

/// Sicherheit im Internet

DIE FREIHEIT DES EINEN DIE GEFAHR DES ANDEREN?

REINHARD BRANDL /// Die Entwicklung des Internets ist eine beispiellose Erfolgsgeschichte. Doch Berichte über die Zunahme von kriminellen und zerstörerischen Aktivitäten im Netz verunsichern die Nutzer und bremsen die Entwicklung. Was kann der Einzelne, die Wirtschaft und insbesondere der Staat für mehr Sicherheit im Internet tun?

Das Internet als Ort der Freiheit und Chancen

Das Internet bietet Menschen, Unternehmen und Organisationen grenzüberschreitend Chancen und Entwicklungsmöglichkeiten, die vor wenigen Jahrzehnten noch undenkbar gewesen wären. Es ist damit zum stetigen Antrieber des gesellschaftlichen und ökonomischen Fortschritts geworden. In Deutschland sind mittlerweile fast 75 % der Bevölkerung online.¹ Nach internationalen Schätzungen sind es weltweit bereits mehr als zwei Milliarden Menschen.² Die Zahl der Internetnutzer liegt bei den unter 40-Jährigen bei über 90 % und wächst in allen Altersgruppen weiter konstant an. Für viele Internetnutzer wäre ein Leben ohne Zugang zum Netz nicht mehr vorstellbar. Die Nutzung des Internets hat sich in den letzten Jahren grundlegend verändert. War das Internet am Anfang

eher eine technisch-geprägte Informations- und Kommunikationsplattform, so hat es sich insbesondere mit dem Erfolg des Web 2.0 und der sozialen Netzwerke zu einer Art „Lebensplattform“ entwickelt, auf der Menschen, die sich nie persönlich begegnet sind, in Verbindung treten und sich über ihre beruflichen, privaten und gesellschaftlichen Interessen austauschen. Es sind aber nicht nur Menschen verstärkt online, sondern es werden immer mehr Alltagsgegenstände, von der Kaffeemaschine bis hin zum Auto, über das Internet verbunden und gesteuert. Eine Unterscheidung zwischen virtueller und realer Welt wirkt angesichts dieser Entwicklungen zunehmend anachronistisch.

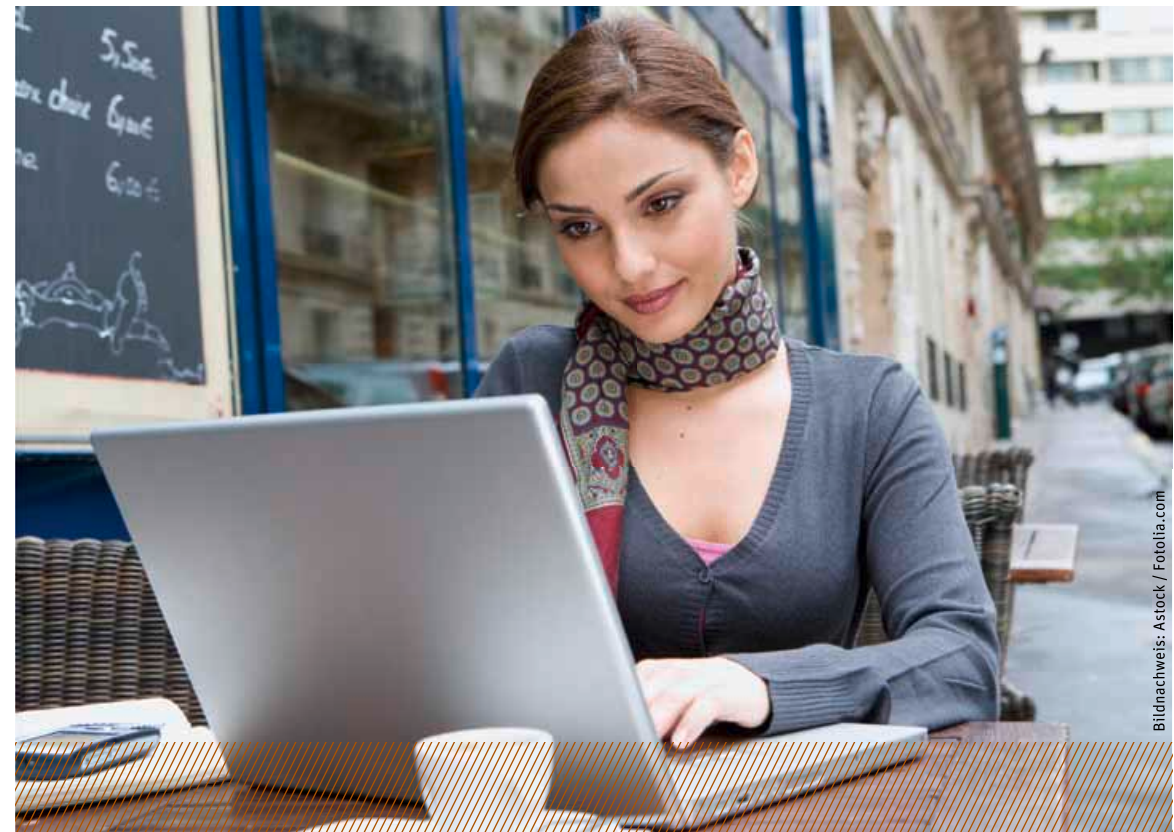
Konstituierende Elemente des Internets sind seine Interoperabilität, seine Unabhängigkeit und die damit verbundene Freiheit. Die Freiheit des Internets

umfasst nicht nur die Freiheit der Kommunikation, sondern auch die fast unbegrenzten Möglichkeiten, im Internet Geschäftsmodelle zu entwickeln und damit Geld zu verdienen. Dadurch sind die Angebote und die Infrastruktur entstanden, die den Erfolg und die Verbreitung des Internets erst ermöglicht haben. Die Gründer von Facebook oder Google zum Beispiel haben mit ihren überlegenen, aber in der aktuellen netzpolitischen Diskussion vielgescholtenen Anwendungen diese Freiheit und die damit verbundenen Chancen genutzt. Facebook wurde 2004 von und ursprünglich auch nur für Studenten der Harvard-Universität gegründet. Von dort aus begann eine bis dato bei-

In DEUTSCHLAND werden trotz der vorhandenen technischen Kompetenz zu wenig Internetfirmen gegründet.

spiellose Erfolgsgeschichte. Im Mai 2011 waren weltweit über 689 Millionen Nutzer bei Facebook angemeldet, 18,6 Millionen davon aus Deutschland. Dies entspricht etwa 22,8 % der Gesamtbevölkerung. Die Tendenz ist weiterhin steigend. Google wurde 1998, ebenfalls von Studenten, in einer Garage gegründet. Heute wickelt das Unternehmen 80 % aller Suchanfragen im Internet ab und beschäftigt über 26.000 Mitarbeiter. Vermutlich arbeiten gerade einige Tüftler in einer ande-

Das Internet bietet grenzenlose Freiheit und Möglichkeiten, öffnet aber ebenso Tür und Tor für Missbrauch.



ren Garage an derjenigen Anwendung, die in fünf Jahren die Diskussion bei uns beherrschen wird. Mit hoher Wahrscheinlichkeit steht diese Garage aber in den USA und es ist davon auszugehen, dass auch dort die überwiegende Zahl der Arbeitsplätze entstehen. Deutschland liegt bei der Gründung und Etablierung von Internetfirmen trotz hoher technologischer Kompetenz und vielfachen Anstrengungen weit hinter den USA. Es ist im Interesse eines starken Wirtschafts- und Wissensstandorts Deutschland, diesen Abstand zu verringern.

Das Internet hat als globales Netzwerk zu einem beispiellosen Austausch von Ideen, Wissen und Leistungen geführt. Durch seine Interoperabilität sind zwischenstaatliche Grenzen nicht mehr von Belang. Damit stellt es auch den Staat als Träger hoheitlicher Gewalt vor völlig neue Herausforderungen. Viel mehr als in anderen Bereichen ist es notwendig, bei Themen, die das Internet betreffen, auf internationale Zusammenarbeit und Kooperationen mit der Wirtschaft zu setzen. Die globale Dimension und die Freiheit des Internets erfordern auch ein gewisses Maß an Gelassenheit von der Politik, wenn ein Angebot nicht unmittelbar deutschen Rechts- und Wertvorstellungen entspricht.

Internet-Kriminalität als Bedrohung der Freiheit

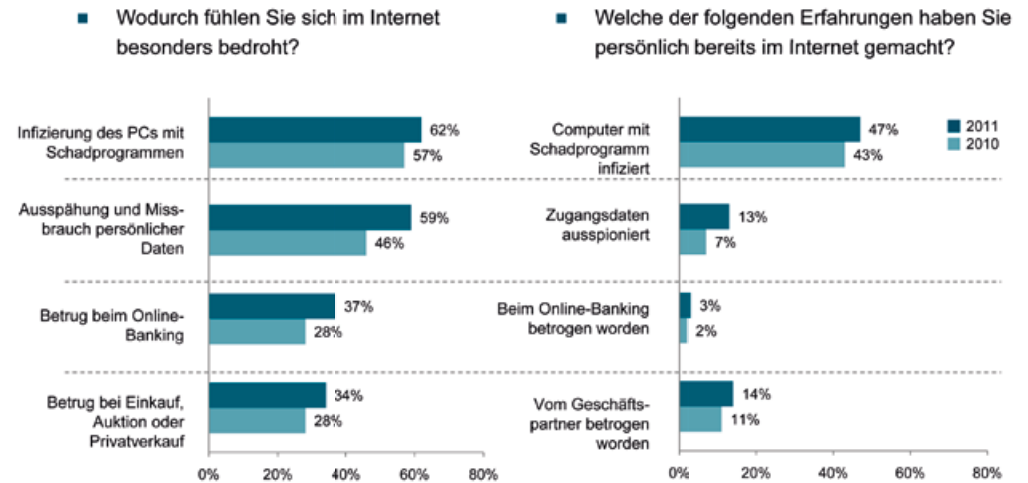
Die Freiheit im Internet wird aber in zunehmender Weise bedroht. Neben zahlreichen Versuchen von diktatorischen Staaten, den Zugriff auf einzelne Inhalte des Internets national zu beschränken,³ wird das Netz auch immer mehr zum Schauplatz krimineller und zerstörerischer Aktivitäten. Das Bundesamt für

Sicherheit in der Informationstechnik (BSI) berichtet in seinem Lagebericht IT-Sicherheit 2011⁴ von einer starken Zunahme an Schadprogrammen und immer arglistigeren Formen der organisierten Online-Kriminalität. Die NATO warnt vor IT-gestützten Angriffen auf kritische Infrastrukturen wie zum Beispiel die Energie- und Wasserversorgung eines Landes und hat die Abwehr derartiger Angriffe zur Bündnisaufgabe erklärt. Dazu kommen regelmäßige Berichte über große Datendiebstähle aus Internetplattformen oder Unternehmensnetzwerken.

Hinter jedem dieser Beispiele steht ein anderer Sachverhalt. Sie haben aber eines gemeinsam: Sie führen zur Verunsicherung und einem dementsprechend veränderten Verhalten der Internetnutzer. In einer im Juni 2011 vorgestellten repräsentativen Umfrage des Branchenverbands BITKOM gaben 85 % der Internetnutzer an, sich von Kriminalität im Web bedroht zu fühlen.⁵ Das ist eine Zunahme um zehn Prozent gegenüber der Umfrage 2010. Über die Hälfte der Befragten glauben, dass ihre persönlichen Daten im Internet „eher unsicher“ (43 %) oder „völlig unsicher“ (12 %) sind. Die Bedenken wirken sich auch auf das Nutzungsverhalten aus. So verzichten z. B. 23 % aus Sicherheitsgründen bewusst auf Online-Shopping, 16 % nehmen deshalb grundsätzlich keine Transaktionen im Web vor. Auch diese Werte sind im Vergleich zur Umfrage von 2010 in der Tendenz gestiegen.

Diese Zahlen geben einen Hinweis darauf, dass für die weitere Entwicklung des Internets das Vertrauen in die Sicherheit des Netzes von entscheidender Bedeutung sein wird. Die Verantwortung dafür liegt bei allen Beteiligten:

Datenspionage: Angst und Gefahr nehmen zu



Quelle: BITKOM/Forsa Juni 2011, Basis: Internet-Nutzer ab 14 Jahren

BITKOM – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

Nutzern, Anbietern und staatlichen Stellen.

Insbesondere bei den Nutzern gibt es noch großen Aufklärungsbedarf. Während die zuvor genannte Gruppe übervorsichtig agiert, gibt es auf der anderen Seite noch 21 %, die ohne jeden Virenschutz oder Firewall im Internet surfen.⁶ Vielen fehlt es an Informationen über die zur Verfügung stehenden Schutzvorkehrungen und dem nötigen Bewusstsein für mögliche Bedrohungen. Aber auch bei professionellen Anbietern und Betreibern von informationstechnischen Systemen zeigen sich immer wieder erschreckende Sicherheitslücken. Prominentestes Beispiel der jüngsten Zeit ist der Zugriff von Ha-

ckern auf 100 Millionen Kundendaten von Sony. Der Vorfall im April 2011 hat zu einem massiven Image- und sicher auch zu einem beträchtlichen wirtschaftlichen Schaden für das Unternehmen geführt. Der Vorfall ist aufgrund der Menge der entwendeten Daten ein Einzelfall, er reiht sich aber nahtlos in eine ganze Reihe erfolgreicher Attacken auf verschiedene große Unternehmen und öffentliche Stellen ein. So wurde im Januar 2011 u. a. die elektronische Plattform für den Handel mit Emissionszertifikaten in Europa manipuliert, im Februar waren eine Datenbank der US-Technologiebörse NASDAQ und im März die Rechner der Europäischen Kommission Ziel eines Angriffs. Neben

solch großen und öffentlich gewordenen Vorfällen werden auch zahlreiche kleinere Unternehmen täglich Opfer von gezielter Wirtschaftskriminalität, insbesondere von Wirtschaftsspionage. Oftmals wird ein Angriff gar nicht bemerkt oder erst, wenn es bereits viel zu spät ist. Auch hier mangelt es an vielen Stellen an Informationen, dem Bewusstsein für Bedrohungen und möglichen Schutzvorkehrungen. Während der Sicherheitsdienst auf dem Unternehmensgelände jeden Abend alle Türen akribisch verschließt und überprüft, steht der eine oder andere Seiteneingang zum Unternehmensnetzwerk oftmals speerangelweit offen.

Mit der zunehmenden Vernetzung, insbesondere auch von Industrieanlagen, steigt das Risiko von Angriffen auf die sogenannten kritischen Infrastrukturen wie zum Beispiel die Energie-, Wasser- oder Telekommunikationsversorgung eines Landes. Der im Juni 2010 entdeckte Virus Stuxnet hat eindrucksvoll die Gefährlichkeit solcher Angriffe bewiesen. Diese Schadsoftware wurde mit hohem Aufwand programmiert, einzig und allein mit dem Ziel, bestimmte Prozesse in Industrieanlagen zu manipulieren. Ein Ausfall von größeren Teilen kritischer Infrastrukturen würde schon nach kurzer Zeit zu einem enormen Schaden für die deutsche Volkswirtschaft führen.

Die Rolle des Staates

Die Verantwortung für die Sicherheit von IT-Systemen – mit oder ohne An-

schluss zum Internet – liegt in erster Linie bei deren Nutzern und deren Anbietern bzw. Betreibern. Die dynamische technische Entwicklung in diesem Bereich macht es für den Staat unmöglich, bestimmte Sicherheitsstandards fest vorzuschreiben und über deren Einhaltung zu wachen. Nichtsdestotrotz kann er in vielfältiger Weise dazu beitragen, die Sicherheit im und das Vertrauen in das Internet zu erhöhen. Nachfolgend werden sieben Bereiche dafür kurz dargestellt.

Förderung von Medienkompetenz

Damit ein Nutzer seinen Teil der Verantwortung für die eigene Sicherheit und die Sicherheit seiner Kommunikationspartner im Internet wahrnehmen kann, benötigt er ein gewisses Maß an Medienkompetenz, die es ihm ermöglicht, Bedrohungen und Risiken realistisch einzuschätzen und sein Handeln darauf abzustellen. Die Vermittlung dieser Kompetenz ist auch Teil eines staatlichen Bildungsauftrags, nicht nur an den Schulen. Das Bundesamt für Sicherheit in der Informationstechnik stellt zum Beispiel ein Informationsportal speziell für Privatanutzer bereit⁷ und bietet auch eine Service-Hotline an. Die Europäische Union veranstaltet jedes Jahr den Aktionstag „Safer Internet Day“, an dem auf Veranstaltungen von öffentlichen Stellen und der Privatwirtschaft öffentlichkeitswirksam auf Maßnahmen zur Steigerung der IT-Sicherheit hingewiesen wird.

Stärkung des Datenschutzes

Im internationalen Vergleich verfügt Deutschland über einen hohen Datenschutzstandard. Neue technische Entwicklungen werfen jedoch immer wieder auch neue datenschutzrechtliche

Der STAAT kann die Medienkompetenz des Users mittels Unterstützung geeigneter Einrichtungen und Angebote fördern.

Fragen auf. Hinzu kommt, dass im Internet viele Anbieter nicht über nationale Betriebsstätten verfügen und somit die Anwendbarkeit des deutschen Datenschutzrechts ausgehöhlt wird. Fehlender Datenschutz führt jedoch immer wieder zu einem erheblichen Vertrauensverlust. Es muss daher ein Anliegen des Staates sein, die aktuellen technischen Entwicklungen sorgfältig zu beobachten und den vorhandenen Datenschutzstandard fortlaufend daran anzupassen. Dies kann sowohl durch entsprechende gesetzliche Regelungen als auch durch die Unterstützung von Selbstregulierungsmaßnahmen der Wirtschaft erfolgen.

Förderung von Forschung und Entwicklung

Die Entwicklung von sicheren IT-Produkten ist nicht nur Aufgabe der Wirtschaft, sondern auch Gegenstand der Forschung. In Deutschland arbeiten bereits zahlreiche universitäre und außeruniversitäre Forschungseinrichtungen an diesem Themenfeld. In München wurde dazu vor kurzem eine neue Fraunhofer-Einrichtung für „Angewandte und Integrierte Sicherheit“ gegründet. Über 60 Wissenschaftler arbeiten dort unter anderem an einer verbesserten Sicherheit von Cloud-Computing und eingebetteten Systemen sowie

am Schutz vernetzter kritischer Infrastrukturen. Solche Anstrengungen sind weiter zu fördern und auszubauen. Der Aufbau von Wissen in diesem Bereich dient nicht nur der Sicherheit im Internet, sondern ist gleichzeitig eine Investition in den IT-Standort Deutschland.

Vorbildfunktion des Staates

Tritt der Staat selbst als Nutzer, Anbieter oder Betreiber eines IT-Systems auf, muss er in Fragen der Sicherheit der benutzten Systeme eine Vorbildfunktion einnehmen. Das gilt insbesondere vor dem Hintergrund, dass viele staatliche Stellen teilweise sensible, personenbezogene Daten von Bürgern verarbeiten. Viele Verwaltungsdienstleistungen werden ins Internet verlagert. Das fördert den Komfort für den Bürger und erleichtert den Zugang zu den Behörden. Allerdings setzt es auch ein Vertrauen in die Sicherheit der Daten voraus, das nicht enttäuscht werden darf. Schließlich können die Bürger nicht wie im kommerziellen Bereich den Anbieter wechseln, sondern sind auf die Integrität und Sicherheit der staatlichen Datenverarbeitung angewiesen.

Schaffung einer sicheren Infrastruktur

Die mit am häufigsten vorkommende Form von Kriminalität im Internet ist der Diebstahl und Missbrauch von Identitäten. Für vertrauensvolle Kommunikations- bzw. Transaktionsvorgänge im Internet muss die Identität des jeweiligen Gegenübers eindeutig sichergestellt sein. Mit dem neuen elektronischen Personalausweis und dem De-Mail Gesetz hat die Bundesregierung in jüngster Zeit zwei infrastrukturelle Grundlagen für Deutschland geschaffen, auf die Anbieter und Nutzer jetzt zugreifen können.

ZUNEHMENDE Cyber-Attacks auf Firmen und Privatanutzer zeigen, dass es mehr Gefahrenbewusstseins und verstärkter Schutzmaßnahmen bedarf.

Der Staat muss die **RECHTLICHEN GRUNDLAGEN** zur Bekämpfung von Kriminalität im Netz schaffen.

Beide Initiativen setzen zudem voraus, dass die mitwirkenden Unternehmen zuvor durch vom Bundesamt für Sicherheit in der Informationstechnik anerkannte Prüfstellen bewertet und zertifiziert werden. Hierdurch sollen die mit dem Einsatz der Informationstechnik verbundenen Risiken weitestgehend minimiert und zusätzliches Vertrauen in die angebotenen Leistungen geschaffen werden.

Bekämpfung von Kriminalität

Eine eindeutige Rolle nimmt der Staat bei der Bekämpfung und Abwehr von Kriminalität ein. Er muss wirksam dagegen vorgehen, unabhängig davon, ob das Internet als Tatmittel eingesetzt wird oder nicht. Würde die Politik hier eine wertende Unterscheidung treffen, würde dies das Vertrauen der Bürger sowohl in den Rechtsstaat als auch in das Internet untergraben. Daher sind die erforderlichen Rechtsgrundlagen für staatliche Eingriffe zur Bekämpfung der Kriminalität im Internet zu schaffen und auch an neue Techniken und Verhaltensweisen fortlaufend anzupassen. Nimmt der Staat diese Aufgabe ernst, muss er zudem dafür sorgen, dass die Behörden entsprechend ausgebildet werden und über die entsprechende technische Ausstattung verfügen.

Schutz von kritischen Infrastrukturen

Das zuvor genannte Beispiel des Schadprogramms Stuxnet zeigt exemplarisch, dass das mit der zunehmenden Vernetzung einhergehende Gefahrenpotenzial nicht nur für den Einzelnen oder für ein Unternehmen vorhanden ist, sondern in seiner Konsequenz für die Gesellschaft als Ganzes. Das Beispiel verdeutlicht aber auch die Schwierigkeit von Seiten des Staates, dieser Bedrohung wirksame Abwehrmaßnahmen entgegenzusetzen. Die ständig steigende technische Komplexität auf der einen Seite und die verteilten Verantwortlichkeiten für Betrieb und Schutz kritischer Infrastrukturen auf der anderen Seite sind es, die dies schier unmöglich erscheinen lassen. Mit dem aus der Cyber-Sicherheitsstrategie der Bundesregierung jüngst hervorgegangenen Cyber-Abwehrzentrum wurde eine Informationsplattform geschaffen, auf der sich staatliche und private Stellen über mögliche Gefahren und im Falle einer konkreten Bedrohung über geeignete Gegen- und Schutzmaßnahmen austauschen können. Dies kann aber nur ein erster Schritt für mehr Schutz von kritischen Infrastrukturen in Deutschland sein.

Fazit

Die Sicherheit im Internet kann nur in einer gemeinsamen Anstrengung aller Beteiligten verbessert werden. Der Staat muss dies durch gezielte Fördermaßnahmen und mit einem entsprechenden Ordnungsrahmen unterstützen. Die Herausforderung an die Politik ist, ei-

Die Sicherheit im Netz fordert die ZUSAMMENARBEIT aller Beteiligten, national wie international.

nen solchen Rahmen zu schaffen, in dem durch die Schutzfunktion des Staates die Freiheit des Einzelnen im Netz vergrößert und nicht unnötig eingeschränkt wird sowie Innovationen von Wissenschaft und Wirtschaft im Inland gefördert und nicht blockiert oder ins Ausland verschoben werden. Gerade weil der digitale Raum keine Nationalstaatsgrenzen kennt, muss der Staat bei seiner Netzpolitik verstärkt die Zusammenarbeit mit internationalen Institutionen wie der Europäischen Union und der Privatwirtschaft suchen. Alles was dort im Wege der Selbstregulierung an Maßnahmen getroffen werden kann, ist im Zweifel wirkungsvoller als eine rein nationale Gesetzgebung. ///



/// DR. REINHARD BRANDL, MDB
Mitglied in der Enquete-Kommission
„Internet und digitale Gesellschaft“ des
Deutschen Bundestages, Berlin.

Anmerkungen

¹ Initiative D21: (N)Onliner Atlas 2011, www.nonliner-atlas.de, Stand: 15.7.2011.

² Freedom House: Freedom on the Net 2011, A global Assessment of Internet and Digital Media, Washington, D.C. 2011, S. 1-11.

³ Ebd.

⁴ Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2011, Bonn 2011.

⁵ Ebd.

⁶ Bitkom: IT-Kriminalität in Deutschland, www.bitkom.org/files/documents/BITKOM_Praesentation_IT-Kriminalitaet_30_06_2011.pdf, Stand: 15.7.2011.

⁷ www.bsi-fuer-buerger.de