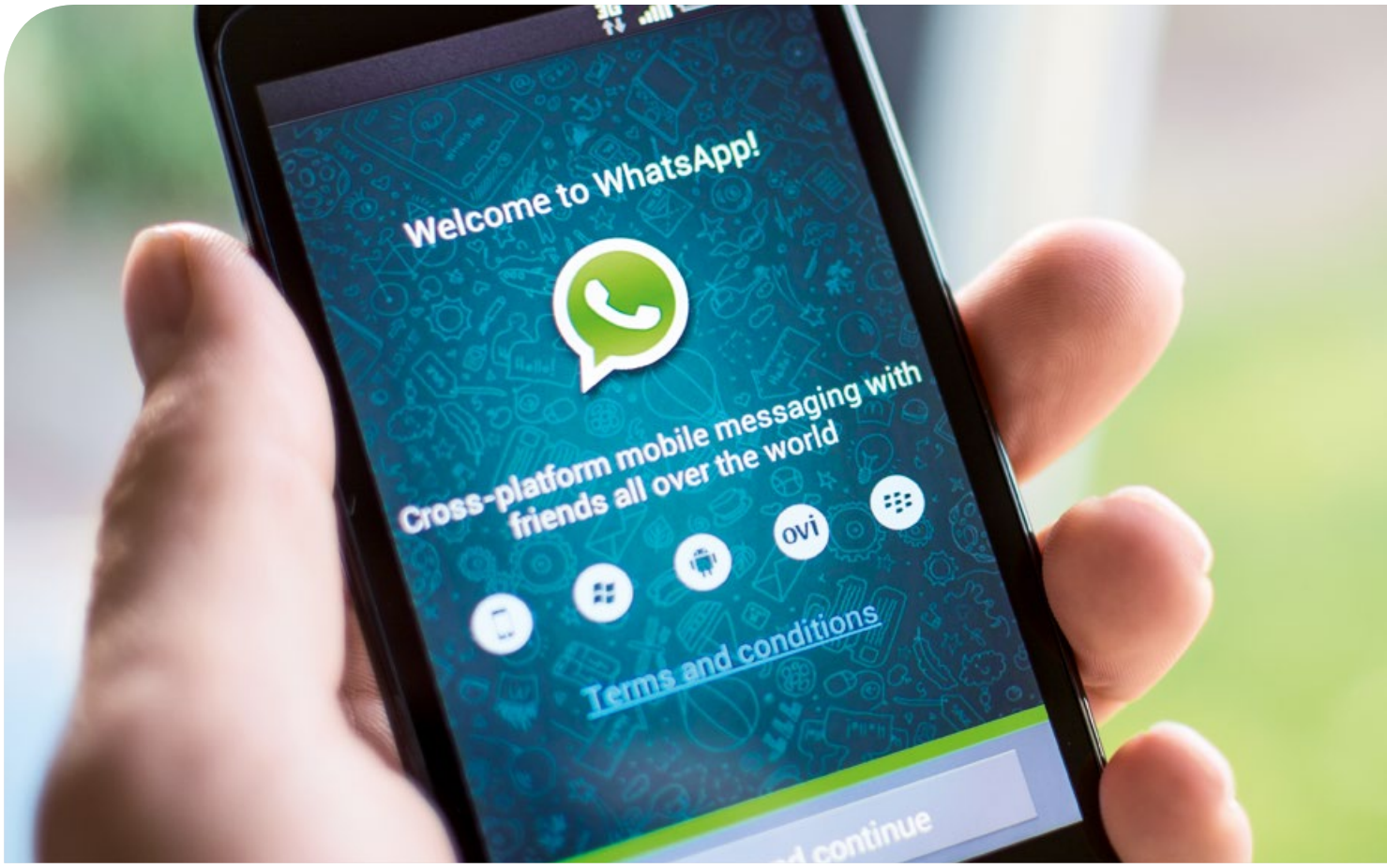
Reinhold Gall. Der Minister setzt auf externe Experten.

Fotos: Leif Piechowski/Innenministerium BW, bibiphoto – Shutterstock

Das Land Baden-Württemberg will gezielt gegen wachsende Cyberkriminalität vorgehen. Innenminister Reinhold Gall: „Wir dürfen nicht zulassen, dass sich das Internet zu einem rechtsfreien Raum entwickelt. Deshalb führen wir die Sonderlaufbahn Cyberkriminalist ein, um extern ausgebildete IT-Spezialisten einstellen zu können."

Es sei geplant, 15 IT-Spezialisten ein Jahr lang zu Polizisten in der Laufbahn des gehobenen Polizeivollzugsdienstes auszubilden. „Wir brauchen Expertenwissen, um Straftaten im Bereich der IT aufzuklären und die Täter ausfindig zu machen. Ohne entsprechende Fachkenntnisse ist es in vielen Bereichen kaum mehr möglich, den Straftätern auf die Schliche zu kommen", betonte der Innenminister.

Informationen zu Bewerbung und Ansprechpartnern finden Interessierte unter www.polizei-bw.de sowie auf den Internet-Auftritten der Polizeidienststellen des Landes Baden-Württemberg. Eingesetzt werden sollen die Cyberkriminalisten in der Fachabteilung Cybercrime und Digitale Spuren beim Landeskriminalamt Baden-Württemberg sowie bei den entsprechenden Kriminalinspektionen der zwölf regionalen Polizeipräsidien, die zum Jahresbeginn 2014 eingerichtet wurden.



Ich bin ein Amerikaner

Das Internet ist eine US-Einrichtung, und ich lebe als rechtloser Immigrant in den Virtuellen Staaten von Amerika.

Harald Lemke

„Just because I'm paranoid doesn't mean they're not out to spy on me."

Der jüngste Mega-Deal der Internetwelt hat in meinem Familienkreis wieder die Frage aufgeworfen, ob ich mit fortgeschrittenen 58 Lebensjahren zu alt für diese Welt bin. Meine in Neuseeland lebende Tochter wollte meine Frau und mich schon länger für WhatsApp begeistern: „Es ist alles so einfach, und wir können dann auch schnell Videos vom neuen Enkelsohn schicken."

Ich war, was WhatsApp angeht, schon immer skeptisch. Neidlos musste ich anerkennen, dass es ein paar unbekannten Menschen irgendwo auf der Welt gelungen war, mit einer relativ einfachen App fast eine halbe Milliarde Telefonbücher abzuzocken. Denn – und das ist beileibe kein Geheimnis – jeder WhatsApp-Nutzer verschenkt freigiebig die Namen, E-Mail-Adressen, Adressen und Telefonnummern seines Bekanntenkreises – ob es den Betroffenen passt oder nicht. Mithilfe dieser Adressbücher lässt sich ein globales Beziehungsdiagramm erzeugen, das wohl alle persönlichen Kommunikationsbeziehungen unseres Planeten umfasst.

Mir war schon immer klar, dass diese Daten den wertvollsten Schatz unserer modernen Welt darstellen, und vor diesem Hintergrund hat mich auch nicht der Kauf von WhatsApp durch Facebook überrascht. Die dafür angeblich auf den Tisch gelegte Summe von 19 Mrd. Dollar geht selbst dann in Ordnung, wenn alle WhatsApp-Kunden dem Appell des Hamburger Datenschutzbeauftragten folgen und ihr Konto kündigen würden.

Ein Gutes hatte das Ganze auf jeden Fall: Man erfuhr endlich mal, dass WhatsApp nicht dem Mossad oder der

Fotos: Twin Design – Shutterstock, Trevor Paglen – wikimedia

Schöne neue Welt?
WhatsApp, Facebook & Co. haben ihre Jünger fest im Griff. Es ist kaum noch möglich, sich dem Zugriff zu entziehen.

NSA gehört (warum kommen die nicht auf so gute Ideen?), sondern einem No-Nonsense-Nerd aus der Ukraine, dem der Schutz der ihm anvertrauten Daten schon immer eine echte Herzensangelegenheit war. Der Verkauf seines Geschäftes mit allen Kunden und Daten an den unverschämtesten Datenkraken des virtuellen Universums zeigt, was die Nutzer von solchen Herzensversprechen halten dürfen.

Wie anfangs erwähnt, platzte dieses Milliardengeschäft just in time in die familiäre Diskussion über die Nutzung von WhatsApp. Ich fühlte mich natürlich in meiner grundlegenden Skepsis bestätigt. An diesem Punkte musste ich mir vorhalten lassen, dass meine Daten doch ohnehin schon bei WhatsApp liegen, weil garantiert irgendeiner meiner Bekannten bereits sein Telefonbuch verschenkt hat: „Nun ist es doch egal, nutze es doch wenigstens!"

„Privacy is dead, get over it." Dieser Spruch ging mir spontan durch den Kopf. Gehört hatte ich ihn erst ein paar Tage zuvor im Vortrag eines Venture-Capital-Managers. Der stellte in erfrischender Ehrlichkeit dar, dass er nur an Geschäftsmodellen interessiert sei, deren Hauptzweck im Sammeln von Daten besteht.

Als Korreferenten hatte er einen Gründer von PayPal dabei, der stolz seine neue, coole Company präsentierte. Die Idee: Man zahlt alle Einkäufe mit seinem Dienst und bekommt ein Zahlungsziel von 30 Tagen. Der Deal: Man stellt als Dankeschön für den finanziellen Aufschub sämtliche privaten Daten dem Zahlungsdienstleister für weitere Verwendungen zur Verfügung. Ich schäme mich fast ein bisschen dafür, nicht aufgestanden zu sein und die beiden Protagonisten der neuen Transparenz gefragt zu haben, ob sie noch alle Tassen im Schrank haben.

Wahrscheinlich hätte dieses persönliche Zeichen auch nichts genutzt. Die Audienz nämlich spendete begeisterten Beifall, und lauter hungrige New-Economy-Jünger liefen beseelt nach Hause und überlegen jetzt noch intensiver, mit welchen tollen Ideen sie an alle unsere Daten herankommen.

Szenenwechsel. Was haben wir in den letzten Monaten für intensive Diskussionen über die Überwachung des Internets durch NSA und GCHQ geführt. Zu Recht, denn es ist zweifelsfrei eine bedrohliche Vorstellung, dass fremde Staaten unsere gesamte elektronische Kommunikation in einem Ausmaß überwachen, den wir dem eigenen Staat nicht und niemals →

Lauschzentrale. Das NSA-Hauptquartier in Fort George G. Meade, Maryland, nordöstlich von Washington. Präsident Truman gründete die Einrichtung in den 1940er-Jahren.

→ zugestehen würden. Nun haben unsere Regierung und die Europäische Kommission unisono glaubhaft versichert, dass sie diese Form einer Totalüberwachung strikt ablehnen und ... nichts.

Was sollte unsere Regierung auch tun? Unser Staat hat keine wirksamen Mittel in der Hand, unsere Grundrechte im global organisierten Netz wirksam zu schützen. sei es vor politisch oder wirtschaftlich motivierter Totalausspähung. In der Tat scheint es auch egal, ob unsere Privatsphäre durch Facebook, WhatsApp, Google, NSA oder GCHQ ausgehöhlt wird.

Ich bin übrigens überzeugt davon, dass man das Phänomen unserer Totalüberwachung ganzheitlich sehen muss. Es macht keinen Sinn, unsere soziale Kommunikation zur frei verfügbaren Datenmine zu erklären – Stichwort Big-Data –, wenn wir uns gleichzeitig über staatliche Datensammelwut empören.

Nur, was bleibt uns außer der Empörung? Unser Land reibt sich die Augen und stellt erstaunt fest, dass das Internet uns nicht gehört. Eine ziemlich naheliegende Erkenntnis, denn was ist das Internet? Es ist nicht der DSL-Anschluss, der Computer oder das mobile Gerät. Das Internet sind vielmehr die vielen Dienste, die das Leben einfacher machen: Suchmaschinen, E-Commerce, Messenger, Cloudspeicher und soziale Netzwerke.

Diese Dienste assoziieren wir mit dem Internet, und diese Dienste haben einen gemeinsamen Nenner: Sie werden von US-amerikanischen Unternehmen beherrscht. Mehr noch, viele dieser Dienste beherrschen als sogenannte Gatekeeper den Zugang anderer Systeme zum Internet. Ein gutes Beispiel ist der AppStore von Apple: Apple betrachtet die mobilen Geräte seiner Kunden als

NEWS

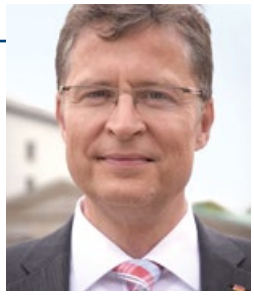
Ausschuss für die digitale Agenda

Berlin – Nur beratende Funktion für die Experten.

Der Ausschuss für die Digitale Agenda (ADA) hat seine Arbeit aufgenommen. Vorsitzender ist Jens Koeppen (CDU). Unter den 16 Ausschussmitgliedern (sieben aus der Union, fünf aus der SPD und je zwei von Grünen und der Linken) sind einige der profiliertesten Netz-Politiker des Bundestages, die bereits in der Enquetekommission Internet und Digitale Gesellschaft zusammengearbeitet haben. Die Kommission hatte die Einrichtung dieses neuen Hauptausschusses empfohlen.

Der Ausschuss hat aktuell nur beratende Funktion und keine Federführung zugesprochen bekommen. Von der Expertise seiner Mitglieder sollen sowohl die Fachausschüsse als auch die Ministerien profitieren.

Jens Koeppen verglich den ADA mit der Einführung des Umweltausschusses, der zunächst auch nicht federführend war. Er kündigte an, externe Experten einzuladen und zu beteiligen, ohne weitere Details zu benennen.



Vorsitzender. Jens Koeppen (CDU) leitet den neuen Ausschuss.

Wie Koeppen ergänzend deutlich machte, soll sich der Ausschuss nicht hauptsächlich mit Sicherheitslücken, Cyberksriminalität und Bürgerrechten im Netz beschäftigen. Vielmehr sollen auch die Chancen des Internets ins Blickfeld rücken und nicht allein die Risiken.

Pilgerziel. Arbeitsteilung in den Stores: Nutzer kaufen und zahlen. Anbieter zocken ab und setzen die Regeln.

eigene Business-Domäne und entscheidet, ob eine App zugelassen wird oder nicht. Neidlos müssen wir die Stringenz und Konsequenz anerkennen, mit der unsere transatlantischen Freunde ihre Geschäfte aufbauen, ausbauen und absichern. Das alles geschieht auch nicht im rechtsfreien Raum. Vielmehr agieren die meisten Internet-Unternehmen nach amerikanischen Wertvorstellungen, die – zumindest bei der Privacy – ganz erheblich von den deutschen Vorstellungen abweichen.

Und so reift langsam die Erkenntnis, dass das Internet eine amerikanische Einrichtung ist und ich als virtueller Immigrant in den USA lebe. Fast könnte ich sagen: „Ich bin ein Amerikaner!" Leider nur ein Amerikaner zweiter Klasse, denn ich habe keinerlei Möglichkeiten, die Governance meiner digitalen Heimat durch demokratische Wahlen zu beeinflussen.

Was nun? Resignation? Nein, wir sollten vielmehr daran denken und darauf vertrauen, dass bisher noch kein Empire ewig gehalten hat. Wenn es einen Bedarf für datensparsame Internet-Dienste gibt, sollten wir in Deutschland und Europa jetzt mit Hochdruck daran arbeiten, ethisch vertretbare Produkte, Dienste und Geschäftsmodelle zu entwickeln. Das braucht Zeit und Geld, aber: WhatsApp hat auch fünf Jahre gebraucht.

Harald Lemke
ist Sonderbeauftragter für E-Government und E-Justice bei der Deutschen Post.

NEWS

Hessen-CIO Westerfeld verabschiedet

Wiesbaden – Ein Nachfolger ist noch nicht in Sicht.

Abschied. Hessens Finanzminister Dr. Thomas Schäfer (l.) verabschiedet Staatssekretär Horst Westerfeld.

Staatssekretär Horst Westerfeld, CIO und Bevollmächtigter für E-Government und Informationstechnologie des Landes Hessen, wurde aus seinem Amt verabschiedet und tritt in den Ruhestand. Finanzminister Thomas Schäfer würdigte die Arbeit des Staatssekretärs: „Er hat sich maßgeblich um eine effektive und effiziente Informationstechnologie in der Landesverwaltung verdient gemacht. Über seine hohe fachliche Kompetenz hinaus werde ich Horst Westerfeld als Freund und politischen Weggefährten vermissen."

Horst Westerfeld, geboren 1951, begann seine Karriere nach einer Ausbildung zum Maschinenschlosser mit den Studiengängen zum Diplom-Ingenieur (1970 bis 1973) sowie Diplom-Mathematiker (1973 bis 1978). Seit Juni 2008 hatte Horst Westerfeld das Amt des Staatssekretärs und CIO inne. Ein Nachfolger für ihn scheint noch nicht gefunden. Auch ist unklar, ob die Position überhaupt neu besetzt wird.

Fotos: HMDF, Frank Nürnberger – wikimedia, Twin Design/ TungCheung – Shutterstock

Das Ohr zur Welt. Wird von der US-Botschaft in Berlin das Regierungsviertel ausspioniert?

Welche Spielregeln sollen künftig gelten?

Wir brauchen internationale Vereinbarungen, um die Netz-Möglichkeiten besser ausbalancieren zu können.

Dr. Göttrik Wewer

Der moderne Staat, so wie wir ihn heute kennen, hat sich seit der Amerikanischen Unabhängigkeitserklärung (1776) und der Französischen Revolution (1789) allmählich entwickelt. In den knapp 250 Jahren, die seither vergangen sind, hat er sich immer wieder verändert. Aus „Vater Staat", der streng über seine Bürger wachte, die Regeln vorgab und deren Einhaltung kontrollierte, ist einer geworden, der eher moderiert, aushandelt und koordiniert. „Kooperativer Föderalismus" (Ernst-Hasso Ritter) statt zentraler Vorgaben; Public-Private Partnerships statt rein staatlicher Aufgabenerfüllung; Regieren in Netzwerken statt hierarchischer Steuerung.

Manche sehen im Staat nur noch eine Plattform zur gesellschaftlichen Selbststeuerung. Ganz abgesehen davon, dass der Staat, so wie wir ihn kennen, auch für bestimmte Inhalte steht, die hoffentlich nicht zur Disposition stehen (wie etwa die Menschenwürde, der Rechtsstaat und die Gewaltenteilung oder die freiheitlich-demokratische Grundordnung), setzt diese Idee voraus, dass die Selbststeuerung der Gesellschaft friedlich erfolgt. Das ist aber keineswegs selbstverständlich. Es gibt genügend Beispiele für failed states oder weak states, die nicht in der Lage sind, verbindliche Spielregeln für alle Bürger tatsächlich durchzusetzen. Wenn es keine Instanz gibt, die einen gewissen Rahmen vorgibt und über die Einhaltung der Spielregeln wacht, dann heißt gesellschaftliche Selbststeuerung nichts anderes als Kampf aller gegen alle, bei dem sich die mächtigeren Interessen und das Recht des Stärkeren durchsetzen.

Ein gegebenes Versprechen. Es gibt also Konstanten, die vorhanden sein müssen, wenn wir überhaupt von einem modernen Staat reden wollen. Dazu gehören die staatliche Souveränität und das staatliche Gewaltmonopol. Wenn beides nicht mehr gegeben ist, ist der moderne Staat am Ende.

Der klassische Staatsbegriff umfasst drei Komponenten: Staatsvolk, Staatsgebiet und Staatsgewalt, nämlich „das Monopol legitimer physischer Gewaltsamkeit" (Max Weber). Das Versprechen, das der moderne Staat seinen Bürgern gibt, lautet: Ich verteidige dich gegen Angreifer von außen, und ich sorge dafür, dass Konflikte im Innern mit friedlichen Mitteln ausgetragen werden. Um das Versprechen einlösen zu können, muss er nach innen wie nach außen souverän

Foto: 360b

sein, also hinreichend unabhängig von irgendwelchen Interessen, um seine Rolle als neutraler Hüter des Gemeinwohls ausfüllen zu können, und stark genug, seine Bürger vor Angriffen, Gewalt und Kriminalität auch wirklich schützen zu können.

Keine technische Plattform. Das staatliche Gewaltmonopol ist praktisch ein Deal: Du (Bürger) kannst darauf verzichten, Gewalt anzuwenden, weil ich (Staat) dich vor Gewalt schütze. Dass der Staat Mord und Totschlag, Vergewaltigung und Einbruch nicht völlig verhindern kann, ändert nichts daran, dass er den Anspruch nicht aufgeben darf, den Bürger zu schützen. Dass nicht jede Straftat aufgeklärt werden kann, ändert nichts daran, dass der Staat den Versuch nicht aufgeben darf, alles in seiner Macht Stehende dafür zu tun.

Das ist der Deal. Wenn der Staat seinen Teil nicht erfüllt, entfällt im Grunde auch die Geschäftsgrundlage für den Bürger, sich an die Regeln zu halten und das staatliche Gewaltmonopol zu akzeptieren. Der moderne Staat ist eben nicht bloß eine technische Plattform, auf der beliebige Inhalte transportiert werden können, sondern er verkörpert gewisse Ansprüche, die wir Bürger an ihn stellen und die diejenigen, die in seinem Namen tätig werden, an sich selbst stellen müssen. Manche Liberale, die im Staat nur ein aufgeblähtes Bürokratiemonster sehen, haben das übrigens nie verstanden.

> Ich schütze dich vor der Gewalt.
>
> **Deal zwischen Staat und Bürger**

Unabhängig und gleich. Souveränität bezeichnet die höchste unabhängige Herrschaftsmacht und Entscheidungsgewalt nach innen wie nach außen. Nach innen verfügt die Staatsgewalt in diesem Modell über sämtliche Hoheitsrechte, →

Regelmacher. Nach Ansicht vieler Experten haben Google & Co. das Sagen.

→ wobei sie in Demokratien durch die Volkssouveränität sowohl legitimiert als auch begrenzt ist. Im Völkerrecht meint Souveränität die Unabhängigkeit und die Gleichheit der Staaten untereinander. Natürlich sind die Staaten politisch, wirtschaftlich, militärisch oder sonst wie unterschiedlich stark oder schwach, und natürlich ist es klug, als kleiner Staat nicht unnötig mit den Muskeln zu spielen. Aber Unabhängigkeit bedeutet, dass man selbst bestimmen kann, ob man sich klug oder weniger klug verhält, und nicht dazu gezwungen werden kann, sich in einer bestimmten Art und Weise zu verhalten. Wenn man fremdbestimmt werden kann oder gar besetzt wird, ist ein Staat nicht mehr souverän.

Wer macht die Regeln? Total souverän ist niemand, auch nicht der Weltpolizist USA. Alle Staaten der Welt sind heute in ein dichtes Gewebe wechselseitiger Abhängigkeiten eingebunden. Deutschland, das seine volle Souveränität erst mit der Wiedervereinigung wieder erlangt hat, hat seine Unabhängigkeit bewusst und freiwillig partiell aufgegeben, indem es sich völkerrechtlichen Abkommen unterworfen und der Europäischen Gemeinschaft und der NATO beigetreten ist. Durch Notenaustausch mit den USA, Großbritannien und Frankreich am 2. und am 6. August 2013 hat die Bundesregierung, wie sie in ihrem Fortschrittsbericht über „Maßnahmen für einen besseren Schutz der Privatsphäre" vom 14. August dargelegt hat, die Vereinbarungen mit den ehemaligen Besatzungsmächten gekündigt, wonach diese zum Schutz ihrer hier stationierten Streitkräfte Eingriffe in das deutsche Brief-, Post- und Fernmeldegeheimnis verlangen konnten.

Digitale Souveränität bedeutet, dass Staaten und ihre Bürger selbst bestimmen können, welchen Spielregeln im Internet sie sich freiwillig unterwerfen wollen und welche sie ablehnen. Diese Regeln entstehen heute nicht über demokratische Willensbildung, sondern werden von den Giganten des Internets, also von privaten Akteuren, gesetzt („code is law"). Das Zeitalter der Privatheit sei vorbei, verkündet Mark Zuckerberg, der Gründer von Facebook. Ein Staat, der gezwungen ist, sich Regeln zu unterwerfen, die andere setzen, zumal Private, ist nicht mehr souverän. Abhängig sind auch Staaten, die darauf angewiesen sind, sich auf technologische Komponenten zu verlassen, die von Herstellern stammen, denen man nur bedingt vertraut. Und wenn erklärt wird, man könne die eigenen Bürger nicht davor schützen, dass

NEWS

Markus Söder neuer CIO in Bayern

München – Er vertritt das Bundesland auch im IT-Planungsrat.

Starker Mann. Markus Söder soll für digitalen Aufbruch sorgen.

Dr. Markus Söder, Bayerischer Staatsminister der Finanzen, für Landesentwicklung und Heimat, ist zum neuen Chief Information Officer (CIO) des Freistaats bestellt worden. Er soll die Digitalisierung in Bayern koordiniert vorantreiben und den Freistaat zur Leitregion des digitalen Aufbruchs machen. Die Digitalisierungskompetenz in Bayern ist im Finanzministerium konzentriert. Söder ist deshalb auch Ansprechpartner für den Bund und wird Bayern im IT-Planungsrat vertreten. Er ist damit der einzige Minister in diesem Gremium. Die Interessen des jeweiligen Landes werden sonst überwiegend durch Staatssekretäre bzw. Staatsräte vertreten.

sie von ausländischen Mächten massenhaft überwacht und ausspioniert werden, dann ist das nichts anderes als eine staatliche Bankrotterklärung.

In der Studie „Zukunftspfade Digitales Deutschland 2020", die der IT-Planungsrat auf den Weg gebracht hat, wird „digitale Souveränität" so verstanden, dass diese dann gegeben ist, wenn der Einzelne souverän im Netz surft. In anderen Studien ist, wenn es darum geht, eher von Medienkompetenz die Rede. Alles beim Nutzer abzuladen, der selbst zurande kommen und sich allein gegen die Giganten des Internets, die die Spielregeln vorgeben, und ausländische Geheimdienste, die ihn ausspähen, zur Wehr setzen soll, ist aber eine staatliche Bankrotterklärung.

Schluss mit einem Mythos. Der Staat gibt seinen Anspruch auf, seine Bürger zu schützen, wo sie sich nicht selbst schützen können. Er kündigt den Deal und gibt damit zugleich ein Markenzeichen auf, das ihn bisher ausgezeichnet hat. Was nützt uns ein Staat, der das Internet als rechtsfreien Raum akzeptiert und der es hinnimmt, dass es nicht demokratische Mehrheiten sind, die dort die Spielregeln vorgeben, sondern private Dritte, die keinerlei demokratischer Kontrolle unterliegen? Dass das Internet unregulierbar sei, ist ein Mythos: Die Giganten des Internets zeigen sich sehr geschmeidig, ihre Dienste nationalen Vorgaben anzupassen, wenn sie bestimmte Märkte unbedingt erobern wollen.

Fackel im Wind.
Weltweite Proteste gegen Ausspähaktionen helfen bisher nicht.

Wenn das Internet unregierbar wäre, müsste man sich auf internationalen Konferenzen nicht über dessen Governance streiten, und dann müssten die Giganten des Internets sich in Brüssel nicht so viel Mühe geben, die europäische Datenschutzgrundverordnung in ihrem Sinne zu beeinflussen. Deutschland ist nicht groß genug, mit seinen Werten das Internet zu prägen, und ein „nationales Internet" oder E-Mails, die nur im Lande zirkulieren, machen wenig Sinn.

Wir brauchen europäische Lösungen und internationale Vereinbarungen, um einen Rahmen zu schaffen, in dem Freiheit und Sicherheit, Vertrauen und Kontrolle, Abhängigkeit und Selbstbestimmung im Netz besser ausbalanciert sind als heute. Deutschland mag nicht groß genug sein, das allein zu stemmen, aber es verfügt über genügend Kompetenz, dafür in Europa und darüber hinaus wichtige Anstöße und Impulse zu geben. Oder andersherum gesagt: Regieren muss man auch wollen!

Dr. Göttrik Wewer
ist Vice President E-Government bei der Deutsche Post Consult GmbH.

NEWS

Nationaler IT-Gipfel 2014

Hamburg – Expertentreffen endlich terminiert.

Nach einigen Anläufen scheint nun der Termin für den nächsten Nationalen IT-Gipfel festzustehen: 21. Oktober in Hamburg.

Ein zweites wichtiges Datum ist – bis Redaktionsschluss – nicht bestätigt. Zur Vorbereitung des Gipfels plant das Bundesministerium für Wirtschaft und Energie ein hochrangiges Treffen der zuständigen Mitglieder des neuen Bundeskabinetts mit führenden Wirtschaftsvertretern. Angedacht ist dieses Treffen noch für den März.

Blickpunkt. Erfüllt das Treffen in der Hansestadt die Erwartungen?

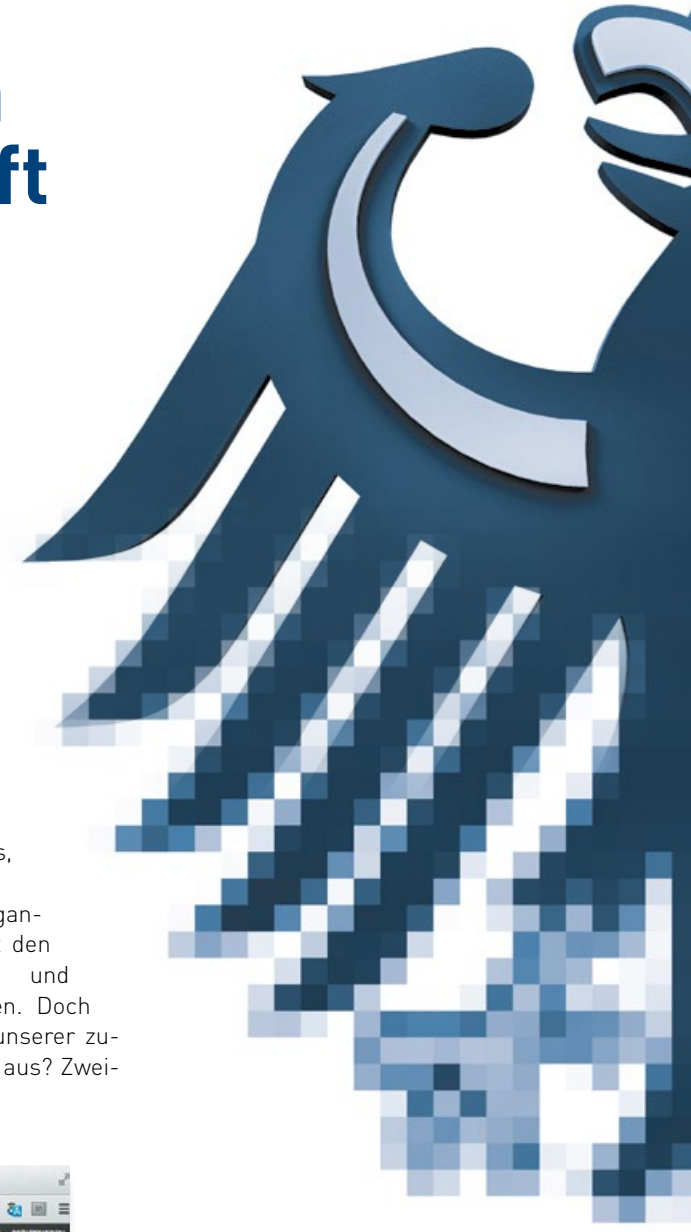
Unabhängig von den Terminen will das Bundesministerium für Wirtschaft und Energie unter www.it-gipfel.de über die bisherigen Ergebnisse des Jahres 2013 und über den Fortgang der Arbeiten des IT-Gipfels informieren.

Fotos: stmflh-bayern, K images/Ken Wolter/Rena Schild – Shutterstock

Staat 4.0 – Revolution von innen als Weg in die Zukunft

Akteure der Konsumgesellschaft haben die „Herrschaft“ übernommen.

Lutz Diwell



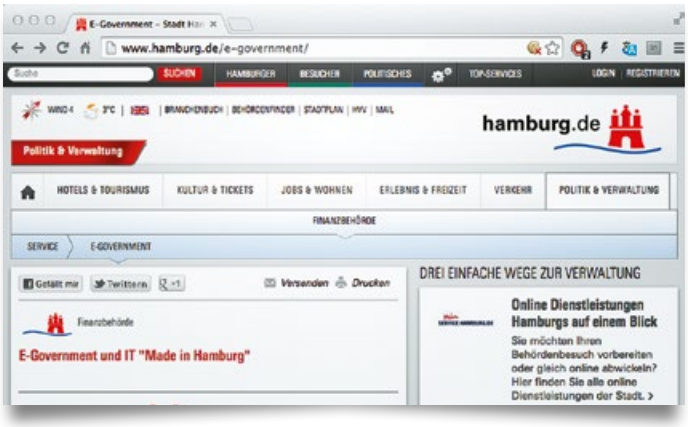
Wenn „Industrie 4.0“ gleichbedeutend ist mit der 4. Revolution auf industriellem Gebiet, wäre dann „Staat 4.0“ gleichbedeutend mit Revolution in Deutschland? Ein struktureller Wandel, abrupt und in kurzer Zeit und gar gewaltsam – ist es das, was wir gerade erleben?

Nein, und doch: Der Staat steht im digitalen Wandel mittendrin!

Mit welchen Rahmenbedingungen sieht er sich konfrontiert? Was sind die Änderungsbedarfe und was die Ziele? Antwortversuche sollten nicht staatsphilosophisch, nicht politikwissenschaftlich, nicht juristisch sein.

Hält der Staat Schritt? Von der Perspektive des Digitalen her hat sich unsere Gesellschaft stark gewandelt und tut es permanent weiter. Was mechanisch oder elektrisch lief, läuft längst digital (Schreibwerkzeuge). Wer Ende-zu-Ende kommunizierte, hat längst den Überblick über die Kommunikationsrouten verloren (analoges Telefon, E-Mail-Routing via USA ins Nachbarzimmer), und wer bei „smart“ an gefällige Gebrauchsgegenstände oder Autos dachte, ist meist längst überfordert mit den s-cities, s-home oder s-health.

Der Staat hat in den vergangenen Dekaden versucht, mit den technischen Entwicklungen und Neuerungen Schritt zu halten. Doch reichen die Bemühungen in unserer zunehmend schnelllebigen Welt aus? Zweifel sind angebracht.



E-Government. Wie hier am Beispiel Hamburg zu sehen, hat sich einiges schon geändert. Der Staat wird langsam zur modernen Servicestelle.

Dabei hat sich tatsächlich bereits einiges gewandelt. Wo der Gang zum Rathaus den Untertan zum Bürger und Beteiligten werden ließ, steht immer öfter ein digitales/e-government-mäßiges Angebot bereit oder wird zumindest demnächst bereitstehen. Der Staat entwickelt sich vom gewährenden Staat zur Servicestelle, die adressatenorientiert informiert und leistet.

Wohin fliegt der Adler? Der Staat hat sich bemüht, mit technischen Entwicklungen Schritt zu halten. Es sind aber Zweifel angebracht, ob die Anstrengungen reichen.

Foto: Pixel-3D – Shutterstock

Der Staat und seine verschiedenen Strukturen haben dabei auch manche Anwürfe hinnehmen müssen: Er führe Daten zusammen, die ihm zweckgebunden für Anspruchsprüfung und Leistungsgewährung hingegeben wurden, und achte das „informationelle Selbstbestimmungsrecht" nicht ausreichend.

Der Staat als Akteur, als Nutzer einer Informationsgesellschaft stellt jedoch schon längst nicht mehr das alleinige oder größte Problem dar. Die Staaten haben sich angepasst, sie überwachen und kontrollieren frei oder nach Regeln, sie schützen und sichern das Gemeinwesen, aber sie (ent)nehmen Daten und Informationen und verknüpfen sie, was regelfrei problematisch bleibt. Insbesondere aber: Die Staaten bewahren auch nicht davor, dass andere es tun!

Denn: Die kaum greifbaren oder steuerbaren Akteure der Konsumgesellschaft haben mit dem digitalen Handel die „Herrschaft" übernommen. Plötzlich erscheinen nicht mehr der eigene Staat und sein Umgang mit Daten als ein wesentliches Thema. Die in weiter räumlicher Ferne weltweit agierende Internet-Großmacht, quasi ein Fremd-Staat, rückt in den Fokus.

Schutz auf vielen Feldern. Der moderne demokratische Staat soll seine Bürger auf vielen Feldern schützen. Vor Regelverstößen des eigenen Bereiches, vor wirtschaftlichen Nutzerinteressen zum Nachteil des Gemeinwesens oder des Einzelnen, vor Eingriffen in Selbstbestimmung und Intimsphäre. Er soll das Zusammenleben der Menschen so organisieren, dass sich jeder über die Regeln klar sein kann. Der Staat soll sich darum kümmern, dass die Einhaltung dieser Regeln sichergestellt ist, Abläufe geschützt und überwacht werden.

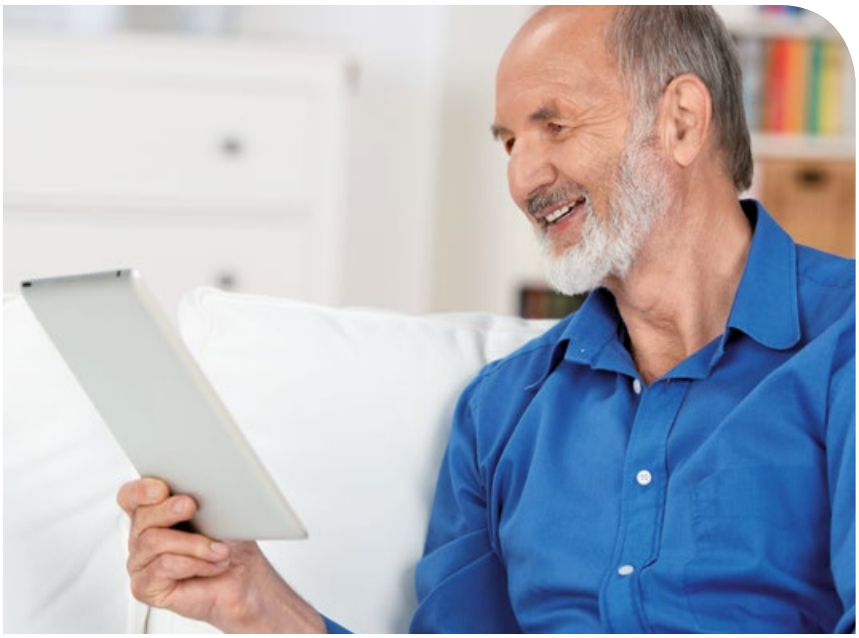
Doch genau da stößt der Staat derzeit an seine Grenzen. Das Netz ist weltweit organisiert, seine Regeln sind offen und unfixiert. Das kann jeder nutzen: der überwachende Nachbarstaat, der Hacker von nebenan, der Online-Shop aus Übersee oder Menschen mit kriminellen Absichten.

Europäisch denken. Steht der Staat also auf verlorenem Posten? Welche Möglichkeiten hat er, wie kann er strukturell und in kurzer Zeit einen Wandel herbeiführen, damit er seine Pflichten gegenüber den Bürgern erfüllen kann? Schon die Frage zeigt, dass ein einzelner Staat in einem globalen Problemfeld wenig wird ausrichten können.

Also gilt es, europäisch/international zu denken und zu handeln. Doch auch im eigenen Bereich kann und muss der Staat sich und die Gesellschaft neu definieren. Es braucht Standards für den Umgang miteinander, es muss Vertrauen geschaffen und es müssen Wege aufgezeigt werden, wie Sicherheit vor jeder Tür, in jedem Device greifen kann!

Der Staat muss sich also selbst revolutionieren, ja neu erfinden, um diesen Spagat zu erreichen. Und diese Revolution von innen heraus erscheint als ein Weg in die Digitale Souveränität auf allen Ebenen: individuell, lokal, regional, national, supranational!

Lutz Diwell
ist Vorstandsvorsitzender des Zukunftsforums Öffentliche Sicherheit. Der frühere Staatssekretär ist aktuell als Rechtsanwalt bei Schellenberg Unternehmeranwälte und als Berater für Roland Berger Strategy Consultants tätig.



Neue Welt. Senioren und Tablet-PCs: Das passt gut zusammen.

Senioren ins Internet!

Eine Initiative der Stiftung Digitale Chancen läuft weiter voll auf Erfolgskurs. Jetzt neue Bewerbungen möglich.

Jürgen Selonke

Zur echten Erfolgsstory entwickelt sich eine Aktion der Stiftung Digitale Chancen, in deren Rahmen ältere Mitbürger durch die kostenlose Übergabe mobiler Endgeräte an das Internet herangeführt werden. Das Projekt, realisiert in Zusammenarbeit mit der E-Plus Gruppe, läuft jetzt bereits im dritten Jahr. Unterstützt wird die Initiative auch von Bundestagspräsidentin a.D. Rita Süssmuth.

Gerade wurden jetzt in Göttingen an die Bewohner eines Wohnstiftes Tablet-PCs mit einer Internet-Flatrate übergeben. Jutta Croll, Geschäftsführerin und Vorstandsmitglied der Stiftung Digitale Chancen: „Tablet-PCs gehören in den Alltag von älteren Menschen ebenso wie in den von Studenten. Ob aktuelle Nachrichten, Videotelefonie mit Verwandten oder das Auffinden der nächsten Apotheke mit Nachtdienst: Die Geräte sind bei der Bewältigung vieler Alltagssituationen hilfreich. Immer mehr Seniorinnen und Senioren möchten daher die Chancen des Internets kennenlernen. So werden auch Berührungsängste mit der neuen Technologie abgebaut."

Rita Süssmuth lobte das Engagement für die Einbeziehung von älteren Menschen, die in Senioreneinrichtungen leben, in unsere Informationsgesellschaft. Sie betonte, dass die ältere Generation von den Vorteilen der neuen Technik nicht ausgeschlossen sein darf. Tablet-PCs könnten beim lebenslangen Lernen im Internet eine große Hilfe sein. Süssmuth: „Es ist nicht schwierig. Diese Geräte machen Spaß, wenn man nicht vergisst, sie aufzuladen."

„Tablet-PCs gehören in den Alltag von älteren Menschen."

Jutta Croll, Stiftung Digitale Chancen

Der anhaltende Erfolg der Aktion, die sich längst bundesweit etabliert hat, soll jetzt weiter gekräftigt und sogar ausgebaut werden. Zum Märzende startet die Stiftung Digitale Chancen wegen der großen Nachfrage einen Wettbewerb für alle Senioreneinrichtungen, die ebenfalls teilnehmen möchten. Jutta Croll: „Senioreneinrichtungen können sich ab sofort für die Teilnahme am Projekt bewerben. Voraussetzung ist die Unterstützung der älteren Menschen in der Einrichtung bei der Nutzung der Geräte. Und für die kreativste Senioreneinrichtung 2014 loben wir eine besondere Auszeichnung aus."

Schritte fallen leicht. Unterstützt werden die Senioren je nach Einrichtung entweder durch ein Kursangebot oder durch eine regelmäßige Sprechstunde, bei der Funktionen erklärt, Anwendungen eingerichtet und Probleme erörtert werden können. Ganz unterschiedlich sind die Erfahrungen und Vorkenntnisse der älteren Menschen, die am Projekt teilnehmen. In den beteiligten Einrichtungen wurde sehr schnell deutlich, dass denjenigen, die der neuen Technik bisher eher zurückhaltend gegenüberstanden, mit Touchscreen und kabellosem Internet-Zugang die ersten Schritte leichter fallen.

Senioren gehören zu den Bevölkerungsgruppen, die das Internet bisher wenig nutzen. Laut einer Studie von BITKOM verbreiten sich Tablet-PCs rasch in der Bevölkerung. Dennoch besitzen nur 6 Prozent der über 60-Jährigen ein Tablet. Viele der älteren Erstnutzer bedauern, dass sie so spät die neue technische Welt für sich entdeckt haben. So erklärte eine 86-jährige Teilnehmerin: „Ich habe mich schon mit 80 Jahren für Computer interessiert, aber man hat mir abgeraten, das wäre Zeitverschwendung. Schade, dass ich nicht früher damit angefangen habe, dann wäre ich heute schon weiter."

Bewerbungen für die Teilnahme am Projekt sind möglich ab dem 25.03.2014 unter www.digitale-chancen.de/TabletPCs

Fotos: racorn – Shutterstock, Stiftung Digitale Chancen

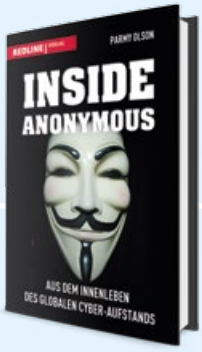
Aktuelle Bücher

Die Berechnung der Welt –
Von der Weltformel zu Big Data

Klaus Mainzer

Big Data verändert alles. Spätestens seit den Enthüllungen Edward Snowdens ist klar: Eine unersättliche Überwachungsmaschinerie hat uns im Griff. Gewaltige Datenmengen, die unser Leben abbilden, werden systematisch ausgewertet. Die Welt der Algorithmen beherrscht uns. Das Buch zeigt, wie es bei dem Vorhaben, die Welt zu berechnen, zu einer Revolution der Denkart kam. „Korrelation" statt „Begründung", lautet die aktuelle Devise. Aber Mainzer stellt nicht nur die neue Art der Wissensgewinnung vor. Sein Buch ist auch ein Plädoyer für die Besinnung auf die Grundlagen, Theorien, Gesetze und die Geschichte, die zu der Welt führen, in der wir leben.

C. H. BECK Verlag, ISBN 978-3-406-66130-3, 24,95 €



Inside Anonymous
Aus dem Innenleben des globalen Cyber-Aufstands

Parmy Olson

Das Anonymous-Kollektiv wurde bekannt durch die Guy-Fawkes-Maske, die Tarnung der Aktivisten. Erzählt wird der Werdegang dreier Mitglieder und die Motivation, die sie zu Hackern machte. Basierend auf exklusiven Interviews entsteht ein Einblick in die Köpfe, die hinter der virtuellen Community stehen.

REDLINE Verlag, ISBN 978-3-86881-349-4, 22,00 €

Smarte neue Welt
Digitale Technik und die Freiheit des Menschen

Evgeny Morozov

Ist unsere smarte neue Welt lebenswerter? Der Autor entlarvt die digitale Utopie als gefährliche Ideologie. Er fordert ein Nachdenken darüber, wie wir das digitale Universum mit unserem analogen Dasein sinnvoll in Einklang bringen und Demokratie, Kreativität und Selbstbestimmung retten können.

Blessing Verlag, ISBN: 978-3-89667-476-0, 24,99 €

Understanding YouTube
Über die Faszination eines Mediums

Roman Marek

Amateurvideos im Internet – „YouTube": Was fesselt Nutzer daran? Das Buch analysiert mit einem neuen Blick auf die Zirkulation der Videobilder Medienpraxen, die zwischen Zerstörung, Intervention, Automatismus, Wiederholung und Nachahmung oszillieren und in die Produktion von Recycling-Videos münden.

Transcript Verlag, ISBN 978-3-8376-2332-1, 34,80 €

Gewalt – Medien – Sucht: Computerspiele

Michael Kunczik

Durch das Internet ist eine Verschiebung der Medien-und-Gewalt-Forschung erfolgt. Im Fokus stehen jetzt die Effekte von Computerspielgewalt. Das Buch umreißt den Forschungsstand zur Wirkung gewalthaltiger Computerspiele. Berücksichtigt werden auch Forschungen zur Medienpädagogik und zur Computerspielsucht.

LIT Verlag, ISBN 978-3-643-12258-2, 19,90 €

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

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

DIVSI
Deutsches Institut für Vertrauen und Sicherheit im Internet