1/2012

Deutsches Institut für Vertrauen und Sicherheit im Internet

DIVSI magazin

DIVSI Milieu-Studie:
27 Millionen sind Digital Outsiders. Zwei Gräben trennen unsere digitale Gesellschaft

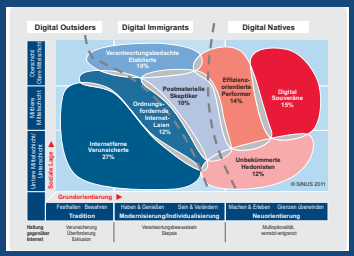
Haben wir Grund zur Angst?
Datenschutz-Diskussion in der Sackgasse

Generationenkonflikt bei der Sicherheit:
Alles Cloud oder was?

Stiftungslehrstuhl für Cyber Trust:
Die große Herausforderung

Joachim Gauck war erster Schirmherr des DIVSI

DIVSI
Deutsches Institut für Vertrauen und Sicherheit im Internet



Haben Sie Fragen oder wünschen Sie weitere Informationen?

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

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

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

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

Anschrift:
DIVSI
Mittelweg 142
20148 Hamburg

Statt eines Vorworts

Ich wünsche DIVSI viel Erfolg

DIVSI – das ist das Deutsche Institut für Vertrauen und Sicherheit im Internet.

Ich hatte die Freude, vor einem Jahr bei der Gründung dieser gemeinnützigen Gesellschaft, die von der Deutschen Post initiiert wurde, dabei zu sein und bei der Ausgestaltung der Ziele und Aufgaben des Instituts mitwirken zu können. Mit meiner Nominierung zur Wahl des Bundespräsidenten trennen sich nun die gemeinsamen Wege von DIVSI und mir.

Die im DIVSI-Team in den vergangenen Monaten zum Thema Sicherheit im Internet entwickelten Grundsätze bleiben wichtig. Die Gesellschaft braucht eine breit angelegte grundsätzliche Diskussion darüber, wie viel Freiheit im Internet sie sich zutraut und wie dabei das Recht der Nutzer auf Datenschutz im Internet gesichert werden kann.

Das DIVSI will diese gesellschaftspolitische Auseinandersetzung fördern und auch selbst dazu Stellung beziehen. Für diesen äußerst wichtigen und spannenden Disput wünsche ich DIVSI viel Erfolg.

Joachim Gauck, 24. Februar 2012


ENCRYPT
operating
standards
hardwarebased
hacker
levels
new
drive
maintained
lost
prevent
hard
software
entered
example
allows actions
file
due
personal
etc
changing
logout
last
attacks
group
however
inaccuracies
international
hacker
compromise
banking
anyone
national
include
administration
harddisk
using
customers
solutions
dongles
device
alternative
financial
used
need
computing
fairly
important
computer
cardinal
protection
offers
dvd
manipulate
unauthoriz
order
form
privilege
legitimate
program
created
image
accessible
connected
login
logging
harddisks
manual
clear
impossible
illegal
developers
security

Vertrauen und Sicherheit im Internet

DIVSI – Vor zwölf Monaten aus der Taufe gehoben. Alles über die Arbeitsbasis, Pläne, Ziele und erste Erfolge.

Von Matthias Kammer

Die Durchdringung von Staat und Gesellschaft mit IT wird immer mehr zunehmen. Schon heute gilt: In vielen Bereichen des täglichen Lebens geht nichts mehr ohne Internet. Das Internet ist längst mehr als eine moderne technische Erscheinung. Es ist eine Kulturleistung der Menschheit. Das Internet bietet große Entwicklungspotenziale und gleichzeitig, wie wir aus der täglichen Berichterstattung wissen, Raum für neuen Missbrauch persönlicher Identitäten und für kriminelle Handlungen. Wir alle sind entweder längst angekommen im Internetzeitalter, befinden uns im Übergang oder werden außen vor bleiben.

tungen, die den Umgang der Menschen miteinander im Lebensalltag prägen. Diese Grundhaltungen sind auch bestimmend für den Zugang und die Entfaltung in der virtuellen Welt. Dabei sind nach unserer Auffassung Vertrauen und Sicherheit von zentraler Bedeutung.

Wie verstehen wir Vertrauen und Sicherheit?

Vertrauen ist eine wichtige Triebfeder unserer Entscheidungsfindung. Das gilt in allen Lebenslagen - mit und ohne Internet. Konkret kann Vertrauen dabei zweierlei bedeuten: Vertrauen in eine Person, in eine Institution, in eine Marke („ich vertraue auf…“) oder in eine Sache („ich bin mit etwas vertraut“). Beide Vertrauensdimensionen bestimmen mit, wie das Internet genutzt wird. Aus diesem Grund ist Vertrauen für uns ein Kernbegriff beim Diskurs über Chancen und Risiken des Internets.

Matthias Kammer *(*1953) ist seit November 2011 Direktor des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI). Er studierte Rechts- und Staatswissenschaften in Freiburg und Hamburg. Seit 1980 war er in diversen Funktionen Mitarbeiter der Hamburger Verwaltung. Zwischen 1985 und 1994 leitete er mehrerer IuK-Projekte (u. a. neues Meldewesen für Hamburg oder PROSA – Projekt Sozialhilfe Automation). 1994 bis 1996 war er Leiter des Amtes für Informations- und Kommunikationstechnik der Hamburger Finanzbehörde, ab 1996 Leiter des Amtes für Organisation und zentrale Dienste der Hamburger Verwaltung. Von 2002 an war er verantwortlich für das Projekt zur Gründung eines gemeinsamen IT-Dienstleisters für die Verwaltungen Hamburgs und Schleswig-Holsteins und wurde nach Ende dieser Planungsphase 2004 Vorstandsvorsitzender von Dataport. Von Dezember 2005 bis November 2008 war Kammer Vorsitzender von VITAKO, der Bundesarbeitsgemeinschaft kommunaler IT-Dienstleister. Seit September 2008 ist er Vorsitzender des Forschungsverbundes ISPRAT e.V.*

Worum geht es DIVSI insgesamt?

Wir beobachten, dass es krasse Unterschiede der gesellschaftlichen Milieus im Umgang mit dem Internet gibt, die überwiegend auch noch diametral gegeneinander stehen. Während die einen regelrecht Angst vor der Nutzung des Internets haben oder die Entwicklung mit Sorge begleiten, wollen die anderen ohne Internet nicht mehr leben und halten Risiken für gering und beherrschbar. Es sind Grundhal-

Sicherheit ist ein menschliches Grundbedürfnis. Das gewünschte Maß an Sicherheit bestimmt unser Handeln und Nutzungsverhalten. Wie sicher wir im Internet wirklich sind, können die wenigsten beurteilen. Einerseits ist die Sicherheit abhängig von der Technik und andererseits von einem gemeinsamen Konsens über sicheres Agieren im Internet. Hier nimmt Datenschutz eine besondere Rolle ein und trägt wesentlich zur Sicherheit bei. Gleichzeitig ist ein übermäßig verordnetes Maß an Sicherheit dazu geeignet, die Freiheit

einzuschränken. In einer freien und demokratischen Gesellschaft gilt es daher immer, die Balance zwischen Sicherheit und Freiheit zu gewährleisten. Sicherheit ist somit der zweite Kernbegriff unseres Verständnisses bei der Gestaltung des Internets. Unser Ziel ist es, zu mehr Vertrauen und Sicherheit im Internet beizutragen.

Wie soll diese Mithilfe aussehen?

DIVSI versteht sich als Forum für einen offenen und transparenten Dialog über Vertrauen und Sicherheit im Internet, in dem ökonomische, regulatorische, rechtliche, soziale, kulturelle, mediale und politische Perspektiven betrachtet werden. Mit unseren Projekten wollen wir den interdisziplinären Austausch von Wissenschaft, Wirtschaft, Gesellschaft und Politik fördern und unterstützen, um neue Erkenntnisse für die Steigerung von Vertrauen und Sicherheit im Internet zu gewinnen.

Das erste Forschungsprojekt - eine bundesweit angelegte bevölkerungsrepräsentative Milieu-Studie zu Vertrauen und Sicherheit im Internet - stellen wir in diesem ersten „DIVSI magazin“ ausführlich vor. In unserem Auftrag und auf der Basis gemeinsam entwickelter Fragestellungen hat das SINUS-Institut geforscht. Die Studie wurde im Januar abgeschlossen. Natürlich existieren bereits Arbeiten in angrenzenden Themengebieten. Eine derart detaillierte Studie gab es bislang jedoch nicht.

Die Entwicklung des Internets verläuft mit einer rasanten Geschwindigkeit. Mit der Studie wollten wir erfahren, welche Motivationen und Einstellungen die in Deutschland lebenden Menschen in ihrem Verhältnis zum Internet bestimmen und welche Erwartungen sie hinsichtlich Sicherheit und Datenschutz haben. Die Studie zeigt uns deutlich: Anders als bisher lautet die übergreifende Frage nicht mehr: Wie viele sind online, wie viele (noch) offline? Heute müssen wir uns mit den unterschiedlichen, ja sehr konträren Grundeinstellungen gegenüber dem Internet auseinandersetzen.

Die Studie eröffnet einen neuen Blick auf die Gesellschaft im Internetzeitalter. Nicht nur deshalb werte ich das 164 Seiten starke Werk als Erfolg. DIVSI stellt die Ergebnisse dieser Forschungsarbeit allen Interessierten kostenlos zur Verfügung.

Wer ist DIVSI ?

Das Deutsche Institut für Vertrauen und Sicherheit im Internet ist ein gemeinnütziges Institut, gegründet von der Deutsche Post AG. Es hat seinen Sitz in Hamburg. Die Gründung von DIVSI wurde auf der CeBIT 2011 bekanntgegeben. Anlässlich der Veröffentlichung der aktuellen DIVSI Milieu-Studie hat Briefvorstand Jürgen Gerdes dieses Engagement der Post bekräftigt: „Das Thema Vertrauen und Sicherheit beschäftigt alle Menschen in Deutschland. Wir brauchen eine Landkarte der Strukturen im Netz, damit wir künftig zeigen können, welche Pfade sicher sind. Und wie wir durch eigenes Verhalten Risiken vermindern können. Solche Landkarten im Web zu erstellen, die Wege darin zu erforschen und daraus neue Erkenntnisse über das Netz zu erzielen, die für uns alle als User wichtig sind – das ist der Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet – kurz DIVSI“.

Stolz sind wir darauf, dass Joachim Gauck uns im ersten Jahr des Instituts als Schirmherr zur Seite gestanden hat. Auf die Verbindung von Joachim Gauck und Internet bin ich mehrfach angesprochen worden: „Wie passt das eigentlich zusammen?“

Es passte, und zwar hervorragend. Joachim Gauck sieht die Bedeutung des Internets unter einem Blickwinkel, der sich hundertprozentig mit der DIVSI-Grundeinstellung deckt. Im Kern hat er sein Engagement stets so begründet: „Das Internet verändert unsere Welt und geht uns deshalb alle an – ob wir es selbst nutzen oder nicht. Wir wollen und müssen daher darauf vertrauen können, dass diese Technologie unserer Gesellschaft nutzt. Dieses Vertrauen erfordert einen transparenten Diskurs darüber, wie wir in Zukunft mit den Chancen und Risiken dieser faszinierenden, aber auch ambivalenten Technologie umgehen. Es ist unübersehbar, welchen Beitrag das Internet für mehr Wohlstand, Verteilungsgerechtigkeit und Freiheit leisten kann. Diese großen Chancen für eine bessere Zukunft müssen wir gemeinsam erhalten und ausbauen.“

Mehr über die Schwerpunkte unserer Arbeit finden Sie auf unserer Homepage (www.divsi.de).

Sieben Thesen zu Vertrauen und Sicherheit im Internet

Joachim Gauck, der erste Schirmherr von DIVSI, hat gemeinsam mit den Verantwortlichen des Instituts sieben Thesen entwickelt. Sie sind Richtschnur für die Arbeit und stehen unverrückbar fest.

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. **Die Menschen müssen darauf vertrauen dürfen, dass die Technologie ihnen nutzt.**
   Dafür ist ein transparenter und demokratischer Gestaltungsprozess erforderlich, in dem Politik, Wirtschaft und Gesellschaft produktiv zusammenwirken. Nur auf dieser Basis wird das Internet sein Potenzial voll entwickeln.

3. **Auch im Netz kann sich Freiheit nur dann entwickeln, wenn berechtigtes Vertrauen in die Sicherheit herrscht.**
   Erforderlich dafür ist eine Sicherheitspolitik, die uns erklärt, mit welchen Maßnahmen sie unser Recht im Internet schützt, von welchen Verhältnismäßigkeitsgrundsätzen sie sich leiten lässt und gegen welche Risiken wir uns in eigener Verantwortung schützen müssen.

4. **Straftaten im Internet müssen in verhältnismäßiger Form verfolgt werden. Die Anonymität des Netzes und die damit erschwerte Arbeit der Justiz wird zunehmend für kriminelle Zwecke missbraucht.**
   Wer solche Taten begeht oder unterstützt, schadet nicht nur den direkten Opfern. Er untergräbt auch das Vertrauen der Menschen ins Internet und gefährdet die großen Chancen dieser Technologie für die gesellschaftliche Entwicklung.

5. **Wirtschaft und Verwaltung haben ihnen anvertraute Daten vor Hackerangriffen zu schützen.**
   Besondere Sorgfalt muss dort walten, wo kritische Infrastrukturen über das Netz gesteuert und überwacht werden. Versorgungsnetze und gefährliche Industrieanlagen gehören nicht ans Internet.

6. **Bürger dürfen die Verantwortung für ihre Sicherheit nicht auf andere abwälzen.**
   Wer ungeschützte Computer am Internet betreibt, handelt fahrlässig. Er gefährdet damit sich und andere. Staat und Wirtschaft sind allerdings in der Pflicht, die Öffentlichkeit nachhaltig über Gefahren aufzuklären.

7. **Das freie und sichere Internet ist eine wichtige Triebfeder für eine Stärkung der Demokratie in aller Welt.**
   Es ist viel zu wichtig, nur Fachleuten überlassen zu werden. Dank Internet haben die Bürger nie dagewesene Möglichkeiten, Staat und Gesellschaft mit zu gestalten. Den Diskurs um die Grundregeln des Zusammenlebens im Internet muss unsere Gesellschaft gemeinsam führen. Bei positiver Nutzung kann das Internet Wohlstand, Verteilungsgerechtigkeit, Bildung und Informationsfreiheit fördern.

Stiftungslehrstuhl für Cyber Trust

Das Deutsche Institut für Vertrauen und Sicherheit im Internet unterstützt die TU München. Ein wichtiger Beitrag auch für den Forschungsstandort Bayern.

DIVSI hat der TU München eine Professur für Cyber Trust gestiftet. Direktor Matthias Kammer erläuterte dazu: „Wir wollen durch Unterstützung von Wissenschaft und Forschung einen Beitrag für mehr Vertrauen und Sicherheit im Internet leisten. Es geht darum, potenzielle Risiken von elektronischer Kommunikation und Transaktion zu untersuchen und zu analysieren."

Im Rahmen interdisziplinärer Forschung sollen durch den neuen Lehrstuhl die Risiken und Chancen des Netzes ganzheitlich analysiert werden, um darauf aufbauend ein umfassendes Risikomanagement zu entwickeln. Die DIVSI-Stiftung ergänzt die bereits bestehende Professur für Sicherheit in der Informatik von Professor Dr. Claudia Eckert. Mit den Ergebnissen wird die TU München wichtige Beiträge zu mehr Sicherheit und Vertrauen im Internet leisten.

Im Beisein von Bundesinnenminister Dr. Hans-Peter Friedrich, Staatssekretär Franz Josef Pschierer, dem Beauftragten der bayerischen Staatsregierung für

Prof. Dr. Helmut Krcmar, TU München, Bundesinnenminister Dr. Hans-Peter Friedrich, Jürgen Gerdes, Vorstand Brief Deutsche Post DHL, Franz Josef Pschierer, CIO Freistaat Bayern (v.l.n.r.)

IT, sowie Prof. Dr. Helmut Krcmar, Dekan der Fakultät Informatik, überreichte Jürgen Gerdes, Vorstand Brief der Deutschen Post, am Rande des Münchner IT-Gipfels die Stiftungsurkunde. Der Umfang dieser Förderung beläuft sich auf 3,5 Millionen Euro.

Jürgen Gerdes erklärte im Rahmen der feierlichen Urkunden-Übergabe: „Unsere Welt ist ohne Internet nicht mehr vorstellbar. Die Chancen für Gesellschaft, Wirtschaft und Staat sind unübersehbar. Die Beherrschung der zunehmenden Risiken dieser Technologie erfordert jedoch grundlegend neue Ansätze. Hier setzt die Stiftungsprofessur an."

Die DIVSI-Stiftung fügt sich nahtlos in die strategische Entwicklung der TU München ein. Darüber hinaus fördert sie die Entwicklung der Landeshauptstadt als Standort für Computersicherheit. Damit leistet die neue Professur auch einen wichtigen Beitrag für den Forschungs- und Technologiestandort Bayern.

Technische Universität München

Die TUM zählt zu den besten Universitäten Deutschlands. Spitzenleistungen in Forschung und Lehre, Interdisziplinarität und Talentförderung zeichnen sie aus. Dazu kommen starke Allianzen mit Unternehmen und mit wissenschaftlichen Einrichtungen auf der ganzen Welt. Die Fächerkombination der TUM ist in Europa einzigartig. Sie bildet rund 31.000 Studierende in 142 Studiengängen aus. Ihre Wissenschaftler lehren und forschen disziplinübergreifend.

Die TU München sieht sich in ihrem Grundverständnis als „Dienerin der Innovationsgesellschaft". Sie ist deshalb dem Innovationsfortschritt auf Wissenschaftsgebieten verpflichtet, die das Leben und Zusammenleben der Menschen nachhaltig zu verbessern versprechen.

Dem Leitbild der unternehmerischen Universität verpflichtet, bekennt sich die TUM zum wettbewerblichen Leistungsprinzip. Sie bringt proaktiv Ergebnisse der Grundlagenforschung in marktorientierte Innovationsprozesse ein und fördert den „entrepreneurial spirit" in allen Bereichen der Universität. Ihr unternehmerisches Handeln richtet sich konsequent danach aus, eine europaweite Führungsrolle bei der Ausgründung wachstumsorientierter Technologie-Start-ups aus der Wissenschaft heraus einzunehmen.

Die große Herausforderung

Darum ist Cyber Trust nur interdisziplinär zu bewältigen.

Von Prof. Dr. Claudia Eckert

Informations- und Kommunikationstechnologie (IKT) ist heute in vielen Bereichen des wirtschaftlichen und gesellschaftlichen Lebens von zentraler Bedeutung. Sowohl im beruflichen als auch im privaten Alltag sind wir umgeben von IT-Systemen, die uns mit Informationen versorgen, uns bei Entscheidungen unterstützen, Geschäftsprozesse beschleunigen oder aber auch einfach unseren Komfort fördern.

IKT als Innovationstreiber

Ohne intelligente, IKT-gestützte medizinische Geräte, ohne die IKT-unterstützte Fern-Diagnose- und Fern-Therapiemöglichkeiten wäre der heutige hohe Standard in der Gesundheitsversorgung nicht möglich. Aber auch unsere hoch-technologisierten Produktions- und Fertigungsanlagen, die Spitzenprodukte z.B. für die Automobilindustrie und den Maschinenbau fertigen, sind ohne komplexe Roboter und IKT-gesteuerte Produktionsanlagen nicht denkbar. Ähnliches gilt für moderne Logistikprozesse, die für eine ressourcenschonende, kosteneffiziente, just-in-time-Produktion unerlässlich sind.

Auch im Privatleben nutzen wir zunehmend Informations- und Kommunikationstechnologien, um beispielsweise über das Internet Einkäufe oder Bankgeschäfte elektronisch abzuwickeln, oder um soziale Kontakte über soziale Netzwerke zu pflegen. Durch mobile Endgeräte hat sich der Anteil der Internet-Nutzer in den letzten Jahren gewaltig erhöht. Medien wie Youtube, oder soziale Netze wie Facebook führen zu einem geänderten Kommunikations- und Interaktionsverhalten und einem ganz anderen Umgang mit persönlichen Daten als dies bislang üblich war. Dies führt gleichzeitig zu einer Veränderung in den Unternehmensabläufen. Mit dem Stichwort „Bring your own Device" wird ein Trend bezeichnet, der den Wunsch vieler Mitarbeiter beschreibt, ihre privaten Geräte auch für Unternehmensprozesse zu verwenden.

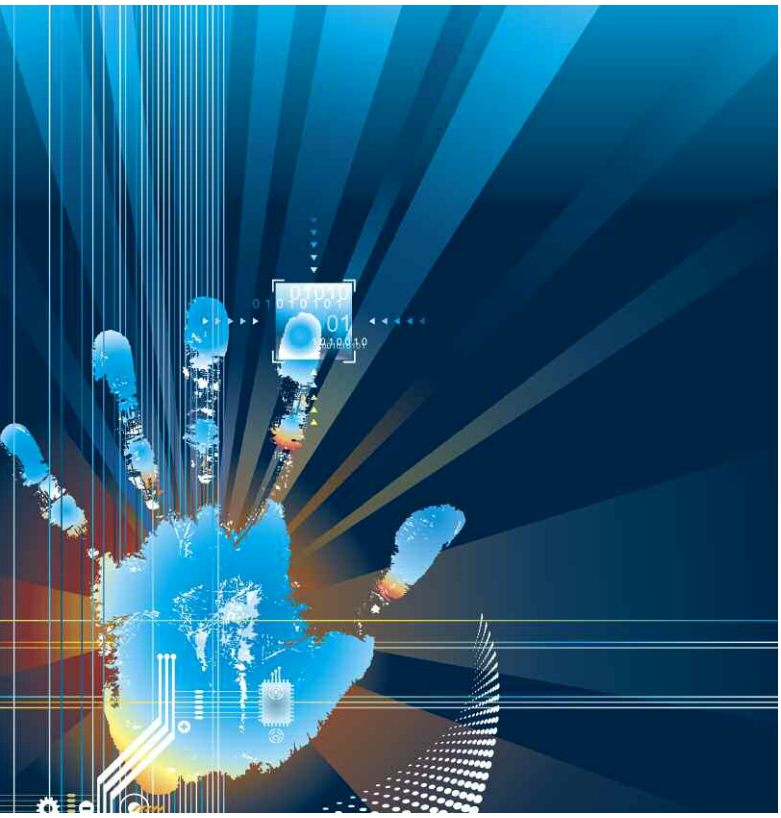
Die Verschmelzung der physikalischen Welt mit der IT-gestützten, virtuellen wird sich in der Zukunft noch weiter verstärken. Es entsteht der so genannte Cyberspace, mit einer Vielzahl von neuen Möglichkeiten, um zentrale gesellschaftliche Herausforderungen, wie die alternde Gesellschaft, die zunehmende Ressourcenknappheit oder auch die Unterstützung selbstbestimmter Mobilität zu meistern. Insbesondere für eine hoch-technologisierte Wirtschaftsnation wie Deutschland ist IKT eine Schlüsseltechnologie für Innovationen und die Festigung des Wirtschaftsstandorts.

IKT benötigt Sicherheit und Vertrauen

Bei allen Aktivitäten im Cyberspace wird täglich eine immense Menge an Daten und Informationen erfasst, auf unterschiedlichsten Wegen, insbesondere über das Internet, übertragen und auf diversen Geräten verarbeitet und gespeichert. Die Daten dienen der Steuerung und Überwachung von unternehmenskritischen Abläufen, sie steuern das Verhalten von Fahrzeugen oder auch von sicherheitskritischen Anlagen wie Chemieanlagen. Eine gezielte Manipulation dieser Daten könnte somit verheerende Konsequenzen haben. Daten und Informationen kön-

***Prof. Dr. Claudia Eckert** (* 1959) ist Leiterin des Lehrstuhls „Sicherheit in der Informatik" an der TU München sowie Leiterin des Fraunhofer AISEC (Angewandte und Integrierte Sicherheit) in München. Ihr Diplom in Informatik erwarb sie an der Uni Bonn, 1993 promovierte und 1999 habilitierte sie an der TU München zur Thematik „Sicherheit in verteilten Systemen". Ihre Forschungs- und Lehrtätigkeiten finden sich in den Arbeitsgebieten Betriebssysteme, Middleware, Kommunikationsnetze sowie Informationssicherheit. Eckert ist Vize-Präsidentin der Gesellschaft für Informatik (GI) und Mitglied in wissenschaftlichen Beiräten, unter anderem im Verwaltungsrat des Deutschen Forschungsnetzes (DFN), OFFIS, Bitkom sowie der wissenschaftlichen Kommission der Einstein-Stiftung Berlin. Außerdem berät sie Ministerien und die öffentliche Hand auf nationaler und internationaler Ebene bei der Entwicklung von Forschungsstrategien und der Umsetzung von Sicherheitskonzepten. Prof. Dr. Eckert arbeitet auch beim Deutschen Institut für Vertrauen und Sicherheit im Internet (DIVSI) mit.*

nen aber auch ein wertvolles Wirtschaftsgut sein, man denke beispielsweise an Finanzdaten oder Forschungsergebnisse, die vor unberechtigten Zugriffen und Manipulationen zu schützen sind. Täglich hinterlassen wir eine Vielzahl von Datenspuren, sei es mehr oder weniger bewusst durch die Nutzung des mobilen Internets oder eher unbewusst, wie beispielsweise über Aufnahmen durch Videoanlagen, die zunehmend aus Gründen der öffentlichen Sicherheit in Geschäften, öffentlichen Anlagen oder Plätzen installiert sind. Aufenthaltsdaten, Bewegungsprofile, Nutzungsprofile oder auch Gewohnheiten werden auf diese Weise erfasst und stellen eine erhebliche Bedrohung für unsere Privatsphäre dar.



Die Gewährleistung einer datenschutzbewahrenden Verarbeitung von Daten ist demnach eine zentrale Aufgabe. Dies allein reicht jedoch nicht aus, um die Sicherheitsbedürfnisse im Cyberspace zu befriedigen. Vielmehr werden sehr viel umfassendere Maßnahmen erforderlich sein, um die Korrektheit, Vollständigkeit und rechtzeitige Verfügbarkeit der Daten sowie die sichere Kommunikation und die Vertrauenswürdigkeit der eingesetzten IT-Komponenten zu gewährleisten. Dies stellt deshalb eine ganz erhebliche Herausforderung sowohl für die Wissenschaft als auch für die Wirtschaft und unsere gesamte Gesellschaft dar. Diese Herausforderung fassen wir unter dem Schlagwort Cyber Trust zusammen.

Cyber Trust – Vertrauen schaffen

Cyber Trust umfasst technologische, organisatorische, aber auch kulturelle Maßnahmen zur Steigerung von Vertrauen in IKT-basierte Systeme und Abläufe. Diese Aufgabenstellung ist von immenser Bedeutung für die Gesellschaft, aber auch für den Wirtschaftsstandort Deutschland. Erforderlich sind neue methodische und technologische Ansätze, um die Sicherheit und Vertrauenswürdigkeit von IKT-Systemen prüfbar und kontrollierbar zu erhöhen. Das mit der Nutzung der IKT-Systemen einhergehende Risiko muss methodisch erfasst und quantifiziert werden und es müssen Prozesse und Verfahren entwickelt werden, um Risiken zu minimieren und um mit den verbleibenden Risiken verantwortungsvoll umzugehen. Cyber Trust ist somit ein sehr komplexes, wissenschaftlich noch neues Themengebiet, das neben den technischen Fragestellungen auch betriebswirtschaftliche, juristische und gesellschaftswissenschaftliche sowie sozialwissenschaftliche Fragestellungen aufwirft. Eine solche breit gefächerte Thematik ist deshalb nur interdisziplinär, mit einer starken Fundierung in den technischen und ingenieurwissenschaftlichen Disziplinen zu bewältigen.

Stiftungsprofessur Cyber Trust

Mit der Stiftungsprofessur Cyber Trust hat das Deutsche Institut für Vertrauen und Sicherheit im Internet (DIVSI) einen wichtigen Schritt getan, dieses wichtige Zukunftsthema in einer exzellenten Umgebung, nämlich in der Fakultät für Informatik an der Technischen Universität München, zu bearbeiten. Zu den geplanten Forschungsschwerpunkten der Stiftungsprofessur zählen die Erforschung von Verfahren und Werkzeugen zur Risiko-Modellierung und zur Risiko-Bewertung komplex vernetzter Systeme, die Entwicklung und Erprobung neuer Methoden und Werkzeuge zur Verwaltung digitaler Identitäten und zum Aufbau von Vertrauen in vernetzten Systemen oder aber auch die Erforschung von datenschutzbewahrenden Technologien für zukünftige Internet-basierte Anwendungen wie beispielsweise Smart-Grids, eHealth oder SmartHome.

Mit der Stiftungsprofessur soll eine Brücke zwischen den ingenieurwissenschaftlichen, den betriebswirtschaftlichen (Risikomanagement) und den gesellschaftlichen Ansätzen zum Umgang mit Risiken und zum Aufbau von Vertrauen geschlagen werden. Die Stiftungsprofessur wird dazu sehr eng mit dem Lehrstuhl für Sicherheit in der Informatik (Prof. Dr. C. Eckert) und dem Lehrstuhl für Wirtschaftsinformatik (Prof. H. Krcmar) zusammenarbeiten. Zusammen mit den bestehenden Lehrstühlen und der Münchner Fraunhofer Forschungseinrichtung für Angewandte und Integrierte Sicherheit (AISEC) soll ein Zentrum für Cyber Trust aufgebaut werden, das neben wissenschaftlich exzellenter Forschung auch den engen Kontakt zur Industrie, zum Verbraucher und zur Politik sucht, um über Veranstaltungen und Veröffentlichungen einen Wissens- und Technologietransfer zu unterstützen und zur Bewusstseinsbildung in der Gesellschaft beizutragen. Das Zentrum wird sehr eng mit internationalen Partnern zusammenarbeiten und renommierten, internationalen Gastwissenschaftlern Möglichkeiten für Forschungsaufenthalte an der TU München eröffnen. Das Zentrum soll noch in diesem Jahr seine Arbeit aufnehmen.

Die Kernbotschaften der DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet

27 Millionen sind Digital Outsiders. Zwei Gräben trennen unsere digitale Gesellschaft. Drei Viertel der Deutschen erwarten, dass Staat und Wirtschaft aktiv für ihre Sicherheit im Internet sorgen.

Von Dr. Silke Borgstedt

Die „DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet" liefert wichtige und neue Erkenntnisse für alle, die sich in welcher Weise auch immer mit dem Internet beschäftigen – sei es aus den Bereichen Politik, Wirtschaft oder Öffentlichkeit. Die Ergebnisse der Studie – im Auftrag von DIVSI durch das Sinus-Institut realisiert – stellen gleichzeitig eine Reihe von festgeschriebenen Behauptungen infrage, die bislang als gesichert galten.

Nie zuvor wurde eine derartige Untersuchung so differenziert und mit solcher Detailgenauigkeit durchgeführt. Deshalb bilden die zentralen Ergebnisse der Studie eine Grundlage, auf der sich verschiedene Maßnahmen zur Steigerung von Vertrauen in das Internet und zur Förderung von Sicherheit im Internet entwickeln lassen.

Grundsätzlich unterscheidet die DIVSI Studie drei Bevölkerungsgruppen in Deutschland in Bezug auf deren Einstellungen zum Internet sowie dessen Nutzung:

- *Digital Outsiders*. Sie sind entweder vollständig offline oder stark verunsichert im Umgang mit dem Internet. Deshalb nutzen sie es so gut wie gar nicht.
- *Digital Natives*. Sie sind mit dem Internet groß geworden und haben es in vollem Umfang in ihr Leben integriert.
- *Digital Immigrants*. Sie bewegen sich regelmäßig aber sehr selektiv im Internet. Vielen Entwicklungen stehen sie skeptisch gegenüber. Dies besonders, wenn es um die Themen Sicherheit und Datenschutz geht.

Eine Unterscheidung zwischen technisch online oder offline spiegelt die Realität nicht richtig wider

Die Untersuchung hat ergeben, dass fast 40 Prozent der Deutschen *Digital Outsiders* sind. Die bisherige Differenzierung von ca. 80 Prozent Onlinern und ca. 20 Prozent Offlinern ist nach den aktuellen Erkenntnissen nicht stimmig. Sie führt vielmehr zu Fehldeutungen über den Zustand der digitalen Gesellschaft in Deutschland.

Dr. Silke Borgstedt *(*1975) studierte Musikwissenschaft, Psychologie und Erziehungswissenschaften an der Carl-von-Ossietzky-Universität Oldenburg und an der Technischen Universität Berlin. 2007 promovierte sie an der Humboldt-Universität zu Berlin mit einem Stipendium der Studienstiftung des deutschen Volkes. Von 2005 bis 2009 war sie als Research Manager bei GIM (Gesellschaft für Innovative Marktforschung) im Bereich der internationalen Konsumforschung mit den Schwerpunkten FMCG, Entertainment Industries und Zielgruppensegmentierung tätig sowie als Lehrbeauftragte an verschiedenen Universitäten. Seit Anfang 2009 ist Dr. Borgstedt Studienleiterin beim Sinus-Institut in Heidelberg. Ihre Arbeits- und Themenschwerpunkte sind Familiensoziologie, Jugend, Trendforschung, Alltagsästhetik, Umweltbewusstsein und -semantik sowie Kultur- und Medienindustrie.*

Die Ergebnisse der DIVSI Studie zeigen, dass tatsächlich doppelt so viele Menschen in Deutschland komplett oder nahezu komplett ohne Internet leben, wie bislang angenommen. Unsere digitale Gesellschaft zählt etwa 72 Millionen Menschen. Davon sind also fast 27 Millionen *Digital Outsiders*.

Eine weitere Erkenntnis: Rund 41 Prozent, sind *Digital Natives*. Das sind Menschen, die mit dem Internet groß geworden sind und es in vollem Umfang in ihr Leben integriert haben. Für sie ist ein Alltag ohne das Netz nicht (mehr) vorstellbar. Ihr Lebensmotto könnte lauten: Ich surfe, also bin ich.

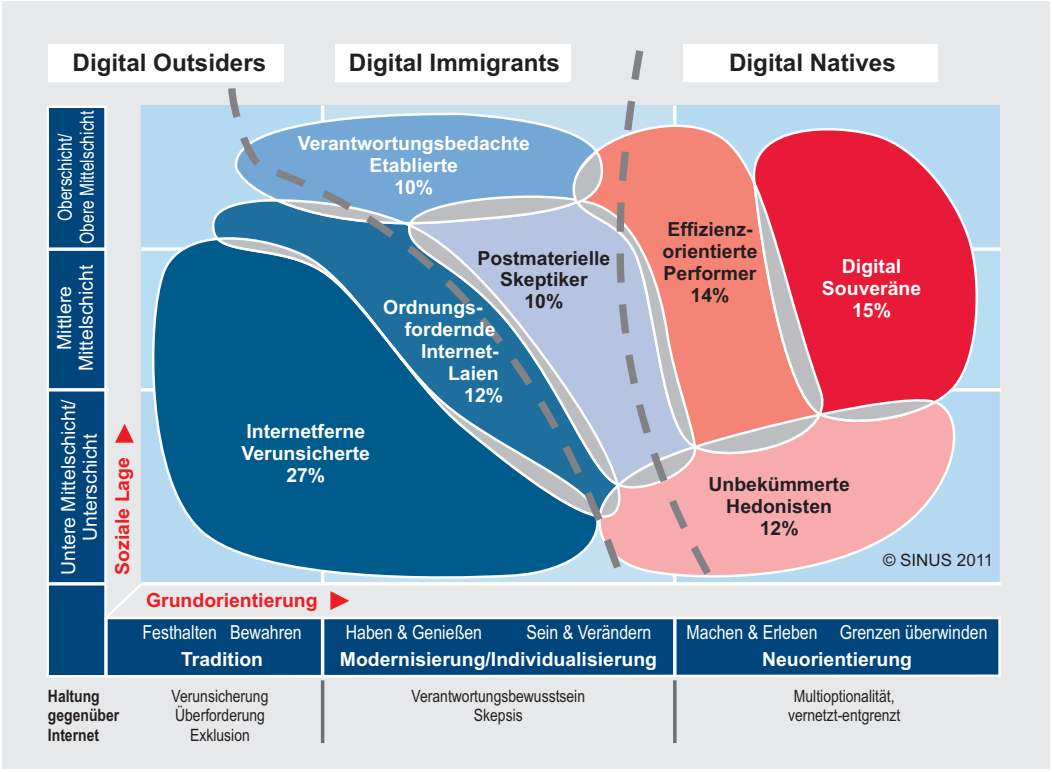
Die verbleibenden ca. 20 Prozent der Deutschen sind *Digital Immigrants*. Sie nutzen das Internet einerseits gezielt dort, wo es einen unmittelbaren Nutzen verspricht – etwa bei der Planung eines Urlaubs oder bei der Suche nach einem Schnäppchen zu bestimmten Artikeln. Andererseits hegt diese Gruppe zum Teil konkrete Vorbehalte gegen das Internet und achtet deshalb darauf, sich von dieser Technik nicht abhängig zu machen.

Der erste trennt die *Digital Outsiders* auf der einen von den *Digital Immigrants* und den *Digital Natives* auf der anderen Seite. Für die *Digital Outsiders* stellt das Internet eine digitale Barriere vor einer Welt dar, von der sie sich ausgeschlossen fühlen und zu der sie keinen Zugang finden.

Der zweite Graben verläuft zwischen den *Digital Natives* auf der einen Seite und den *Digital Immigrants* und den *Digital Outsiders* auf der anderen Seite. Die *Digital Natives* begreifen das Internet als einen Tummelplatz, in dem sie sich frei und ganz selbstverständlich bewegen. Für sie stellt die digitale Welt einen wesentlichen Teil des Lebens dar. Sie stehen ihr sehr positiv gegenüber und können nicht nachempfinden, dass sich die anderen Gruppen im Internet nicht ebenso zuhause fühlen.

Neben diesen Befunden zeigt die „DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet" einen weiteren wichtigen Ergebniskomplex. Dieser enthält zwei wesentliche Aspekte. Es geht dabei um ganz unterschiedliche Verant-

Die nebenstehende Abbildung zeigt eine Projektion der Typen auf das Bezugssystem der Sinus-Milieus mit den beiden Hauptachsen Grundorientierung (horizontal) und soziale Lage (vertikal). In diesem soziokulturellen Raum sind die sieben Typen entsprechend ihres jeweiligen dominanten Milieu-Hintergrunds positioniert. Je höher eine Gruppe in dieser Grafik angesiedelt ist, desto gehobener sind Bildung, Einkommen und Berufsgruppe; je weiter nach rechts sie sich erstreckt, desto moderner im soziokulturellen Sinn ist die Grundorientierung.



Bei allen Diskussionen um den Zustand der digitalen Gesellschaft in Deutschland ist man bislang davon ausgegangen, dass diese nur durch den Graben zwischen Onlinern und Offlinern gespalten sei. Eine auf technisch online oder offline beschränkte Unterscheidung spiegelt jedoch die Realität nicht richtig wider. Es muss auch beachtet werden, wie die Menschen das Internet tatsächlich nutzen. Nach einer solchen Betrachtung kommt die Studie zu dem Ergebnis, dass es zwei Gräben in der digitalen Gesellschaft gibt.

wortungskonzepte in Bezug auf die Internet-Nutzung. Die einen fordern mehr staatliche Hilfe zur sicheren Nutzung des Internets. Die anderen betonen die Eigenverantwortlichkeit jedes Users. Konkret hat die Studie gezeigt: Fast drei Viertel der Deutschen (74 Prozent) erwarten, dass Staat und Wirtschaft aktiv für ihre Sicherheit im Internet sorgen. Die Mehrzahl der *Digital Natives* dagegen sieht hier den Nutzer selbst in der Pflicht. Diese Gruppe fühlt sich souverän genug, die Risiken des Internets zu kennen und damit umgehen zu können. Freiheit, Nutzen und Flexibilität haben absoluten Vorrang vor staatlicher Reglementierung, die sie zum Teil kategorisch ablehnen.

Ganz unterschiedliche Überzeugungen ermittelt die Studie in der Frage, wie sicher das Internet überhaupt sein kann. Etwa ein Drittel der Internetnutzer glaubt, dass vollständige Sicherheit im Netz möglich ist. Dieser Ansicht ist in besonderem Maße die Gruppe der *Digital Natives*. Etwa die Hälfte der Nutzer ist dagegen überzeugt, dass eine vollständige Sicherheit im Netz nicht möglich ist. Der verbleibende Rest wagt zu dieser Frage keine klare Stellungnahme.

Die Ergebnisse der „DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet" machen insgesamt deutlich: Die Politik steht vor der schwierigen Herausforderung, diametrale Sicherheitsbedürfnisse befriedigen zu müssen. Noch einmal die beiden Eckpunkte:

- Fast drei Viertel der Bevölkerung erwarten staatliche Maßnahmen zur Gewährleistung von Sicherheit im Internet.

- Die von solchen staatlichen Maßnahmen am stärksten betroffene Gruppe der *Digital Natives* lehnt staatliche Reglementierung mehrheitlich ab und hat z. T. kein Verständnis für die Probleme und Bedürfnisse der anderen Bevölkerungsgruppen in Bezug auf das Internet und dessen Nutzung.

Die große gesellschaftspolitische Herausforderung liegt also darin, diese unterschiedlichen Welten zu versöhnen.

sinus HEIDELBERG BERLIN ZÜRICH
Partner von INTEGRAL Wien

Die SINUS Markt- und Sozialforschung GmbH, Heidelberg, ist Spezialist für psychologische und sozialwissenschaftliche Forschung und Beratung. Gegenstand der Arbeit ist seit über 30 Jahren die Alltagswirklichkeit der Menschen, der soziokulturelle Wandel, die Verfassung der Gesellschaft sowie die Anwendung der SINUS-Forschungen im Zusammenhang mit Trends, Zielgruppen und Märkten. SINUS entwickelt Expertisen und Strategien für Unternehmen und Institutionen in den Bereichen Konsum, Ökologie, Kultur und Politik mit besonderem Fokus auf Wertewandel, Lebenswelten (Sinus-Milieus®), Alltagsästhetik sowie soziokulturelle Strömungen, Trends und Zukunftsszenarien. Das SINUS-Institut unterhält eine Vielzahl internationaler Forschungs- und Beratungs-Kooperationen und hat weltweit ein Netzwerk von Experten aus den unterschiedlichsten Disziplinen aufgebaut: Führende Agenturen und Berater, spezialisierte Forschungsinstitute, Markentechniker, Direktmarketer und namhafte Designexperten kooperieren seit Jahren – zum Teil exklusiv – mit Sinus.

Milieu-Studie überrascht

Bundesweit große Resonanz auf die Pressekonferenz in Berlin. Diskussion angestoßen, die der Thematik nur dienlich sein kann

DIVSI-Direktor Matthias Kammer hat bei einer Pressekonferenz in Berlin gemeinsam mit Dr. Silke Borgstedt (SINUS) die Ergebnisse der bevölkerungsrepräsentativen „Milieu-Studie zu Vertrauen und Sicherheit im Internet" vorgestellt.

DIVSI-Direktor Matthias Kammer erläuterte gemeinsam mit Dr. Silke Borgstedt (SINUS) die „Milieu-Studie zu Vertrauen und Sicherheit im Internet" in den Räumlichkeiten der Bundespressekonferenz.

Die bundesweite Resonanz auf die vorgelegten Fakten quer durch alle unterschiedlichen Medien ist gewaltig. Matthias Kammer: „Unser erstes Ziel ist damit erreicht. Wir haben eine Diskussion angestoßen, die der Thematik insgesamt nur dienlich sein kann."

Mit Überraschung wurde in der Öffentlichkeit die Erkenntnis aufgenommen, dass in Deutschland 39 Prozent der Bevölkerung über 14 Jahre (rund 27 Millionen Menschen) noch immer zu den „Digital Outsiders" zählen. Matthias Kammer verdeutlichte im Rahmen der Pressekonferenz, was darunter genau zu verstehen sei: „Das sind Menschen, die entweder gar nicht online sind oder ihren Internetzugang aus Unvermögen, Angst, Unsicherheit oder Misstrauen wenig bis gar nicht nutzen."

Beim Thema Datenschutz und Sicherheit seien viele überfordert und daher misstrauisch, erläuterte Matthias Kammer weiter. Etwa drei Viertel der Deutschen erwarten Schutzmaßnahmen von Staat und Wirtschaft, der Rest lehnt diese ab. Das daraus resultierende Problem fasst der DIVSI-Direktor so zusammen: „Wer sich im Internet nicht auskennt, fordert Schutz. Wer sich sicher fühlt, wünscht Freiheit."

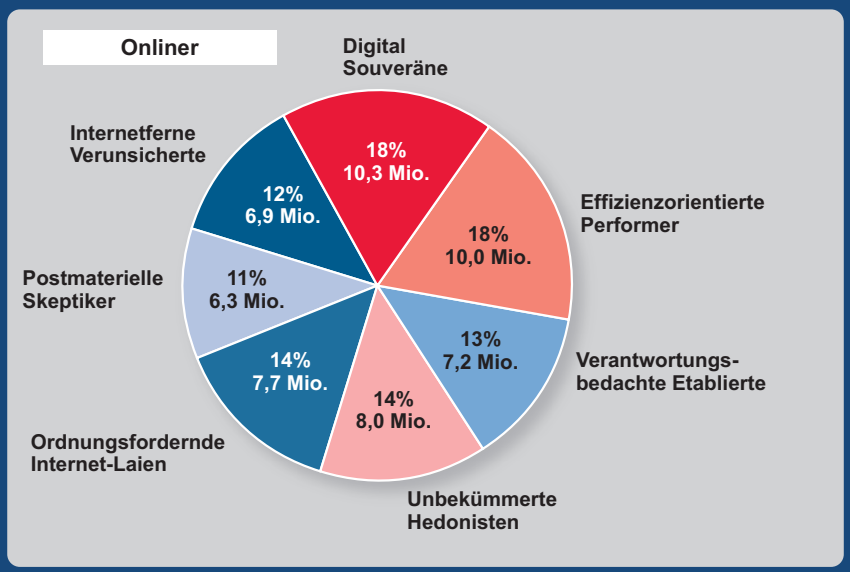
Laien, Souveräne, Hedonisten und Co.

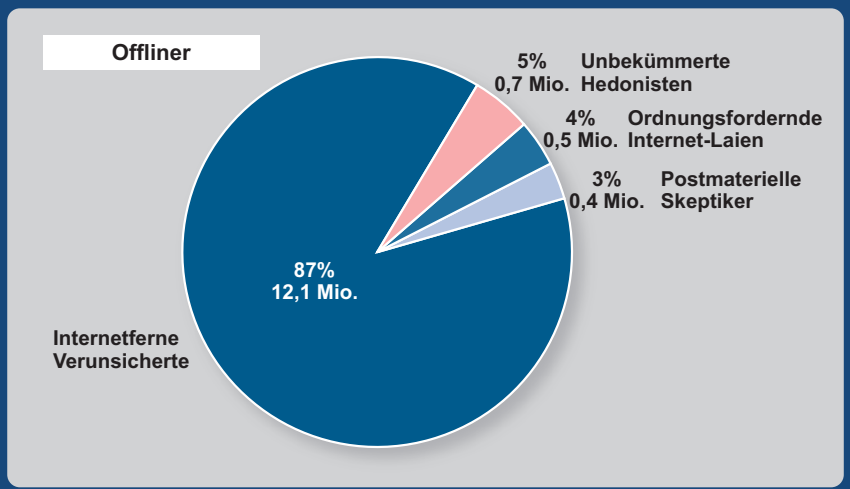
Eine Studie, sieben unterschiedliche Mileus. Welcher Typ Mensch verbirgt sich jeweils dahinter? Aufschluss bringt eine Kurz-Charakteristik.

Von den „Internetfernen Verunsicherten" bis zu den „Digital Souveränen" kennzeichnet die Milieu-Studie zu Vertrauen und Sicherheit im Internet sieben unterschiedliche Milieus.

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

Internet-Milieus: Verteilung bei Onlinern und Offlinern





Basis: Onliner ab 14 Jahren, n = 1.605 (80%), ca. 56,441 Mio.
Offliner ab 14 Jahren, n = 395 (20%), ca. 13,891 Mio.

Welcher Typus steckt jeweils hinter den sieben Internet-Milieus? Aufschluss dazu geben die folgenden Kurz-Charakteristika.

Digital Souveräne

Sie sind meist schon mit dem Internet aufgewachsen. Technik-Faszination und entspannter Fortschrittsoptimismus sind zentrale Motivatoren, sich mit moderner IT auseinanderzusetzen. Der Umgang mit Computer und Internet gehört für sie zentral zu ihrer Alltagswirklichkeit. 88 Prozent dieser Gruppe können sich ein Leben ohne Internet überhaupt nicht mehr vorstellen. Keine andere Gruppe bewegt sich so selbstsicher im Netz. Sie haben hier keine Berührungsängste. Einerseits fühlen sie sich kompetent, andererseits legen sie großes Vertrauen in digitale Medien. Chancen und Möglichkeiten sind für sie bei weitem gewichtiger als die Risiken.

Effizienzorientierte Performer

Sie sind Intensiv-Nutzer des Internets. Auch sie zählen mit zu dem Kreis, die von Anfang an die digitale Revolution miterlebt und befördert haben. Für 89

Prozent dieses Typus ist ein Leben ohne Internet nicht mehr vorstellbar. Diese große Selbstverständlichkeit geht auch damit einher, dass in ihrem Arbeitsalltag nahezu alle produktiven, organisatorischen und kommunikativen Prozesse mit dem Internet verknüpft sind. Viele von ihnen verstehen sich als moderne Leistungsträger der Gesellschaft. Ihre tägliche Internetnutzung mit 65 Prozent liegt weit über dem Bevölkerungsdurchschnitt.

Unbekümmerte Hedonisten

In ihrem Leben spielt das Internet eine zentrale Rolle als schneller, unkomplizierter Weg zu Unterhaltungsangeboten aller Art. Das Internet bedeutet für sie grenzenloser Freiraum und Austausch mit Gleichgesinnten. Die Zukunft sehen sie eindeutig digital und gehen davon aus, dass das Internet vieles erleichtern wird, was heute noch mühsam und umständlich ist. Bei technologischen Neuerungen zählen sie nicht zu den ersten Entdeckern, sind aber recht frühzeitig dabei. Sie verfügen über mittlere Internet-Kompetenz und –Erfahrung, haben jedoch wenig Berührungsängste mit dem Medium.

Postmaterielle Skeptiker

Dieses Gesellschaftssegment vereint ein kritischer Blick auf blinden Forschrittsoptimismus, ungebremste Wachstumsgläubigkeit sowie zunehmende Fragmentierung sozialer Beziehungen. Entschieden sprechen sie sich dafür aus, dass Technologien und Internet nicht die Alltagsgestaltung dominieren sollten. Es geht ihnen hingegen darum, aus den vielfältigen Handlungsoptionen zu selektieren und dabei Kosten und Risiken gegeneinander abzuwägen. Trotz ihrer Skepsis gegenüber neuen Medien gehören sie jedoch nicht zu den Nachzüglern in Sachen Internet. Im Umgang mit dem Computer ist dieser Typ geübt und neugierig.

Verantwortungsbedachte Etablierte

Diese Gruppe beinhaltet anspruchsvolle, selektive Nutzer. Man ist interessiert an technischen Innovationen und deren Nutzungsmöglichkeiten, verfügt aber nur über eine mittlere Internet-Expertise. Vertreter dieses Typs nutzen das Internet primär als Arbeits- und Kommunikationsmedium, nicht zur Unterhaltung. Insgesamt gehen sie sehr gezielt und verantwortungsbewusst vor. Ausgeprägtes Sicherheitsbewusstsein und Schutzmaßnahmen haben hohe Priorität. Das weniger aus Angst, sondern weil es dazu gehört. Dieses Gruppe ist bestrebt, ihre Privatsphäre durch Zurückhaltung, Kontrolle und Vermeidung zu schützen.

Ordnungsfordernde Internet-Laien

In ihrem Leben spielt das Internet keine große Rolle. Sie haben ein zwiespältiges Verhältnis zu moderner Informationstechnik. Einerseits zeigen sie sich aufgrund fehlender Kompetenz im Umgang damit verunsichert. Andererseits ist ihnen bewusst, dass dem Internet die Zukunft gehört und sie sich dem fortschreitenden Digitalisierungsprozess nicht verschließen dürfen, wenn sie berufliche Chancen und sozialen Anschluss nicht aufs Spiel setzen möchten. Das „Mithalten-Wollen“ ist für sie zentraler Motivator, sich mit Computer und Internet auseinanderzusetzen. Als preisbewusstes und serviceorientiertes Gesellschaftssegment erkennt diese Gruppe zunehmend die Convenience-Vorteile im Internet.

Internetferne Verunsicherte

Zwei Drittel von ihnen sind Offliner. Der Rest dieser Gruppe ist Gelegenheitsnutzer mit sehr geringem Internet-Wissen und nur geringen Berührungspunkten mit digitalen Medien im Alltag. Das Internet ist für sie eine fremde Welt, die verunsichernd und bedrohlich wirkt. Nur wenige sind motiviert, sich mit den technischen Neuerungen zu beschäftigen. Der Weg ins Netz wird als mühsam und weit empfunden. Konfrontiert mit internettypischen Abkürzungen und Zeichen fühlen sie sich einem Gerät ausgesetzt, das eine fremde Sprache spricht und ihr Anliegen nicht versteht. Das Internet erscheint ihnen als ein gänzlich fremder Kosmos.

Generationenkonflikt bei der Sicherheit

Der Vater: Clouds im Cyberspace – Fortschritt oder Konterrevolution? Wolken ziehen im Internet auf, die Cloud kommt. Sie will meine Daten und verspricht mir dafür, dass ich immer und überall darauf zugreifen kann. Ich frage mich: Macht die Cloud uns freier oder fängt die Revolution jetzt an, ihre Kinder zu fressen?

Von Harald Lemke

Der Personal Computer löste in den 70ern des vorigen Jahrtausends eine globale Revolution aus. Die von der Herrschaft der Großrechner befreiten Benutzer vernetzten sich bald über Usenet, AOL und Compuserve zu einer digitalen Gemeinde, ohne die der weltweite Siegeszug des Internets nicht möglich gewesen wäre.

Dabei war „das Netz" schon immer ein Widerspruch in sich. Es nimmt nicht gefangen, sondern macht frei. Die herausragende Rolle des Internets für mehr Demokratie und Befreiung von Terror-Herrschaft ist evident. Dabei war der eigene PC schon immer ein essenzieller Teil dieser Freiheit. Ein kleiner, aber souveräner Planet im Cyberspace, auf dem sein Besitzer unmittelbare Kontrolle über die eigenen Daten hat.

__Harald Lemke__ (1956) ist seit Juli 2010 Sonderbeauftragter für E-Government und E-Justice bei der Deutschen Post. Von 2003 bis 2008 arbeitete er im Range eines Staatssekretärs als CIO für das Land Hessen. Es war das erste Mal überhaupt, dass in einem Bundesland eine solche Position eingerichtet wurde. Zwischenzeitlich war Lemke Berater für McKinsey&Company. 2002/2003 arbeitete er als IT-Direktor des BKA in Wiesbaden und war dort unter anderem zuständig für die Einführung von INPOL-neu. Er gehört der Enquete-Kommission Internet und digitale Gesellschaft des Bundestages an und leitet dort die Projektgruppe „Zugang, Struktur und Sicherheit im Internet".*

Geht diese Souveränität dem Ende zu?

Der aktuelle Anlass für meine Sorge ist schnell geschildert: Ich denke in Bildern. Bilder helfen mir, Komplexität zu beherrschen und für andere begreifbar darzustellen. Ein Bild sagt eben mehr als tausend Worte. Deshalb war mir das iPad als mobiler Skizzenblock hochwillkommen und Ideas von Adobe meine Lieblings-App. Viel flexibler als ein Block Papier und immer dabei.

Dann habe ich mein iPad durch ein Android-Tablet ersetzt. Freiheit war übrigens das Hauptmotiv für diesen Wechsel. Raus aus einem geschlossenen System unter der Diktatur von Apples iTunes. Ideas war die erste Android App, die ich mir kaufte. Und dann der Schock. Denn als ich meine Skizze wie gewohnt als PDF exportieren wollte, ging das nicht mehr. Nach dem Willen von Adobe läuft das nur noch über die Creative Cloud, natürlich von Adobe. Ich soll also meine eigenen Dokumente über die Adobe Cloud mit mir selbst „sharen", so das neue Buzzwort zur Cloud.

Völlig sichere Sache, verspricht Adobe. Niemand könne auf meine persönlichen Dokumente zugreifen. Und was ist mit einer verschlüsselten Ablage? Fehlanzeige, natürlich. Schließlich muss Adobe meine Dokumente lesen können, damit sie für mich die PDF-Konvertierung durchführen kann. Dabei ist Adobe kein Einzelfall. Flickr, Evernote, Dropbox und GoogleDocs sind weitere Beispiele für Anwendungen, bei denen Nutzer die Kontrolle über persönliche Dokumente für immer aus der Hand geben.

Selbst Spracherkennung auf Tablet-PCs und Smartphones läuft nur noch über die Cloud. Ich rede in mein Gerät und irgendein hilfreicher Geist in den Weiten des Cyberspace überträgt die Worte in lesbaren Text. Das klingt kompliziert, funktioniert aber tatsächlich. Nur, wo bleiben meine persönlichen Aufzeichnungen? Wo werden sie gespeichert und wie lange? Was passiert mit meinen Daten, wenn das hoffnungsvolle Startup-Unternehmen in Palo Alto pleite geht oder von einem anderen Unternehmen geschluckt wird? Vielleicht liegen meine Dokumente auch gar nicht bei meinem Vertragspartner, sondern auf irgendeiner angemieteten Festplatte in China oder wer weiß wo in dieser Cloud?

Vielleicht bin ich paranoid. Doch der Gedanke will mir nicht behagen, dass ich im Laufe meines digitalen Lebens alle persönlichen Dokumente bei Hunderten von Providern irgendwo in der Cloud verteile. Ganz nebenbei gehen mir langsam die Passwörter aus. Denn bekanntlich sollte niemand jedem Provider sein Master-Passwort überlassen. Die Pannen der letzten Monate machen überdeutlich, wie es tatsächlich um die Sicherheit dieser Zugangsdaten bestellt ist. Immerhin werden die CEOs der Internetfirmen nicht müde, mir auf ihren Homepages hoch und heilig zu versprechen, dass sie Datenschutz und Sicherheit absolut ernst nehmen. Wer sich jedoch durch ihre AGBs kämpft, sucht meist vergeblich nach konkreten Hinweisen darauf, wie das vollmundige Versprechen in die Tat umgesetzt wird.

Um es deutlich zu machen, es geht hier nicht um Twitter oder Facebook. Das sind digitale Litfass-Säulen zur Selbstdarstellung. Jeder Nutzer weiß das oder sollte es zumindest wissen. Bei der Cloud geht es ans Eingemachte. Nämlich um meinen digitalen Hausrat, meine intimsten Privat- und Geschäftsgeheimnisse. Deshalb meine ich: Wenn der Trend zur Cloud sich durchsetzt, müssen wir den Persönlichen Computer neu definieren. Mein PC, meine Daten – das wird zukünftig keine sichere Bank mehr sein.

Was ich fürchte, ist eine Zwangsbeglückung. Habe ich es zukünftig mangels Alternativen überhaupt noch in der Hand, wo meine Daten und Dokumente bleiben? Wem soll ich in der Cloud eigentlich vertrauen? Bisher hatte ich das Selbstvertrauen, meine persönliche Technik zu beherrschen. Ich fühle mich auch rechtlich gut geschützt. Selbst das Bundesverfassungsgericht hat festgestellt, dass der PC zum intimen Lebensbereich des Menschen gehört und besonderen Schutz genießt. Die Verfassungsrichter meinten damit bestimmt nicht Bildschirm und Tastatur, sondern unsere persönlichen Daten auf unseren persönlichen Computern.

Alles vorbei? Werde ich jetzt praktisch gezwungen, mein Vertrauen in eigene Kompetenz, Vorsicht und den höchstrichterlichen Schutz zugunsten zweifelhafter Bequemlichkeit aufzugeben – nur weil Cloud modern ist?

Ich will die Vorteile dieser Technologie nicht kleinreden. Sicher bietet sie viele Chancen und neue Möglichkeiten. Wer zum Beispiel sein Smartphone oder seinen Tablet-Computer effizient nutzen will, kommt beispielsweise um ein Netzwerk-Laufwerk in der Cloud kaum herum. Daher brauchen wir Vertrauen in die neuen Dienste. Was ich deshalb fordere, ist vollständige Transparenz über den Verbleib meiner persönlichen Daten. Wo werden sie gespeichert und wer hat wann darauf Zugriff. Ich will präzise wissen, mit welchen Schutzmaßnahmen meine Dokumente gesichert werden. Und ich will sicher sein, dass meine Daten auch wirklich weg sind, wenn ich sie gelöscht habe. All diese Fragen will ich beantwortet haben, nicht in Statements, sondern in glasklaren, einklagbaren Geschäftsbedingungen. Ein Gütesiegel für Datensicherheit und Datenschutz würde ebenfalls helfen, Vertrauen in die neuen Dienste zu fassen.

Bei der Cloud geht es ans Eingemachte. Nämlich um meinen digitalen Hausrat, meine intimsten Privat- und Geschäftsgeheimnisse.

Solche Vertrauensanker und Garantien suche ich heute meist vergeblich. Dort, wo ich das nicht finde, ist die Cloud für mich nur undurchsichtiger Nebel mit viel Potenzial zur hagelvollen Gewitterwolke.

Kryptische Warnungen, die keiner versteht

Die Tochter: Ein Leben ohne Internet? Unvorstellbar. Ein Leben im vollkommen sicheren Netz? Auch unvorstellbar.

Von Melanie Lemke

Mein Berufsumfeld ist durch das Netz geprägt, schließlich arbeite ich bei einem internationalen Handelsunternehmen, das den größten Teil seines Umsatzes über das Internet abwickelt. Aber auch privat ist das Internet ein wichtiger Bestandteil meines Alltags.

Ich habe meinen MBA in Neuseeland gemacht und dort jede Menge neue Freundschaften geschlossen. Mit Menschen aus vielen Ländern unserer Erde. Wir haben gemeinsam studiert, sind danach in die Heimat zurück gegangen. Facebook hilft mir heute, den Kontakt zu diesem weltweiten Freundeskreis zu halten. Bequem, blitzschnell, wann immer ich will. Das finde ich großartig.

Mein neues iPhone ist ein kleines Wunder. Man hat ständig alle Informationen parat, hat die Kamera und Musik immer dabei, kann sehr bequem sein Taxi rufen, und telefonieren kann man auch noch damit. Und ja, ich finde die Sprachsteuerung mit Siri eine wirklich gelungene Sache, das macht die Bedienung dieses multifunktionalen Geräts sehr viel einfacher.

Und natürlich kaufe ich im Internet ein. Gerade wenn man viel arbeitet, ist es einfach praktisch und man hat immer den Überblick, was die Objekte meiner Begierde woanders kosten.

Bin ich deshalb ein Digital Native? Hier bin ich unsicher, denn zum Lebensgefühl eines echten Digital Natives gehört doch irgendwie die technische Überlegenheit gegenüber seinen Eltern. Das ist in unserer Familie schwierig, schließlich habe ich einen Informatiker zum Vater, der die Entwicklung der letzten 30 Jahre nicht nur hautnah miterlebt, sondern auch mit gestaltet hat. Ich brauche also nicht, wie viele meiner Freundinnen und Freunde, als „Internet-Nachhilfelehrer" für Vater, Mutter, Onkel und Tante zu arbeiten. Ich gebe sogar gern zu, dass ich häufig seine Hilfe in Anspruch nehme, zum Beispiel um meinen neuen Laptop oder Router einzurichten.

Die Einstellungen zur Sicherheit. Hier offenbart sich inzwischen ein kleiner Generationenkonflikt.

Eines allerdings lasse ich ihn nicht mehr machen: die Einstellungen zur Sicherheit. Hier offenbart sich inzwischen ein kleiner Generationenkonflikt. Ich will den mal anhand des PC meines Vaters beschreiben. Wenn meine Schwester oder ich zu Besuch bei meinen Eltern sind, nutzen wir den natürlich auch. Da hängt schon seit geraumer Zeit ein gelber Post-it-Zettel dran: „Liebe Mädels, bitte nach Benutzung bei Facebook, E-Mail etc. ausloggen." Ja, da hat er zwar grundsätzlich recht, aber große Bedenken haben ich auch nicht, wenn ich mal nicht daran denke. Schließlich vertraue ich meinem Vater, dass er nicht in meinen Mails herumstöbert. Richtig nervig sind allerdings die

Einstellungen seines Browsers. Keine Seite kann man mehr aufrufen, ohne dass irgendeine Warnung vor Scripts oder Cookies aufpoppt. Viele Internet-Seiten funktionieren nicht mehr, weil ein Script-Blocker die Links blockiert. Wenn ich ein PDF ansehen will, kommt erst mal eine kryptische Warnung, die ohnehin kein Mensch verstehen kann, was soll ich damit anfangen? Natürlich vertraue ich dem Versender, sonst hätte ich doch die Seite erst gar nicht aufgerufen.

Für mich ist es unerheblich, was in einer Cloud über mein Nutzerverhalten möglicherweise von Unbefugten abzulesen ist.

Informationstechnik muss für mich effizient und benutzerfreundlich sein. Dazu gehört nach meinem Verständnis ganz sicher nicht, ständig irgendwelche unverständlichen Sicherheitsfragen zu beantworten!

Um nicht falsch verstanden zu werden: Ich weiß, was ich tue, wenn ich im Internet bin. Natürlich weiß ich, dass Google, Facebook & Co. meine Daten sammeln und dass meine Daten einen großen Wert für diese Unternehmen darstellen. Aber ich bin eher amüsiert, wenn GoogleMail auf das Stichwort „hangover" reagiert und mir den Pizza-Service offeriert. Das ist zwar gefühlt eine eklatante Verletzung des Briefgeheimnisses, aber das muss man eben wissen, wenn man im Internet unterwegs ist, und sich entsprechend verhalten.

Ich laufe doch auch im richtigen Leben nicht verschleiert herum, sondern nenne freimütig meinen Namen, wenn ich mit irgendwem kommuniziere. Warum sollte ich mich im Internet anders verhalten?

Eine hundertprozentige Sicherheit kann es nie geben, auch nicht im Netz. Deshalb sind die Bedenken meines Vaters im Hinblick auf die Cloud für mich kaum nachvollziehbar. Ich finde den Cloud-Dienst sehr praktisch. Damit habe ich endlich von allen meinen Geräten Zugriff auf meine Daten. Ich habe da nur einen vollständig anderen Kritikpunkt: So ein Dienst müsste auch für Nicht-Techniker einfacher einzurichten sein. Muss ich mir kummervolle Gedanken machen, weil Apple meine Siri-Sprachsteuerung auswerten könnte? Dann bekomme ich eben ein paar Werbemails mehr und im schlimmsten Fall weiß Apple, welche SMS ich versendet habe. Das weiß Vodafone schließlich auch.

Natürlich kenne ich die Risiken sozialer Netzwerke, weiß einiges über Cyber-Kriminalität. In einer Welt, die mehr und mehr „data-driven" ist, glaube ich auch, dass Daten eines der wichtigsten Güter meiner und zukünftiger Generationen sein werden. Deshalb erwarte ich hier noch heftige Konflikte. Aus Erfahrung wissen wir, dass Konflikte über wichtige Rohstoffe in Politik und Wirtschaft nicht ausbleiben, warum sollte es also bei diesem wertvollen Gut anders sein?

Aber die Vorteile von Facebook & Co. wiegen mehr, jedenfalls für mich persönlich. Übervorsichtige Regulierungen, die den Fortschritt aufhalten oder gar zurückdrehen würden, lehne ich daher ab. Schließlich habe ich auch nichts zu verbergen. Also – was soll ich mich aufregen! Für mich ist es unerheblich, was in einer Cloud über mein Nutzerverhalten abzulesen ist. Oder nehmen wir Location-based Marketing. Das ist ein Megatrend. Bislang gebe ich meine Positionsdaten nicht frei, noch nicht. Wenn alle meine Freunde das machen würden und es mir nutzen würde, könnte die Sache jedoch anders aussehen.

Ich weiß jetzt schon, was mein Vater dazu sagen wird. Vielleicht ist die Einstellung zur Sicherheit doch eine Frage des Alters, eben ein Generationenproblem. Hoffentlich wird das Internet nicht allein durch diese Generation reguliert, eine digitale Gerontokratie wäre das Letzte.

***Melanie Lemke** (*1984) hat an der Wirtschaftsakademie Hamburg Betriebswirtschaft studiert und in Neuseeland ein MBA-Studium absolviert. Sie ist in einem großen Hamburger Handelsunternehmen als Senior Managerin im Beteiligungscontrolling tätig. In ihrer Freizeit hält sie sich mit Yoga fit und reist gern und viel, um ihren weltweiten Freundeskreis zu pflegen. Das Internet ist ein selbstverständlicher Teil ihres beruflichen und privaten Lebens.*

Sicherheit durch Software?

Was wirklich getan werden muss, um das Vertrauen ins Netz nachhaltig und dauerhaft zu steigern.

Von Dr. Göttrik Wewer

Nach einer aktuellen BITKOM-Studie ist es um das Vertrauen in die Sicherheit sozialer Netzwerke insgesamt eher schlecht bestellt: Bei allen abgefragten Netzwerken gibt jeweils mindestens die Hälfte der Nutzer an, der Plattform eher nicht oder gar nicht zu vertrauen. Dem Marktführer Facebook misstrauen 62 Prozent, Google plus 64 Prozent und Twitter sogar 70 Prozent. Am wenigsten vertraut wird der Online-Community Netlog (85 Prozent).

Fast alle Nutzer sind der Ansicht, dass die Netzwerke für einen besseren Datenschutz sorgen müssen (94 Prozent). 86 Prozent wünschen sich ein Datenschutz-Siegel für soziale Netzwerke. 78 Prozent sprechen sich für strengere staatliche Vorgaben für den Datenschutz in sozialen Netzwerken aus. Und zwei Drittel der Befragten geben an, dass sie nicht genug Informationen darüber haben, was sie selbst für den Datenschutz in solchen Communities tun können. Nur fünf Prozent der Befragten stimmen der Aussage zu, ihnen sei es persönlich egal, was mit ihren Daten in sozialen Netzwerken geschieht.

Bei der Auswahl eines sozialen Netzwerks ist nahezu allen Befragten die Sicherheit ihrer persönlichen Daten wichtig oder sehr wichtig (96 Prozent). Ähnlich viele (92 Prozent) legen großen Wert auf die Einstellungen zur Privatsphäre und auf die Benutzerfreundlichkeit (89 Prozent). Erst danach folgt das Kriterium, dass Freunde oder Kollegen in dem gleichen Netzwerk angemeldet sind (82 Prozent).

Sicherheit und Datenschutz sind also wichtig, wenn es um die Akzeptanz digitaler Angebote geht. Die sozialen Netzwerke sind dafür nur ein Beispiel. „Vertrauen ins Internet ist (der) Schlüssel zur Gesellschaft der Zukunft“, schreibt Hannes Schwaderer, der Präsident der Initiative D21. Nur wenn die Menschen glauben, dass ihre Daten im Internet sicher sind und damit kein Schindluder getrieben werden kann, werden sie die vielfältigen Angebote des eCommerce, die das Netz bietet, tatsächlich intensiv nutzen.

Absolute Sicherheit gibt es nicht, weder im realen Leben noch in der virtuellen Welt. Das wissen die Menschen auch. Insofern geht es immer um eine individuelle Abwägung zwischen Sicherheit und Freiheit, zwischen Vertrauen und Kontrolle. Es geht um das Maß an „tragbarer Unsicherheit“ (Niklas Luhmann) bzw. das noch „akzeptable Risiko“ (Anthony Giddens), das letztlich jeder für sich selbst definieren muss. Es geht, könnte man auch sagen, um eine Art von Risikomanagement: Wie viel Risiko ist man bereit zu gehen, wie viel Vertrauen ist man bereit zu schenken?

Sich sicher zu fühlen, hängt nicht nur von Zahlen, Daten und Fakten ab, sondern auch von persönlichen Dispositionen. Wer ein ausgeprägtes Selbstbewusstsein hat, dürfte eher bereit sein, Risiken einzugehen, als jemand der sich unsicher fühlt und mit moderner Technik nicht so vertraut ist. Der eine legt sein Geld lieber in „sicheren“ Papieren an, der andere spekuliert munter an der Börse. Manche gehen immer volles Risiko, andere eher auf „Nummer Sicher“.

Die tatsächliche Gefährdung (die „objektive" Sicherheitslage) und die „gefühlte" Sicherheit (das subjektive Sicherheitsgefühl) sind praktisch nie deckungsgleich. Wird die Kluft aus der Sicht vieler zu groß, bekommen Regierungen politisch oder Unternehmen ökonomisch ein Problem. Die Menschen müssen sich sicher fühlen, nur dann sind sie bereit, bestimmte Angebote im Internet wahrzunehmen. „Sicherheit" ist ein Konstrukt, das sich auf unterstellte soziale Gewissheiten bezieht, nicht primär auf objektive Tatbestände. Emotionen – Sorgen und Ängste – lassen sich mit Statistiken nicht beruhigen.

Ähnlich ist es mit Vertrauen. Vertrauen ist ein Vorschuss, den wir anderen gewähren, eine Investition, gewissermaßen Risikokapital. Wir geben anderen eine Art Kredit, aber nicht bedingungslos, sondern innerhalb gewisser Grenzen und nach bestimmten Maßstäben, die als vernünftig und vertretbar angesehen werden. Im Internet zahlen wir nicht mit unserem guten Namen, sondern mit unseren vielen Daten. Im Grunde zahlen wir nicht, wir tauschen: Nutzen gegen Risiko. Wenn der Nutzen, den wir aus einer Aktivität im Netz erwarten, größer erscheint als das Risiko, das wir eingehen, dann sind wir auch bereit, persönliche Daten preiszugeben. Man weiß oder ahnt, dass es ein riskantes Tauschgeschäft sein kann, und will wenigstens das Gefühl haben, dass der Deal einigermaßen fair ist. Sonst machen wir ihn lieber nicht.

Vertrauen kann enttäuscht werden. Ein Datenskandal allein reicht meist noch nicht, Vertrauen komplett zu zerstören. Es sind nicht einzelne Vorgänge, die zum Überdenken einer Geschäftsbeziehung führen, sondern gewisse Schwellen, die nicht überschritten werden dürfen. Dann allerdings kann auch eine Kleinigkeit „das Fass zum Überlaufen" bringen.

Vertrauen ist eine soziale Kategorie, keine technische Kategorie. Wir haben unsere eigenen Erfahrungen mit bestimmten Angeboten im Internet gemacht und wir haben Erfahrungen aus ähnlichen Konstellationen. Wir vertrauen Menschen, die wir kennen, also Freunden, Kollegen, Bekannten, Sportkameraden, die wir fragen können (indirekte Erfahrungen). Wir vertrauen Menschen, die wir zwar nicht persönlich kennen, aber sympathisch finden, und Autoritäten, die etwas von der Sache verstehen (müssten), also Fachleuten, Experten. Wenn diese versichern, man könne ein bestimmtes Angebot bedenkenlos nutzen, dann glauben wir ihnen (vorerst).

Ansonsten verlassen wir uns auf das öffentliche Image von Unternehmen, Produkten und Dienstleistungen. Wenn diese einen guten Ruf haben, sind wir eher bereit, uns darauf einzulassen, als auf Firmen und Angebote, die man kaum kennt und schwer einschätzen kann. Wer neu am Markt ist und keine etablierte Marke, muss sich Vertrauen erst erarbeiten. Transparenz im Umgang mit den Daten ist dabei ein wichtiges Instrument, freiwillige Überprüfungen durch unabhängige Sachverständige oder Gütesiegel wären ein anderes. Angebote, die der Einzelne nicht durchschaut, haben es jedenfalls leichter, als vertrauenswürdig angesehen zu werden, wenn in ihnen Elemente des Misstrauens und Mechanismen der Kontrolle von vornherein eingebaut sind. „Blindes" Vertrauen ist nämlich selten – selbst in der Liebe.

Ratgeber, wie man sich möglichst sicher im Netz bewegen kann, empfehlen einerseits technische Absicherungen (wie Firewalls, Virenscanner, regelmäßige Backups usw.) und andererseits ein vorsichtiges Verhalten. Technische Lösungen sind eine notwendige, aber keine hinreichende Bedingung für Vertrauen. Wer sich unsicher fühlt im dunklen Raum des Internets, der verliert sein Misstrauen nicht durch die Installation einer Sicherheitssoftware. Wenn Hacker sogar in das Pentagon eingedrungen sind, wie soll man dann glauben, der eigene PC sei sicher? Profis sind den Laien immer überlegen. Und verlässliche Spielregeln für das Internet, auf die man sich berufen und die man notfalls einklagen kann, gibt es nur bedingt. Insofern sind technische Vorsichtsmaßnahmen oder auch Information und Aufklärung, wie man sich besser schützen kann, zwar wichtig, aber nicht ausreichend, um Vertrauen zu schaffen. Forscher betonen jedenfalls den Grundsatz: „People trust people, not technology".

***Dr. Göttrik Wewer** (*1954) studierte Politikwissenschaft, Soziologie, Volkswirtschaftslehre, Öffentliches Recht und Neuere Geschichte in Braunschweig und Hamburg. Anschließend folgten Tätigkeiten an der Universität Hamburg und als Geschäftsführer der Deutschen Vereinigung für Politische Wissenschaft (DVPW) und ab 1991 in der öffentlichen Verwaltung, u.a. in der Staatskanzlei des Landes Schleswig-Holstein und als Direktor der dortigen Verwaltungsfachhochschule. Von 2001 bis 2003 war Wewer Staatssekretär im niedersächsischen Kultusministerium sowie 2003 bis 2006 im Bundesministerium des Innern. Anschließend wirkte er als Staatsrat für Bildung und Wissenschaft bzw. für Inneres und Sport in Bremen und später als Geschäftsführer der Nationalen Anti-Doping-Agentur (NADA). Seit 2010 ist Wewer Vice President E-Government bei der Deutsche Post Consult GmbH.*

Haben wir Grund zur Angst?

Die Datenschutz-Diskussion ist in eine Sackgasse geraten. Vieles behindert die notwendige Entbürokratisierung.

Von Prof. Dr. Hans Peter Bull

Neue Technik, die wir nicht durchschauen, macht uns unsicher. Vor den Produkten und Systemen der Informations- und Kommunikationstechnik stehen wir entweder fasziniert oder angstvoll. Es sind Apparate, die viel Nützliches können. Aber wir trauen ihnen auch Schlimmes zu – wir fürchten ihren Einfluss auf unser tägliches Leben, Pannen und Schäden durch Schlamperei, Fehlsteuerung und Missbrauch.

Während interessierte Unternehmen die Chancen ausmalen, die sich eröffnen, und IT-Freaks die „schöne neue Welt" des Internets anpreisen, wird in Medien und Politik vornehmlich über die Risiken gesprochen. Die eine Seite erwartet vom Internet enormen wirtschaftlichen Aufschwung, eine lebendigere Demokratie und für den Einzelnen mehr Entfaltungsfreiheit durch Kontakte mit der ganzen Welt. Die andere aber sagt den Niedergang der Kultur und das Ende der Privatsphäre voraus.

Bei näherer Betrachtung steht uns weder das eine noch das andere bevor. Wir können die Risiken beherrschen und die Chancen angstfrei nutzen, wenn wir einen rationalen Zugang zu den Problemen finden. Dazu bedarf es einer

- genauen Erkundung der tatsächlichen Verhältnisse – daran fehlt es vielfach
- angemessenen Ordnung der Techniknutzung durch Rechtsnormen – davon haben wir mehr als die meisten wissen – oder durch soziale Normen, die von den Beteiligten und Nutzern selbst entwickelt werden
- konsequenten Zurückdrängung negativer Entwicklungen, also vor allem der Durchsetzung der geltenden Regeln – hier hapert es noch gewaltig.

Die Probleme sind nicht technischer Art. Zu lösen sind vielmehr politische, soziale, wirtschaftliche oder psychologische Probleme, und zwar vor allem Durchsetzungsprobleme. Die Sorge davor, dass Maschinen die Menschen überwältigen, dass sie den Herren der Daten zu viel Macht über die Betroffenen vermitteln, dass die Freiheit der Meinungsäußerung gefährdet wird oder dass Fremde in die Rückzugsräume des Individuums eindringen – all das kann nicht durch technische Regeln ausgeräumt werden, sondern muss durch verbindliche Regeln des staatlichen Rechts oder durch Selbstregulierung der Beteiligten bewältigt werden. Alternative technische Gestaltungsweisen können solche Konflikte allenfalls abmildern.

Deshalb ist die „Netzpolitik" zu einem neuen Arbeitsfeld für Politiker aller Parteien geworden. Allenthalben entstehen Arbeitskreise und Initiativen, die für den Ausbau der Netze plädieren und über den Datenschutz in den sozialen Netzwerken nachdenken. Auf Parteitagen werden Beschlüsse zur „digitalen Demokratie" gefasst, und die „Piraten" haben mit ihrer Forderung nach „Freiheit im Internet" erste Wahlerfolge erzielt. Jedoch: Allzu undurchsichtig erscheinen die verschiedenen Einwirkungen auf das „Kampf-Feld". Wie viel Einfluss haben die Unternehmen, die das Internet betreiben und mit Inhalten bestücken? Geht es den Streitenden wirklich um Grundrechte oder nicht doch vor allem um Geld und Macht?

Besonders erbittert wird derzeit darüber gestritten, ob das Urheberrecht der Künstler und Autoren gegen das üblich gewordene illegale Herunterladen von Musik, Filmen und Texten durchgesetzt werden kann und soll. In den USA werden neue Gesetze vorbe-

reitet; dabei stehen sich die Medienkonzerne, die über die Rechte an den Inhalten verfügen, und die Internetbetreiber, die ihr Geld mit Werbung verdienen, welche sie den inhaltlichen Angeboten hinzufügen, unversöhnlich gegenüber.

Ein anderes Beispiel: Wenn ein Staat bestimmte Internetseiten sperren will – z.B. weil sie Kinderpornografie enthalten –, wird ihm vorgeworfen, er betreibe Zensur. Und in der Tat gibt es ja Staaten, die ihre Bürger vom weltweiten Netz abschneiden, weil sie unliebsame Kritik fürchten. Im einen wie im anderen Fall sind Lösungen nötig, die den entgegengesetzten Interessen möglichst weit gerecht werden – Lösungen im Sinne einer „praktischen Konkordanz" (Konrad Hesse) der kollidierenden Grundrechte. Das kann im ersten Fall eine neue (pauschalere) Form des Urheberrechts sein und im zweiten Fall statt der Sperrung die Löschung der verbotenen Bilder (so hat es die Internet-Gemeinde gegen die zuständige Bundesministerin geschafft: „Zensursula" von der Leyen musste sich geschlagen geben).

Den Einzelnen aber treibt wohl stärker als diese Themen die Frage um, was mit den eigenen persönlichen Daten im Internet geschieht. Was machen Google, Facebook und Twitter mit all den Datenspuren, die wir hinterlassen? Wer sich genau umschaut, wird freilich feststellen, dass die meisten Horrorgeschichten, die über die Datensammlung im Netz verbreitet werden, nicht stimmen.

Richtig: Die Internet-Unternehmen speichern unzählige Angaben über die Personen, die ihre Webseiten aufsuchen, und stellen daraus Listen von User-Gruppen zusammen, die nach ihren bisherigen Einkäufen und ihren erkannten Vorlieben und Interessen geneigt sein könnten, neue Angebote anzunehmen. Alles dreht sich um Werbung und Marketing, denn davon „lebt" das Internet und nur so werden die meisten Informationsangebote finanziert. Aber bedeutet das wirklich eine große Gefahr für die Privatsphäre? Verletzen gezielte Werbesendungen das Persönlichkeitsrecht?

Für mich ist die Verwendung von Personendaten zu Werbezwecken ein völlig harmloser Vorgang. Die Personen, deren „Profil" dabei hergestellt wird, sind für die Unternehmen nicht mehr als Individuen von Interesse. Nur diejenigen Eigenheiten sind für die Wirtschaft relevant, die einen Bezug zu der angebotenen Ware oder Dienstleistung herstellen, und gerade nicht die Kombination persönlicher Eigenschaften, die den Einzelnen unverwechselbar macht. Nur wenn die Daten zu ganz anderen Zwecken verwendet werden, muss man um die Interessen der Betroffenen fürchten. Das aber ist gerade nicht erlaubt, und so läuft wieder alles auf die Durchsetzung der Regeln hinaus. Man kann trotzdem gegen die übermäßige Kommerzialisierung sein und den Missbrauch der eigenen Daten fürchten. Doch sollten diese Vorbehalte nicht dazu führen, dass etwas verboten oder unnötig erschwert wird, was an sich vernünftig oder wenigstens akzeptabel ist.

Die Datenschutz-Diskussion ist in eine Sackgasse geraten: Die vielfältigen Bemühungen, „mehr Datenschutz" zu schaffen, laufen auf neue Rechtsnormen hinaus, stehen also quer zur notwendigen „Entbürokratisierung". Zu dieser Fehlentwicklung hat auch das Bundesverfassungsgericht beigetragen – in Urteilen, die von Liberalen in Politik und Medien begeistert gefeiert worden sind, weil sie die vermeintliche Überwachungswut der Behörden einschränken. Die Karlsruher Richter haben versucht, die Menschen vor einem „diffus bedrohlichen Gefühl des Beobachtetseins" zu schützen, für das es keine realistische Basis gab und gibt. Das damit geäußerte Misstrauen gegen die Sicherheitsbehörden macht deren Arbeit zwar nicht unmöglich, aber schwerer.

Die Europäische Kommission hat den Ehrgeiz, das Datenschutzrecht in der gesamten EU zu perfektionieren. Ihr Ende Januar dieses Jahres veröffentlichter Vorschlag einer EU-Datenschutz-Verordnung ist freilich ein Musterbeispiel dafür, was dabei herauskommt, wenn man ohne Gewichtung nach Relevanz „alles" regeln und dabei immer „mehr" Rechtsschutz für die Betroffenen, einführen will, ohne mit kollidierenden Rechten abzuwägen. Gut gemeint, aber als Ansammlung von Generalklauseln geradezu ein Anreiz zu Auslegungsstreitigkeiten, ein Konjunkturprogramm für Juristen. Über dieses Papier muss also noch sorgfältig beraten werden.

***Prof. Dr. Hans Peter Bull** (*1936) studierte von 1956 bis 1960 Rechtswissenschaft in Hamburg, Marburg und an der Freien Universität Berlin. Es folgten 1963 die Promotion zum Doktor der Rechte und 1966 das zweite Staatsexamen. 1972 habilitierte sich Bull für Staats- und Verwaltungsrecht und war als Professor für öffentliches Recht an der Uni Hamburg tätig. 1978 wurde er zum ersten Bundesbeauftragten für den Datenschutz berufen. Dieses Amt hatte er bis 1983 inne, nahm dann wieder seine Tätigkeit als Professor an der Uni Hamburg auf. 1988 bis 1995 übernahm Hans Peter Bull das Amt des Innenministers von Schleswig-Holstein. Danach wirkte er erneut als Professor an der Universität Hamburg. Seit 2002 ist er im Ruhestand. Von 1997 bis 2003 war er stellvertretender Vorsitzender der Bundesschiedskommission der SPD. In den Jahren 2002 bis 2006 fungierte er als Präsident der Deutschen Sektion des Internationalen Instituts für Verwaltungswissenschaften.*

Alle Alarmglocken sollten schrillen

Das BKA zu Cybercrime: Wie die Internet-Kriminalität weiter steigt und selbst Kinder zu den Tätern zählen

Von Mirko Manske

Der stetige Aufwärtstrend von zuletzt etwa 20 Prozent jährlicher Steigerung im Bereich der Internet-Kriminalität hält weiter an. Die Anzahl der durch die Bundesländer im Rahmen des polizeilichen Informationsaustauschs an das BKA in 2011 gemeldeten Vorgänge wird sich nach momentanem Trend gegenüber den Eingängen des Jahres 2010 mehr als verdoppeln.

Die Strafverfolgungsbehörden unterscheiden grundsätzlich zwischen zwei Arten der im allgemeinen Sprachgebrauch als „Internet-Kriminalität" beschriebenen Kriminalitätsphänomene. Zum einen sind das die „konventionellen" Modi Operandi, die vornehmlich aus dem Betrugsbereich kommen und bei denen die potenziellen Opfer via E-Mail aufgefordert werden, Vorauszahlungen für in Aussicht gestellte Erbschafts- oder Lotteriegewinnzahlungen zu leisten. Hier nutzen die Täter die heute vorhandene technische Infrastruktur für ihre Zwecke – die dahinter stehenden Straftaten haben sich jedoch nicht wesentlich geändert. Derartige Straftaten, und dazu gehören auch die „normalen" Betrugsstraftaten im Online- oder Auktionshaushandel, bei denen nach Vorauskasse keine, minderwertige oder gefälschte Ware versandt wird, werden aus Sicht der Strafverfolgungsbehörden als „Cybercrime im weiteren Sinne" verstanden.

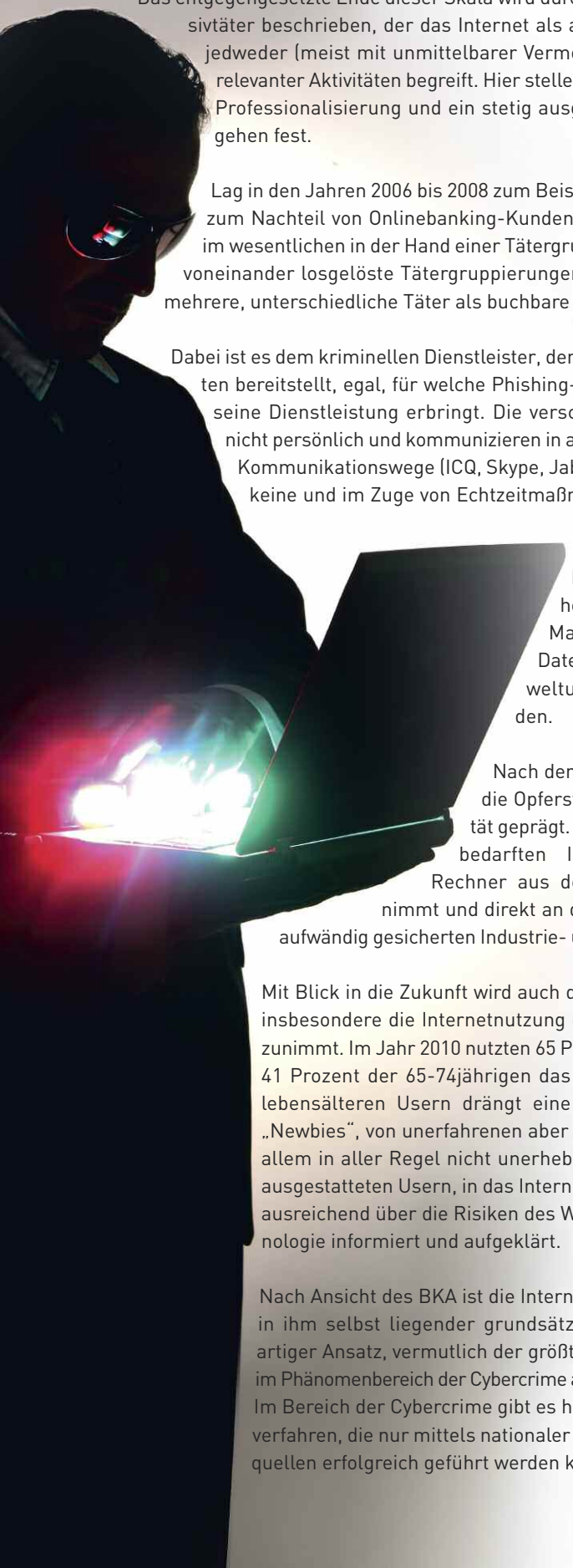
In Abgrenzung dazu betrachtet die Polizei die Delikte der „qualifizierten Cybercrime". Darunter fallen Straftaten, die erst durch das Internet selbst ermöglicht wurden oder sich gegen das Internet selbst richten. Sie tauchen in den unterschiedlichsten Erscheinungsformen auf – vom meist trojanerbasierten digitalen Identitätsdiebstahl in jedweder Ausprägung über das Einbrechen und den unberechtigten Zugriff auf gesicherte Systeme mit nachgelagertem Diebstahl dort vorhandener Daten bis hin zur digitalen Schutzgelderpressung, bei der Webseiten zunächst mittels DDoS-Angriffen für eine bestimmte Zeit lahmgelegt und die Inhaber sich dann kurze Zeit später finanzieller Forderungen der Täterseite zur Verhinderung erneuter Angriffe ausgesetzt sehen.

Es ist schwer, die Verbrechen korrekt in absoluten Zahlen zu umreißen. Nach Einschätzung des BKA ist dies auf ein sehr großes Dunkelfeld zurückzuführen, da die überwiegende Anzahl der Straftaten durch die Opfer gar nicht bemerkt bzw. nicht bei den Strafverfolgungsbehörden angezeigt wird. Die offizielle Statistik weist für 2010 insgesamt 246.607 erfasste Straftaten mit dem Merker „Tatmittel Internet" aus. Qualifizierte Cybercrime wurde in 2010 mit 59.839 Straftaten (gegenüber 50.254 in 2009) erfasst.

Nach BKA-Einschätzung werden sich mit der weiter fortschreitenden Technisierung der Gesellschaft auch in den kommenden Jahren immer mehr Erscheinungsformen von Kriminalität ins Internet verlagern oder dort entstehen. Das hat vor allem auch mit dem für die Täter deutlich geringeren Entdeckungsrisiko im Internet zu tun.

Das BKA hat festgestellt, dass die Täter einen weiten Bogen spannen. Bekannt sind Jugendliche, teilweise sogar noch Kinder, die mit erheblichem technischen Verstand und beeindruckender Begabung – gepaart mit einer großen Portion Neugier und teilweise auch krimineller Energie – Trojaner und an-

Mirko Manske *(*1972) schloss seine Ausbildung im Bundeskriminalamt 1993 ab. Er war seither in verschiedenen Bereichen des BKA eingesetzt – unter anderem in der polizeilichen Software-Entwicklung, der Geldwäsche-Bekämpfung und bei der Bekämpfung des islamistischen Terrorismus. Anfang 2006 übernahm Manske verantwortlich den Arbeitsbereich „Operative Auswertung Cybercrime" (Cybercrime Intelligence Operations) als Sachgebietsleiter im damals neu gegründeten Referat SO43. Manske ist Erster Kriminalhauptkommissar und gilt als profunder Kenner dessen, was allgemein als „Internet-Kriminalität" umschrieben wird. Ende 2011 referierte er in Berlin vor der Enquete-Kommission „Internet und digitale Gesellschaft" des Deutschen Bundestages. Sein Beitrag im DIVSI-Magazin ist eine aktualisierte, gekürzte Fassung des damaligen Vortrags.*



dere Schadsoftware konzipieren, entwickeln und einsetzen. Häufig passiert dies zunächst nur, um innerhalb der Szene an Ansehen, an „Standing", zu gewinnen.

Das entgegengesetzte Ende dieser Skala wird durch den hochkriminellen Intensivtäter beschrieben, der das Internet als allumfassenden Aktionsraum jedweder (meist mit unmittelbarer Vermögensrelevanz) strafrechtlich relevanter Aktivitäten begreift. Hier stellen wir eine weiter zunehmende Professionalisierung und ein stetig ausgebautes arbeitsteiliges Vorgehen fest.

Lag in den Jahren 2006 bis 2008 zum Beispiel im Bereich des Phishings zum Nachteil von Onlinebanking-Kunden noch der gesamte Tatstrang im wesentlichen in der Hand einer Tätergruppierung, so sehen wir heute voneinander losgelöste Tätergruppierungen, die einzelne Bausteine für mehrere, unterschiedliche Täter als buchbare Dienstleistung anbieten.

Dabei ist es dem kriminellen Dienstleister, der z.B. Finanz- und Warenagenten bereitstellt, egal, für welche Phishing- oder Cardinggruppierung er seine Dienstleistung erbringt. Die verschiedenen Täter kennen sich nicht persönlich und kommunizieren in aller Regel über anonymisierte Kommunikationswege (ICQ, Skype, Jabber), die retrograd so gut wie keine und im Zuge von Echtzeitmaßnahmen auch nur sehr eingeschränkt erfolgsträchtige Ermittlungen ermöglichen. Die Cyberkriminellen von heute sind auf einem globalen Markt angekommen, auf dem Daten, Tatmittel und Infrastruktur weltumspannend gehandelt werden.

Nach den Erkenntnissen des BKA sind die Opferstrukturen von großer Diversität geprägt. Die Bandbreite reicht vom unbedarften Internetnutzer, der seinen Rechner aus dem Karton des Discounters nimmt und direkt an das Internet anschließt bis zu aufwändig gesicherten Industrie- und Sicherheitseinrichtungen.

Mit Blick in die Zukunft wird auch die Tatsache bedeutsam, dass insbesondere die Internetnutzung durch ältere Menschen stark zunimmt. Im Jahr 2010 nutzten 65 Prozent der 55-64-jährigen und 41 Prozent der 65-74jährigen das Internet. Gerade mit diesen lebensälteren Usern drängt eine Vielzahl von so genannten „Newbies", von unerfahrenen aber mit viel Neugier, Zeit und vor allem in aller Regel nicht unerheblichem finanziellen Potenzial ausgestatteten Usern, in das Internet. Dabei sind sie jedoch nicht ausreichend über die Risiken des Webs und der modernen Technologie informiert und aufgeklärt.

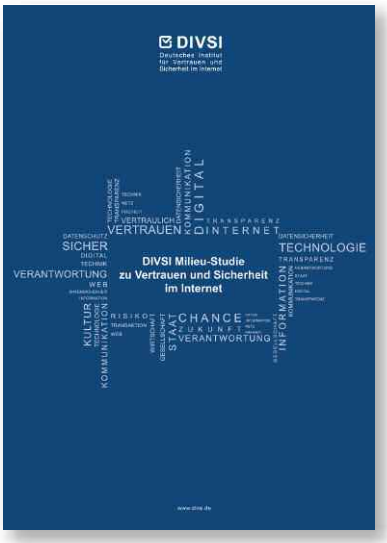
Nach Ansicht des BKA ist die Internationalität des Internets, sein in ihm selbst liegender grundsätzlich globaler und netzwerkartiger Ansatz, vermutlich der größte Schutzfaktor, den die heute im Phänomenbereich der Cybercrime aktiven Täter gezielt ausnutzen. Im Bereich der Cybercrime gibt es heute kaum noch Ermittlungsverfahren, die nur mittels nationaler Aktivitäten und Informationsquellen erfolgreich geführt werden können.

Auslandsermittlungen – und sei es nur die Anfrage bei einem ausländischen Internetservice-Provider oder Zahlungsdienstleister zu IP-Logs und Verbindungsdaten – sind an der Tagesordnung. Sie bedingen in aller Regel justizielle Rechtshilfe-Ersuchen, die (wenn sie denn gestellt werden) den Ermittlern benötigte Informationen nur mit erheblichen Zeitverzögerungen zur Verfügung stellen. Die durch das BKA sowie Dienststellen der Bundesländer gestellten außereuropäischen Rechtshilfe-Ersuchen, insbesondere in die USA, wohin aufgrund der technischen Gegebenheiten des Internets ein besonders starker Bezug gegeben ist, aber auch in die Ukraine und die Russische Föderation, wo häufig Täterspuren zu finden sind, haben im günstigsten Falle eine Laufzeit von wenigstens drei Monaten gezeigt. Die so erlangten Daten sind dann, wenn sie schließlich bei der ermittlungsführenden Dienststelle in Deutschland angekommen sind, in aller Regel bereits inaktuell und „kalt".

Als Vorteil der schon fast zwingenden internationalen Ermittlungen im Phänomenbereich Cybercrime ist festzustellen, dass immer mehr in der Verfolgung der Cybercrime involvierte und aktive Staaten erkennen, dass neue Arten der Zusammenarbeit gefunden werden müssen. Diese Wege müssen effektiver und vor allem schneller als der klassische Weg über die Interpol-Zentralstellen sein.

Diese Erkenntnis hat über die vergangenen fünf Jahre beim BKA zum Aufbau eines mittlerweile weltweiten Netzwerkes von im Phänomenbereich der Cybercrime eingesetzten Spezialisten geführt. Kollegen in Washington, Pittsburgh, Seoul, Bangkok, Kiew, Moskau oder Riga, zu denen persönliche Kontakte bestehen, sind nur noch einen Telefonanruf oder Jabber-Chat entfernt. Diese Kontakte tragen und ermöglichen es immer wieder, die Widrigkeiten der verschiedenen Rechtssysteme und der zwingenden Rechtshilfemaßnahmen im Rahmen des rechtlich Möglichen zu minimieren.

Aktuelle Bücher



DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet

Eine Grundlagenstudie des SINUS-Instituts Heidelberg im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI)

Das Internet hat sich von einem rein technischen Angebot zum erweiterten Lebensraum der Menschen in Deutschland entwickelt. Entsprechend erweitern sich nicht nur die Chancen, sondern auch die Risiken und Unsicherheiten. Diese Studie zeigt auf, welche Meinungen und Vorstellungen es zu diesem Thema (bei Offlinern wie bei Onlinern) gibt, welche datenschutz- und sicherheitsrelevanten Einstellungs- und Verhaltenstypen existieren. Ziel war es, eine bevölkerungsrepräsentative Typologie zum Thema Vertrauen und Sicherheit zu entwickeln. Aus dieser Typologie lassen sich Handlungsempfehlungen für Politik, Wissenschaft, Wirtschaft und Gesellschaft ableiten.

Herausgeber: DIVSI, Mittelweg 142, 20148 Hamburg; kostenfrei im Internet oder unter www.divsi.de

Trust, but test!: Das Vertrauen in virtuellen Gemeinschaften

Autor: Udo Thiedeke

Warum sollte man im Netz vertrauen? Ist Kontrolle nicht die bessere Strategie, wenn es darum geht, virtuelle Gemeinschaften im Cyberspace zu gründen und fortzuschreiben? Auf der Grundlage von Luhmanns Systemtheorie entwickelt Thiedeke (er lehrt als Privatdozent für Soziologie an der Johannes Gutenberg Universität Mainz) ein Modell der virtuellen Gemeinschaft als soziales System. Dabei untersucht er die Operationsweise und Entwicklung von Vertrauen als Reduktionsmechanismus sozialer Komplexität und Selektionsmechanismus sozialer Erwartungsstrukturen bei Warez Communities, eBay, Wikipedia, im Usenet und in Online-Spielewelten – eine spannende sozialwissenschaftliche Untersuchung virtueller Gemeinschaftsbildung.

UVK Verlagsgesellschaft mbH, ISBN: 978-3-89669-622-9, Preis € 39,00

Die Datenfresser

Autoren: Constanze Kurz/ Frank Rieger

Dieses Buch mit dem Untertitel „Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen" ist besonders für Menschen geeignet, die sich bisher wenig mit dem Internet oder Fragen zur Datensicherheit beschäftigt haben. Ihnen vermittelt es Einblicke darüber, wo Gefahren lauern und wie sie sich vermeiden lassen. Constanze Kurz (Informatikerin, wissenschaftliche Mitarbeiterin an der Humboldt-Universität Berlin und Mitglied der Enquete-Kommission „Internet und digitale Gesellschaft" des Deutschen Bundestages) sowie Frank Rieger (technischer Geschäftsführer eines Unternehmens für Kommunikationssicherheit) bieten Hintergrundwissen. Dabei bleibt ihr Buch frei von hysterischer Empörung. Dadurch wirken die ausgesprochenen Warnungen umso eindringlicher.

Fischer Verlage, ISBN: 978-3-10-048518-2, Preis € 16,95

Die Praxis des Vertrauens

Autor: Martin Hartmann

Vertrauen ist als Thema allgegenwärtig. Ob von Politikverdrossenheit, Bankenkrise oder Missbrauchsskandalen die Rede ist – stets wird vorausgesetzt, dass Vertrauen eine zentrale Ressource sozialen Handelns ist, die nur schwer hergestellt, aber schnell zerstört werden kann. Aber was ist Vertrauen? Wie wird es geschaffen, wie zerstört? Wem sollten wir vertrauen, wem eher mit Misstrauen begegnen? Hartmann, Professor für Philosophie am Philosophischen Seminar der Uni Luzern, versucht, Vertrauen sowohl begrifflich als auch historisch zu klären. Er veranschaulicht seine theoretischen Überlegungen mit konkreten Beispielen aus Politik, Wirtschaft und Familie. Vertrauen, so zeigt er, ist ein komplexes Phänomen, das deutlich macht, wie zerbrechlich und anspruchsvoll Prozesse der Vertrauensbildung sind.

suhrkamp taschenbuch wissenschaft, ISBN: 978-3-518-29594-6, Preis: € 18,00

Impressum

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

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

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

Autoren:
Dr. Silke Borgstedt, Prof. Dr. Hans Peter Bull, Prof. Dr. Claudia Eckert, Matthias Kammer, Harald Lemke, Melanie Lemke, Mirko Manske, Dr. Göttrik Wewer

Realisation:
PubliKom Kommunikationsberatung GmbH, Hamburg

Bildnachweis:
dpa, Sinus, CSM Stock, private Archive, Tom Maelsa

Verbreitete Auflage:
7.500 Exemplare
Abgabe kostenlos


DIVSI
Deutsches Institut für Vertrauen und Sicherheit im Internet

www.divsi.de