

Die Web-Community: Doof, ahnungslos und korrupt? Verkennt unsere Wirtschaft das Risiko

Sie haben „eine der großartigsten Errungenschaften der Menschheit“ in Händen. Aber sie wissen nicht vernünftig damit umzugehen. Sie haben von den Risiken gehört, aber sie unterschätzen sie völlig. Sie könnten die Vielfalt der Möglichkeiten unter moralischen Aspekten nutzen, aber sie lassen sich von niedrigen Instinkten leiten – und von Geld. Aus der Sicht von Führungskräften der deutschen Wirtschaft leidet die große Gemeinde der Internetnutzer unter gewaltigen Defiziten im Umgang mit Technik und Verantwortung. Deshalb sehen sie in großer Mehrheit ein Enthüllungsportal wie Wikileaks nicht als Chance für mehr Demokratie, das zu Unrecht als „Robin Hood des Informationszeitalters“ salonfähig gemacht werde. Machtvoll lassen darum die Teilnehmer an der aktuellen Umfrage der CGC Consulting GmbH, München, den Ruf nach einer übergeordneten Kontrollinstanz erschallen.

Die Veröffentlichung vertraulicher Daten aus dem US-Außenministerium durch die Online-Plattform „Wikileaks“ hat die Aufmerksamkeit der Öffentlichkeit auf eine bisher eher ignorierte Eigenschaft des Internets gelenkt: Durch die weltweit ungehinderte Verfügbarkeit, durch seine Schnelligkeit und durch seine Anonymität erleichtert es die Publikation ursprünglich vertraulicher Daten um ein Vielfaches. Bei aller klammheimlichen Anerkennung für den Coup – die Reaktion der Amerikaner untermauerte die Treffsicherheit der Aktion – ließ die Aktion gleichwohl in den Führungsetagen von Politik und Wirtschaft rund um den Globus die Alarmglocken schrillen: „Und wann bringen die etwas von uns?“ Vor allem für Unternehmen erwächst eine neue Form der Bedrohung – und damit eine neue Herausforderung.

Denn während verantwortliche Führungskräfte der Wirtschaft vielfach in dem Glauben verharren, dass technische Lösungen wie Virens Scanner und Firewalls ausreichend Schutz davor bieten, dass Internes nach draußen dringt und das Externe nach innen vorstoßen, zeigte der Wikileaks-Finger auf einen bisher eher vernachlässigten Faktor: **die Menschen im Unternehmen**. Obgleich der käufliche Verräter schon seit biblischen Zeiten zur Grundausstattung jeder „Personengruppe größer 1“ zählt und die Geschichte zahllose Beispiele von Enthüllungen durch Menschenhand kennt, überraschten doch Dimension und Leichtigkeit, mit der hier die Inhalte geheimer Depeschen an die Öffentlichkeit drangen.

Sind Unternehmen ausreichend gewappnet, dieser neuen Herausforderung entgegen zu treten? Haben sie die Ansatzpunkte erkannt, an denen dies gelingt? Wie kritisch schätzen sie die Lage grundsätzlich ein? Und: Wie bewerten sie Portale wie Wikileaks in ihren gesellschaftlichen, wirtschaftlichen und politischen Folgen? Welche Schritte scheinen ihnen als Antwort angemessen?

Die CGC Consulting GmbH, München, hat in einer aktuellen, bundesweiten Studie mit dem Thema „Wikileaks und die Folgen“ untersucht, wie deutsche Unternehmen zu dem Thema Datenlecks und verantwortungsvollem Umgang mit den Möglichkeiten des Internet stehen. Darüber hinaus ermittelte die Studie, was aus Sicht der Firmen noch getan werden muss, um der Entwicklung erfolgreich entgegenzutreten.

Die Ergebnisse sind zum Teil überraschend. So lehnte das Panel zwar mit großer Mehrheit Einschränkungen der Meinungsfreiheit ab, trat aber gleichzeitig ebenfalls massiv für die Schaffung eines übergeordneten Kontrollgremiums ein, ähnlich einem „globalen Ethikrat“. So sahen die befragten Führungskräfte im offenen Internet eine der größten Errungenschaften der Menschheit, hielten die selbe aber für zu unbedarft und schlecht vorbereitet für den Umgang damit. So gehen die Befragten zwar davon aus, dass die Missbrauchsrisiken im Internet völlig unterschätzt werden – vor radikalen Schutzmaßnahmen im Betrieb schrecken sie dann aber doch zurück.

Methodik der Umfrage

Für die bundesweite Umfrage hat die CGC Consulting GmbH einen strukturierten Fragebogen entwickelt und im Januar 2011 rund 600 Führungskräfte und Personalentscheider in Deutschland befragt. An der Studie teilgenommen haben Betriebe jeder Größenordnung, die im nationalen und internationalen Umfeld tätig sind. Die Auswertung gibt stets die Nennungen in Relation zur Anzahl der Gesamtnennungen in Prozent an. Bei Mehrfachnennungen sind die Anteile der jeweiligen Nennung an der Zahl der Teilnehmer berechnet.

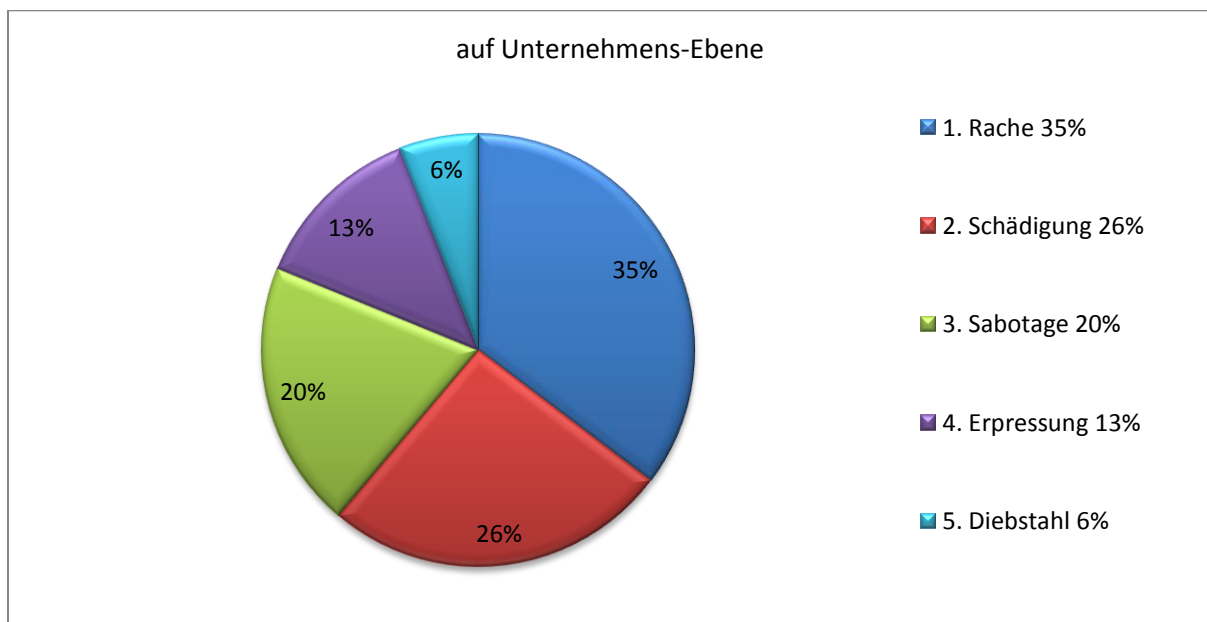
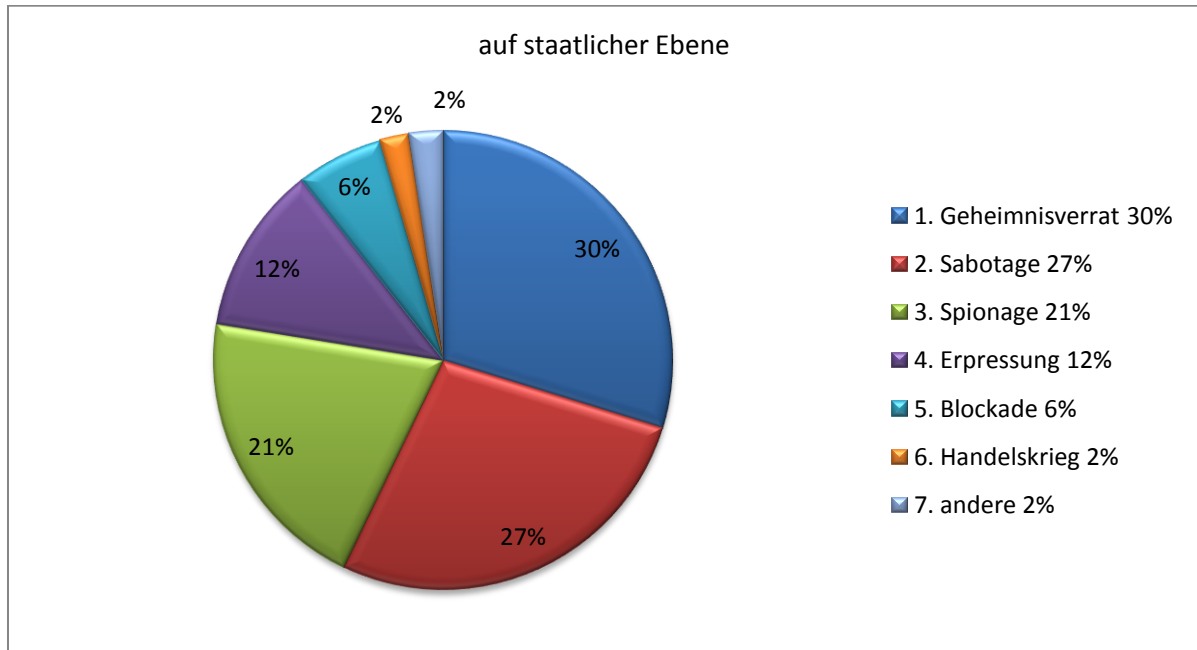
CGC Wirtschaftsforschung

Die CGC Wirtschaftsforschung, Wien, analysiert im Auftrag der Personalberatung CGC – Claus Goworr Consulting GmbH, München, Entwicklungen und Trends im Personalsektor und sorgt mit regelmäßigen Publikationen für deren Veröffentlichung. Das Team von CGC Consulting München steht für langjährige, fundierte Erfahrung im Bereich Executive Search. Berater und Mitarbeiter verfügen über branchenspezifisches Know how. Das Unternehmen ist seit Jahren äußerst erfolgreich in der verdeckten Suche nach Führungskräften und Spezialisten tätig.

Ranking

Frage 1

In welchen Bereichen kann das Internet missbraucht werden?



Wenn es um großangelegte Coups im Internet geht, dann kennt die Vorstellungskraft von Führungskräften der deutschen Wirtschaft keine Grenzen. Ganz egal, ob es sich um Attacken auf staatlicher Ebene geht oder um Angriffe auf Unternehmen: Aus Sicht der Befragten taugt das WWW für jede Schandtat. Während auf der Länderebene die üblichen Gemeinheiten wie Geheimnisverrat, Sabotage und Spionage auf der Liste stehen, genießen auf der Geschäftsebene das Rache-Motiv und die Absicht direkter Schädigung den schlechtesten

Ruf. Die hohen Werte deuten zudem an, dass es sich aus Perspektive der Befragten nicht mehr um potentielle, sondern schon um eher reale Bedrohungen handelt.

In den Ergebnissen schwingt ein gewisser Respekt für die Multifunktionalität des Mediums Internet mit. Wie ein Schweizer Messer scheint es geeignet für alle Fälle des Geheimen. Wobei die „weichen“ Methoden eher als realistisch betrachtet werden, als harte Attacken wie Handelskriege, Blockaden oder Diebstähle. Die bekanntgewordenen Fälle aus jüngster Zeit belegen das Gegenteil: Im Cyberwar geht es schon lange nicht mehr ums Tricksen, sondern ums wirkungsvolle Attackieren und Zerstören.

In diesem Zusammenhang sei auf die Ergebnisse zu nachfolgenden Fragen verwiesen: Ein globaler Ethikrat oder eine vergleichbare Institution ist aus Sicht der Befragten wünschenswert, um mit den genannten Bedrohungen und weiteren Missständen aufzuräumen. Darin spiegelt sich die Erwartungshaltung nach einem politischen Konsens auf internationaler Ebene: Abrüstung im Internet auf UN-Ebene – oder Rüstungskontrolle und Blauhelme im Cyberspace.

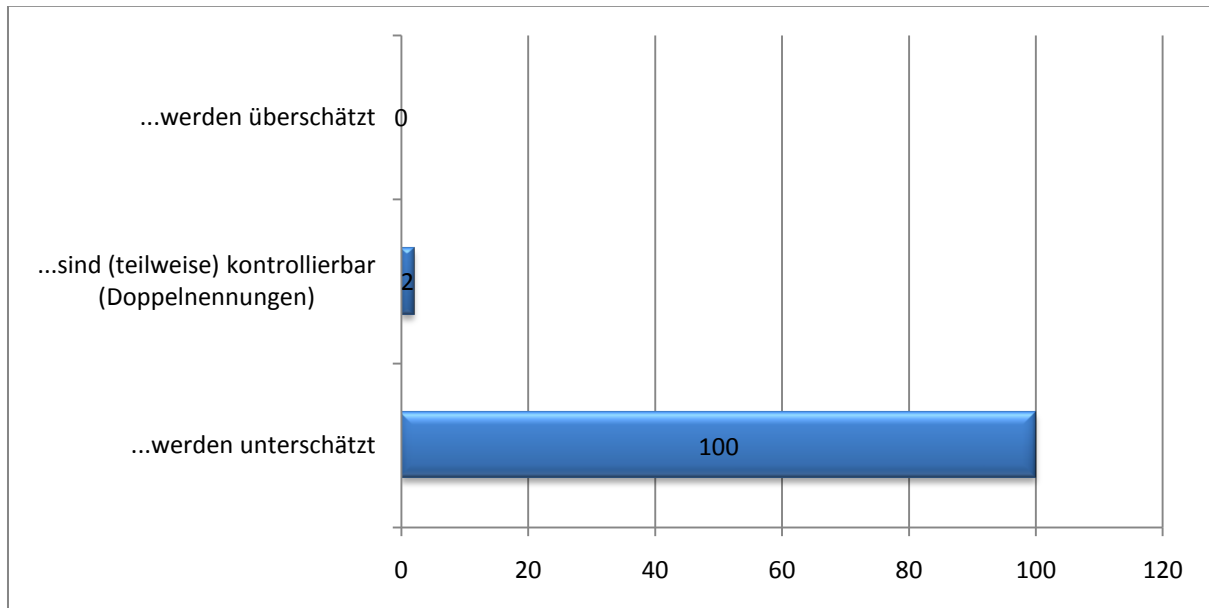
Angesichts der hohen Werte, mit denen auf Unternehmens-Ebene die Risiken „Rache“, „Schädigung“ und „Sabotage“ bewertet werden, besteht akuter Handlungsbedarf in den Firmen und für die Politik, hier schnelle und wirkungsvolle Gegenmaßnahmen zu entwickeln und anzuwenden. Die häufig beschworenen „Human Resources“ gewinnen vor diesem Hintergrund eine zusätzliche Komponente, die es zu erfassen, zu betreuen und zu gestalten gilt. Der Aspekt „Loyalität“ erhält im Rahmen der Personalentwicklung damit zusätzliches Gewicht.

Frage 2

Die Möglichkeiten zum Missbrauch des Internets

a)	werden unterschätzt	100,00
b)	sind (teilweise) kontrollierbar	2,34*
c)	werden überschätzt	0,00

* Doppelnennungen



In einem Punkt sind sich alle Befragten einig: Die Möglichkeiten zum Missbrauch des Internets werden völlig unterschätzt. Einige wenige merkten zusätzlich (aber nicht alternativ!) an, dass sie die Missbrauchsmöglichkeiten wenigstens teilweise für kontrollierbar halten. Aber kein einziger konnte sich zu der Meinung durchringen, die Risiken würden überschätzt.

Im Kontext mit Frage 1 lässt sich dies auch zur Erkenntnis umformulieren: Der Phantasie sind bei vorstellbaren Missbrauchsszenarien keine Grenzen gesetzt. Offenbar steht aus Sicht der Panel-Teilnehmer zu befürchten, dass das World Wide Web nicht nur im Rahmen der üblichen Schad-Möglichkeiten genutzt wird, sondern dass Missbraucher mitunter ganz neue Ansätze entwickeln können. Dafür spricht zum Beispiel, dass Themen wie Trojaner und Malware noch vor 20 Jahren nicht existent waren, heute aber als bedrohlicher für einen reibungslosen Betrieb der Unternehmensinfrastruktur gelten als Stromausfälle – ein beliebtes Vorsorgethema zur Jahrtausendwende. Auch das Auftauchen des Sabotagevirus „Stuxnet“ in einer iranischen Atomanlage 2010 kam für eine breite Öffentlichkeit, aber auch für Führungskräfte in der deutschen Wirtschaft überraschend.

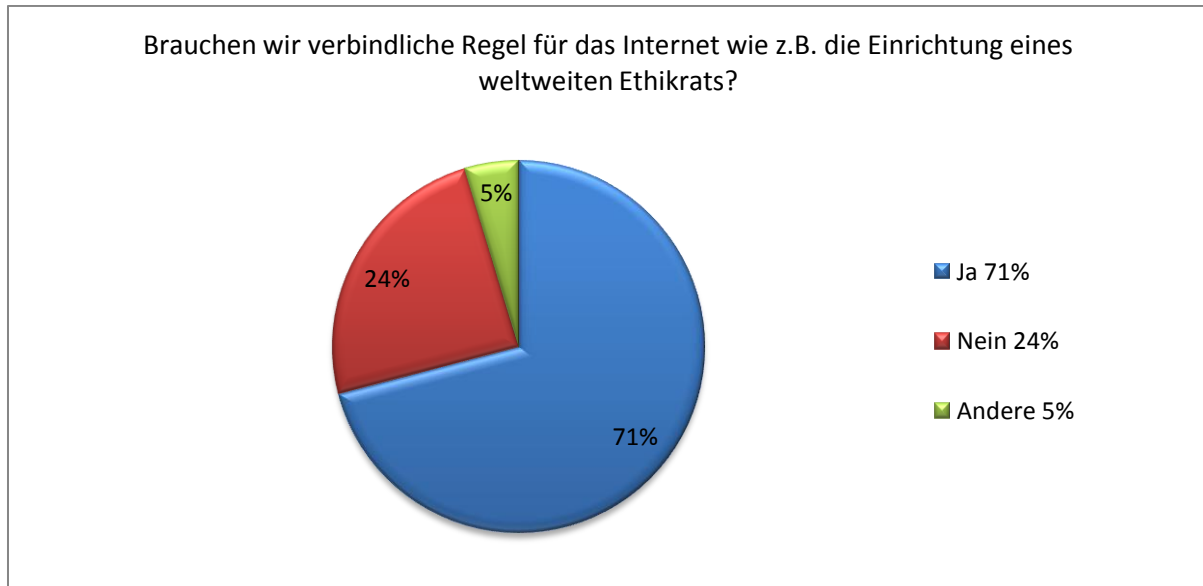
„Teilweise Kontrollierbarkeit“ darf man getrost so interpretieren, dass hier der Wunsch der Vater des Gedankens ist. Ähnlich wie bei Grenzwertdiskussionen oder der Beschwörung

gesetzlicher Schutzmechanismen ist hier die Hoffnung erkennbar, dass es – wenn man nur sorgfältig genug aufpasst – schon so schlimm nicht werden wird.

Gleichzeitig ist vielleicht ein Phänomen zu beobachten, dass stets dann auftritt, wenn es um den unbequemen Verzicht auf liebgewordene Gewohnheiten (Zigaretten, Bierchen, Chips) geht: Man blickt der Gefahr wissenden Auges ins Antlitz...

Frage 3

Brauchen wir verbindliche Regeln für das Internet wie z.B. die Einrichtung eines weltweiten Ethikrats?



Der Deutsche Ethikrat, so steht es in seinen Statuten, „verfolgt die ethischen, gesellschaftlichen, naturwissenschaftlichen, medizinischen und rechtlichen Fragen sowie die voraussichtlichen Folgen für Individuum und Gesellschaft, die sich im Zusammenhang mit der Forschung und den Entwicklungen insbesondere auf dem Gebiet der Lebenswissenschaften und ihrer Anwendung auf den Menschen ergeben“. Unter anderem soll er auf dieser Basis Stellungnahmen sowie von Empfehlungen für politisches und gesetzgeberisches Handeln erarbeiten.

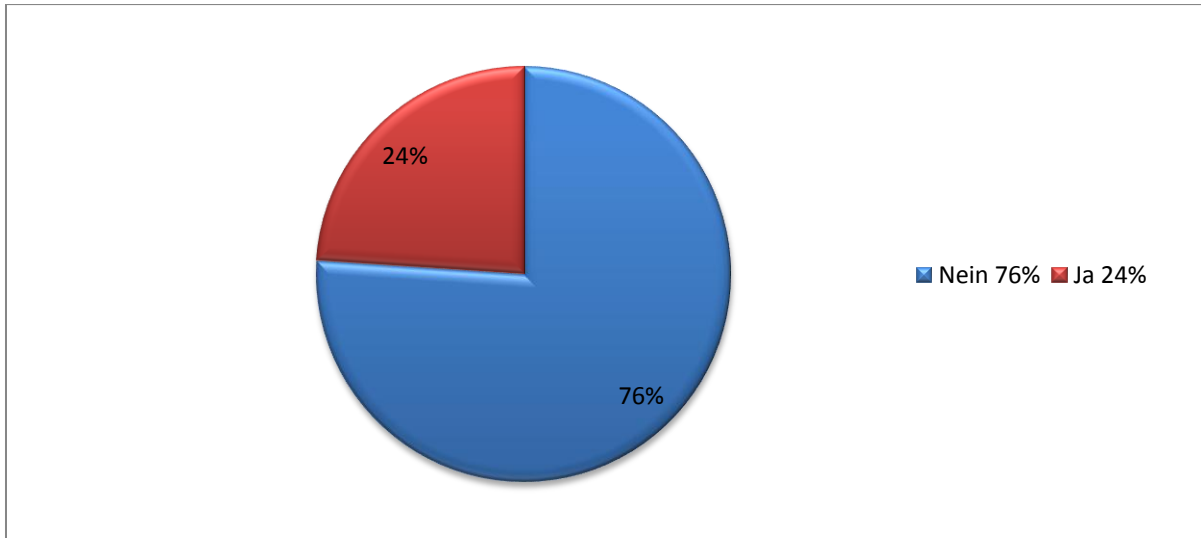
Dieses Prinzip sähen die Teilnehmer an der Umfrage mit großer Mehrheit gern auch in Gestalt einer „übergeordneten Kraft“ auf das Internet angewendet, um negative Auswüchse und Missbrauch einzudämmen. Dies ist umso bedeutsamer, als damit einem „Meinungs- und Gesinnungsregulierer“ das Wort geredet wird, der auch die Bewegungsfreiheit der Unternehmen selbst einschränkt.

Ein gutes Viertel der Befragten lehnt eine solche Lösung ab, zum Teil mit Begründung: „politisch nicht realistisch“, „Verbindlichkeit zweifelhaft“, „Aufgabenstellung zu differenziert“, „Kulturen übergreifend nicht umzusetzen“ oder „das ist unbezahlbar“ heißt es auf Seiten der Kritiker.

Alternative Lösungsvorschläge von Seiten der Befragten sehen zum Beispiel die, in der Internetcommunity seit langem diskutierte und heftig umstrittene, Einführung einer Kostenkomponente vor, um den Missbrauch wenigstens nicht mehr „kostenlos“ möglich zu machen. So sollen Gebühren für den Mailversand helfen, das Spam-Volumen einzudämmen. Oder sie schlagen radikale Gegenmaßnahmen wie „Hacker im Staatsdienst“ vor, die aktiv gegen den Missbrauch vorgehen. Eine stark idealisierte Vorstellung: Wie wir in Ländern rund um den Globus beobachten können, finden Staaten durchaus Gefallen daran, besoldete Datenkrieger für zielgerichteten Missbrauch zu engagieren.

Frage 4

Sollten Beschränkungen der sogenannten „Freien Meinungsäußerung“ für das Internet bei Unternehmen und Staaten erlassen werden, um internationale Beziehungen, wirtschaftliche Interessen oder kulturelle und religiöse Empfindungen nicht zu beschädigen?



Drei von vier Befragten lehnen eine Einschränkung der freien Meinungsäußerung als Maßnahme gegen die missbräuchliche Nutzung des Internets ab. Diese Antwort macht ambivalente Einstellung des Panels in der Angelegenheit deutlich. Denn die von fast ebensovielen Befragten geforderte Schaffung einer Institution wie einem „weltweiten Ethikrat“ würde konsequenterweise genau in diesen Schritt münden.

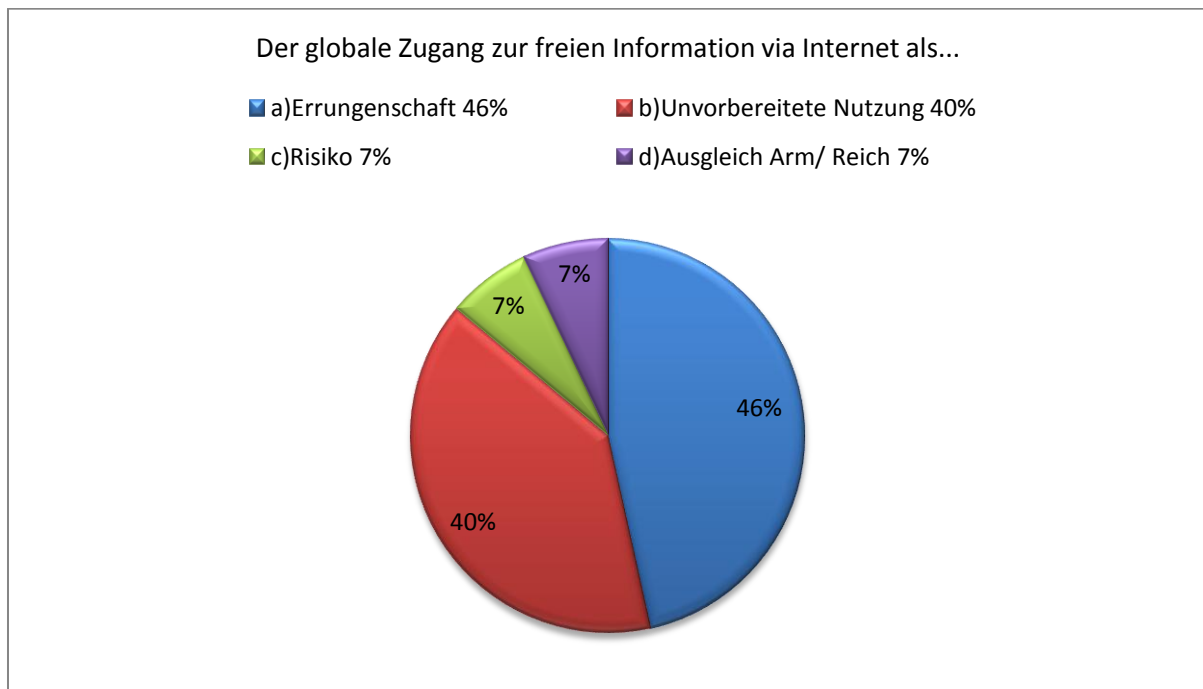
Immerhin ein Viertel glaubt bereits, dass neue Kommunikationswege unter Umständen auch neue Kommunikationsregeln nötig machen.

Bewusst wurde hier die generelle Bereitschaft abgefragt, ob Beschränkungen akzeptabel sind. Bereits ein Viertel der Befragten würde schon jetzt für mehr Sicherheit im Internet einen Teil der Meinungsfreiheit opfern.

Frage 5

Der globale Zugang zur freien Information via Internet ...

- a) ... ist eine der größten Errungenschaften der Menschheit
- b) ...trifft auf eine Menschheit, die für die Nutzung dieser Information völlig unzureichend vorbereitet und ausgebildet ist
- c) ...bringt deutlich mehr Risiken als Vorteile
- d) ...ist der erste Schritt zum Ausgleich zwischen Arm und Reich, weil er mit dem Wissensmonopol der Mächtigen aufräumt



Über das neue „Werkzeug Internet“ freut sich die Wirtschaft sichtlich. So räumt fast die Hälfte von Befragten dem uneingeschränkten Zugang zu freier Information im World Wide Web den Rang „einer der größten Errungenschaften der Menschheit“ ein. Auch wenn sich das Management gelegentlich öffentlich über die Produktivitätsverluste beklagt, die durch übermäßigen E-Mail-Verkehr und private Nutzung von Internet am Arbeitsplatz entstehen, so zeigt die hohe Wertschätzung des Mediums doch, dass die Chancen erkannt werden, die sich aus seiner Nutzung ergeben. Das ist die eine Seite der Medaille.

Denn auf der anderen Seite sehen fast genauso viele Befragte mit Skepsis, dass das Internet auf eine Weltbevölkerung trifft, die „für die Nutzung dieser Information völlig unzureichend vorbereitet und ausgebildet ist“. Man könnte der Gruppe der Panel-Teilnehmer, die sich zu dieser Einschätzung bekennt, Arroganz vorwerfen. Man kann ihr aber – gerade im Kontext der gesamten Umfrage – unterstellen, dass sie von Angst und Sorge erfüllt ist, wohin fehlende Medienkompetenz bei breiten Schichten der Bevölkerung führt.

Aus Sicht der Befragten verhält es sich so gesehen mit dem Internet in etwa so wie vor rund 40 Jahren mit der Atomenergie – oder wie vor 175 Jahren mit der Eisenbahn. Daraus erwächst für die Firmen nicht nur ein akuter Bedarf an Aufklärung und Weiterbildung ihrer Mitarbeiter. Sie müssen sich auch auf die Folgen eines unzureichend reflektierten Umgangs

mit freien Informationen einstellen und präventive Strategien entwickeln zu Gerüchten, Vorurteilen und Halbwissen entwickeln, die das eigene Unternehmen und sein politisches, gesellschaftliches, technologisches und soziales Umfeld betreffen.

Diese Aufgabe lässt sich nur in sehr eingeschränktem Umfang delegieren. Zwar untermauert der sich im Antwortverhalten spiegelnde Pessimismus den vielfach geäußerten Wunsch, eine übergeordnete Instanz – also die Politik - möge die Verantwortung abnehmen und verbindliche Verhaltensmaßregeln vorgeben und festlegen, um dieses Element des technischen Fortschritts in den Griff zu bekommen. Wirksam und glaubwürdig sind hier indes nur eigene Initiativen.

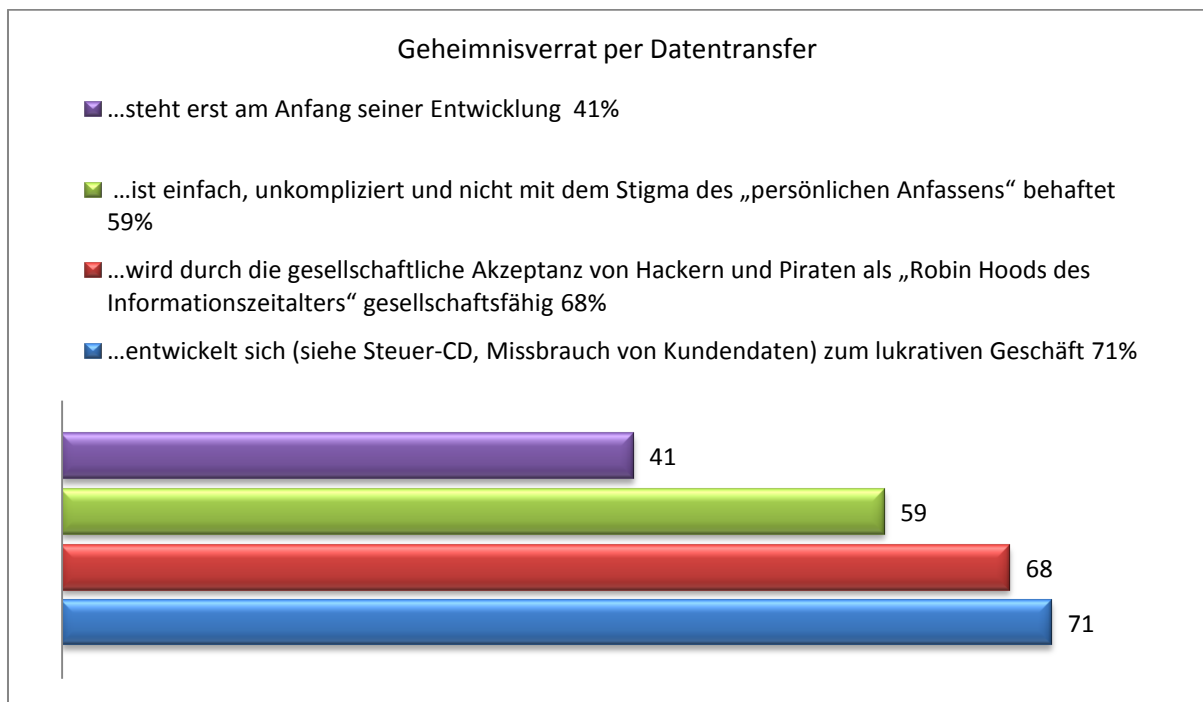
Das Lob für die „Errungenschaft“ entspricht dem in Frage 4 gezeigten Widerstand gegen Einschränkungen der freien Meinungsäußerung – ein Indiz dafür, dass beide Qualifizierungen eher subjektiv denn objektiv vorgenommen werden. Konträr dazu ist die Reaktion auf die beiden weiteren Antwortmöglichkeiten von Realismus geprägt. Dass das Internet mehr Risiken als Vorteile brächte, dürfte nur größten Pessimisten so erscheinen und steht im direkten Widerspruch zu allem innovatorischen Unternehmergeist. Zumal die Wahrnehmung der Vorteile im betrieblichen Alltag – von der schnellen Mail „an alle“ bis zur Abfrage von Rohstoffpreisen und der Recherche zu Fachthemen – inzwischen ebenso verbreitet ist, wie die Störung des betrieblichen Lebensalltags durch gefährliche Elemente eine Ausnahme ist. Das betrifft sowohl die Intensität als auch die Frequenz einschlägiger Erlebnisse.

Schließlich der Glaube daran, dass technischer Fortschritt zum gesellschaftlichen Ausgleich beitrüge. Ganz nüchtern betrachtet aber lässt sich feststellen: Welcher Unternehmer würde den Wettbewerbsvorteil eines Wissensvorsprungs der Gerechtigkeit halber aufgeben?

Frage 6

Geheimnisverrat per Datentransfer...

- a) ...entwickelt sich (siehe Steuer-CD, Missbrauch von Kundendaten) zum lukrativen Geschäft
- b) ...wird durch die gesellschaftliche Akzeptanz von Hackern und Piraten als „Robin Hoods des Informationszeitalters“ gesellschaftsfähig
- c) ...ist einfach, unkompliziert und nicht mit dem Stigma des „persönlichen Anfassens“ behaftet
- d) ...steht erst am Anfang seiner Entwicklung



Lukratives Konzept oder Robin-Hood-Effekt: Beide Optionen tragen aus Sicht der Befragten als Grundlage fürs Geschäftsmodell „Geheimnisverrate per Datentransfer“. Wie sich anhand der Mehrfachnennung zeigt, erscheint die Methode „Geldmaschine“ bei 71,37 Prozent der Teilnehmer als wahrscheinlich – und wird die Gesellschaftsfähigkeit von Hackern und Piraten als Gesetzesbrecher mit edlen Motiven von 67,87 Prozent ebenfalls sehr häufig registriert. Auffällig: Bei fast 80 Prozent der Fragebogen, auf denen die „lukrativen Geschäfte“ angekreuzt waren, gab es auch Zustimmung zu „Robin Hood“.

Ganz offenkundig wird das Internet auch als wohlfeile Gelegenheit wahrgenommen, den Geheimnisverrat einfach und unkompliziert vorzunehmen. Eine deutliche Arbeitserleichterung gegenüber früheren Methoden – und nicht mehr mit dem Stigma das „persönlichen Anfassens“ behaftet, wie 58,50 Prozent der Befragten meinen.

Die Tatsache, dass 41,5 Prozent der Umfrageteilnehmer die Entwicklung beim „Geheimnisverrat per Datentransfer“ erst an ihrem Anfang sehen, ließe sich theoretisch mehrerlei schließen:

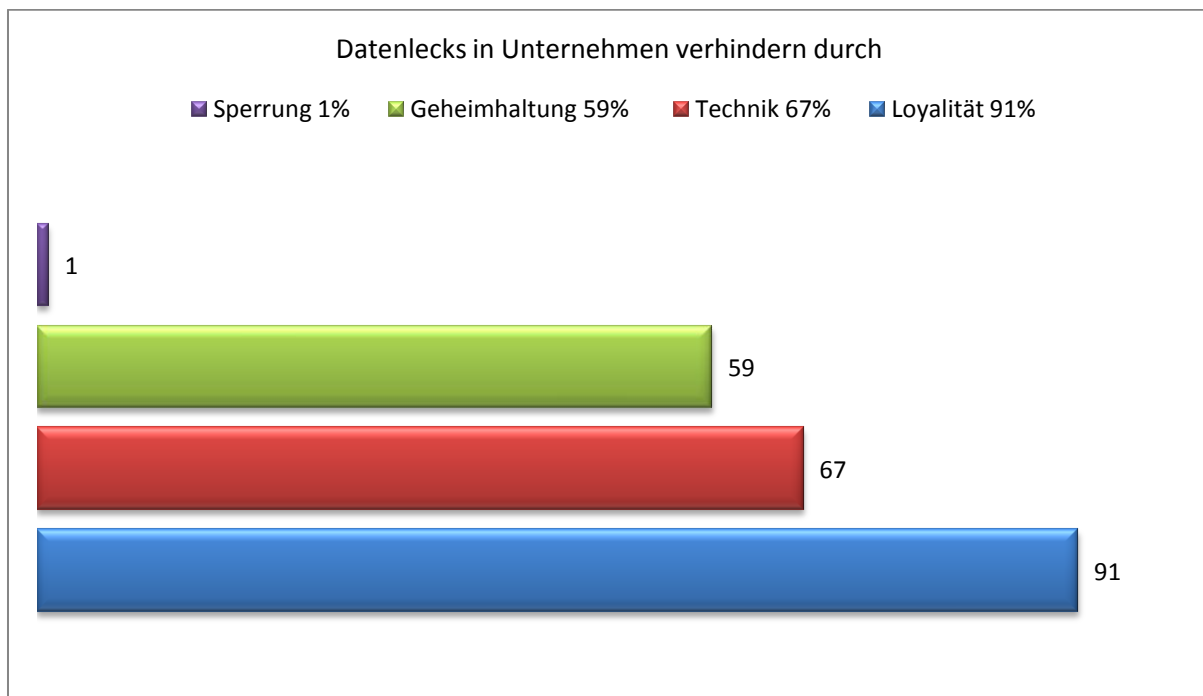
- Vielleicht haben jene fast 60 Prozent, die hier kein Kreuzchen machten, die Hoffnung, das Thema sei erkannt und „durch“.
- Es sind vier von zehn Entscheidern besorgt, dass alles noch viel schlimmer wird ...
- ...und dass wir erst die Spitze des Eisbergs zu sehen bekommen haben.
- Bei einem großen Teil der Befragten herrscht die Überzeugung, dass die Sache nicht mehr aufzuhalten ist...
- ...und das man dies hinnehmen muss wie Naturkatastrophen.

Am wahrscheinlichsten ist aber, wenn wir uns die Antworten auf die nächste Frage ansehen, dass die Mehrheit glaubt, man könne das Problem noch in den Griff bekommen.

Frage 7

Wer Datenlecks in Unternehmen verhindern will...

- a) ...sollte maximalen Aufwand in die Loyalität seiner Mitarbeiter stecken
- b) ...muss massiv in technische Systeme zur Datensicherung und Verschlüsselung investieren
- c) ...legt größten Wert auf Geheimhaltung und hält den Kreis von Insidern sehr klein
- d) ...sperrt im Unternehmen alle privaten Internet-Zugänge, USB-Sticks und sonstige Datenspeichermöglichkeiten und verbietet alle mobilen Kommunikationsgeräte auf dem Firmengelände



Positiv betrachtet: Der Glaube daran, dass eine funktionierende menschliche Ebene eher als technische Systeme dazu geeignet ist, Datenlecks in Unternehmen zu verhindern, spricht für die emotionale Intelligenz der Befragten. Kurz gesagt: Die Sicherheit, die wir brauchen, kaufen wir uns. Entweder, indem wir Geld dafür ausgeben, dass die Loyalität von Mitarbeitern wachse und gedeihe. Oder, indem wir ein technisches Fort Knox aufrichten, in dem alle wertvollen Daten vor der Öffentlichkeit geschützt sind.

Kritisch interpretiert sind die Werte von 91 Prozent pro Loyalitätsprogramm und nur 67 Prozent pro Schutztechnik dahin gehend zu deuten, dass offenbar menschliche Korruptierbarkeit als bedrohlicher empfunden wird als technische Unzuverlässigkeit. Dem eher generalistischen Ansatz, Geheimhaltung zu forcieren und die Zahl der Eingeweihten klein zu halten, neigt immerhin noch deutlich mehr als die Hälfte der Befragten zu. Vielleicht auch deshalb, weil bei der Fragestellung bewusst das „Wie“ offen gehalten wurde. Die Mehrheit der bislang bekannten Datenlecks kamen zustande, weil Fahrlässigkeit, mangelnde Kontrolle und unzureichende Sicherungssysteme sie ermöglichten. Die alte Erfahrung, dass nicht mehr geheim ist, was zwei Menschen wissen, macht deutlich, dass dieser Vorschlag die Situation an sich zwar entschärfen mag – ein Werkzeug zur sicheren Verhinderung von Lecks ist er nicht.

Der eigentliche Knackpunkt dieses Themenkomplexes liegt ganz woanders: Schaut man sich an, wie wenige Führungskräfte sich für grundlegende und präzise Vorschläge wie das rigorose Verbot ungesicherter Schnittstellen und mobiler Daten-Weg-Träger begeistern kann, bewegt sich deren Problembewusstsein im weiten Feld zwischen maximalem Vertrauen und maximaler Unbedarftheit: Nur 1,17 Prozent von ihnen können sich für diesen radikalen Schritt begeistern. Und öffnen damit nahezu unsichtbaren Spionage-Werkzeugen wie dem USB-Stick Tür und Tor.

Wenn man sich vor Augen hält, welche Dimension inzwischen das sogenannte „Social Engineering“ einnimmt (früher sagte man: Anwerben und Auspähen), erstaunt dieser Grad der Naivität. Zumal wirklich jeder gerade erst durch Wikileaks vor Augen geführt bekam, welche Folgen das nach sich zieht.

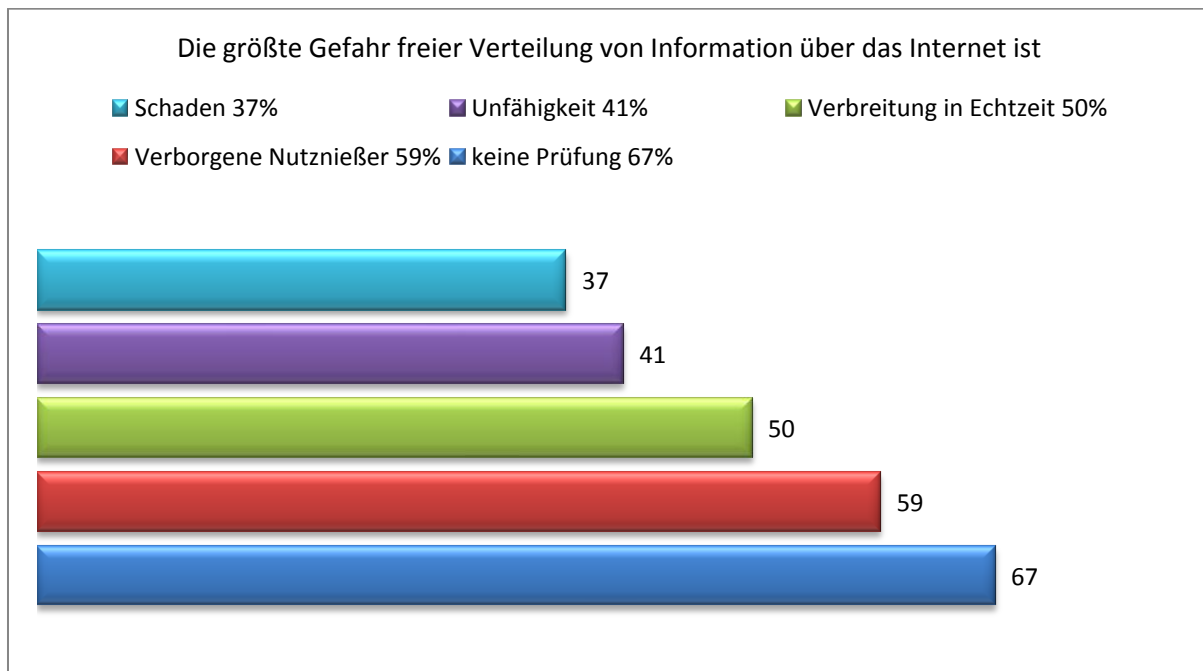
Wie anfällig viele Unternehmen für *Social Engineering* oder einfache Unachtsamkeit mit Datensicherheit zum Beispiel im Zusammenhang mit USB-Sticks sind, zeigt eine im Januar 2007 durchgeführte *Security Awareness Campaign* der britischen NCC Gruppe: Sie verschickte 500 präparierte USB-Sticks an Finanzverantwortliche britischer Unternehmen mit einer anonymen Einladung zu einer Feier. Die Bestätigung sollte über eine Webseite geschehen, die von dem USB-Stick aufgerufen wurde, sobald dieser in den Rechner gesteckt wurde. 47% der Empfänger steckten den USB-Stick in den Rechner, klickten eine Warnung beiseite und die Webseite wurde geöffnet.

(Quelle: www.ernw.de/content/e15/e28/.../ERNW_Newsletter_22_v1.0_ger.pdf)

Frage 8

Die größte Gefahr freier Verteilung von Information über das Internet ist...

- a) ...dass keine Prüfung auf Echt oder Falsch erfolgt.
- b) ...dass sich die wahren Nutznießer im Verborgenen halten können
- c) ...die unkontrollierbare Verbreitung in Echtzeit rund um die Welt.
- d) ...die Unfähigkeit der Menschen, damit verantwortungsvoll umzugehen.
- e) ...der Schaden, der durch ihre mutwillige Verbreitung erfolgt – und von den Verbreitern in Kauf genommen wird.



Mit Produkt- und Markenfälschung befassen sich Unternehmen schon lange. Künftig werden sie wohl auch verstärktes Augenmerk auf die Echtheit von Nachrichten legen müssen. Denn hier ruht nach Einschätzung des Umfragepanels das größte Risiko bei der freien Verteilung von Information: dass falsche oder ungeprüfte Nachrichten in Umlauf kommen und Schaden anrichten.

Zwar erzielen alle Optionen bei dieser Frage, nicht zuletzt wegen der Möglichkeit zur Mehrfachnennung, hohe Werte. Gleichwohl ergibt sich ein diffuses Bild, eine Art „Angst Cloud“. Die beiden Ausreißer nach oben und unten deuten darauf hin, dass sich das Problembewusstsein allmählich konkretisiert – ausgeprägt ist es noch nicht. Immerhin: Die Zweifel am Wahrheitsgehalt dessen, was sich da alles übers Internet ausbreitet, sind angebracht. Von Hoax-Meldungen über vermeintlich nachgewiesene Phänomene über gezielte und irrtümliche Falschmeldungen bis zum Abfischen von persönlichen Daten über gefälschte Websites begegnet dieses Problem allen Befragten täglich. Realistisch betrachtet müsste dieser Wert deutlich höher liegen. Aber vermutlich ist die mangelnde Erkenntnis dem Umstand geschuldet, dass die Menschheit für die Nutzung von Informationen aus dem Internet unzureichend vorbereitet und ausgebildet ist (Frage 5).

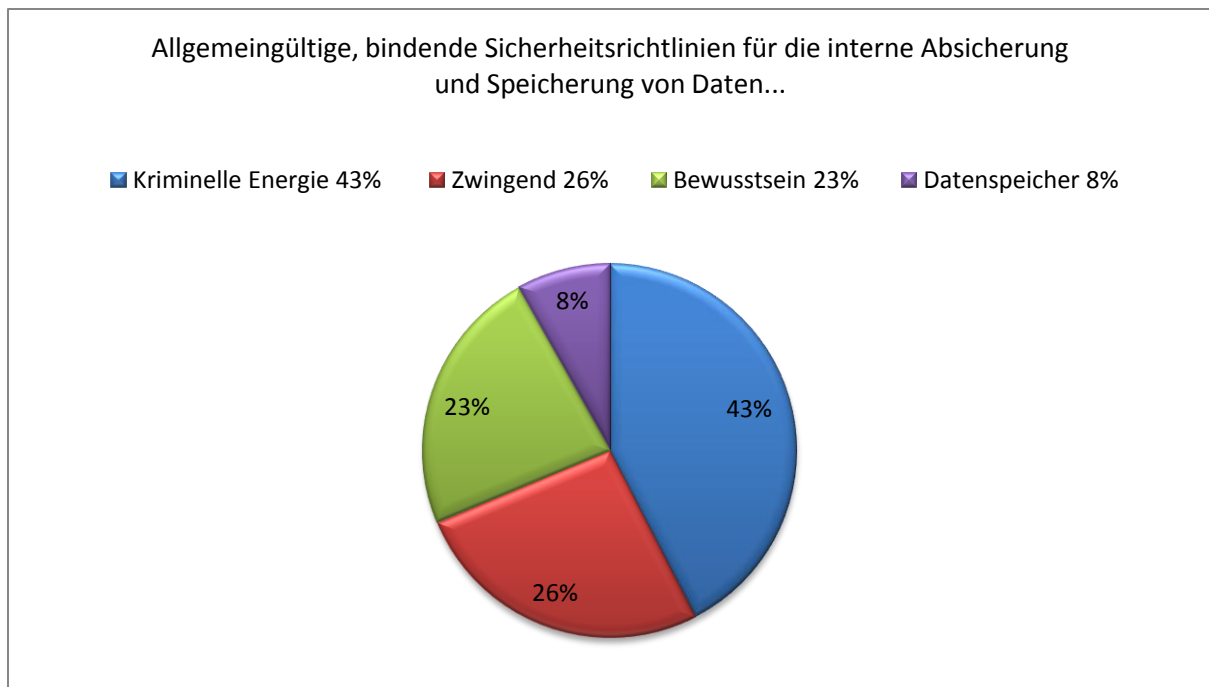
Letztlich weist das erkennbare Angst-Schema durchaus Parallelen zu dem auf, das bei Flugangst erkennbar ist. Die Sorge darüber, dass etwas im Verborgenen passiert, dass Zustände unkontrollierbar sind, dass Verantwortliche mit ihren Aufgaben unverantwortlich umgehen, dass „die“ Technik mächtiger ist als „der“ Mensch – all das spiegelt sich in den Antworten zu diesem Thema ebenso wie in der Verdichtung der gefühlten Bedrohungspotentiale.

Dass nur gut ein Drittel der Befragten den real erkennbaren Schaden als Gefahr sieht, gleichzeitig aber drei Viertel von ihnen eine übergeordnete Instanz wünschen, die immateriellen Schaden durch ihr Eingreifen verhindern soll, gehört zu den bemerkenswerten Ungereimtheiten im Umgang mit dem Internet.

Frage 9

Allgemeingültige, bindende Sicherheitsrichtlinien für die interne Absicherung und Speicherung von Daten...

- a) ...können noch so perfekt formuliert sein, schützen aber nie vor der Kraft krimineller Energie.
- b) ...sind zwingend erforderlich, denn der Diebstahl oder Verlust von Daten sowie missbräuchliche oder unbeabsichtigte Veröffentlichungen stellen den tatsächlichen Datenskandal dar.
- c) ...wären ein guter Anfang, um das Bewusstsein für den sorgfältigen Umgang mit Daten zu sichern.
- d) ...adressieren nicht das Kernproblem: dass vertrauliche Inhalte nicht in Datenspeicher gehören.



Zitat Bundesamt für Sicherheit in der Informationstechnik: „Bedrohung + Schwachstelle = Gefährdung; dies ist die Kernformel für die Betrachtung von Gefährdungen und Gegenmaßnahmen. Eine Bedrohung allein, wie sie durch einen Hacker, einen Spion, jegliche Form von Schadsoftware (Viren, Würmer, Trojanische Pferde ...) oder aber auch durch höhere Gewalt besteht, wäre für ein perfektes IT-System (sofern es so etwas gäbe) nicht gefährlich. Erst dadurch, dass das System oder die das System umgebenden Personen, Räumlichkeiten oder Regelungen eine Schwachstelle aufweisen, die durch eine Bedrohung ausgenutzt werden kann, entsteht eine Gefährdung und damit verbunden ein Risiko.“ Um sicherzustellen, dass jeder Mitarbeiter die ihn betreffenden IT-Sicherheitsaspekte kennt und beachtet, empfiehlt das BSI (Quelle: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Musterrichtlinien/Uebersicht.pdf?blob=publicationFile>), unterschiedliche Sicherheitsrichtlinien und Teilkonzepte zu erstellen, die einzelne IT-Sicherheitsthemen bedarfsgerecht darstellen. So erhalten Mitarbeiter genau die Informationen, die sie zu einem bestimmten Thema wirklich benötigen.

Das Vertrauen in diese Maßnahme ist offenbar begrenzt. Nach Auswertung der Antworten, die kriminelle Energie als machtvoller bewerten denn aktive Sicherheitsmaßnahmen, stellen sich die Fragen: Sind interne Sicherheitsvorschriften das Papier nicht wert, auf dem sie gedruckt sind? Halten ausgeklügelte Richtlinien und Datenschutzmaßnahmen nicht stand, wenn sie mit krimineller Energie attackiert werden? Sind diese Richtlinien nicht tiefgreifend und detailliert genug, um tatsächlich Wirkung zu zeigen? Oder: Gehen die Verantwortlichen aus Fatalismus vielleicht nur mit halbem Herzen an die mühsame Aufgabe heran, individuelle, betriebsgerechte Richtlinien zu erarbeiten?

Immerhin: Zwei von fünf Befragten sehen unter den angebotenen vier Optionen jene als wahrscheinlichste, die Kriminellen die stärkere Position unterstellt. Nach dem Motto: „Das können wir uns gleich sparen, das hilft sowieso nichts,“ legen sie damit potentiellen Angreifern nicht nur den Hausschlüssel auf die Fußmatte, sondern hängen gleich auch noch den Wegweiser daran, wo im Unternehmen sich die Schätze befinden.

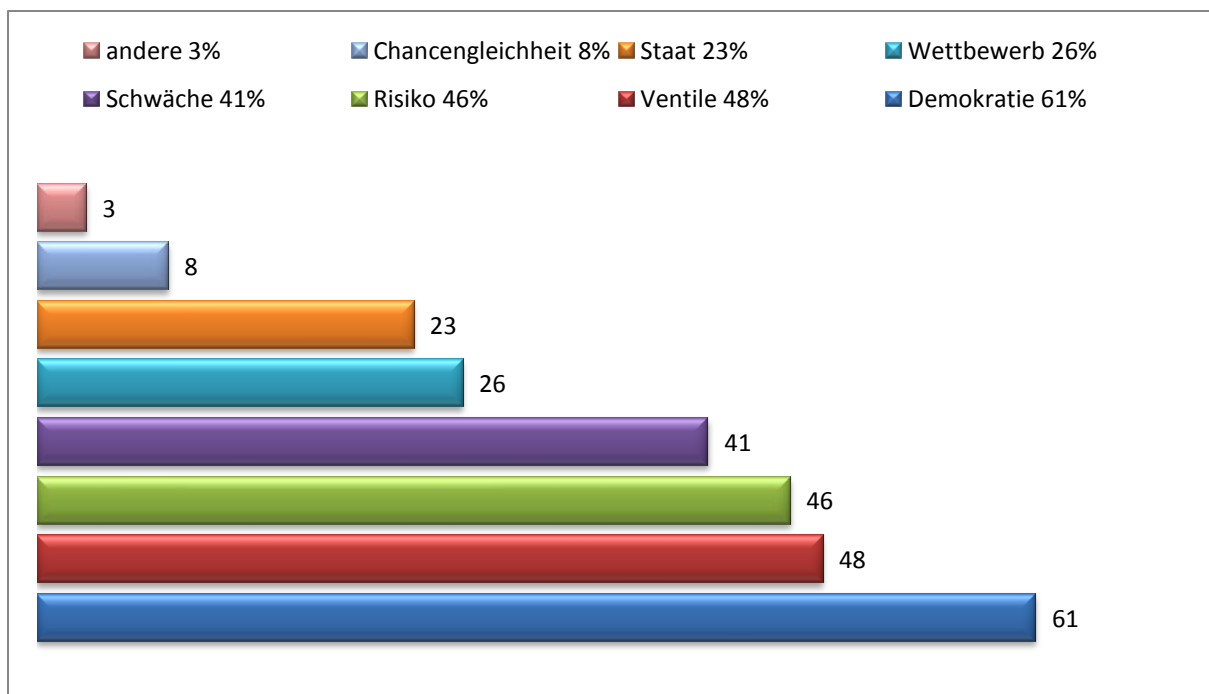
Es stimmt allerdings zuversichtlich, dass zwei andere aktive und positive Optionen zusammengenommen diese fatalistische Sicht der Dinge überstimmen. Jeweils rund ein Viertel der Befragten ist entweder der Meinung, dass Sicherheitsrichtlinien im Betrieb zwingend erforderlich sind, weil Diebstahl oder ungesichertes Durchsickern von Daten den „eigentlichen Skandal“ darstellen. Oder sie sehen darin einen „guten Anfang, um das Bewusstsein für den sorgfältigen Umgang mit Daten zu sichern“. Dieses Berücksichtigen des menschlichen Faktors korreliert mit dem Spitzenreiter aus Frage 7, den „Investitionen in Loyalität“. Dennoch bleibt eine Diskrepanz in der Gewichtung: Während dort 9 von 10 Befragten einen wirksamen Ansatz zum Stopfen von Datenlecks im Unternehmen sehen, bestätigen nur gut 2 von 10 die Wirksamkeit bewusstseinsbildender Maßnahmen.

Nur jeder zwölfte Befragte sieht das Kernproblem darin, dass vertrauliche Daten erst gar nicht in Datenspeicher gehören. Darin spiegelt sich Pragmatismus. Die unausgesprochene Gegenfrage lautet: „Wo sollen wir sie denn sonst hintun?“ Immerhin scheint es ein paar Führungskräfte zu geben, die dafür schon eine Idee haben.

Frage 10

Portale wie Wikileaks...

- a) ...werden zu Unrecht als Chance für mehr Demokratie gesehen.
- b) ...sind gefährliche Ventile für illoyale oder frustrierte Mitarbeiter.
- c) ...stellen ein ernsthaftes Risiko für Wirtschaft und Politik dar.
- d) ...nutzen die Schwächen offener Gesellschaften, sind gegenüber totalitären Regimes machtlos.
- e) ...werden sich mittelfristig in einem Wettbewerb befinden und damit selbst regulieren.
- f) ...werden über kurz oder lang außer Kontrolle geraten, wenn der Staat nicht massiv eingreift.
- g) ...schaffen Chancengleichheit zwischen Ehrlichen und Tricksern.



Die Gefahr ist erkannt: Portale wie Wikileaks stellen ein Risiko für die Wirtschaft dar. Fast jede zweite unternehmerische Führungskraft fürchtet, dass sich auf diese Weise gefährliche Ventile für illoyale oder frustrierte Mitarbeiter öffnen. Die Erkenntnis dürfte auf den Motiven der bisher bekannt gewordenen Fälle beruhen, die – von der Steuer-CD bis zur Diplomantendepesche – durch die Hände unzufriedener Geheimnisträger an die Öffentlichkeit gelangten. Unzufriedenheit? Illoyalität? Frust? Dagegen ist nun wirklich keine Firma gefeit.

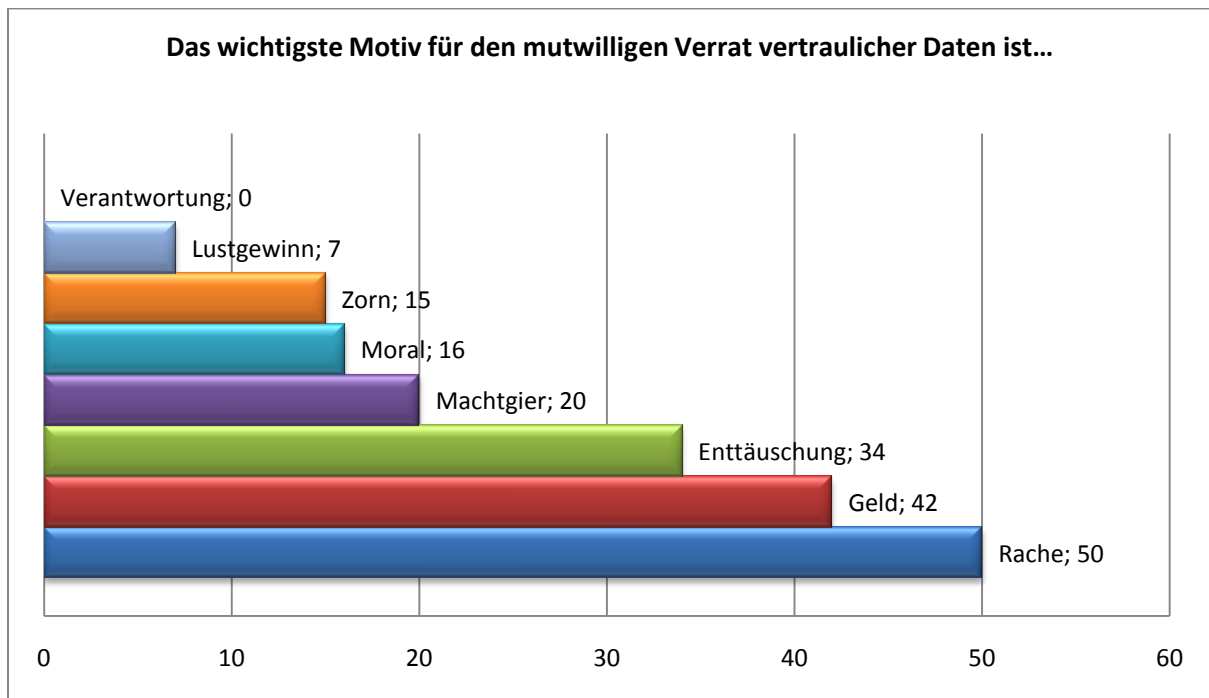
Mit gut 60 Prozent die am stärksten ausgeprägte Position heißt zwar: „Portale wie Wikileaks werden zu Unrecht als mehr Chance für Demokratie gesehen.“ Das spricht dafür, dass die befragten Unternehmer nicht ausschließlich ökonomische Dimensionen im Blick haben, sondern auch politische Aspekte berücksichtigen. Die beiden folgenden Positionen, die Wikileaks & Co. als „gefährliche Ventile für illoyale und frustrierte Mitarbeiter“ (47,97%) sehen und in ihnen ein „ernsthaftes Risiko für Wirtschaft und Politik“ (45,63%) erkennen, zeigen indes den Realitätssinn des Panels. Diese Einschätzung ist im Kontext mit den

Antworten auf Frage 8 gesehen werden, wo die fehlende Prüfung auf die Echtheit der veröffentlichten Dokumente als größte Gefahr bei der freien Verteilung von Informationen über das Internet bewertet wurde.

Auf den ersten Blick verblüffend, aber letztlich nicht verwunderlich: Kaum einer der Befragten mag daran glauben, dass einem Enthüllungsportal wie Wikileaks eine gesellschaftlich ausgleichende Funktion zukommt. Die „Chancengleichheit zwischen Ehrlichen und Tricksern“ herzustellen, also eine Art Umverteilung der Kommunikationsmacht vorzunehmen, das vermögen nur die wenigsten Panel-Teilnehmer zu erkennen. Dreimal so viele sehen vielmehr staatliche Kräfte gefordert, die verhindern sollen, dass solche Portale nicht über kurz oder lang außer Kontrolle geraten.

Gleichzeitig werfen vier von zehn Befragten diesen Portalen vor, sich die Schwächen offener Gesellschaften zunutze zu machen, während sie totalitären Regimes gegenüber machtlos blieben. Ein Vorwurf, der sich durchaus auf die Welt der Wirtschaft übertragen lässt, wo Veröffentlichungen über vermeintlich „Böse“ (Banken, Großkonzerne, Steuerflüchtlinge etc.) wahrscheinlicher und lukrativer sind als jene über die „Guten“ (z.B. Umweltorganisationen, Stiftungen). Dass veröffentlichte Inhalte vom Zufall oder individuellen Motiven bestimmt sind und wenig zum hehren Enthüllungsanspruch beitragen, äußert sich auch noch in einem anderen Wert: Nicht einmal jeder vierte Befragte glaubt daran, dass – ähnlich wie im bisherigen Medienmarkt – sich mittelfristig über einen Wettbewerb von Enthüllungsportalen ein Selbstregulativ entwickeln wird.

Frage 11



Rache und Geld sind aus Sicht von Führungskräften in der deutschen Wirtschaft führend unter den unedlen Motiven, die Menschen dazu bewegen, mutwillig vertrauliche Daten zu verraten. Wie sowohl die Umfrage, bei der Mehrfachnennungen möglich waren, wie auch das wirkliche Leben mit seinem florierenden Handel mit Steuer-CDs zeigen, ist durchaus auch die Kombination dieser Motive zu beobachten.

Eine weitere negative Emotion, die Enttäuschung, folgt erst mit einigem Abstand, dicht gefolgt von einem Motiv, das sich je nach persönlichem Standpunkt positiv wie negativ deuten lässt: der Machtgier.

Die untere Hälfte der Tabelle machen tendenziell positive Motive wie moralisch-ethische Überlegungen, Zorn und Lustgewinn aus. Ihre Bedeutung ist indes eher marginal. Die kumulierten Nennungen erreichen gerade einmal den gleichen Wert wie „Enttäuschung“.

Nur jeder sechste der Befragten sah die Preisgabe vertraulicher Daten unter Umständen durch ethisch-moralische Motive begründet. Es ist bezeichnend, dass nicht ein einziger der Befragten „Verantwortung“ als Beweggrund zu erkennen mag.

Fazit

Wikileaks & Co. haben die deutsche Wirtschaft auf dem falschen Fuß erwischt. Wie die vorliegende Studie zeigt, ist die Sorge wegen unkontrollierten Daten- und Informationsflusses sehr groß und sind sich die befragten Unternehmer und Führungskräfte des Risikos für ihr Geschäft durchaus bewusst. Enthüllungsportale wie Wikileaks sind aus ihrer Sicht daher ein grundsätzliches Übel und in ihrem Nutzen für die Gesellschaft zweifelhaft. Verantwortungslosigkeit im Umgang mit den Daten, mangelhafte Prüfung der Seriosität der Dokumente, eine Tarnung für Profiteure und kriminelle Organisationen – das sind die zentralen Argumente der Ablehnung.

Wenn es jedoch um aktives Handeln zur Gefahrenabwehr geht, besteht völlige Unsicherheit angesichts der vielen Ge- und Missbrauchsmöglichkeiten. Viele Unternehmer und Entscheidungsträger empfinden das Internet löchrig wie einen Schweizer Käse. Das zeigt sich zum Einen in der Haltung pro „globalen Ethikrat“ und contra „Einschränkung der Meinungsfreiheit“. Es äußert sich zum Anderen aber auch in den Zweifeln an technischen Lösungen, die entweder unbequem sind, weil sie rigide Anwendung erfordern, oder deren Wirksamkeit gegenüber krimineller Energie nicht ausreichend erscheint. Das in mehreren Aspekten weit gespreizte Meinungsbild deutet vor allem auf eines hin: Rat- und Konzeptionslosigkeit. Gut erkennbar und fast schon verständlich ist daher der Wunsch, die Handlungspflicht auf anonyme Dritte abzuwälzen. Eine Initiative der Bundesregierung scheint jedoch nicht in Sicht.

Rache, Geld, Enttäuschung und Machtgier sind es, die den Verbreitern illegal erworbener Firmendaten als überwiegende Motive für ihr Handeln unterstellt werden. Mit der Erkenntnis, dass sich Investitionen in die Loyalität von Mitarbeitern auszahlen, liegt die Wirtschaft daher sicher richtig.