Digital Confidence

Grundlagen für digitales Wachstum von morgen

LIBERTYGLOBAL
POLICY SERIES

booz&co.

Digital Confidence

Grundlage für digitales Wachstum von morgen

Übersetzt aus dem Englischen

DIGITAL CONFIDENCE – DIE KERNPUNKTE

• Bis 2012 wird Europas digitale Wirtschaft voraussichtlich um 18% pro Jahr wachsen, von 236 Mrd. € (2008) auf 436 Mrd. Dollar.

• Bisher beruhte das Wachstum vor allem auf Infrastruktur-Roll-outs und technischen Innovationen, etwa dem Übergang zum digitalen Fernsehen oder neuen Stufen der Breitband-Evolution.

• Hier wird es in Zukunft eine deutliche Verschiebung der Werttreiber geben: Weg vom reinen Netzzugang – ein zwar immer noch profitables, aber nur einstellig wachsendes Geschäft – hin zu E-Commerce, digitalen Content-Angeboten und Online-Advertising.

• In den nächsten 5 Jahren wird die steigende Nutzung und Zahlungsbereitschaft der User zum Motor des Wachstums werden. Der Markt für Content und Werbung wird zweistellige Zuwachsraten verzeichnen. In absoluten Zahlen bleibt E-Commerce der wichtigste Markt.

• Diese Wachstumstreiber werden sich jedoch gegen starke Störfaktoren innerhalb der europäischen Informationsgesellschaft durchzusetzen haben, beispielsweise ein plattformübergreifendes Web-2.0-Angebot (Online, DTV, Mobil) sowie eine junge „Born Digital"-Konsumentengeneration mit hohem Vernetzungs- und Partizipationsgrad und ebenso starkem Selbstbewusstsein – was auch auf Presse und Politik abfärben wird.

• Darüber hinaus birgt der Siegeszug des „Digital Life" für Verbraucher wie für Unternehmen zunehmende Unsicherheiten in Bezug auf die Vertrauenswürdigkeit und Gefahrlosigkeit der digitalen Umgebung.

• Vor diesem Hintergrund wird Digital Confidence, also das Maß an Vertrauen, das Kunden und Zulieferer digitalen und Online-Angeboten entgegenbringen, zum zentralen Faktor für Erfolg (oder Misserfolg) in der Digital Economy werden. Betroffen ist ein mögliches Marktvolumen von 124 Mrd. € (2012) bzw. rund 1% des Bruttoinlandsprodukts der EU-27 und hier ganz besonders die Segmente Content und Werbung. Gelingt es, Sicherheit und Vertrauen signifikant zu erhöhen, könnten die Märkte gegenüber dem Basisszenario von 436 Mrd. sogar 11% (46 Mrd. €) stärker wachsen. Gravierender wäre das Scheitern von Digital Confidence: 18% des Umsatzes (78 Mrd. €) würden entweder verlorengehen oder deutlich verzögert.

• Alle Player der Branche sind sich bewusst, wie wichtig es ist, Glaubwürdigkeit und Referenzen hinsichtlich Digital-Confidence aufzubauen, und haben unterschiedlichste Maßnahmen auf den Weg gebracht – allerdings bisher ohne erkennbare Linie oder gemeinsame Strategie. In den meisten Fällen handelt es sich um Ad-hoc-Maßnahmen infolge von bekannt gewordenen Zwischenfällen oder politischem Druck.

• Die Gesetzgeber allein können mit der Geschwindigkeit und Tragweite der Herausforderungen nicht mithalten. Erfolgreiche Unternehmen tun daher mehr, als ihnen gesetzlich vorgeschrieben ist: Sie treiben Digital Confidence proaktiv voran und entwickeln eigene Strategien und Maßnahmen.

• Digital Confidence beruht auf vier Säulen, die in ihrer Gesamtheit die vier elementaren Unsicherheitsbereiche bei Verbrauchern und Unternehmen abdecken:

1. Netzintegrität und Quality of Service (QoS) – bezieht sich auf die Bereitstellung sicherer und belastbarer Technologieplattformen für das „digitale Leben" und ein optimales Kundenerlebnis.

2. Datenschutz und Schutz der Privatsphäre – setzt sich mit den Datenschutz-Bedenken bei der Nutzung digitaler Infrastrukturen und beim Transfer persönlicher Informationen auseinander.

3. Minderjährigenschutz – widmet sich dem Schutz von Kindern und Jugendlichen in der Online-Welt.

4. Vermeidung von Piraterie und Diebstahl – garantiert allen Stakeholdern eine sichere digitale Geschäftsumgebung.

• Netzbetreiber sind für die Kundenbeziehung direkt verantwortlich und müssen daher Strategien und Maßnahmen entwickeln, die ihre Kunden akzeptieren können. Dies geht über die gesetzlichen Anforderungen oder die Interessen einzelner Stakeholder hinaus.

• Die Strategien und Maßnahmen sollten daher nicht bei einzelnen Problemen (wie zum Beispiel Produktpiraterie) ansetzen, sondern eine ganzheitliche Betrachtung der Digital Confidence widerspiegeln, denn zum einen konvergieren die politischen Konsequenzen der einzelnen Bereiche und zum anderen hat sich gezeigt, dass sie von den Stakeholdern sehr unterschiedlich aufgenommen werden.

• Fallstudien aus der ganzen Welt haben gezeigt, dass eine „Can do"-Haltung zur Digital Confidence durchaus realistisch ist. Dazu dürfen und sollten die Netzbetreiber über ihre primäre Rolle als „reine Durchleiter" (Carrier) beziehungsweise als Aufklärer/ Erzieher hinausgehen, müssen aber Richtlinien zu akzeptablen Kundenprozessen einhalten und rechtsverbindliche Grundlagen schaffen.

• Ausgehend von den analysierten Fallstudien, zeichnen sich beim Thema Kundenakzeptanz eine Reihe von Best Practices ab:

  • Verbraucher akzeptieren vor allem transparente und unaufdringliche Maßnahmen – Netzbetreiber, Content- und Plattform-Anbieter müssen gemeinsam mit dem Regulierer auf eine solche Kommunikation hinarbeiten.

  • Die Verbraucher sind besorgt darüber, wie Netzbetreiber mit ihren digitalen Daten umgehen – klare Aussagen und die Schaffung konsequenter, zuverlässiger Regelungen haben hier oberste Priorität.

  • Verbraucher wollen Kontrolle über das Risiko, dem sie sich aussetzen – dazu brauchen sie die entsprechenden Tools, Opt-in-/Opt-out-Möglichkeiten und Informationen.

  • Verbraucher akzeptieren Maßnahmen eher, wenn sie die Qualität der Dienstleistung sichern – auch wenn dies beispielsweise aktives Traffic-Management bedeutet. Sie müssen aber offen als Nutzungsbedingungen kommuniziert werden.

• Um die Angemessenheit von Interventionen zu garantieren und bei der Einführung neuartiger Strategien und Maßnahmen eine allgemeine Nutzerakzeptanz zu erreichen, sollten die Netzbetreiber dem stufenweisen „E3-Paradigma" folgen: Educate (zuerst aufklären), Empower (dann den Nutzer stärken) und Enforce (nur wenn nötig gezielt eingreifen).

• Digital-Confidence-Strategien und -Maßnahmen müssen fest in den einzelnen Organisationen verankert sein. Interne Protokolle und Governance-Strukturen müssen geschaffen werden, die der Steuerung von Produkt- und Service-Roadmaps, der Auswahl und dem Roll-out netzbasierter Technologien und Sicherheitslösungen sowie der Kommunikation mit Kunden und anderen Stakeholdern (Industriepartnern, Rechteinhabern, Regulierern) dienen.

I. MANAGEMENT SUMMARY

DER NÄCHSTE SCHUB IM „DIGITAL LIFE“: NUTZUNGSINTENSITÄT, NICHT NUTZERZAHL, ALS NEUER WACHSTUMSTREIBER

Europas digitale Wirtschaft hat eine realistische, positive Wachstumsperspektive, seit Web-2.0-typische Angebote, die auf der Funktionalität, Ubiquität und Kapazität von Breitbandverbindungen beruhen, zum Mainstream geworden sind. Doch die Abwanderung von Nutzern auf neue Zugangsnetze, eine starke Zunahme von „next generation“ Netztechnologien und die immer selbstbewusster auftretende „Born Digital“-Generation könnten sich im Ökosystem der digitalen Wirtschaft störend auswirken. Der Paradigmenwechsel stellt die gesamte Industrie, aber auch Entscheidungsträger und Regulierer, vor große Herausforderungen.

Auf dem Spiel stehen hohe Summen: Wir rechnen damit, dass der Markt für digitale Dienstleistungen in Europa bis 2012 auf 436 Mrd. € anwachsen und ein jährliches Wachstum von 18% aufweisen wird (2007–2012).

Bisher basierte das Wachstum digitaler Dienste vor allem auf technischen Innovationen wie DSL oder Digital-TV. Den Netzzugang haben die heutigen Technologieanbieter in vielen Märkten schon fast bis zur Sättigung vorangetrieben. Insofern wird sich der nächste digitale Umsatzschub nicht aus steigenden User-Zahlen ergeben, sondern aus der Stimulierung der Ausgabebereitschaft pro Anwender. Erreicht wird der Umsatzanstieg, so ist zu erwarten, durch zahlreiche neue Produkte und Dienstleistungen in Verbindung mit innovativen Geschäftsmodellen, die neue Zahlungsströme generieren. Als wichtigste Wachstumsfelder gelten (in der Reihenfolge der Wachstumsrate): Werbung, Content, E-Commerce und Netzzugang.

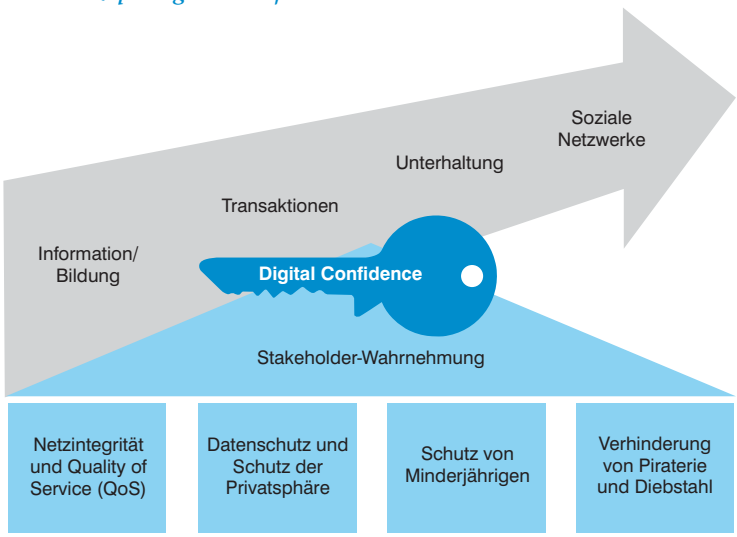
Doch mit dem Erfolg des „Digital Life“ gehen sowohl bei Verbrauchern als auch bei Unternehmen große Unsicherheiten bezüglich der Vertrauenswürdigkeit und Gefahrlosigkeit des neuen digitalen Umfelds einher. Das Vertrauen, das Kunden in das Geschäftsverhalten und die Sicherheit von Dienstleistungen und Netzen der Service- und Plattformanbieter, aber auch in die Durchsetzbarkeit von Verbraucherschutzmaßnahmen seitens Gesetzgebern und Regulierungsbehörden setzen, entwickelt sich momentan zur wichtigsten Voraussetzung für die erfolgreiche Ausschöpfung des digitalen Wachstumspotenzials.

Es ist daher dringend erforderlich, eine gemeinsame Sichtweise der Prioritäten im Bereich Vertrauensbildung und Sicherheit zu entwickeln, sich über mögliche/machbare Rollen und Verantwortlichkeiten der Beteiligten zu verständigen und zu evaluieren, welche Tools und Maßnahmen zur Anwendung kommen können und sollen. Ziel dieser Studie ist es, für diese Debatte eine Faktenbasis zu schaffen und ein einheitliches Bezugsraster, Begriffe und Ideen einzuführen, die eine gemeinsamen Sichtweise fördern und, wo nötig, die Entwicklung allgemeingültiger – oder koordinierter – Normen und Initiativen begünstigen.

DIGITAL CONFIDENCE: ZUKUNFTSSICHERUNG FÜR DIGITALE MÄRKTE

Vor diesem Hintergrund wird die Förderung von Vertrauen und Sicherheit zum zentralen Erfolgsfaktor für das künftige Wachstum digitaler Märkte, schon deshalb, weil selbstbewusste „Born Digital“-Verbraucher eventuelle Unzufriedenheit schnell mit Nichtnutzung quittieren oder öffentlichkeitswirksam kommunizieren – häufig mit Mitteln des Web 2.0. Anhand der Befragung von 50 Branchenexperten aus Europa und den USA und einer systematischen Bewertung von Marktdaten, Best Practices und Branchen-

Das Konzept Digital Confidence



einschätzungen kristallisierten sich vier eng miteinander verbundene, teils interdependente Säulen heraus, die unserer Ansicht nach die zentralen Anforderungen an das „Digital Life“ von heute und morgen darstellen:

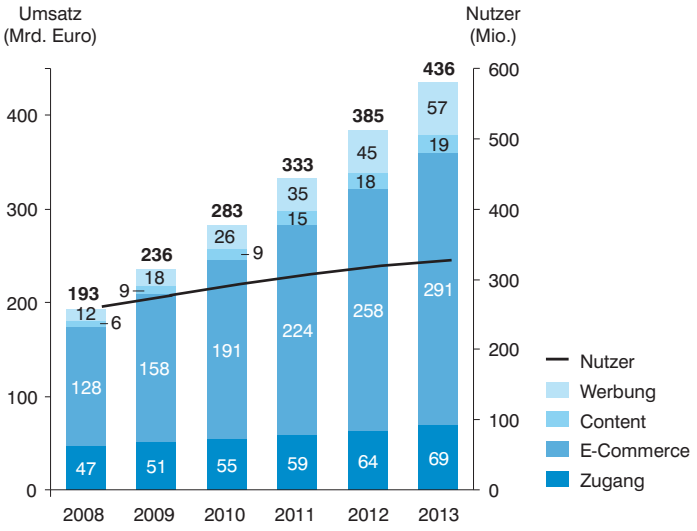
- **Sicherung von Netzintegrität und Quality of Service (QoS)** für Verbraucher und kommerzielle Kunden, besonders der Schutz von Technologieplattformen gegen kriminelle Attacken sowie die Sicherung optimaler Internet-Konnektivität selbst bei Spitzenauslastung oder externen Angriffen sowie die Abschirmung privater und geschäftlicher Computerumgebungen gegen Viren und Malware.

- **Datenschutz und Schutz der Privatsphäre,** also die Sicherheit privater elektronischer Informationen (Identitäten, Passwörter, Nutzerprofile, Nutzungsdaten etc.) vor unerlaubtem Zugriff, vor Veröffentlichung oder Verwertung sowie die Verhinderung von Identitätsklau und Betrug.

- **Schutz von Minderjährigen** vor ungeeigneten Inhalten, vor „Bullying“ und anderen aggressiven Verhaltensweisen und vor Annäherungsversuchen und Übergriffen durch Erwachsene; Bekämpfung von Kinderpornografie.

- **Vermeidung von Piraterie und Diebstahl,** Bekämpfung der unerlaubten Vervielfältigung urheberrechtlich geschützter Inhalte sowie sichere E-Commerce-Transaktionen für alle Beteiligten.

Digitales Leben – Umsätze in Europa



Hinweis: Europa einschl. EU-27, Norwegen und Schweiz
Quelle: Forrester e-Commerce Forecast, Finanzbericht Apple, Finanzbericht Google, EU TV und Broadband Forecast Model, Booz & Company-Analyse

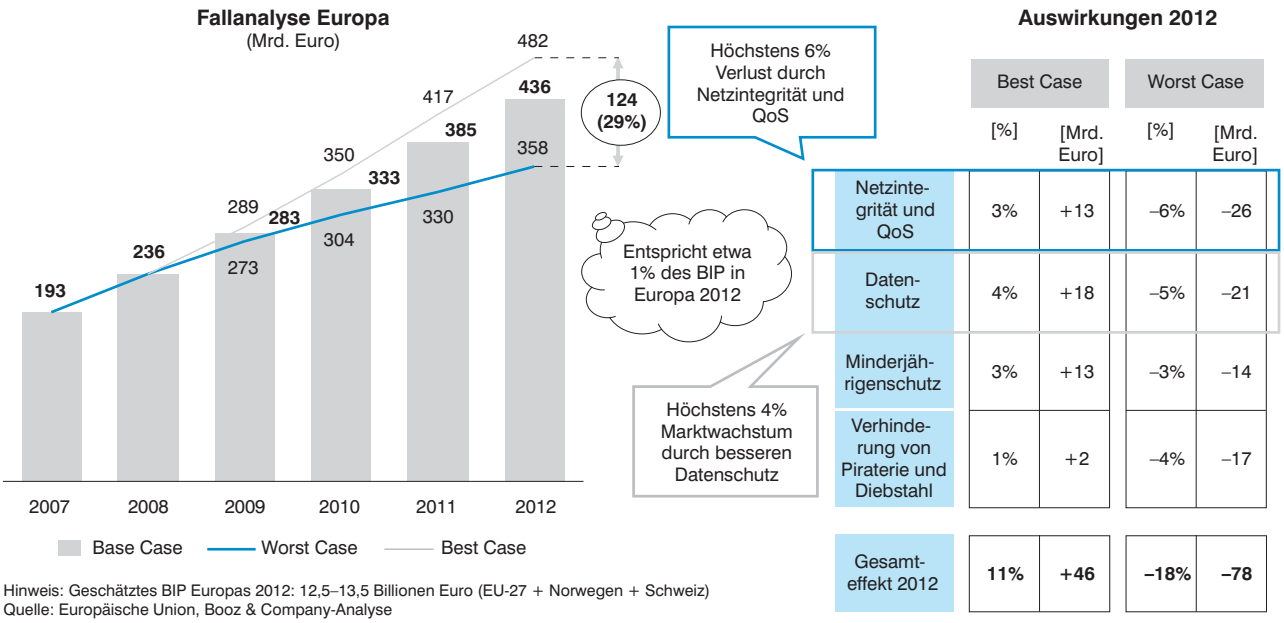
Die Industrie muss hier proaktiv vorgehen und die genannten Bereiche möglichst ganzheitlich betrachten. Für solch ein Vorgehen steht das Konzept der Digital Confidence. Ihre Förderung muss über die Einhaltung der gesetzlichen Bestimmungen hinausgehen, denn Digital Confidence entwickelt sich zunehmend zur wichtigen Erfolgsbedingung und „Licence to Operate“ am Markt. Wie manche unserer Fallstudien deutlich machen werden, schafft die bloße Befolgung von rechtlichen oder regulatorischen Vorschriften noch keine Verbraucherakzeptanz. Verhalten und Geschäftspraktiken der Betreiber müssen vielmehr auf die Gesamtheit der Herausforderungen kohärent antworten. Nur so kann die nächste Wachstumsstufe der Digital Economy realisiert werden.

RISK-BENEFIT-ANALYSE: DIGITAL CONFIDENCE ZAHLT SICH AUS

Nach Analyse von Booz & Company ist 2012 mit einem Markt von 436 Mrd. Euro für Netzzugang, Online-Handel, Content und Online-Werbung in Europa zu rechen. Von der Frage, ob Unternehmen Digital Confidence fördern (Best Case) oder im negativen Falle kein vertrauenswürdiges digitales Umfeld schaffen, hängen rund 124 Mrd. Euro bzw. knapp 30% des gesamten Markvolumens ab – etwa 1% des gesamten BIP der EU-27+2 im Jahre 2012! Dabei sind die Folgen eines Scheiterns mit 78 Mrd. Euro weit höher anzusetzen als der Best Case von 46 Mrd. Euro. Den Ausschlag werden vor allem die Bereiche „Netzintegrität und QoS“ und „Datenschutz“ geben, denn sie berühren sämtliche Aspekte der Digital Economy und beeinflussen Nutzungsintensität und Nutzerzahlen in allen wichtigen Marktsegmenten.

Der Bereich Datenschutz ist auch – aber nicht ausschließlich – wegen seiner Relevanz für innovative Werbemodelle („Targeted Advertising“) wirtschaftlich interessant. Hier besteht die Gefahr, dass sich Kunden von E-Commerce, dem Kauf digitaler Inhalte oder innovativen digitalen Services abwenden, wenn sie Zweifel am korrekten Umgang mit ihren sensiblen Daten haben. „Netzintegrität und QoS“ sind hingegen wichtig, um das ständig expandierende Content- und Bewegtbild-Angebot im Internet voll zu unterstützen. Gut gemanagt, werden Netze künftig hohe Bandbreiten mit einer Dienstqualität bieten können, die allen Nutzern ein „Digital Life“ ermöglicht. Der Bereich „Piraterie und Diebstahl“ ist sowohl für die Inhaber von Content-Rechten als auch für Online-Händler relevant. Neben der offensichtlichen wirtschaftlichen Bedeutung für den Schutz bestehender Rechte und die Einfüh-

Der Effekt von Digital Confidence – Indikative Sensitivitätsanalyse



Hinweis: Geschätztes BIP Europas 2012: 12,5–13,5 Billionen Euro (EU-27 + Norwegen + Schweiz)
Quelle: Europäische Union, Booz & Company-Analyse

rung innovativer digitaler und internetbasierter Content-Modelle besteht in diesem Zusammenhang auch ein beträchtliches Risiko: Wegen der negativen Auswirkungen auf E-Commerce-Transaktionen könnten Nutzer ihren Konsum auf Offline-Kanäle verschieben, was für viele neue Geschäftsmodelle (zum Beispiel Online-Auktionen) nicht möglich ist.

Von allen Umsatzkategorien sind Content und Online-Werbung die sensibelsten Bereiche, was Digital Confidence angeht. Bei beiden handelt es sich um „junge" Märkte, die hochgradig von Online-Vertrauen leben. Innovative Werbung könnte durch ablehnendes Nutzerverhalten zurückgeworfen werden, wenn bei der Umsetzung nicht an Kundenakzeptanz gedacht wird, oder durch zu restriktive Gesetzgebung. Eine sehr strenge Handhabung des Datenschutzes beispielsweise könnte neue Marketingmodelle, die auf gezielter, individueller Kundenansprache beruhen, stark beeinträchtigen – und damit einen der wesentlichen Teile des europäischen Online-Werbemarkts von 57 Mrd. Euro im Jahr 2012 gefährden. Auch bei der Verwertung der neuen, schnell wachsenden Web-2.0-Services wird Werbung eine zentrale Rolle spielen, etwa bei sozialen Netzen oder innovativen Content-Angeboten. Die Contentprovider fürchten jedoch, dass exzessive Piraterie ihre digitalen Geschäftsmodelle untergraben könnte. E-Commerce ist zwar etwas weniger gefährdet, aber indirekt besonders betroffen, da das große Gesamtvolumen den Worst Case von Digital Confidence mit 52 Mrd. Euro belastet bzw. rund die Hälfte des Best Case ausmacht.

Selbst bei rein wirtschaftlicher Betrachtung und wenn man die breiteren gesellschaftlichen Implikationen für den Moment außer Acht lässt, zeigt eine Risk-Benefit-Analyse, dass die Digital Economy erhebliche Vorteile hat, wenn sie alle Bereiche der Digital Confidence konsequent anspricht, um das Worst-Case-Szenario zu vermeiden und die bestmögliche Gewinnsituation anzustreben.

Alle Player der Branche sind sich der Wichtigkeit von Digital-Confidence-Referenzerfolgen bewusst und haben unterschiedlichste Maßnahmen auf den Weg gebracht – allerdings bisher ohne erkennbare Linie oder gemeinsame Strategie. Meist sind es Ad-hoc-Maßnahmen infolge von bekannt gewordenen Zwischenfällen oder politischem Druck.

Der fundamentale Unterschied zwischen Best-Case- und Worst-Case-Szenario ist der Grad der Koordination der Branchenplayer untereinander bei der Umsetzung von Digital Confidence. Wobei „Koordination" nicht bedeuten soll, dass alle Beteiligten stets das Gleiche tun: Gemeint ist vielmehr der Grad der Bereitschaft, in die gleiche Richtung zu marschieren, sich also branchenweit über die gemeinsame Stoßrichtung, die obersten Prioritäten der Umsetzung und die sich daraus ergebende Verantwortung für den einzelnen Stakeholder abzustimmen.

Netzbetreiber müssen auch weiterhin eine starke Position innehaben, schließlich ist ihre

Leistung eine der Grundvoraussetzungen für die oben genannten Wachstumstreiber. Der Grad der Netzintegrität der Betreiber übt einen wesentlichen wirtschaftlichen Einfluss aus, selbst wenn ihr Kerngeschäft – Netzzugang – zunächst am wenigsten von den Herausforderungen der Digital Confidence betroffen scheint.

EIN BEZUGSRAHMEN FÜR HANDLUNGSOPTIONEN

Bei allen vier Säulen der Digital Confidence besteht dringender Handlungsbedarf. Die stark miteinander verflochtenen Bereiche bestimmen gemeinsam die allgemeine Wahrnehmung der digitalen Welt als sicherer Ort – oder Gefahrenzone.

Aufgrund der Komplexität der Probleme und der gegenseitigen Abhängigkeiten in der Wertschöpfungskette wird schnell klar, dass jeder Player der Digital Economy hier eine spezifische Rolle übernehmen muss. Wenngleich Netzbetreiber durchaus in vielen Bereichen Lösungen beisteuern werden, wären sie mit der Verantwortung für die Lösung des gesamten Puzzles überfordert.

Zur Abbildung der verschiedenen Rollen, die Netzbetreiber in den analysierten Problemfeldern einnehmen können, wurde ein „Positionsrahmen Digital Confidence“ entwickelt. Diese Matrix visualisiert, welche Arten des Engagements möglich sind (z. B. passiv nach dem Motto „Hände weg“ oder aktiv mit einem „Volle Kontrolle“-Ansatz), und ordnet sie zugrundeliegenden Prinzipien zu. Dabei entsprechen die daraus resultierenden Rollen allgemeinen gesellschaftlichen Rollen:

- Der Lehrer klärt die Nutzer so gut wie möglich über Angebote und Gefahren auf, verhängt aber normalerweise keine Sanktionen (vgl. Entwicklung von Lernmaterial zum richtigen Internetverhalten durch „Web Wise Kids“).

- Auch der Erziehungsberechtigte klärt auf, führt aber anders als der Lehrer proaktive Maßnahmen durch, um die Nutzer zu schützen (vgl. Ausfiltern von Copyright-Material durch YouTube).

- Der Schiedsrichter vertraut auf freiwillige Regeln, die er fallbezogen durchsetzt, und setzt auf Richtlinien statt Aufklärung. Die Regeln basieren jedoch auf Absprachen (vgl. proaktive Abschottung von Kinderpornografie-Domains durch UPC Niederlande).

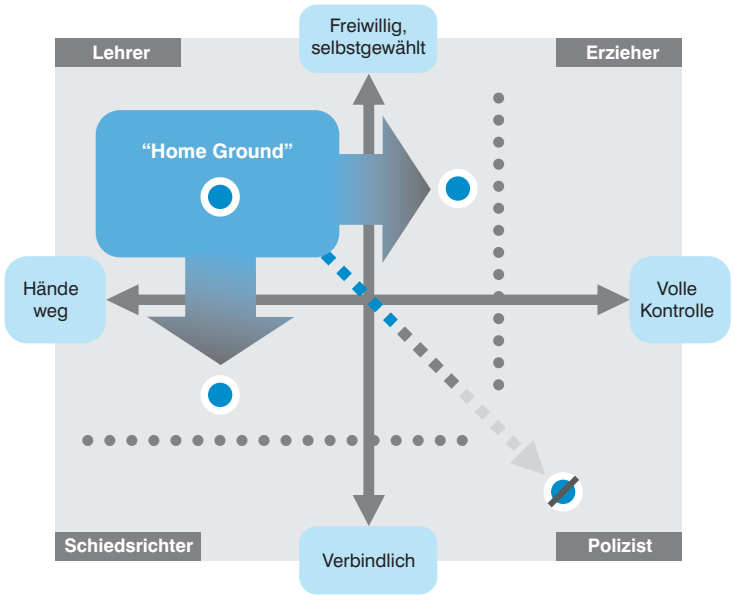
- Der Polizist bevorzugt natürlich starke Sanktionen auf Basis gesetzlicher Vorschriften. Er sorgt für die Ergreifung aller nötigen Maßnahmen und hält sich strikt an die Regeln, etwa das totale Verbot einer illegalen Aktivität (z. B. durch „Beim 3. Mal bist du draußen“-Regel bei Copyright-Verletzungen).

Bei der Festlegung ihrer Position innerhalb der Matrix sollten Netzbetreiber jedoch äußerst vorsichtig sein, wenn sie Rollen außerhalb ihres primären Verantwortungsbereichs übernehmen. Entscheidungen, die ihre starke Position als reiner Infrastrukturanbieter untergraben und sie unkontrollierbarer Haftbarkeit aussetzen, sind letztendlich nicht dazu angetan, digitales Vertrauen zu fördern, während bei den Endverbrauchern falsche Erwartungen geweckt würden.

Unsere Analyse von Erfolgen und Misserfolgen im Bereich Digital Confidence zeigt, dass es für Netzbetreiber ein traditionelles Zuhause oder „Home Ground“ der Vertrauensbildung gibt – den des „Lehrers“: Sie konzentrieren sich darauf, die Nutzer so gut wie möglich über Angebote und Gefahren aufzuklären, verhängen aber normalerweise keine proaktiven Sanktionen. Eine solche Haltung beschränkt sich dementsprechend auf das gesetzlich Vorgeschriebene. Doch unsere Analyse zeigt klar, dass diese Haltung zukünftig nicht mehr ausreichen wird.

Denn den Gesetzgebern gelingt es nur mühsam, mit der Geschwindigkeit und der Tragweite der Entwicklungen Schritt zu halten. Hingegen müssen die Netzbetreiber, da sie direkt für die

Positionierung – „Home Ground“ für Netzbetreiber



Kundenbeziehung verantwortlich sind, schon früh Strategien und Maßnahmen entwickeln, mit denen sie eine maximale Kundenakzeptanz erreichen. Und das geht über die Einhaltung von Vorschriften und die Interessen einzelner Stakeholder hinaus.

Erfolgreiche Unternehmen geben sich daher nicht mit der Einhaltung der gesetzlichen Bestimmungen zufrieden. Sie entwickeln eigene Digital-Confidence-Prinzipien:

- Sie arbeiten an vertrauensbildenden Prozeduren und Protokollen.

- Sie sind in ihrer Kundenkommunikation so offen und transparent wie möglich.

- Sie bemühen sich, Verbraucher aufzuklären und ihnen Tools an die Hand zu geben, um ihre eigenen Interessen in der digitalen Welt zu schützen.

Um die Angemessenheit von Interventionen zu garantieren und bei der Einführung proaktiver Strategien und Maßnahmen die allgemeine Akzeptanz der Nutzer zu erreichen, sollten die Netzbetreiber dabei den stufenweisen Ansatz des so genannten „E3-Paradigmas“ befolgen: Educate (erst aufklären), Empower (Nutzer stärken) und Enforce (nur wenn nötig gezielt durchgreifen).

Basierend auf den analysierten Cases zeichnen sich folgende Best Practices zur Verbraucherakzeptanz ab:

- Verbraucher akzeptieren vor allem transparente und unaufdringliche Maßnahmen. Netzbetreiber, Content- und Plattform-Anbieter müssen gemeinsam mit dem Regulierer auf eine solche Form der Kommunikation hinarbeiten.

- Die Verbraucher sind besorgt darüber, wie Netzbetreiber und ISPs ihre digitalen Daten handhaben und überwachen. Klare Aussagen und konsequente, zuverlässige Rahmenbedingungen haben hier oberste Priorität.

- Verbraucher wollen Kontrolle über das Risiko, dem sie sich aussetzen. Dazu brauchen sie die entsprechenden Tools, Opt-in-/Opt-out-Möglichkeiten und damit verbundene Aufklärung.

- Verbraucher akzeptieren Maßnahmen, wenn sie die Qualität der Dienstleistung sichern. Auch wenn dies aktives Traffic-Management voraussetzt, sind sie dazu bereit, wenn die Bedingungen offen und klar kommuniziert werden.

Diese Prinzipien sind auf alle Stakeholder anwendbar.

Als nächstes müssen die Maßnahmen und Strategien fest in der jeweiligen Organisation verankert werden. Betrachtet man die Konsequenzen für Netzbetreiber, so sind zum Erreichen einer neuen Stufe des digitalen Vertrauens koordinierte Maßnahmen erforderlich. Die Betreiber können auf 5 Ebenen handeln:

1. RICHTLINIEN UND MASSNAHMEN

Jeder Netzbetreiber und ISP sollte ein Positionspapier vorhalten, das seine Strategie und Position für jede der Digital-Confidence-Säulen definiert. Alle weiteren Maßnahmen sollten auf diesem Papier aufbauen. Es muss präzise genug sein, um konkrete Hilfestellung zu den mit den Einzelproblemen verbundenen prinzipiellen Fragestellungen zu bieten – etwa dazu, wie ein Unternehmen den Zielkonflikt zwischen unerwünschtem Content und Meinungsfreiheit ausbalanciert.

In einem weiteren Schritt gilt es, die Maßnahmen in den Kernprozessen des Unternehmens zu verankern. Dies hat in den meisten Fällen direkten Einfluss auf die Produktentwicklung, da immer garantiert sein sollte, dass Produkte und Services den eigenen Standards entsprechen.

Darüber hinaus müssen Netzbetreiber ihre Digital-Confidence-Richtlinien und -Prozeduren ständig aktualisieren, indem sie sie regelmäßig juristischen, politischen und technischen Überprüfungen unterziehen.

Aus allen analysierten Cases lässt sich ein Fazit ziehen: Digital Confidence bedeutet Vertrauen, und Vertrauen entsteht durch offene Kommunikation. Transparenz zahlt sich aus. Deshalb sollten Unternehmen die angewendeten Richtlinien und die damit verfolgten Ziele – einschließlich geschäftlicher Ziele – deutlich kommunizieren. Die Erfahrung zeigt, dass die Akzeptanz steigt, sobald über Regeln und ihren zugrundeliegenden Zweck offen gesprochen wird. So entsteht ein Dialog mit dem Verbraucher, der entscheidend zur Optimierung von Lösungen beitragen kann.

2. STEUERUNG

Probleme der Digital Confidence sind meist komplex, äußerst sensibel und funktionsübergreifend. Häufig erfordern sie die Definition grundlegender Positionen, etwa: Wie geht mein Unternehmen mit sexuellem Missbrauch im

Internet um? Jeder Fehler kann enorm ruf- und umsatzschädigend sein. Daher ist es besonders wichtig, dem Thema die gebührende Aufmerksamkeit auf höchster Managementebene zu widmen. Digital Confidence sollte tief in den Organisationsstrukturen verankert sein, beispielsweise durch ein Digital Confidence Board unter Aufsicht des Topmanagements, das alle entsprechenden Aktivitäten überblickt und umsetzt.

3. TECHNOLOGIE

Den Großteil der „Enabling Technologies" für Digital Confidence gibt es bereits. Entscheidungen zur individuellen Positionierung, zur Ausgestaltung von Regelwerken und zum Aufbau der Organisation haben eindeutig Priorität. Dennoch werden die meisten Netzbetreiber um gewisse technologische Investitionen nicht herumkommen, wenn sie zukunftssicher bleiben wollen. Die Rede ist von Investitionen, die die Dienstequalität (QoS) auch bei steigendem Online-Traffic gewährleisten. Hier gilt es, die Vorteile von Kapazitätserweiterungen und aktivem Traffic-Management – beispielsweise durch Staffelpreise und weitere, technische Lösungen – abzuwägen. Netzbetreiber und ISPs sind gut beraten, gemeinsam mit den Contentprovidern ihre Netze für Multimedia-Datenströme fit zu machen und neue Technologien wie Peer-to-Peer-Caching (vgl. Ansätze der P4P Initiative) oder Content-Delivery-Netze zu integrieren. Dabei müssen sie den Regulierern vermitteln, dass die Probleme aktiv angegangen werden.

Ein weiterer Problembereich ist momentan das Enduser-Equipment. Es ist im Allgemeinen nur schlecht gegen Bedrohungen wie Viren, Botnets und andere Formen von Malware geschützt. Zwar sind Softwarelösungen vorhanden, doch deren Einsatz muss den Kunden noch aktiver als bisher nahegelegt werden. Daneben sollten Tools und Lösungen angeboten werden, die es den Kunden selbst ermöglichen, den Grad des Risikos zu bestimmen (beispielsweise durch eine Opt-in-/Opt-out-Möglichkeit). Das erfordert aber einen Wechsel der Gangart: Es wird nicht mehr ausreichen, entsprechende Programme zum kostenlosen Download vorzuhalten. Vielmehr müssen Netzbetreiber und ISPs die Installation beim Kunden aktiv vorantreiben und die Anzahl ständig überwachen.

4. AUFKLÄRUNG DER VERBRAUCHER

Gemeinsam mit NGOs sollten Netzbetreiber und ISPs gezielte Programme entwickeln und eigene Aufklärungsinitiativen, wie etwa Informationskampagnen auf ihren Websites, durchführen. Die Programme müssen alle Bedrohungen im Zusammenhang mit Datennutzung, kontextbezogener Werbung, Piraterie und Online-Verhalten allgemein abdecken, einschließlich „Bullying" und unzulässiger Inhalte für Minderjährige.

Dabei ist gezielt vorzugehen, mit Botschaften, die auf die einzelnen Nutzergruppen (auch Eltern und Kinder) zugeschnitten sind: Elternprogramme sind auf Beaufsichtigung und Schaffung von Problembewusstsein bei den Kindern abgestellt und stellen Werkzeuge vor, mit denen sie die Online-Umgebung der Minderjährigen kontrollieren können. Aufklärung für Kinder zielt auf die Erkennung und Meisterung von Gefahren.

5. REGULIERUNG

Im Rahmen der proaktiven Vertrauensbildung kommt Netzbetreibern und ISPs die Aufgabe zu, Regulierer auf Handlungsfelder hinzuweisen, die eindeutig nicht im Verantwortungsbereich der Infrastrukturprovider liegen (wie z. B. die Indizierung von illegalem Content oder Strafverfolgung). Die Regulierer sollten ihrerseits keine vorschnellen Maßnahmen ergreifen, solange die Verhältnismäßigkeit im Einzelfall nicht gewährleistet werden kann.

Im Gegenzug muss die Industrie durch Eigeninitiative unter Beweis stellen, dass es ihr mit Digital Confidence ernst ist, und entsprechende kohärente Lösungen entwickeln. Diese sollten von allen Akteuren unterstützt werden, wobei die Kosten der Umsetzung proportional zum wirtschaftlichen Nutzen aufzuteilen sind. Die Regulierer dürfen die Industrie nicht daran hindern, diese Konzepte zu entwickeln, Kooperationen mit Stakeholdern und finanzielle Unterstützungsprogramme anzubahnen und dabei den Wettbewerbsdruck zum Vorteil des Verbrauchers zu nutzen – im Gegensatz zu einer Regulierung, die, selbst wenn sie gut gemeint ist, vom Verbraucherstandpunkt kontraproduktiv sein kann und wirtschaftlichen Schaden verursacht. Unsere Analyse zeigt beispielsweise, dass eine strikte Regulierung der QoS bei gleichzeitigem Verbot der effektivsten Verfahren des Traffic-Managements den Investitionsbedarf der europäischen Netzbetreiber um bis zu 6 Mrd. Euro erhöhen würde – letztlich zum Schaden der Konsumenten.

Bei der Umsetzung der Maßnahmen auf diesen fünf Handlungsebenen ist den Netzbetreibern allgemein zu empfehlen, auf möglichst breiter Front mit NGOs zusammenzuarbeiten.

Viele Aspekte können effektiver angesprochen werden, wenn ein Provider gemeinsam mit einer NGO aktiv wird, denn das garantiert Neutralität und branchenweite Akzeptanz durch den guten Ruf der gemeinnützigen Organisatoren: Jüngste Umfragen zeigen, dass NGOs im Verbrauchervertrauen ganz oben liegen.

PRIORITÄTEN FÜR REGULIERER

Regulierer und Regierungsbehörden sind aufgefordert, ihre Position im Bereich Digital Confidence zu definieren, zwischen Zensur und Aufklärung, strenger Regulierung und freier, marktwirtschaftlicher Selbstregulierung. Dabei erfordert die grenzüberschreitende Natur von Digital-Confidence-Bedrohungen eine besonders enge internationale (legislative) Zusammenarbeit, ein stärkeres Bewusstsein für die Dringlichkeit der Probleme sowie die Bereitstellung von Ressourcen zur Schaffung von Abwehrstrukturen und Public-private-Partnerships durch Regierungen und zuständige Behörden. Bis jetzt schadet das Fehlen einheitlicher Strategien letztendlich dem Konsumenten, der Transparenz und Hilfestellung bei den Risiken des digitalen Lebens vermisst, während die Unternehmen gleichzeitig herausgefordert sind, zukunftssichere digitale Geschäftsmodelle zu entwickeln.

In der Politik und im Bereich Regulierung scheint der Trend weg von einseitiger Gesetzgebung hin zu mehr Stakeholder-Beteiligung und Co-Regulierung zu gehen. Dies erfordert jedoch eine kontinuierliche Überprüfung der Angemessenheit aller Regulierungsaktivitäten, ganz besonders jedoch stark interventionistischer Praktiken (wie z. B. der „Three Strikes"-Regel oder Bestrebungen, eine obligatorische Netz-Filterung durchzusetzen), die grundlegende Internet-Freiheiten und Verbraucherrechte (z. B. Datenschutz) einschränken und angestammte Rechtsspielräume der Industrie untergraben.

Den Regulierern kommt zweifelsohne eine Schlüsselrolle bei der Bildung von digitalem Vertrauen zu, denn bei der Komplexität der Problematik ist die Förderung der Zusammenarbeit aller beteiligten Parteien ein wichtiges Mittel zum Ziel. Nach den Analysen dieser Studie erfordern folgende Bereiche die besondere Aufmerksamkeit der Regulierer:

- Anregung der Netzbetreiber und ISPs zur Ausgestaltung von Digital-Confidence-Leitlinien und -Prozeduren sowie Verhaltenskodex-basierter Selbstkontrollen auf Seiten der Industrie, insbesondere in Bereichen, in denen eine stärker eingreifende Regulierung (z. B. zum Traffic-Management) negative wirtschaftliche Auswirkungen haben oder Verbraucherrechte bedrohen würde (z. B. Regel „Beim 3. Mal bist du draußen").

- Erwägung von Maßnahmen zur Begrenzung des Rechts- und (in einigen Fällen) Image-Risikos, das Netzbetreibern und ISPs mit der Einführung von Digital-Confidence-Strategien und -Maßnahmen eingehen – etwa durch Vorantreiben der Entwicklung und branchenweiten Einführung eines Registers verbotener Seiten zum Schutz Minderjähriger oder durch Harmonisierung der momentan noch verstreuten europäischen Ansätze zu einem ein international koordinierten Vorgehen beim Minderjährigenschutz.

- Schaffung von Anreizen für die Branche, sich aktiver um die Aufklärung der Verbraucher zu bemühen: Bereitstellung finanzieller Mittel und Gründung von Dachinitiativen, die Skaleneffekte ermöglichen, beispielsweise auf Basis der beim Safer Internet Programme gemachten Erfahrungen.

- Verstärkung der Bemühungen um internationale Zusammenarbeit bei der Entwicklung globaler Lösungen oder Handlungsrahmen für primär globale Probleme, z. B. beim Copyright-Schutz.

- Verständnis für die Verflechtungen zwischen den einzelnen Digital-Confidence-Bereichen und entsprechend ausgewogene Entscheidungsfindung. So könnte z. B. die Durchsetzung strenger QoS-Anforderungen dazu führen, dass die Industrie deutlich gestiegene Kosten für Netz-Upgrades hinnehmen muss, was letztlich steigende Verbraucherpreise zur Folge hat.

Als Fazit lässt sich sagen: Die erfolgreiche Umsetzung von Digital Confidence bedeutet nicht unbedingt einen hohen Investitionsaufwand. Ein Scheitern würde die Branche und letztlich auch alle technologisch entwickelten Gesellschaften jedoch teuer zu stehen kommen. Natürlich ist die erfolgreiche Umsetzung von Digital-Confidence-Programmen keine leichte Aufgabe und durchaus mit Kosten verbunden. Zahlreiche CEOs werden zu Recht der Ansicht sein, dass sich ihre Unternehmen schon längst in vielen der oben genannten Felder engagieren. Doch in den meisten Fällen wird dieses Engagement nicht ausreichen. Bei Digital Confidence geht es um mehr, als Informationsmaterial zum Download

bereitzuhalten. Es geht darum, mit den führenden Institutionen in diesem Bereich – private und öffentliche – auf Top-Management-Ebene in Dialog zu treten, sowie um die Initiierung präziser, aufmerksamkeitsstarker Kampagnen. Dazu müssen Investitionen getätigt, Zielkonflikte gemanagt und möglicherweise ganz neue Fähigkeiten im Unternehmen entwickelt werden. Denn digitales Vertrauen entsteht nicht dadurch, eine umfangreiche Datenschutzerklärung „auf Halde“ zu haben. Es entsteht durch ein gewandeltes Bewusstsein, wie im Unternehmen mit Digital Confidence umgegangen wird und wie das Thema intern, aber auch gegenüber Kunden und der Gesellschaft, kommuniziert wird. Kurz: Digital Confidence braucht Führung von oben, um auf breiter Front erfolgreich zu sein.

II. DER NÄCHSTE SCHUB IM „DIGITAL LIFE": NUTZUNGSINTENSITÄT, NICHT NUTZERZAHL, ALS WACHSTUMSTREIBER

1. DIGITAL LIFE: EIN ÜBERBLICK

Digitale Technologien haben das tägliche Leben vom Büro bis in den Alltag mit atemberaubender Geschwindigkeit verändert. Kurze Entwicklungszyklen und immer leistungsstärkere Endgeräte, kombiniert mit drastisch verkürzten Ersetzungszyklen, haben zu einer Durchdringung des Massenmarkts mit digitaler Technologie geführt. Ob Filme sehen, Freunde treffen, Musik hören oder Fotos machen – das heutige Leben ist digital. Die Datentechnik hat sich dabei längst von ihrem Image als Spielzeug für Technikfreaks verabschiedet und ist zum Mittelpunkt des modernen Lebens geworden. Die meisten Verbraucher reagieren gereizter auf den Ausfall ihrer DSL-Verbindung als auf eine Telefonstörung.

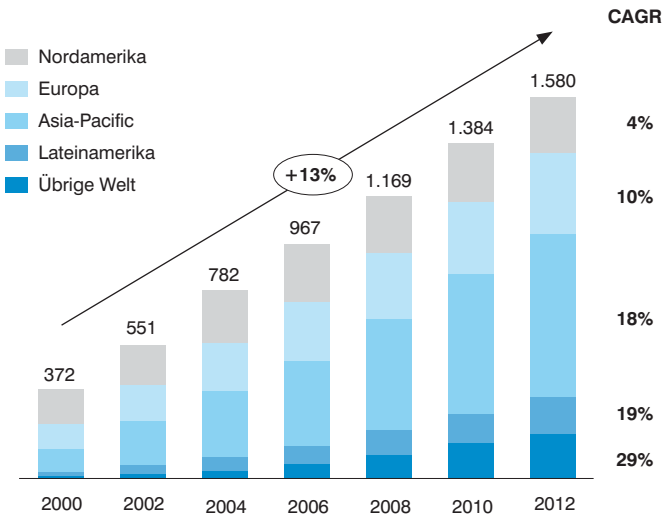
Die neusten Entwicklungen bei den digitalen Technologien, von Digital-TV bis zu Web-2.0-Anwendungen, haben deutlich gezeigt: Das volle Potenzial dieser Services wird nur dann freigesetzt, wenn alle Komponenten und Applikationen miteinander vernetzt sind – physisch und logisch. Was ist die wahre Revolution der Digitalfotografie? Dass die Zelluloid-Filmrollen aus den Regalen verschwunden sind oder dass man die Bilder schon Minuten später mit Freunden austauschen kann? Gerade diesen Community-Aspekt der digitalen Technologie unterstreichen auch Web-2.0-Anwendungen wie Facebook und YouTube. Wenn wie hier Kommunikation, Community, Content und Online-Handel verschmelzen, entstehen enorme Mehrwerte für den Konsumenten und oft ganz neue Wege der Umsatzgenerierung. Dafür sind die explodierenden Wachstumsraten in westlichen Ländern und weit darüber hinaus ein eindrucksvoller Beweis. Interessanterweise machen alle diese Dienstleistungen sofort gebrauch vom Community-Aspekt: „Viral Marketing", also direkte Peer-to-Peer- beziehungsweise PC-zu-PC-Kommunikation ist ihr wichtigster Wachstumstreiber. All das ist nur in einer vernetzten Umgebung denkbar.

In diesem Zusammenhang lohnt der Hinweis, dass die Mehrheit der europäischen Haushalte schon jetzt oder in naher Zukunft über drei digitale Netzanbindungen verfügen wird: Internet, Digital-TV und Mobiltelefon, alle mehr oder weniger fähig, Breitband-Services zu liefern und alle – auch hier mit Abstufungen – interaktiv.

Der Internet- und Breitbrand-Markt ist saturiert: In den meisten mitteleuropäischen Märkten liegt die Durchdringung bei über 70%.

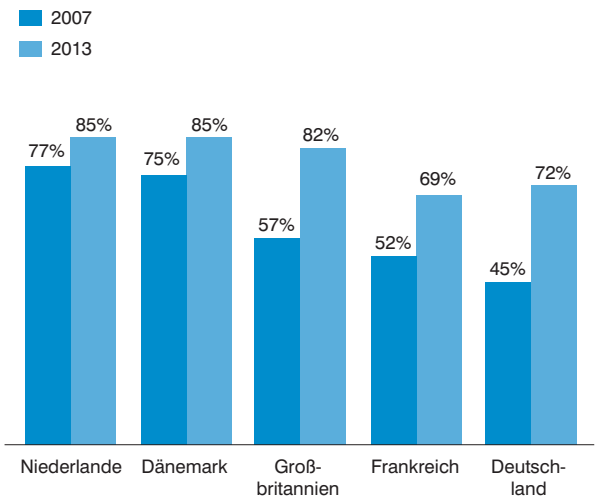
Der aktuelle Übergang von Breitband- auf Next-Generation-Datennetze wird die Entwicklung des digitalen Lebens noch weiter beschleunigen. Die nächste Generation von Kabelnetzen (auf Grundlage der EuroDOCSIS-3.0-Tech-

Abb. 1: *Internetnutzer global (Mio.)*



Quelle: Economist Intelligence Unit

Abb. 2: *Breitbandpenetration (Prozent der Haushalte)*



Quelle: OECD

nologie), Telekommunikationsnetzen (xDSL), Mobilfunkanbietern und lokalen FTTH-Netzbetreibern werden in Kombination mit Wireless-Clustern wie digitalen terrestrischen Netzen und Satelliten den wachsenden Bedarf an höheren Übertragungsgeschwindigkeiten, ubiquitärer Konnektivität und individuellem Medienkonsum plattformübergreifend bedienen.

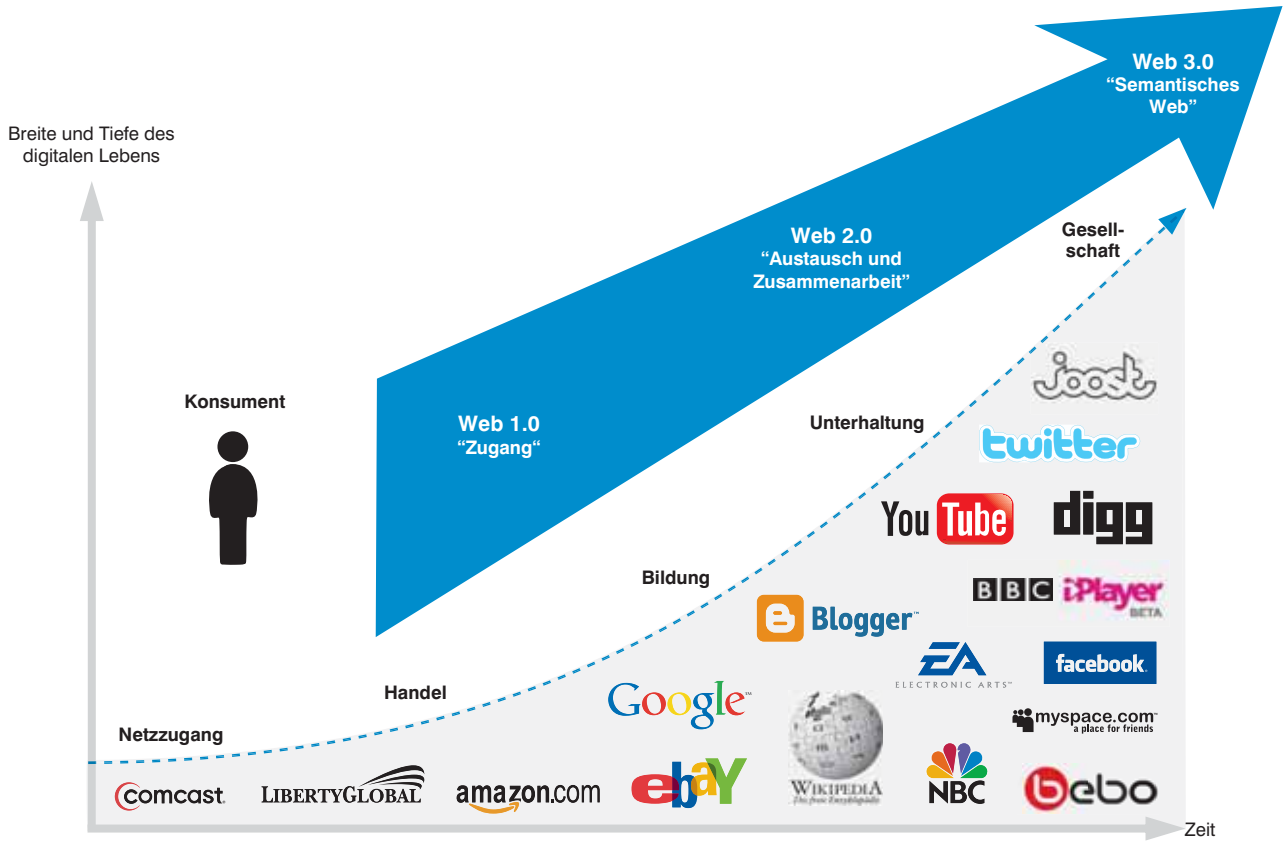
Die Erreichbarkeit und Akzeptanz des Internets ist inzwischen so hoch, dass in vielen europäischen Ländern die Durchdringung mit DSL bei über 70% liegt und damit ein medialer Massenmarkt ähnlich Fernsehen und Radio entstanden ist. Diese Tatsache wird auch den kommenden Wandel im Verbraucherverhalten vorantreiben: Der Verbraucher erwartet, jederzeit und an jedem Ort Zugriff auf einen gewünschten Service zu haben, und zwar mit dem gerade vorhandenen Gerät.

Schon jetzt verändern die Konsumenten ihre Verhaltensmuster. Sie verbringen nicht nur mehr Zeit online, sie interagieren auch verstärkt im Web – über soziale Netze und Plattformen, die eine Möglichkeit zum Austausch von Gedanken, Inhalten und Ideen bieten. Auf der Anbieterseite zeigt ein Vergleich eher traditioneller Medienkonzerne mit den neuen „digitalen Giganten“ deutlich, wo in den letzten Jahren die Wachstumsbereiche lagen (Abb. 4). Und sogar unter den klassischen Konzernen wuchsen diejenigen mit höherem Online-Anteil schneller. Ein gutes Beispiel ist News Corp. mit starken digitalen Aktivitäten wie MySpace.

2. „DIGITAL LIFE“: RICHTUNGWEISEND FÜR WIRTSCHAFT, POLITIK, GESELLSCHAFT UND ERZIEHUNG

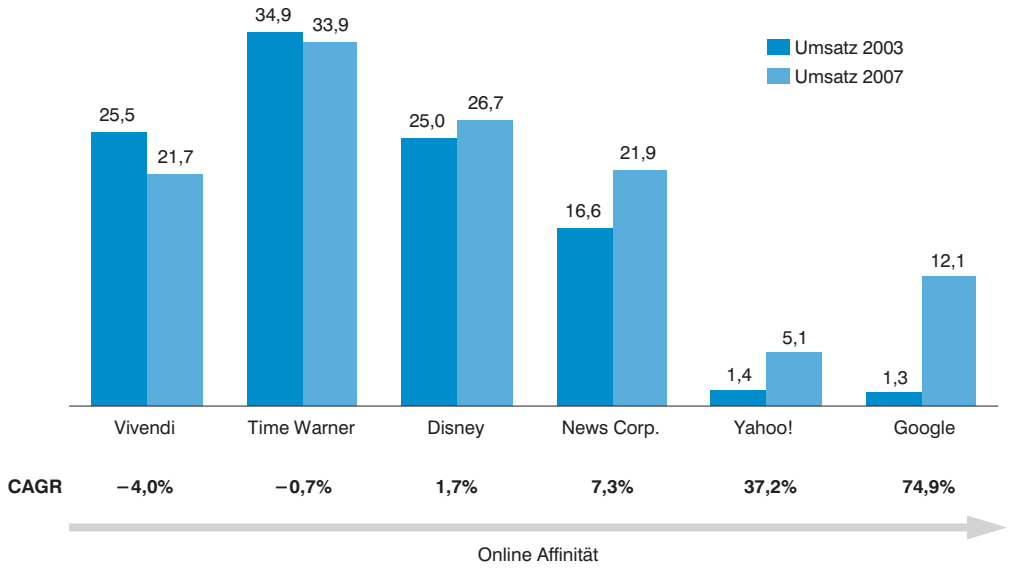
Bisher war es vor allem die Einführung neuer Technologien, die das Internet-Wachstum beflügelte. Endanwender-Equipment wie PCs und mobile Geräte bieten heute kostengünstigen Netzzugang und ausreichend Speicherplatz. Breitband-Netze sind dabei, auf extrem schnelle Next-Generation-Netze zu migrieren. Alle relevanten Infrastrukturen haben eine hohe Kapazität (bei Standard-DSL-Leitungen liegt sie um die 5 Mbps, in technisch weiter ent-wickelten Ländern sogar bei 25 bis 100 Mbps) in Kombination mit Interaktivität und 24/7-Erreichbarkeit. Und mit „3G“ ist es den MNOs (Mobilfunknetzbetreibern) endlich gelungen, das mobile Internet in ganz Europa erreichbar zu machen.

Abb. 3: *Die Evolution der digitalen Welt*



Quelle: Booz & Company

Abb. 4: *Medien- und Online-Konzerne im Vergleich (Umsatz in Mrd. Euro)*



Quelle: OneSource, Unternehmensberichte

Die heutigen Technologie-Anbieter haben in vielen Märkten die Durchdringung mit Internet-Access fast bis zur Sättigung vorangetrieben. Der nächste digitale Wachstumsschub wird daher auf einer intensiveren Ausbeutung der grundlegenden Technologien beruhen statt auf stärkerer Marktpenetration. Es geht nicht länger darum, die Anzahl der Nutzer zu erhöhen, sondern die Nutzung und das Nutzerverhalten zu verändern. Dass die Verbrauchergewohnheiten schon heute einem dramatischen Wandel unterliegen, lässt sich in vielen Märkten beobachten: Die wichtigste Informationsquelle beim Kauf eines Autos ist mittlerweile das Internet, in den USA wird bereits fast jedes zweite Buch online bei Amazon gekauft und der amerikanische Kabelbetreiber Comcast verzeichnet pro Monat rund 40 Mio. Video-on-Demand-Downloads.

Als Antwort auf den Wandel im Medienkonsum wenden sich Unternehmen zunehmend dem Internet als Werbe- und Marketingträger zu. In Großbritannien werden schon 15% der Werbebudgets an Online-Medien vergeben.

Das Internet und die digitale Welt haben sich zu einer attraktiven Plattform für diverse Werbe- und Marketingaktivitäten entwickelt. Nicht nur, dass die Verbraucher immer mehr Zeit mit digitalen Medien verbringen, diese Medien haben auch deutliche Effizienz- und Effektvitätsvorteile gegenüber anderen Werbeformaten – ein zentraler Aspekt. Viele fortgeschrittene Werbekonzepte (speziell solche, mit denen Kunden gezielter als bisher angesprochen werden sollen), können nur dann umgesetzt werden, wenn die digitalen Medien auf eine Fülle von Nutzer- und Nutzungsinformationen zurückgreifen können.

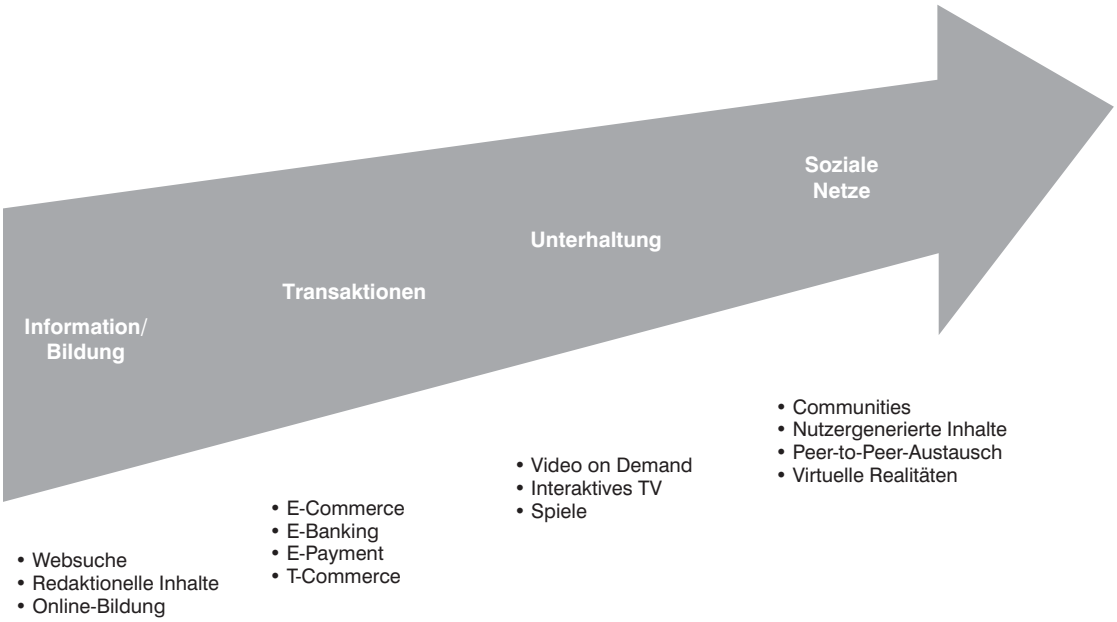
Das Internet verändert Branchen: In den USA wird fast jedes zweite Buch online über Amazon verkauft, der Medienumsatz (4,5 Mrd. Dollar) entspricht fast dem von Barnes & Noble im klassischen Buchhandel.

So werden beispielsweise Nutzer des Google-E-Mail-Angebots „Gmail“ mit Werbeinhalten bespielt, die zum Inhalt ihrer Mails passen. Auf ähnliche Weise könnten auch Browser-Verläufe, vom User aktiv verwaltete Profile oder andere Informationen verwendet werden, um Werbung gezielt auf Kunden zuzuschneiden. Im Bereich Digital-TV können Daten über die Set-Top-Box nachverfolgt und für „Targeted Advertising“-Angebote an bestimmte Gruppen oder individuelle Anwender genutzt werden. Und Werbung im digitalen TV bietet die gleichen Interaktionsmöglichkeiten wie das Internet.

Werbetreibende investieren mehr ins WWW: In Großbritannien gehen schon 15% des Gesamtwerbebudgets an Online-Medien.

Dabei kommt dem Datenschutz von Verbraucherseite sicherlich ein hoher Stellenwert zu, dem sorgfältig entsprochen werden muss, auch dann, wenn Daten nur in aggregierter, anonymisierter Form geschäftlich genutzt werden. Aber selbst wenn dies zunächst recht „interventionistisch“ klingt: Marktforschung zeigt, dass

Abb. 5: *Wachstumstreiber der digitalen Welt*



maßgeschneiderte Werbeangebote, wenn sie gut gemacht sind, die Verbraucherakzeptanz eher noch erhöhen – eben weil sie für den Konsumenten relevant sind. Darüber hinaus gibt es viele Möglichkeiten, sie so zu gestalten, dass eine unfreiwillige Teilnahme ausgeschlossen ist. Im Rahmen von Opt-in-/Opt-out-Prozeduren kann es zum Beispiel dem Kunden überlassen werden, ob er seine Daten für Werbezwecke freigibt. Wenn nicht, könnten die Werbeausfälle durch höhere Servicegebühren kompensiert werden. Alles in allem wird Werbung eines der wichtigsten Finanzierungsmittel für Dienstleistungen und Angebote bleiben, genauso, wie Werbung seit Jahrzehnten die klassischen Medien finanziert. Vor diesem Hintergrund und mit den Digital-Economy-Erfahrungen der letzten 15 Jahre ist es sehr wahrscheinlich, dass „Werbung" im weitesten Sinne auch im künftigen digitalen Wachstumsmarkt eine der größten Ertragsquellen sein wird. Doch dafür wird es nötig sein, sich mit den tatsächlichen und „gefühlten" Bedrohungen der digitalen Welt stärker auseinanderzusetzen. Besonders vor dem wachsenden Druck, neue Web-2.0-Services gewinnbringend zu verwerten, wird dies für alle Branchenplayer eine der größten Herausforderungen sein.

Aus der Anwendungsperspektive sehen wir vier große Wachstumsfelder für das „Digital Life":

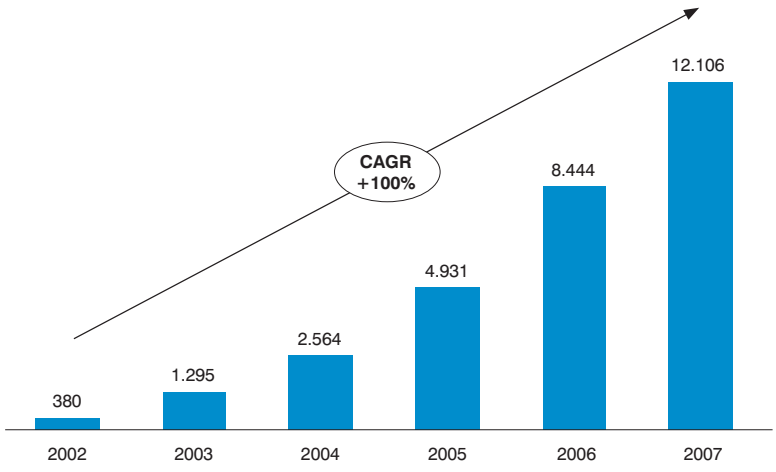
- **Information und Wissensvermittlung:** Klassische Web-1.0-Applikationen mit einer Reihe von Web-2.0-Optimierungen, beispielsweise nutzergenerierte Inhalte im E-Learning.

- **Transaktionsservices:** In erster Linie E-Commerce und Online-Banking.

- **Unterhaltung:** Digital-TV, Video-Services (Streaming- und Video-on-Demand-Angebote wie YouTube), Gaming und Download-Portale wie iTunes.

- **Soziale Netze:** Alle Dienste, die auf menschlicher Interaktion beruhen, beispielsweise Communitys, Austausch von selbst generiertem Content oder Kontakt in virtuellen Realitäten.

Abb. 6: *Google-Wachstum (Umsatz in Mio. Euro)*



Quelle: Google

INFORMATION UND WISSENSVERMITTLUNG

Vielfältige Informationsangebote und ganz besonders die Online-Suche gehörten von Beginn an zu den Treibern der Internetnutzung. Suchmaschinen kommt das Verdienst zu, die Unmengen von Daten im Web für den Enduser erst nutzbar gemacht zu haben.

Das Internet begünstigt auch kollaborative Modelle, die Wissen und Bildung über nutzergenerierte Inhalte bereitstellen. Ein Beispiel ist Wikipedia mit seinen über 10 Millionen von Anwendern geschriebenen Artikeln in 250 Sprachen. Erst 2001 ins Leben gerufen, entwickelt sich Wikipedia heute zur meistbesuchten Quelle für enzyklopädisches Wissen – und zwar überhaupt, nicht nur im Netz. Damit wird das Portal zu einem der wichtigsten heute existierenden Werkzeuge für Wissenschaft und Forschung. Das geht so weit, dass diskutiert wird, ob Studenten die Fähigkeit zur „realen" Recherche in Bibliotheken langsam verlieren. Das offene, Community-artige Konzept, sowohl was die Erzeugung von Inhalten als auch die Steuerung durch die Nutzer selbst angeht, macht Wikipedia zu einem Paradebeispiel für eine echte Web-2.0-Applikation, die in den Wissens- und Bildungsbereich vordringt. Manche behaupten, dass seine dynamische Struktur für weit akkuratere Informationen sorgt als sie in statischen Informationsquellen zu finden sind.

Über 45% aller Unternehmen veranstalten regelmäßig Schulungen im Internet.

Digitales Fernsehen ist eine weitere Triebfeder des Informationszeitalters. Heute gibt es in Europa beeindruckende 1.703 Fernsehsender (2005) – verglichen mit 93 vor nur 18 Jahren. Eine Vielzahl von ihnen versorgt die Zuschauer mit Nachrichten und Dokumentationen sowie fremdsprachigen Programmen, die zu Analogzeiten noch gar nicht existierten oder nicht empfangen werden konnten.

Auch Universitäten und andere weiterbildende Institutionen machen sich die Möglichkeiten digitaler Infrastrukturen immer stärker zunutze, etwa zum effizienten Informationsaustausch oder für die hochfunktionale Interaktion über Lösungen wie WebEx (eine internetbasierte Konferenz- und Kollaborationssoftware). Besonders Fernuniversitäten, die noch vor 15 Jahren viel physischen Aufwand erforderten (Anreise zu Veranstaltungen, Einschicken von Übungen etc.), profitieren von diesen Möglichkeiten. Mehrere Universitäten und Schulen, wie beispielsweise die englische Open University, haben sich dem „Second Life" zugewandt und versetzen ihre Klassenräume in die virtuelle Realität. Wirtschaftsunternehmen nutzen das Internet und die damit verbundenen digitalen Medien zur Schulung ihrer Mitarbeiter, wobei Formate wie Webcasts oder „Web-based Training" (WBT), eine Weiterentwicklung des traditionellen „Computer-based Training" (CBT), zum Einsatz kommen.

Information und Wissensvermittlung werden dem digitalen Leben auch weiterhin Wachstumsimpulse geben. Insbesondere die durch Online-Werbung finanzierte Web-Suche wird stark anwachsen. Der Umsatz von Google, dem Vorbild für das Modell, Suchdienste in Werbeeinahmen umzumünzen, weist in den letzten 5 Jahren eine durchschnittliche jährliche Wachstumsrate (CAGR) von über 100%auf. Google hat seine Geschäftsmodelle entschieden vorangetrieben und seine Angebote kontinuierlich verbessert – mit dem Ergebnis, dass Google heute mehr als zweimal so groß ist wie der größte europäische Fernsehsender, RTL Group.

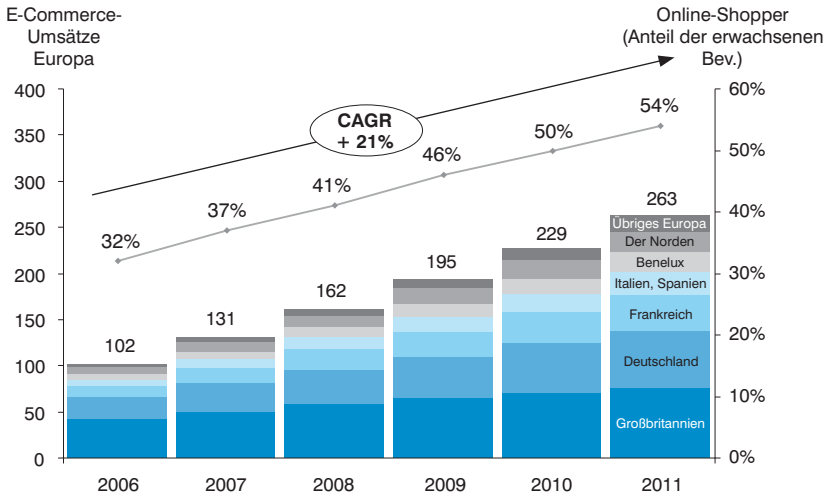
TRANSAKTION

Das Internet hat sich als ideales Medium für Transaktionen erwiesen.

Beim Online-Einkauf profitieren Kunden von wettbewerbsfähigen Preisen, Vergleichsmöglichkeiten auf verschiedenen Webseiten und vielen anderen Vorteilen. Heute, bei einem Online-Käufer-Anteil von über 40% der Bevölkerung,

Mehr als 40% der Verbraucher kaufen online. Inzwischen macht E-Commerce 4% des europäischen Einzelhandels aus.

Abb. 7: *Umsätze Online-Einzelhandel (Mrd. Euro)*



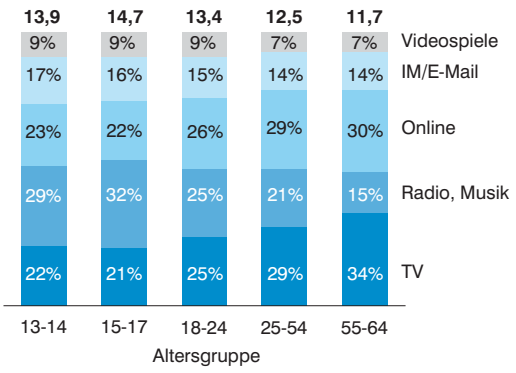
Quelle: Forrester

übersteigt das jährliche Geschäftsvolumen in Europa die 150 Mrd. Euro-Marke. Allein in den letzten 2 Jahren ist es um 50% gestiegen. Das E-Commerce-Volumen entspricht heute 4% vom gesamten Einzelhandelsumsatz in Europa. Bis 2011 soll es auf 11% anwachsen. Bei bestimmten Produkten wie Tickets, Reisen und Medien (Bücher, Musik, Video, Software) wird 2011 sogar ein Anteil von 25 bis 35% vorausgesagt.

Darüber hinaus hat das Internet durch seine Transaktionsfähigkeit die Art revolutioniert, wie Verbraucher ihre Finanz- und Bankgeschäfte managen. In dem Rahmen, wie sich das Internet den Ruf relativer Zuverlässigkeit erworben hat, entwickelte sich auch das E-Banking zu einem Massenphänomen. Und parallel zum wachsenden Online-Handel etablierte sich ein breites Spektrum an E-Payment-Lösungen, wie beispielsweise PayPal, rund um die steigende Nachfrage nach Produkt- und Dienstleistungskäufen. Bei der besonders hohen Sensibilität von Finanztransaktionen sind diese Bereiche natürlich auch den stärksten Sicherheitsbefürchtungen ausgesetzt.

Neue Geschäftsideen basieren zunehmend auf „Internet only"-Modellen. Sie machen sich die Chance zunutze, ein virtuelles Unternehmen zu einem Bruchteil der Kosten eines stationären Betriebes führen zu können, und nutzen das Web als kostengünstigen Vertriebskanal und Basis für effizientes Supplychain-Management. Aber auch der stationäre Handel profitiert von einer zusätzlichen Low-Cost-Plattform für Kundenservice- und Billing-Aufgaben. Oft werden dabei Premiumpreise verlangt, wenn der Kunde das Internet nicht nutzen will. Mobilfunkanbieter haben solche „Nur im Internet"-Angebote schon vor einigen Jahren eingeführt.

Abb. 8: *Zeit für Medienkonsum (Std. pro Tag, USA 2007)*



Quelle: eMarketer

UNTERHALTUNG

Auf dem Gebiet der Unterhaltung wird sich für die Verbraucher wahrscheinlich der tiefgreifendste Wandel vollziehen. Der durchschnittliche Konsument verbringt zwischen 160 und 240 Minuten pro Tag vor dem Fernseher und noch mal bis zu 140 Minuten im Internet – und zwar zunehmend auch, um Entertainmentinhalte abzurufen. Addiert man beide Aktivitäten, dann ist der Konsum interaktiver Medien bei weitem die Nummer 1 unter den europäischen Freizeitaktivitäten bezogen auf den Zeitaufwand. Und genau dieses Erlebnis verändert sich zurzeit dramatisch. In vielen hochentwickelten Ländern ist das Internet schon jetzt das führende Medienformat: Die Menschen verbringen mehr Zeit im Web oder mit E-Mails als vor dem Fernseher (siehe Abb. 8).

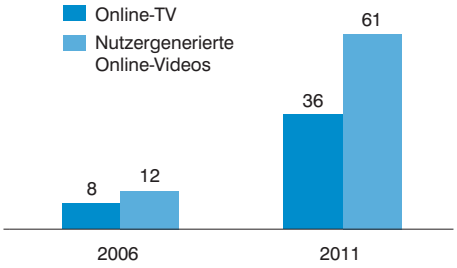
Da Konsumenten heute zunehmend unter Zeitdruck stehen, verlangen sie Entertainment-Angebote, die sie immer und überall und in der von ihnen favorisierten Weise abrufen können. Die höhere Kapazität der Breitband-Netze erlaubt die kostengünstige Versorgung beispielsweise mit Video on Demand.

Das Digital-TV ist dabei, die Fernsehgewohnheiten der Verbraucher zu revolutionieren. In den letzten Jahren ist die Zahl der TV-Sender explosionsartig angestiegen. Viele Regional- und Spartenprogramme sind hinzugekommen. Zudem bietet das digitale Fernsehen zukünftig durch HDTV deutlich bessere Bildqualität. Digital-TV ist auch für eine Reihe neuartiger Funktionen verantwortlich, etwa Video auf Abruf oder zeitversetzte Sendung, und unterstützt spezielle Features wie Interaktivität und die „elektronische Programmzeitschrift" (Electronic Programme Guide EPG).

Daneben entstehen kommerzielle Plattformen, die von der höheren Kapazität der Breitband-Netze profitieren und Multimedia-Unterhaltung online verbreiten. So bietet der „iPlayer" der BBC in ganz England TV-Shows und Radio per Internet.

Über die Hälfte der amerikanischen Intenet-User (57%) hat bereits Filme im Internet gesehen. Fast 20% von ihnen tun dies Tag für Tag. Bei Nutzern mit Breitband-Anschluss liegt der Anteil sogar noch höher (74%). Einige findige Start-ups haben im letzten Jahr damit begonnen, das Internet in einen echten Kabelsender umzuwandeln: Joost, Babelgum und andere bieten in einem so genannten „Over the top"(OTT)-Ansatz – zusätzlich zum Kabelnetz und unabhängig von einem Netzbetreiber – Fernsehen in hoher Qualität, angereichert mit Web-2.0-Elementen.

Abb. 9: *Online-Videostreams in den USA (Mrd. Video Streams)*



Quelle: eMarketer

Diese Trends erhöhen nicht nur den Wert des Internets als Werbemedium, sie etablieren es auch als zunehmend wichtigen Meinungsbildner. Befürworter der freien Meinungsäußerung und eine gut informierte Öffentlichkeit (Politik, Sozialwissenschaften und kulturelle Institutionen) werden zunehmend Interesse an diesem Wandel im Medienkonsum zeigen.

SOZIALE NETZE

Durch Portale wie Facebook oder Bebo erlebt unsere Gesellschaft einen Anstieg der Interaktion. Soziale Netze haben Funktionalitäten ermöglicht, die vor dem Internet nicht denkbar gewesen wären und die den Menschen einerseits erlauben, ohne Rücksicht auf physikalische Distanz Online-Bekanntschaften zu knüpfen, andererseits aber auch Besorgnis über das traditionelle Sozialverhalten hervorrufen, weil direkte Interaktionen und Partnerschaften an Wert verlieren.

Soziale Netze sind ein relativ neues Phänomen, das den allgemeinen Web-2.0-Trend zu Online-Communitys noch verstärkt. Ihre Nutzer – größtenteils Angehörige der „Born Digital"-Generation – gehören netzbasierten sozialen Interessengruppen an, die eigenen Content generieren, ins Netz stellen und untereinander austauschen. Immer mehr Internet-Nutzer betreiben regelmäßig Social Networking, die meisten auf mehreren Portalen gleichzeitig.

Sozialverhalten im Umbruch: Das Internet ermöglicht den schnellen Kontakt zu immer größeren Gruppen.

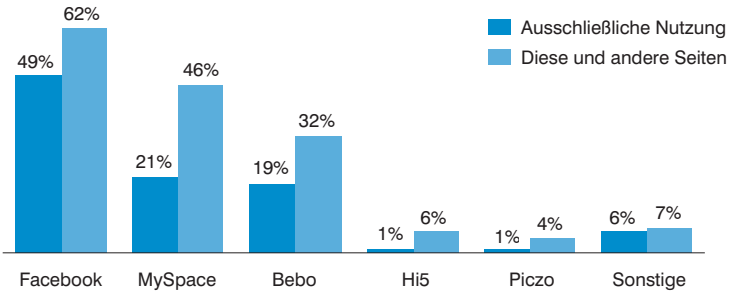
Das Internet beeinflusst das soziale Verhalten der Konsumenten schon seit geraumer Zeit. Im Jahre 2004 stellte eine amerikanische „Social Ties"-Studie fest, dass durchschnittliche Internet-Anwender mit mehr Menschen regelmäßig interagieren: 37 sozialen Kontakten bei Internet-Usern standen 30 bei Nicht-Usern gegenüber. Über 30% der Internet-Nutzer gaben überdies an, durch das Web habe sich die Anzahl ihrer Kontakte und Bekanntschaften erhöht.

GESELLSCHAFTLICHER WANDEL

Wie oben dargelegt – und wie im weiteren Verlauf dieser Studie noch genauer untersucht werden wird –, ist digitale Technologie schon heute ein wichtiger Wirtschaftsfaktor, der in Zukunft an Bedeutung gewinnen wird. Doch sollte „Digital Life" nicht nur unter Wirtschaftsgesichtspunkten betrachtet werden. Speziell das Internet, aber auch das ganze Spektrum digitaler Dienstleistungen, leitet einen Wandel mit weitreichenden Konsequenzen ein, die weit über den Verkauf von Büchern oder Flugtickets hinausgehen. Digitale Technologien ermöglichen jedem, sich Gehör zu verschaffen und in dem für ihn relevanten Kontext ein großes Publikum zu erreichen.

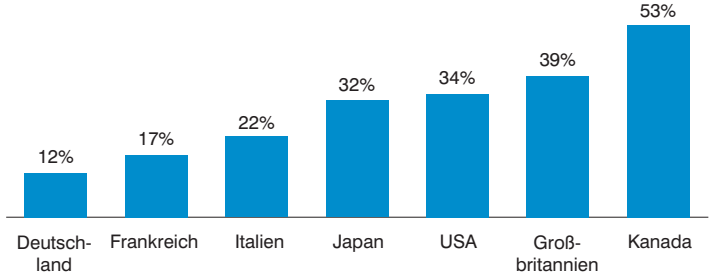
Das Web als wichtigster Meinungsbildner: Google wird weltweit als eine der zuverlässigsten Nachrichtenquellen zitiert, gleich nach CNN und BBC.

Abb. 10: *Nutzung sozialer Netze durch Erwachsene (GB 2007, Prozent aller Nutzer sozialer Netzwerke)*



Quelle: Ofcom

Abb. 11: *Nutzung sozialer Netze durch Erwachsene (2007, Prozent der Internetnutzer eines Landes)*



Quelle: Ofcom, Nielsen

n=391

Die „Born Digital"-Generation: Digital Confidence rückt in den Vordergrund

Die Kinder und Jugendlichen in den Industrieländern bilden die erste Generation, die mit der digitalen Welt aufgewachsen ist. Sie absorbieren mühelos neue Technologien und sind im Vergleich zu ihren Eltern wahre IT-Spezialisten. Bei vielen Älteren lässt die „digitale Wiedergeburt" hingegen noch auf sich warten.

Die Zeitschrift Wired beschreibt diese Generation so:

- Selbstcharakterisierung „Born Digital": „Gemeinsam mit dem PC haben wir krabbeln gelernt, zusammen mit dem Internet sind wir erwachsen geworden. Als erste dabei, perfekt vernetzt, immer am Ball".

- Über Technologien: „IM, MP3, P2P – was wir heute testen, ist morgen schon Allgemeingut. Andere sehen der digitalen Zukunft begeistert entgegen, wir finden sie total normal. Es ist ein Unterschied wie zwischen Fremdsprache und Muttersprache."

Die „Born Digital"-Generation unterscheidet nicht mehr so stark zwischen Online und Offline wie viele Erwachsene. Sie sieht viel stärkere Verbindungen zwischen den beiden Welten und lebt in realen und virtuellen Gemeinschaften – oft mit sehr verschiedenen Altersgruppen. Und sie hat ihre eigene Online-Kultur, -Sprache und -Etikette.

Doch die „Born Digital"-Generation stellt auch eine Herausforderung dar – für sich selbst und für die Gesellschaft:

- Reichlich paradox: Sie stellen bereitwillig persönliche Daten in sozialen Netzen ein (Preisgabe der Privatsphäre), wehren sich aber vehement, sobald sie mit der Datenverwendung nicht einverstanden sind – wie im Fall von Facebook Beacon: 2007 erklärten sich 50.000 User in einer Petition nicht damit einverstanden, dass Facebook mit externen Partnerwebsites integriert wird, um Cross-Referencing und Targeted Advertising zu ermöglichen.

- Eltern und Schule (die „Natürlichen Erzieher") sind mit der Tragweite der neuen Phänomene und der Innovationsgeschwindigkeit überfordert.

- Traditionelle Gesetze lassen sich auf die „unklaren" digitalen Verhältnisse weniger leicht anwenden und werden dort weniger akzeptiert, Beipiel: Schutz urheberrechtlich geschützter Inhalte.

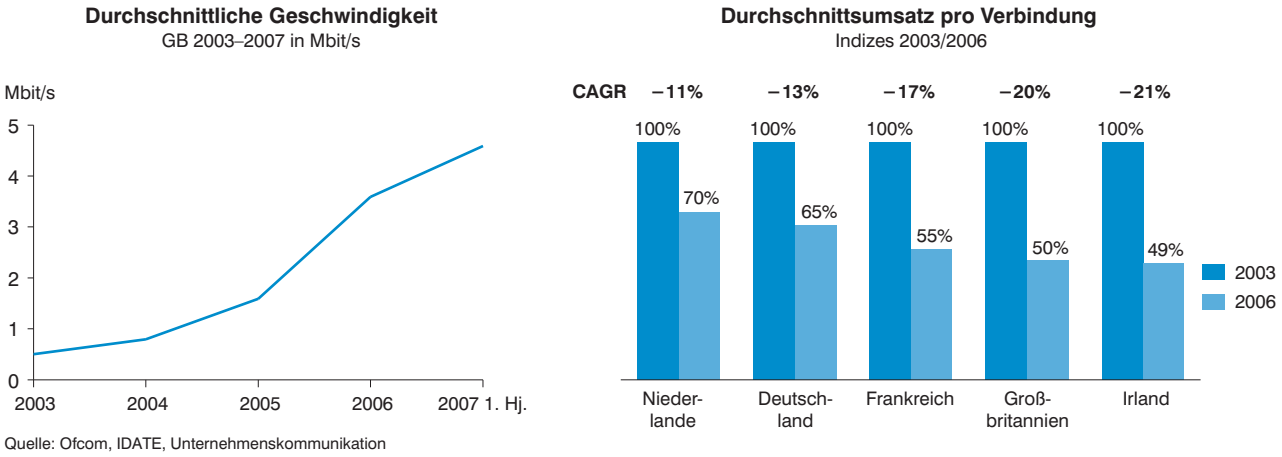
Insgesamt erhalten die „Born Digitals" nicht genug Verhaltensregeln für digitale Welten. Das setzt schon seit Jahren Business-Modelle unter Druck, zum Beispiel im Bereich von Copyright-Verletzungen, und wird sich bei der Einführung neuer Werbe-Geschäftsmodelle noch verstärken.

Politiker nutzen das Internet, um sich und ihre Ideen zu präsentieren, mit ihren Anhängern zu interagieren und ihre Kampagnen zu organisieren. So setzt Präsidentschaftskandidat Barack Obama auf breiter Front Social-Networking-Applikationen in seinem Wahlkampf ein. Mehr als 30.000 Mitglieder auf „Twitter" sind seine Anhänger und erhalten regelmäßige kurze Updates von ihm. Fast ein Viertel der Amerikaner nutzt das Internet als Quelle für Partei- und Wahlkampf-Informationen. In der Altersgruppe 18–29 beträgt der Anteil sogar über 40%. Obama hat den Einsatz des Web als Politikinstrument zu neuen Höhen getrieben: Er benutzt es auch, um Spendengelder zu generieren. Mehr als 1 Million Wähler spendeten für seine Kampagnen durchschnittlich 105 Dollar. Vor 10 Jahren noch ein Ding der Unmöglichkeit – heute eine der wichtigsten Quellen der Wahlkampffinanzierung.

Das Internet verändert die Gesellschaft: 60% der US-Verbraucher würden auf ihr Telefon verzichten, nur 55% auf ihren Internetanschluss.

Blogs, Podcasts, Chat-Seiten, Userforen, Newsgroups und andere neuartige Kommunikations- und Online-Publishing-Tools haben nicht nur neue Anforderungen an die geschäftliche Kommunikation zur Erreichung von Business-Zielen geschaffen, sie haben auch die Geschwindigkeit und Reichweite erhöht, mit der sich Neuigkeiten und Gerüchte austauschen und verbreiten lassen. Eine der Folgen war, dass Unternehmen sich plötzlich gezwungen sahen, strikte Informations- und Kommunikationsrichtlinien zu erarbeiten, um insbesondere ihre vertraulichen Firmendaten zu schützen. Verbraucherportale wie „ciao" (das in mehreren Ländern Europas aktiv ist und pro Monat mehr als 38 Mio. Besucher verzeichnet) sowie Weblogs haben eine völlig neuartige Grundlage für Preis- und Qualitätsvergleiche entstehen lassen, die sich für den einzelnen Markenartikler, Dienstleister, Einzelhändler etc. sehr günstig oder sehr negativ auswirken kann. Die Macht von Blogs und Online-„Syndication" (also der Verbreitung von Inhalten über Onlinemedien) reicht dabei weit über den reinen E-Commerce und selbst die digitale Welt hinaus: Kate Hanni, eine einzelne Flugreisende, die von den Praktiken des Flugriesen American Airlines genug hatte, gründete gemeinsam mit einigen Leidensgenossen die „Coalition for an Airline Passengers' Bill of Rights", nachdem sie im Dezember 2006 „auf dem Flughafen Austin bis zu 9 Stunden in verschiedenen American-Air-

Abb. 12: *Das Breitband-Dilemma*



Quelle: Ofcom, IDATE, Unternehmenskommunikation

lines-Maschinen ausharren“ musste, und zwar „ohne Nahrung, Wasser oder Zugang zu funktionierenden Toiletten“. Heute zählt die Vereinigung 20.000 Mitglieder und nutzt eine Website und ein Blog zum Publizieren von „Horrorstorys“ und zur Kommunikation ihrer Ziele. Nach wiederholten Besuchen bei Kongressabgeordneten werden nun Gesetzesänderungen erwogen, um weitere Schreckensmeldungen zu vermeiden.

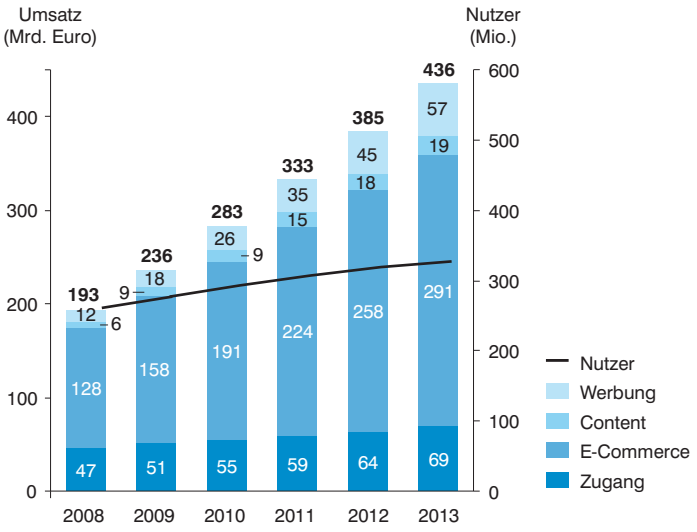
Die Marktmacht von Web-2.0-Angeboten wie Verbraucherportalen oder Nutzer-Rezensionen auf Amazon findet ihren Niederschlag auch in „Edelman’s Trust Barometer“: Die 2008er-Ausgabe des Rankings zeigt, dass Verbraucher einer Informationsquelle, die „so ist wie ich“ weit mehr Vertrauen entgegenbringen als offiziellen Informanten, einschließlich der Geschäftsleitung. In allen Ländern gaben vier von fünf Befragten an, dass sie „dem, was sie von einem Unternehmen sehen, lesen oder hören, mehr Vertrauen schenken, wenn es ein Bekannter schon einmal erwähnt hat“. Im Bereich der Institutionen gelten hingegen gemeinnützige Organisationen als am meisten vertrauenswürdig im Vergleich zu Unternehmen, Medien und der Politik. In Großbritannien, Deutschland und Frankreich führen NGOs die Rankings mit deutlichem Vorsprung an.

Für viele von uns ist die Geschwindigkeit, mit der sich der digitale Wandel vollzieht, atemberaubend. Gleichzeitig wächst jedoch eine Generation heran, für die die Möglichkeiten digitaler Welten so normal und unspektakulär sind wie noch vor 50 Jahren Fernsehen oder Radio. „Born Digitals“ sind „Frühanwender“ neuer Technologien und im Vergleich zu ihren Eltern wahre IT-Spezialisten. Sie trennen nicht – wie viele Erwachsene – scharf zwischen Online und Offline, leben vielmehr in realen und virtuellen Gemeinschaften gleichzeitig, wobei sie oft im Kontakt mit sehr unterschiedlichen Altersgruppen stehen. Und sie haben ihre eigene Online-Kultur, -Sprache und -Etikette. Doch die „Born Digital“-Generation stellt auch eine Herausforderung dar, denn ihr fehlt es an Regeln zu richtigem sozialen Verhalten, etwa beim Umgang mit persönlichen Daten oder mit urheberrechtlich geschütztem Material. Das belastet die Jugendlichen nicht nur selbst und wird damit zu einer Erziehungsaufgabe für die Gesellschaft, es stellt auch ein ernstes Problem für digitale Geschäftsmodelle wie Content providing oder innovative Werbekonzepte dar. In Sachen „Born Digitals“ sollte die Industrie daher dringend zu einer koordinierten, abgestimmten Haltung gelangen und neue Wege der Zusammenarbeit finden.

FAZIT

Die identifizierten Wachstumstreiber des digitalen Lebens werden allen Bereichen von Wirtschaft und Gesellschaft neue Impulse versetzen. Sicher ist, dass das „Digital Life“ das Wirtschaftswachstum und die Konjunktur weiterhin begünstigen wird und dass es künftig eine noch zentralere Rolle in unserem Leben spielen wird. Dabei werden die digitalen Infrastrukturen neue Arten der Interaktion, Kommunikation und Wertschöpfung ermöglichen, die bis heute nur in Ansätzen realisiert sind.

Abb. 13: *Digitales Leben – Umsätze in Europa*



Hinweis: Europa einschl. EU-27, Norwegen und Schweiz
Quelle: Forrester e-Commerce Forecast, Finanzbericht Apple, Finanzbericht Google, EU TV und Broadband Forecast Model, Booz & Company-Analyse

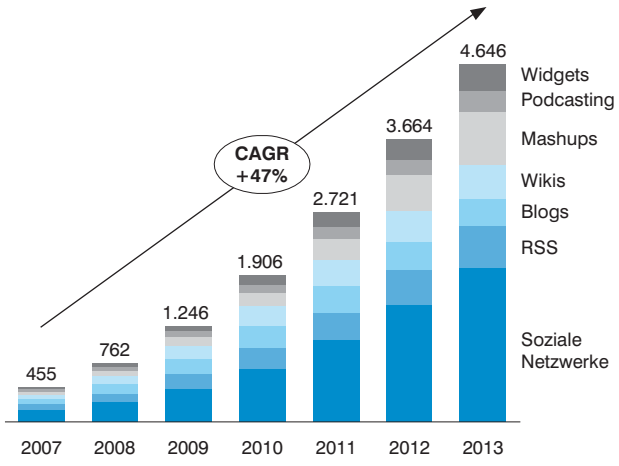
3. DIE NEUEN WACHSTUMS- UND UMSATZTREIBER: INHALTE UND WERBUNG STATT NETZZUGANG

In den identifizierten Bereichen ergeben sich für die Digital Economy zusätzliche Einnahmemöglichkeiten in folgenden Umsatzkategorien:

1. Werbung: Sämtliche Formen von Online-Advertising einschließlich „Click-through Revenue“[1] , Werbung in Web TV-Spots und Sponsoring (zum Beispiel Online-TV-Shows mit Sponsorkennung: „Diese Sendung wird Ihnen präsentiert von XYZ“).

(1) „Click-through Revenue“ bezeichnet die volumenbasierte Bezahlung einer Suchmaschine für die Weiterleitung eines „Sponsored Link“ an eine externe Website.

Abb. 14: *Weltweiter Jahresumsatz „Enterprise 2.0“ (Mio. US-Dollar)*



Quelle: Forrester

2. Content: Online abrufbare Inhalte wie Video on Demand, Gaming, Fernsehen (bezahltes Web-TV und Video-Streams) und Musik-Downloads.

3. E-Commerce: Produkte und Services, die online bestellt und auf klassischem Weg versendet werden (zum Beispiel Buchbestellung bei Amazon oder Ticketkauf auf der Website einer Fluggesellschaft).

4. Netzzugang: Datentransport im World Wide Web und Anschluss an digitales Kabelfernsehen sowie Einnahmen der Telefon- und Kabelnetzbetreiber für den Breitbandinternetzugang.

E-Commerce ist die etablierteste und größte Umsatzkategorie. Online-Werbung und Content sind relativ neu entstandene Felder mit einem Wachstum von 32 beziehungsweise 22%, allerdings auf niedrigem Ausgangsniveau (siehe Abb. 13).

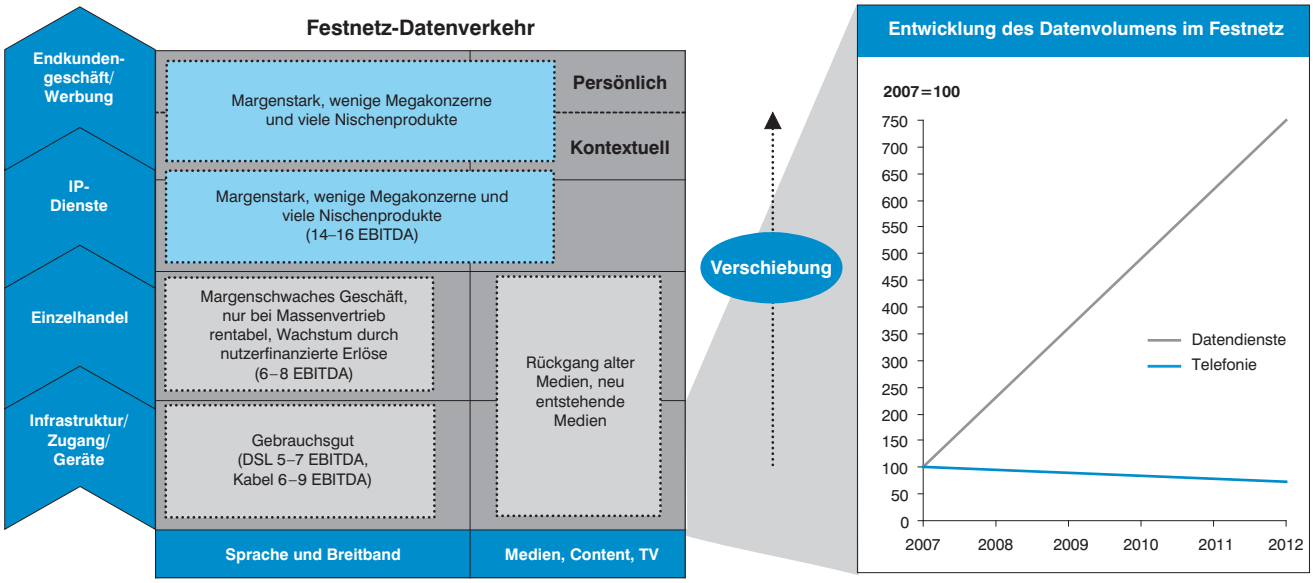
Der nächste Wachstumsschub des „Digital Life“ entsteht nicht durch mehr Nutzer, sondern intensivere Nutzung.

Bisher war die Entwicklung der digitalen Wirtschaft vor allem von technischen Neuerungen abhängig. So bewirkte der Übergang von der Einwahl- zur DSL-Leitung eine Explosion der Internetverbreitung und -nutzung. In vielen Teilen Europas und Asiens sowie in Nordamerika ist Breitband damit zu einem Massenphänomen geworden und nähert sich in manchen Regionen schon dem Sättigungsgrad. Dies gilt besonders für Westeuropa, während manche süd- und osteuropäischen Länder sich langsamer entwickeln. Daher rechnet man in diesen Ländern weiterhin mit stabilen Umsätzen bei Netzzugangs-Leistungen mit einstelligen Wachstumsraten. Die Transfer-Infrastruktur wird jedoch immer mehr zum selbstverständlichen Massengut. Grund ist ein stark umkämpfter Markt mit etablierten technischen Lösungen und begrenztem Differenzierungspotenzial.

Das Marktvolumen des „Digital Life“ wird jährlich 18% wachsen und bis 2012 436 Mrd. € erreichen.

Das verlangsamte Anwachsen der Nutzerzahlen und die eher bescheidene Entwicklung der Umsätze im Netzzugang, aber auch „bandbreitenhungrige“ Anwendungen wie Video on Demand und P2P, setzen die Netzzugangs-Margen unter Druck. Insgesamt wird der Markt-

Abb. 15: *Datenverkehr*



Hinweis: EU-27+2 (CH, NOR), also mit weniger entwickelten Breitband Märkten. Konservative Schätzung für entwickelte Märkte.
Quelle: Ovum, Booz & Company-Analyse

anteil von heute 24% auf unter 16% im Jahr 2012 abschmelzen.

Dass sich die Umsätze in den kommenden Jahren voraussichtlich schneller entwickeln als die Zahl der Internetnutzer (18% CAGR im Vergleich zu 4% Neunutzern), deutet auf eine fundamentale Verschiebung der Wertschöpfungsstufen hin. Künftige Gewinne werden sich durch Intensivierung der einzelnen Kundenbeziehung ergeben, nicht durch Ausweitung der Nutzerzahl. Es wird erwartet, dass sich dieses Wachstum durch neuartige Produkt- und Dienstleistungsangebote im Verbund mit innovativen Geschäftsmodellen realisieren lässt, die neue Zahlungsströme generieren.

Infrastruktur ist nicht länger wichtigste Einnahmequelle: Der Marktanteil von Netzzugang wird in den nächsten 5 Jahren von 24 auf weniger als 16 Prozent abschmelzen.

Die neuen Services werden sich sowohl an Privatkunden als auch an die Wirtschaft wenden. Beispielsweise geht Forrester davon aus, dass der Web-2.0-basierte B2B-Umsatz um 47% pro Jahr steigt und bis 2013 weltweit um 5 Mrd. Dollar anwächst.

Als „Enabler" des digitalen Lebens müssen Netzbetreiber mit steigendem Traffic und niedrigeren Margen rechnen.

Demnach wird der nächste Wachstumsschub der Digital Economy auf dem Gebiet neuer Dienstleistungen und Anwendungen liegen. Dieser lässt sich aber nur im Einklang mit der jeweiligen Breitband-Entwicklung realisieren: In Ländern mit großem „digitalem Nachholbedarf" wird der Infrastruktur-Roll-out weiterhin eine große Rolle spielen, während in Märkten mit fast ausgereiztem Breitband-Potenzial der Übergang zu Next-Generation-Netzen (NGNs) vorangetrieben werden muss, um dem erwarteten Traffic-Anstieg durch allgemein intensivere Nutzung und insbesondere der Verbreitung von hochauflösenden Fernseh- und Videoangeboten gerecht zu werden.

Netzbetreiber brauchen neue Geschäftsmodelle, die auf Dienstleistungen und Anwendungen statt auf Infrastruktur setzen. Um das Potenzial auszuschöpfen, muss auch in Next-Generation-Netze (NGNs) investiert werden.

III. DIGITAL CONFIDENCE: DAS WACHSTUM DER DIGITALEN WELT SICHERSTELLEN

1. GEFAHREN FÜR DAS „DIGITAL LIFE“

Das Wachstum der digitalen Märkte kann durch kontinuierliche Intensivierung von Online-Nutzung und -Ausgaben verstetigt werden. Um dies zu erreichen, müssen Kunden und Unternehmen Vertrauen in die Umgebung haben, mit der sie arbeiten.

Bei Verbrauchern und Unternehmen herrscht Unsicherheit über Vertrauenswürdigkeit und Unbedenklichkeit der neuen digitalen Welten.

Die Verbraucher müssen aufgeklärt werden, welche potenziellen Gefahren im Internet bestehen und wie man mit ihnen umgeht. Sie müssen sich sicher fühlen – und auch wirklich sicher sein. Für die Industrie besteht daher eine der Hauptaufgaben darin, für zuverlässige Netzumgebungen und ein optimales Kundenerlebnis zu sorgen.

Die Verbreitung anwenderfreundlicher Technologien und ubiquitärer Konnektivität haben das Web zum bevorzugten Ort des digitalen Lebens werden lassen. Durch plattformübergreifende Strategien und zunehmende „Webifikation“ anderer Systeme werden aber beispielsweise auch Digital-TV oder Mobilfunk an Relevanz für das „Digital Life“ gewinnen.

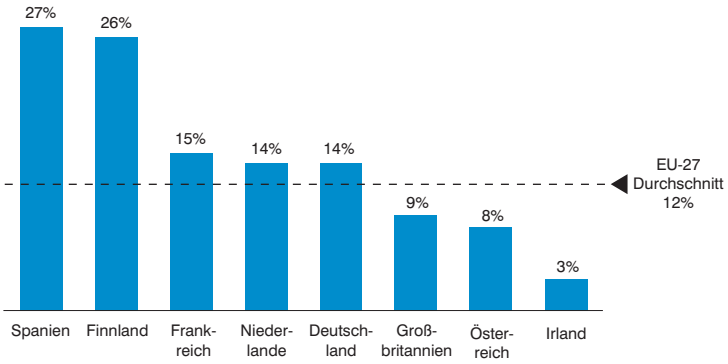
Mit dem Anwachsen der Web-2.0-Wirtschaft sind aber auch Unsicherheiten entstanden, die sich zum einen auf das Verhalten der Anwender beziehen – zum Beispiel die Preisgabe von immer mehr persönlichen Daten bei der Profilerstellung in sozialen Netzen. Der generelle Druck auf Plattformanbieter, ihr Web-2.0-Angebot zu vermarkten (speziell Social-Networking-Portale) beziehungsweise Infrastrukturinvestitionen wieder hereinzuholen, erhöht auch den kommerziellen Druck auf den Verbraucher: Werbebasierte Geschäftsmodelle und individualisierte Marketingkonzepte nutzen sein Online-Profil aus. Auch in der Arbeitswelt können Nutzerprofile, Blogs und Fotoalben Konsequenzen haben, beispielsweise wenn sich künftige Arbeitgeber online über Kandidaten informieren.

Andere Sorgen betreffen bösartige Verletzungen der Netzsicherheit, die im Netz hinterlegte persönliche Daten oder den Geschäftsbetrieb bedrohen und die wachsende Zahl von Angeboten, die auf sichere Netzumgebungen angewiesen sind, unterminieren (siehe Abb. 17). Die Befürchtungen sind in vielen Fällen berechtigt. So zeigt beispielsweise die Analyse der 10 häufigsten Formen von Internetbetrug in den USA 2007, dass die meisten Fälle im Zusammenhang mit E-Commerce standen und pro Person mit bis zu 4.000 Dollar Schaden zu Buche schlugen (siehe Abb. 18). 12% aller Europäer meiden den Online-Handel aufgrund von Sicherheitsbedenken (siehe Abb. 16). Neben Betrügereien fürchten Unternehmen die wachsende Zahl von Attacken durch böswillige Internetnutzer. Die Daten legen nahe, dass die Industrie schon 2005 jährlich über 1.000 Mrd. Dollar weltweit bei solchen Angriffen verloren hat – durch Downtime und entgangenen Umsatz, Reparaturen an beschädigten Systemen und die damit einhergehenden Imageeinbußen. Diese Kosten haben sich zwischen 2000 und 2005 wegen des rasanten Wachstums des „Digital Life“ besonders stark entwickelt (siehe Abb. 19). Selbst heute können Branchenexperten den insgesamt entstandenen Schaden nicht beziffern.

Jeder 8. Verbraucher meidet E-Shopping aus Sicherheitsgründen.

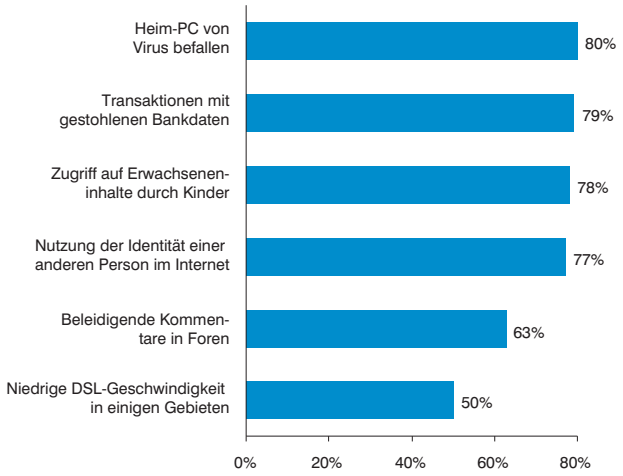
Durch Online-Piraterie und die unter „Born Digital“-Nutzern weit verbreitete Ansicht, Content müsse immer kostenlos sein, stellt das Web 2.0 auch für Anbieter visueller Medien eine Gefahrenquelle dar. Die Medienindustrie

Abb. 16: *Anteil der Verbraucher, die Online-Einkäufe aus Sicherheitsgründen meiden (Europa 2007)*



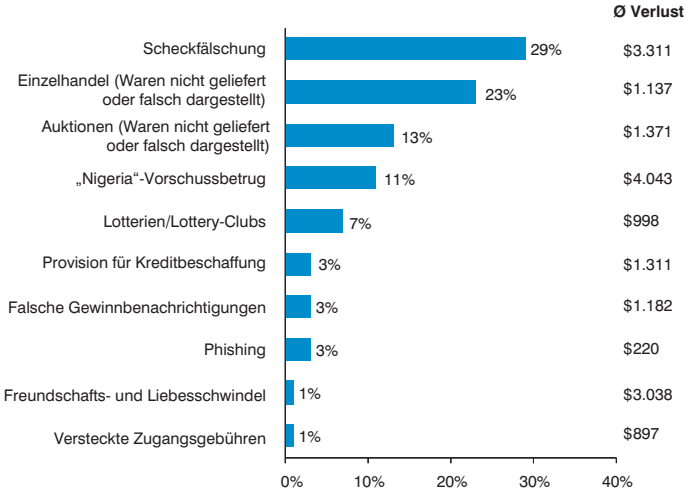
Quelle: Eurostat

Abb. 17: *Bekanntheitsgrad verschiedener Internet-Probleme (gestützte Umfrage, GB 2007)*



Quelle: Ofcom

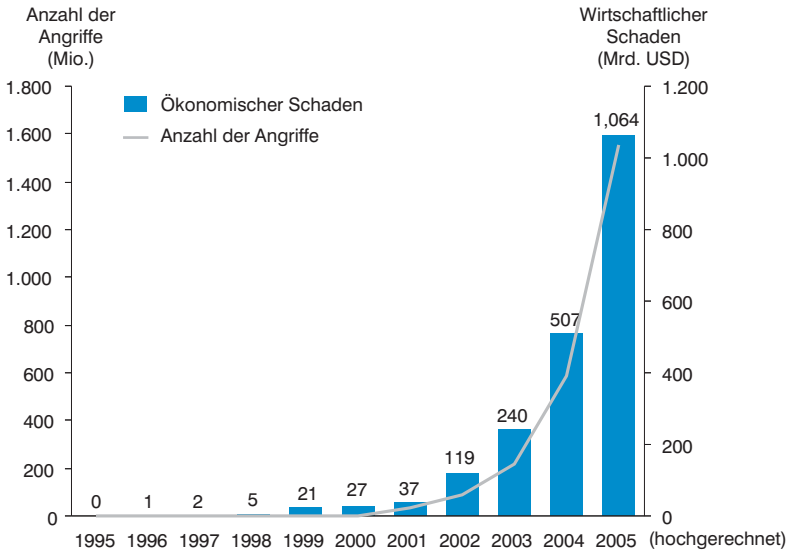
Abb. 18: *Die zehn häufigsten Formen von Internetbetrug (USA 2007)*



Quelle: NCL's Fraud Center

Hinweis zu „Auktionen": Im Herbst 2003 entfernte der Online-Riese eBay den Link zu „fraud.org" von seiner Website. Daraufhin sank die Anzahl der beim NCL Fraud Center eingehenden auktionsbezogenen Beschwerden auf einen Bruchteil.

Abb. 19: *Zunahme offener digitaler Angriffe (weltweit)*



Quelle: NCL Fraud Center, Congressional Research Service, mi2g, Craig Fosnock, Eurobarometer E-Communications Household Survey 2007, Symantec, McAfee, Booz & Company-Analyse

Als „offen" gelten alle Angriffe, die von der Öffentlichkeit bemerkt werden, z. B.:
- Angriffe, bei denen die Vertraulichkeit, Authentizität oder Integrität von Daten verletzt wird
- Angriffe, bei denen Netzwerksteuerungs- oder Admin-Systeme geschädigt werden

kämpft mit einer veralteten Rechtsprechung, die zudem unter der „unklaren" digitalen Rechtslage – beispielsweise beim Austausch von Copyright-geschützten Inhalten – noch weniger eingehalten wird. Die Unternehmen sind gefordert, Wege zu finden, aktiv für die Einhaltung des Copyrights im Internet zu sorgen und die junge Nutzergeneration darüber aufzuklären. „Born Digital" zu sein, ist keine Entschuldigung für gesetzwidriges Verhalten, aber eine mögliche Erklärung: Die Nutzer haben sich an das „Kostenlos-Prinzip" des Internets gewöhnt und gehen deshalb davon aus, jede Art von digitalem Content gebührenfrei abrufen zu dürfen.

Mittlerweile hat das Internet eine ganze „Underground-Economy" entstehen lassen, die den verschiedensten illegalen Aktivitäten ein Forum bietet. Hier kann man digitale „Produkte" wie E-Mail-Adressen und -Passwörter kaufen oder auch „Dienstleistungen" wie Spamming oder Bots – komplett mit Custom-Funktionen, die im anvisierten Unternehmen garantiert verheerende Schäden anrichten. Unternehmen haben die Bedrohung erkannt und beginnen, sich zu wehren. Microsoft beschäftigte im Januar 2008 allein 65 Ermittler und Rechtsanwälte, die nichts anderes tun, als Cyber-Kriminalität zu bekämpfen.

Um digitales Wachstum abzusichern, müssen die Verbraucher über Gefahren aufgeklärt werden und Informationen und Tools an die Hand bekommen, mit denen sie sie meistern können.

Insgesamt löst das heute erkennbare Risiko in der digitalen Welt sowohl bei Verbrauchern als auch bei Unternehmen Unsicherheiten aus, die das ungehinderte Wachstum des Internet- und Digitalmarkts bedrohen.

2. DIGITAL CONFIDENCE: KONZEPT UND ÜBERBLICK

Der Grad des Vertrauens, den sowohl traditionelle als auch „Born Digital"-Nutzer in die Branche setzen – Vertrauen in ihr Geschäftsver-

halten und die Sicherheit ihrer Dienstleistungen und Infrastruktur –, aber auch ihr Vertrauen in Gesetzgeber und Aufsichtsbehörden, Verbraucherschutzmaßnahmen wirksam durchzusetzen, entwickelt sich momentan zur wichtigsten Voraussetzung für die erfolgreiche Ausschöpfung des digitalen Wachstumspotenzials. Damit wird Digital Confidence ein zentraler Wachstumsfaktor – oder Wachstumskiller – für die digitale Wirtschaft und ist ein Maßstab, wie stark Verbraucher und Zulieferer den digitalen Anwendungen im weitesten Sinne „vertrauen", das heißt sie bedenkenlos anwenden.

Digital Confidence ist ein bedeutender Wachstumsmotor – oder Hemmschuh – für die Digital Economy.

Der Industrie wird immer stärker bewusst, wie wichtig es ist, im Bereich Digital Confidence vorausschauend aktiv zu werden. Sie hat teilweise damit begonnen. Doch es handelt sich um ein äußerst komplexes Feld mit vielen Akteuren, gekennzeichnet von gegensätzlichen Positionen und Interessen sowie verstreuten, bruchstückhaften Initiativen, mit denen lediglich auf öffentlich gewordene Vertrauenslücken reagiert wird, wie aktuell beispielsweise die Datenschutzdiskussion in Deutschland illustriert.

In Zukunft wird es für die Branche unvermeidbar sein, sich auf die Kernkriterien zu konzentrieren, die dem Verbraucher bei der Beurteilung neuer Digital- und Online-Dienstleistungen und -Plattformen besonders wichtig sind. Diese Kriterien für „digitales Vertrauen" wurden abgeleitet aus aktuellen Web-2.0-Regulierungs- und -Rechtssprechungsprozessen, Parlamentsdebatten, internationalen (Branchen-)Abkommen, Blogbeiträgen und Medienberichten.
Insgesamt erstrecken sie sich auf vier Bereiche:

- Netzintegrität und QoS.
- Datenschutz und Schutz der Privatsphäre.
- Minderjährigenschutz.
- Vermeidung von Piraterie und Diebstahl.

Diese vier Bereiche, die zusammen das im Rahmen dieser Studie entworfene Digital Confidence-Konzept ausmachen, müssen von proaktiven Maßnahmen ganzheitlich abgedeckt werden. Die Förderung von Digital Confidence geht über Corporate Responsibility und die Einhaltung von Gesetzen weit hinaus. Dabei entwickelt sie sich zunehmend zur wichtigen Erfolgsbedingung und „Licence to Operate". Wie einige unserer Fallstudien zeigen werden, schafft die Einhaltung bestehender Vorschriften allein noch keine Verbraucherakzeptanz.

Abb. 20: *Digital Confidence – die vier Säulen*

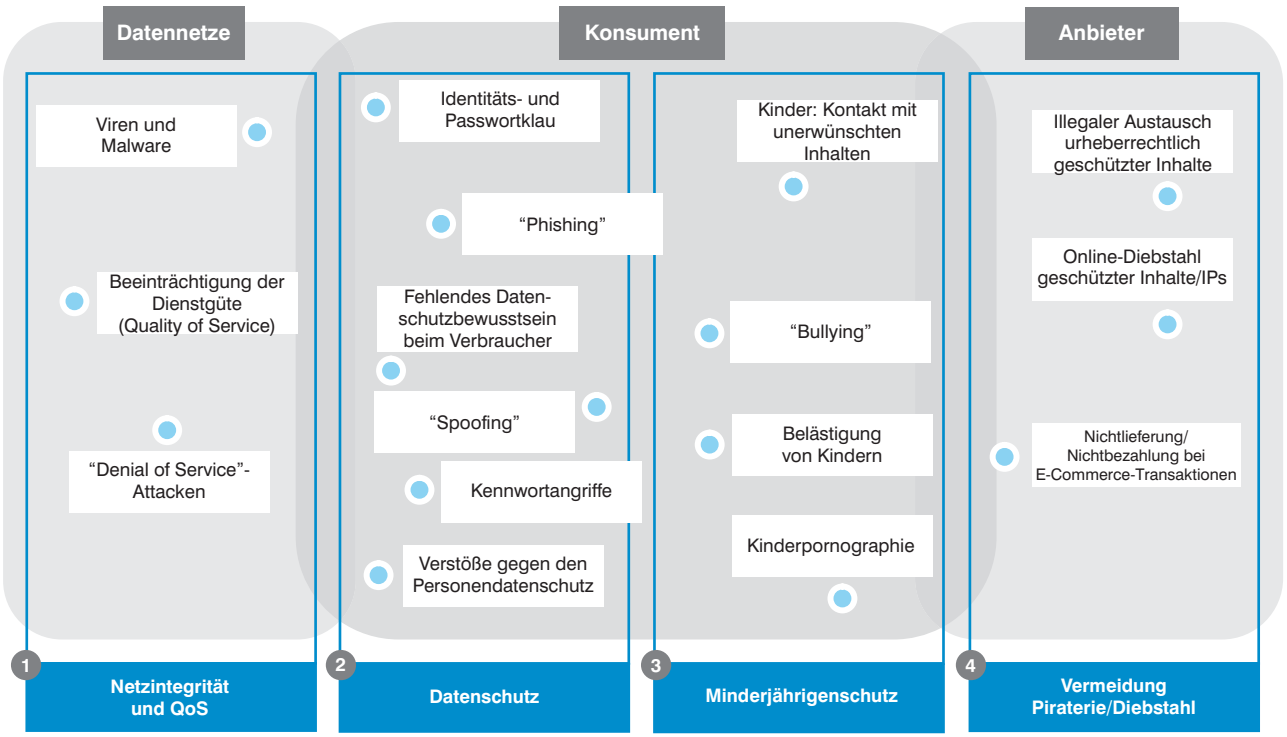
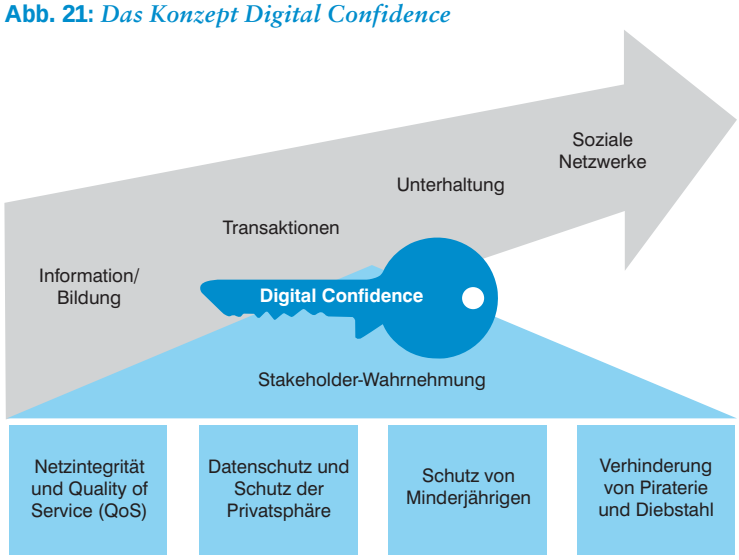


Abb. 21: *Das Konzept Digital Confidence*



Die vier Säulen der Digital Confidence decken alle Gefahren, Probleme und Bedrohungen ab, die heute relevant sind und die vom Verbraucher im Netz erlebt werden (siehe Abb. 21).
Der Bezugsrahmen strukturiert und identifiziert die Risiken, die angegangen werden müssen, und zeigt die Ziele von Digital Confidence in jedem der vier Felder:

- **Netzintegrität und Quality of Service (QoS):** Wie erhält man die Netzintegrität bei bösartigen Attacken aufrecht? Welche Netz-Management-Methoden ermöglichen ein garantiertes Kundenerlebnis? Faire Verteilung der Bandbreite in Spitzenzeiten, Traffic-Anstieg managen, Schutz vor Malware.

- **Datenschutz und Schutz der Privatsphäre:** Wie geht man mit Kundendaten online um und schützt sie? Vermeidung von Identitätsklau, versehentlichem Verlust persönlicher Daten und professionelle Datenverwertung.

- **Minderjährigenschutz:** Wie sorgt man für ein kindersicheres Netz? Schutz vor unerwünschten Inhalten, „Bullying“, Annäherungsversuchen und Kinderpornografie.

- **Vermeidung von Piraterie und Diebstahl:** Was tun gegen Copyright-Verstöße? Bekämpfung des Diebstahls von urheberrechtlich geschütztem Material und Sicherung von E-Commerce-Transaktionen.

In jedem der vier Bereiche gibt es verschiedene Stakeholder, die Digital Confidence beeinflussen oder davon beeinflusst werden.

Diese Studie präsentiert verschiedene Fallstudien zu Best Practices im Bereich Digital Confidence und destilliert daraus Handlungsanweisungen zur schnelleren Umsetzung proaktiver, industriegeführter Initiativen. Darüber hinaus will die Studie zur Diskussion um geeignete und angemessene Interventionsstufen sowie um Formen der Kooperation zwischen Wirtschaft und Politik beitragen – zur Förderung von Digital Confidence im Einklang mit den fundamentalen Freiheiten und den wirtschaftlichen Anforderungen des Internets.

*Soziale Netze fördern „Cyberbullying“: Seit ihrem Aufkommen werden 70% mehr Jugendliche schikaniert.**

*Quelle: Pew Internet & American Life Project

(2) Bei einer Denial-of-Service(DoS)-Attacke senden viele Computer Nachrichten an einen einzigen Zielserver und binden durch Überflutung mit Spams dessen Ressourcen. Das Zielsystem stürzt entweder ab oder wird unbrauchbar.

3. NETZINTEGRITÄT UND QUALITY OF SERVICE (QOS)

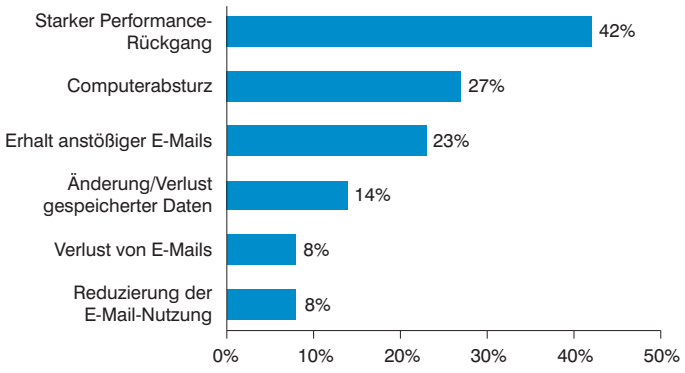
Dieser Bereich betrifft die Sicherung der dem digitalen Leben zugrundeliegenden Technologie-Plattformen und hat zwei Hauptthemen:

1. Sicherstellen einer integren, vor äußeren Angriffen geschützten Netz- und Rechnerumgebung für Verbraucher und Wirtschaft. Strategien gegen Störungen durch böswillige Online-Angriffe mit Viren, Malware (wie Spyware oder Trojaner, die Daten sammeln und vernichten) und Denial-of-Service-Attacken(2).

Spam belastet das Vertrauen in E-Mail: 18% der Verbraucher fühlen sich gestört.

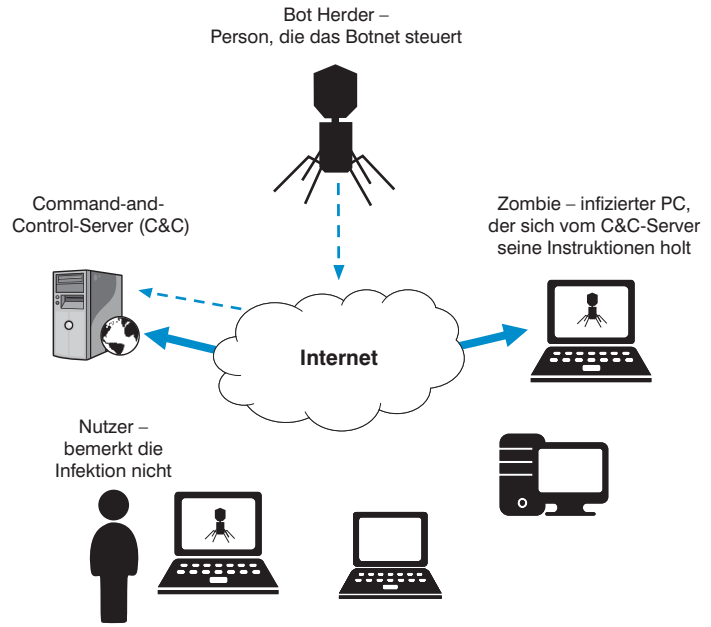
2. Sicherstellen, dass die Endverbraucher eine konsistente Dienstgüte (Quality of Service, QoS) erhalten. Absicherung des Netzes gegen steigende Datenströme, sodass das Nutzererlebnis selbst in Spitzenzeiten bei starker Ressourcenauslastung gleichbleibend und verlässlich gut ist.

Abb. 22: *Von Spam und Viren verursachte Probleme (GB 2007)*



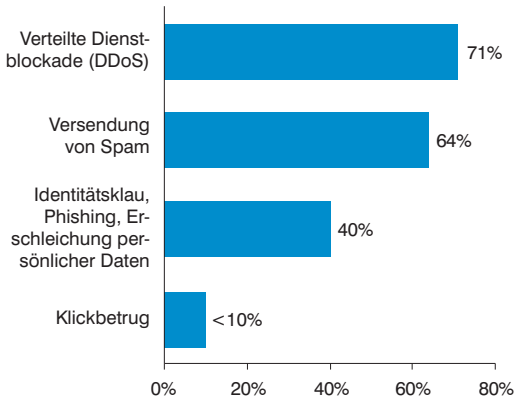
Quelle: Eurobarometer E-Communications Household Survey 2007

Abb. 23: *Botnets – der „Bot-Herder“und seine „Zombies“*



Quelle: WatchGuard

Abb. 24: *Nutzung von Botnets für Angriffe*



Quelle: Arbor

VIREN UND MALWARE

Viren und Malware stellen bösartige Attacken auf Endverbrauchergeräte und Local Area Networks dar und verursachen verschiedenste Probleme (siehe Abb. 22). Das Bewusstsein über ihre Auswirkungen schwankt deutlich je nach Grad der Internetnutzung. Länder mit starker Nutzung kennen und verstehen die Risiken besser und treffen stärkere Vorkehrungen gegen Atacken. Die skandinavischen Staaten und Benelux sind gute Beispiele hierfür: 35% der Nutzer geben an, schon einmal Opfer einer Spam- oder Virusattacke geworden zu sein. In Südeuropa ist das Risikobewusstsein hingegen weniger stark entwickelt: Nur 15% glauben, schon einmal Probleme gehabt zu haben. In den USA sagen 55% der Internet-User, dass Spam ihr Vertrauen in den E-Mail-Verkehr herabgesetzt hat und 18% sehen die Massenmails als „großes Problem“.

80% des weltweiten Spam kommt aus so genannten „Botnets“

Die häufigste Folge von Spam, Viren und Spyware sind Schäden an der Hardware. Wie die amerikanische „Consumers Union“ herausfand, tauschten in einem halben Jahr fast 1 Mio. US-Bürger wegen Spyware-Befall ihre Computer aus.

Mit wachsendem Bewusstsein für dieses spezielle Risiko sind Verbraucher anscheinend auch bereit, selbst etwas für die Abschottung ihrer Hardware gegen Viren und Spam zu tun. In der Tat beträgt der weltweite Markt für Sicherheits-Software inzwischen 9,1 Mrd. Dollar. Er wächst jedes Jahr um zirka 12%.

BOTS, ZOMBIES UND BOTNETS

Unter Bot versteht man eine Software zur „halbintelligenten“ Automatisierung bestimmter Aufgaben.[3] Solche Bots können auch in bösartiger Absicht eingesetzt werden: Der „Bot Herder“ (Bot-Hirte) steuert dann andere Computer, so genannte „Zombies“, die für den Angreifer alle möglichen Aufgaben übernehmen (siehe Abb. 23).

Botnets werden für viele Zwecke eingesetzt, von Spamming und Denial-of-Service(DoS)-Attacken über Phishing und Klickbetrug (Angriffe auf Werbetreibende im Netz, bei der Bots mehrere tausend Mal pro Stunde ein Werbemittel anklicken) und Identitätsklau (siehe Abb. 24).

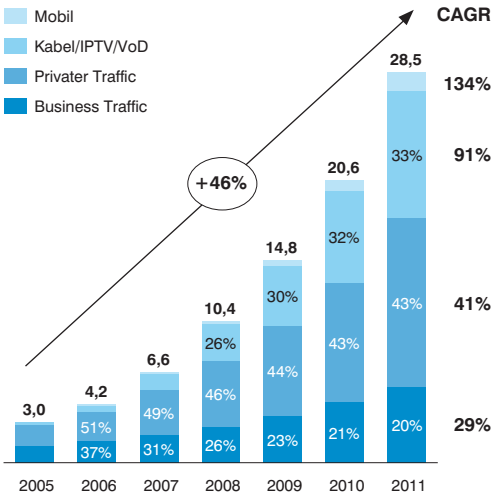
Die kombinierte Leistung tausender, meist über DSL vernetzter PCs kann gewaltige DoS-Lawinen auslösen. Botnets sorgen für schätzungsweise 80% des weltweiten Spams.

Als Botnet bezeichnet man die Gesamtheit aller Zombies unter einem „Bot Herder“. Bekannte Botnets sind:

- **Kraken:** Fast 500.000 Zombies, darunter infizierte PCs in 50 Fortune-500-Unternehmen, mit Antivirus-Software kaum zu entdecken.

(3) Bots sind Programme, die lokal ausgeführt werden, aber Instruktionen von einem externen Server erhalten. Der Bot erledigt die Aufgabe weitgehend autonom und wartet dann auf neue Anweisungen.

Abb. 25: *Wachstum des weltweiten IP-Traffics (2005–2011, Exabyte pro Monat)*



Quelle: Cisco

- **Srizbi:** Über 300.000 Zombies.
- **Storm**: Etwa 150.000 bis 200.000 Zombies.
- **Bobax:** Entweder Vorgänger von Kraken oder eigenes Botnet.

Nicht nur Konsumenten und Unternehmen fallen Botnets zum Opfer. Ganze Länder können zur Zielscheibe werden, wie eine DoS-Attacke auf Estland 2007 gezeigt hat. Angegriffen wurden das estnische Parlament, fast alle Staatsministerien, politische Parteien, drei der sechs großen Nachrichtenorganisationen des Landes, zwei der größten Banken sowie eine Reihe von Kommunikations-Firmen.

Netzintegrität und die Aufklärung Minderjähriger

Frankreich im Mai 2008: Die Polizei verhaftet 22 Personen, die im Verdacht stehen, einem internationalen Hacker-Ring anzugehören. Dass sechzehn der Verhafteten unter 18 sind, löst Bestürzung aus.

Die Sicherheitsexperten von Sophos gratulieren zum Fahndungserfolg. Aber sie fragen auch: „Was läuft bei der Erziehung falsch, wenn junge Leute der Ansicht sind, Hacker zu sein, sei völlig in Ordnung? Es muss mehr getan werden, damit Kinder schon in der Schule lernen, wie sie mit ihren PC-Kenntnissen verantwortungsvoll umgehen“.

QUALITY OF SERVICE

Sofern Quality-of-Service-Probleme mit dem Netz selbst zusammenhängen (QoS bezieht sich natürlich auf die gesamte End-to-End-Verbindung im Internet), beruhen sie auf zwei Faktoren: Allgemein steigende Traffic-Raten und die Spitzenauslastungen durch Power-User, die zur gleichen Zeit „bandbreitenhungrige“ Angebote nutzen.

Das Traffic-Volumen im Internet hat sich in den letzten Jahren besonders rasant entwickelt. Es ist zu erwarten, dass diese Tendenz in Zukunft anhält (siehe Abb. 25). Deshalb müssen Maßnahmen getroffen werden, mit denen die steigenden Datenströme durch Video on Demand, HDTV, Filesharing, private Videos und anderen datenintensiven Content, P2P und Online-Gaming bewältigt werden können, denn diese Anwendungen bilden den nächsten Wachstumsschub der digitalen Welt. In dieser Studie bezieht sich der Begriff „QoS“ ausschließlich auf IP-basierte Leistungen. Kabelanbieter sichern die Qualität ihrer Dienstleistung mit DVB-C und einem dedizierten Spektrum, das die Netzgeschwindigkeit nicht beeinträchtigt. In IP-Umgebungen ist das nicht so: Hier wirken sich (multiple) IPTV-Streams belastend auf die Breitband-Kapazität aus.

Power-User belasten die Qualität für alle Teilnehmer.

Ein weiterer Problempunkt sind die so genannten „Power-User“. Breitband-Netze sind, wie alle Netze, für bestimmte Spitzenbelastungen ausgelegt, wie sie in den Hauptnutzungszeiten zu erwarten sind. Power-User verursachen eine Überschreitung dieser Spitzenwerte. Ohne ein aktives Netz-Management müssten alle Endanwender Einbußen in der Servicequalität hinnehmen – wobei der Grad der Verschlechterung von der jeweiligen Applikation abhängt (zum Beispiel wäre Online-Banking von der Qualitätsverschlechterung weniger betroffen als beispielsweise ein MP3-Download). In DSL-Netzen, wo sich die Teilnehmer die Kapazität teilen müssen, würde sich dies in einer Verlangsamung oder im Extremfall in einer Serviceunterbrechung bemerkbar machen.

Um solche Auswirkungen zu vermeiden, können die Netzbetreiber entweder zusätzliche Kapazitäten schaffen (durch Aufbau neuer und Nachrüstung bestehender Infrastruktur über die regelmäßigen Netzupgrades hinaus), wodurch zusätzliche Investitions- und Fixkosten entstehen. Oder sie wenden aktives Traffic-Management an und reservieren so Bandbreite für bestimmte Anwendungen – zum Vorteil aller User.

Auf den ersten Blick scheint die Erweiterung der Kapazität die naheliegendste Lösung zu sein. Allerdings hat sie auch wirtschaftliche Nachteile. Wegen des raschen Anstiegs der Datenströme müssten die Anbieter ihre Netze ständig erweitern, die Kosten für die Nachrüstung würden mithin kontinuierlich steigen. Im Rahmen der Geschäftsmodelle der Netzanbieter sind diese Kosten aber an die Anwender weiterzugeben – höhere Endverbraucherpreise wären die Folge. Hinzu kommt, dass Kapazität allein das Problem der Serviceverschlechterung während Spitzenseiten nicht beseitigt. Je nach Internet-Anwendung, Dimensionierung des Netzes und Geschwindigkeit der Quellgeräte wird bei Spitzenauslastungen immer auf die gesamte Bandbreite zurückgegriffen, egal wie viele Kapazitäts-Upgrades der Netzanbieter vornimmt.

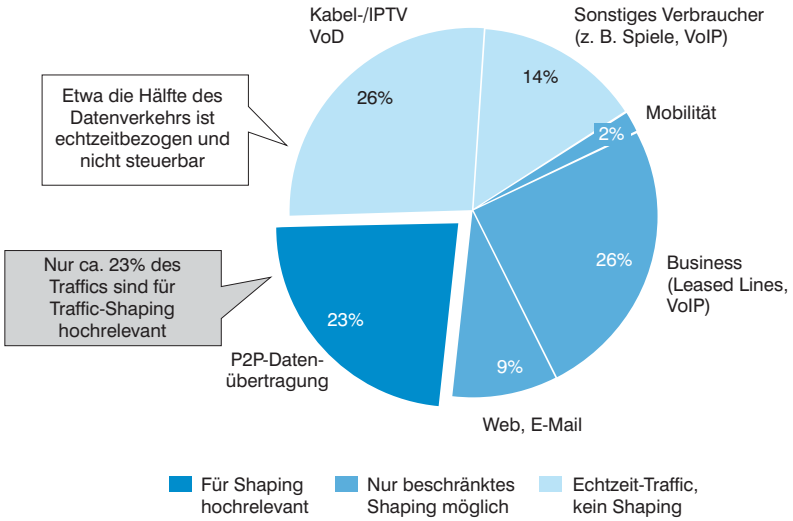
Um den Datenstau durch bandbreitenintensive Anwendungen in den Griff zu bekommen, setzen Netzbetreiber deshalb inzwischen Methoden des aktiven Traffic-Managements ein. Hier sind neben rein technischen Lösungen neuerdings auch nutzungsbezogene Gebühren in der Diskussion. Solche Preismodelle halten Nutzer davon ab, das Internet zu Spitzenzeiten zu verwenden.

Technikbasiertes Traffic-Management wird auch als Bandbreiten-Management oder „Traffic-Shaping“ bezeichnet. Aktives Traffic-Management ist in der Lage, weniger priorisierten, nicht echtzeitbezogenen Datenverkehr zu erkennen und ihm einen niedrigeren Status zuzuweisen. Durch Bandbreiten-Management verzögern sich nicht zeitgebundene Anwendungen (zum Beispiel ein Musikdownload von iTunes) ein wenig, zeitkritische Applikationen wie Musikstreams oder VoIP-Telephonie bleiben jedoch unberührt.

Dennoch: Aktives Traffic-Management kann nur Teil einer Lösung für den optimalen Datenfluss in Breitband-Netzen sein, denn Shaping-basierte Kontrollformen lassen sich ohne Störung der Nutzer nur auf nicht zeitkritischen Traffic anwenden. Und der macht nur ein Viertel bis maximal die Hälfte des gesamten IP-Traffics aus (siehe Abb. 26).

Die Tatsache, dass ein kleiner Teil von Internet-Usern einen unverhältnismäßig großen Teil des Netzverkehrs verursacht, ist in der Industrie schon seit längerem bekannt. Für die meisten Netzanbieter gilt, dass etwa 80% der Bandbreite von weniger als 10% der Nutzer verbraucht werden. Das bedeutet nicht nur ein Ungleichgewicht im „Fair Usage“, sondern verstärkt auch das Bandbreiten-Problem zu Zeiten der Spitzenauslastung. Die besonders hohen Volumina entstehen oft bei Peer-to-Peer- und Video-

Abb. 26: *Anwendbarkeit von Traffic-Shaping: Verteilung des weltweiten IP-Traffics 2008*



Quelle: Cisco, Booz & Company-Analyse

Applikationen, daher sind es vor allem diese beiden Nutzungsarten, bei denen Netzbetreiber Datenstaus befürchten. Ein Beispiel für den plötzlichen Anstieg des Transfervolumens durch Video-Streaming war die Einführung des BBC iPlayer.

Die Situation in Großbritannien nach dem iPlayer-Launch kann als typisch für das Bandbreiten-Dilemma innerhalb der Branche gelten. Über den iPlayer werden Radio- und Video-Inhalte der BBC im Internet vertrieben und abgespielt. Nach seiner offiziellen Einführung im Dezember 2007 wurden in den ersten 3 Monaten mehr als 42 Millionen Sendungen gestreamt oder heruntergeladen. Das beispiellose Datenaufkommen, das die Plattform damit generierte, führte zu heißen Debatten zwischen dem Betreiber BBC, mehreren Internetprovidern und der Regulierungsseite. Besorgt über den extremen Bandbreitenbedarf, verlangte eine Reihe von ISPs, dass die BBC nötig gewordene Netz-Upgrades teilweise mitfinanziert. Solche Forderungen wies der Sender als „reine Polemik“ zurück und warnte die ISPs ihrerseits, Inhalte nicht zu „stauchen, stutzen oder shapen“. Sonst würden die Contentprovider auf ihren Sites bald ausweisen, bei welchen ISPs ihr Content am besten läuft – und welche man meiden sollte.

Weniger als 10% der Nutzer erzeugen zirka 80% des Traffics.

Nach Schätzungen des britischen Regulierers Ofcom müssten die britischen Netzanbieter über 5 Jahre hinweg bis zu 831 Mio. £ in die Nachrüstung ihrer Infrastruktur investieren, um

Case-Study BBC iPlayer

Nach Daten des britischen ISPs Plusnet vom Februar 2008 schossen die Datentransfervolumen mit dem Launch des BBC iPlayer in die Höhe:

- Das Videostreaming pro Nutzer stieg von 180 MB im Dezember auf 292 MB im Januar: Eine Steigerung um 62%.
- Es gab 8-mal so viele Streams wie Downloads.
- Im gleichen Zeitraum verdreifachten sich die Kosten für Streaming-Traffic.

Dies könnte auf einen Trend hinweisen: Wenn Nutzer die Wahl zwischen einem hochauflösenden Streaming und Download haben, wählen sie ersteres, um nicht so lange warten zu müssen. Bei Musik verhält sich die Sache möglicherweise anders, schließlich möchten viele die Musik nach dem Herunterladen wirklich besitzen. Video wird aber lieber direkt online konsumiert.

Sollte dies tatsächlich der Trend sein, würde Traffic-Management immer weniger effektiv, denn gerade auf die zeitkritischen Streams lässt es sich nicht anwenden. Dann fiele die Hauptlast wieder dem Netzausbau zu.

die zusätzlichen 3 GB Datentraffic aufzufangen, die jeder iPlayer-User monatlich generiert. Für ISPs stellt sich die Frage, wer die Kosten für die Extraleistung letztendlich übernimmt: Der Dienstanbieter oder die Verbraucher? Im April 2008 gab die Behörde ihre Position zu diesem Problem bekannt. Laut Ofcom-Geschäftsführer Ed Richards ist „die Investitionslast von den Netzbetreibern und den Verbrauchern zu tragen, wobei schnellere Verbindungen vermutlich höhere Preise nach sich ziehen werden". Ofcom befürwortet in diesem Zusammenhang „Content-geleitete Tarifmodelle", bei denen ISPs und Contentprovider gemeinsam Services entwickeln, die im Netz reibungslos laufen – dies jedoch zu angemessenen Verbraucherpreisen.

Das Managen von Spitzenlasten ist der effektivste Weg, die Servicequalität für das Gros der Nutzer zu sichern.

Transfervolumina und Netzkapazitäten zu managen, bringt für den Endverbraucher sicherlich Vorteile, da er so die erwartete gleichbleibende Dienstqualität erhält. Doch das Anwachsen des Traffics aufgrund von datenintensiven Anwendungen wie Video on Demand erfordert zusätzliche Investitionen, die über höhere Preise, gestaffelte Zugangsprodukte oder klar differenzierte Methoden des Managements von Spitzenlasten mitfinanziert werden könnten. Letztlich wird über Traffic-Management-Techniken ein Ausgleich zwischen QoS-Anforderungen und Infrastruktur-Investments angestrebt, um die Steigerungen im Verbraucherpreis im Rahmen zu halten.

Mit der Migration von den heutigen DSL-Netzen auf Next-Generation-Netze mit deutlich höheren Kapazitäten wird die Bandbreitennachfrage auch bei zeitkritischen Anwendungen zumindest teilweise ausgeglichen. Im Bereich der nicht zeitgebundenen Dienste wird Traffic-Management aber nach wie vor eine Rolle spielen.

ACTIVE TRAFFIC MANAGEMENT IM ÜBERBLICK

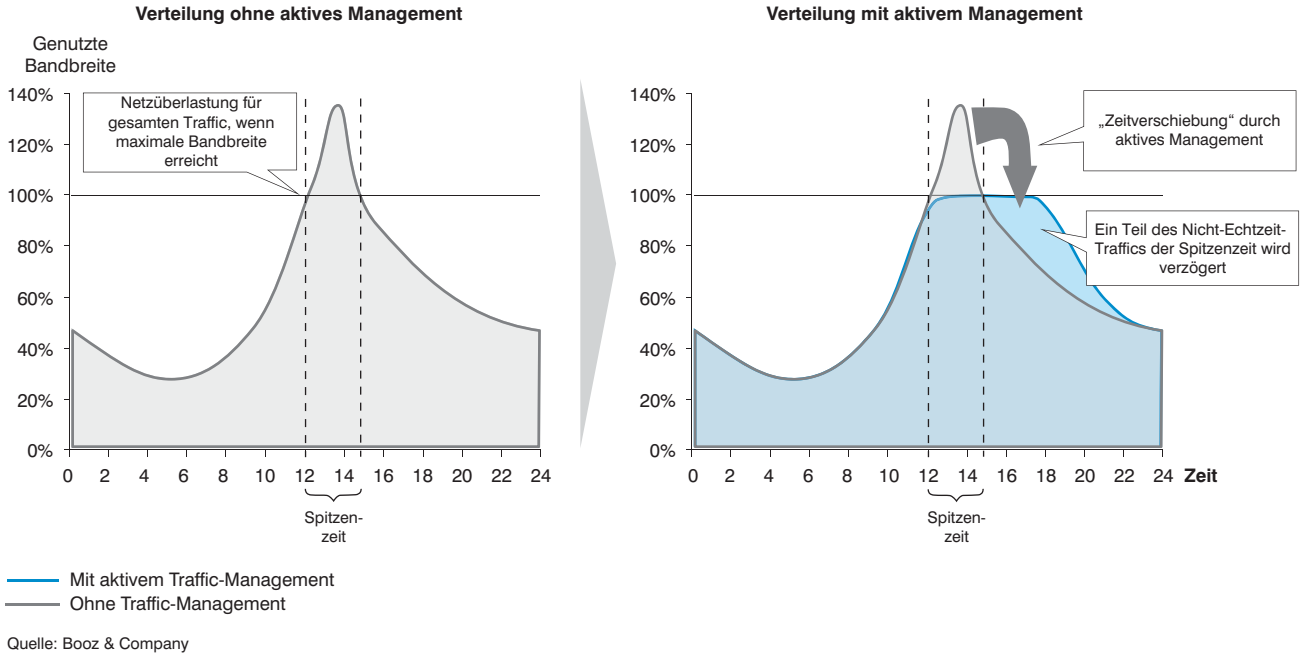
Für Netzbetreiber gibt es verschiedene technische Möglichkeiten, ihre Datenströme aktiv zu managen und so die Verfügbarkeit zu optimieren. Sie alle beruhen auf dem Prinzip, in Spitzenzeiten mehr Bandbreite für bestimmte Services frei zu machen. Das Management teilt sich in zwei Phasen: 1) Identifizierung von „formbarem" Traffic und 2) Herabstufung seiner Priorität und Verringerung der damit belegten Bandbreite.

TRAFFIC-ERKENNUNG UND -PRIORISIERUNG

Es gibt verschiedene Verfahren, den für „Shaping" geeigneten Traffic zu identifizieren (Siehe Abb. 28). Eine einfache Methode stützt sich lediglich auf Quell- und Ziel-IP-Adressen oder Ports, etwa um eine faire Einhaltung von Volumengrenzen zu erzwingen. Doch diese Art der Identifizierung ist nicht sehr spezifisch: Es werden große Traffic-Blöcke ausgewählt, die mehrere Anwendungen gleichzeitig beeinträchtigen können (zum Beispiel, wenn mehrere Systeme denselben Port verwenden).

Einen weit aufwändigeren Ansatz stellt die so genannte „Deep Packet Inspection" (DPI) dar. Hierbei wird jedes IP-Paket gescannt, sein zugrundeliegendes Protokoll identifiziert und eine Signatur erstellt. Sie kann anschließend mit einer Liste bekannter Signaturen abgeglichen werden, sodass das Paket klassifiziert werden kann – zum Beispiel als Teil eines „Video on

Abb. 27: *Traffic-Management im Überblick*



Quelle: Booz & Company

Demand"-Streams. Anhand dieser Identifizierung lassen sich gezielt Protokolle und sogar ausgewählte Services für Traffic-Shaping auswählen (beziehungsweise, bei Echtzeit-Traffic, davon ausschließen). Ein kritischer Aspekt von DPI bleibt die nötige Pflege und häufige Aktualisierung der Signatur-Datenbanken aufgrund der schnell wachsenden Internet-Architektur.

Doch der größte Nachteil von DPI sind die Kosten: Da jedes einzelne Paket inspiziert werden muss, sind die technischen Anforderungen hoch. Viele Systeme wenden daher ein Hybridmodell an, bei dem der Traffic nach IP-Adresse und Port vorgefiltert wird und nur ausgewählte Pakete der DPI unterzogen werden.

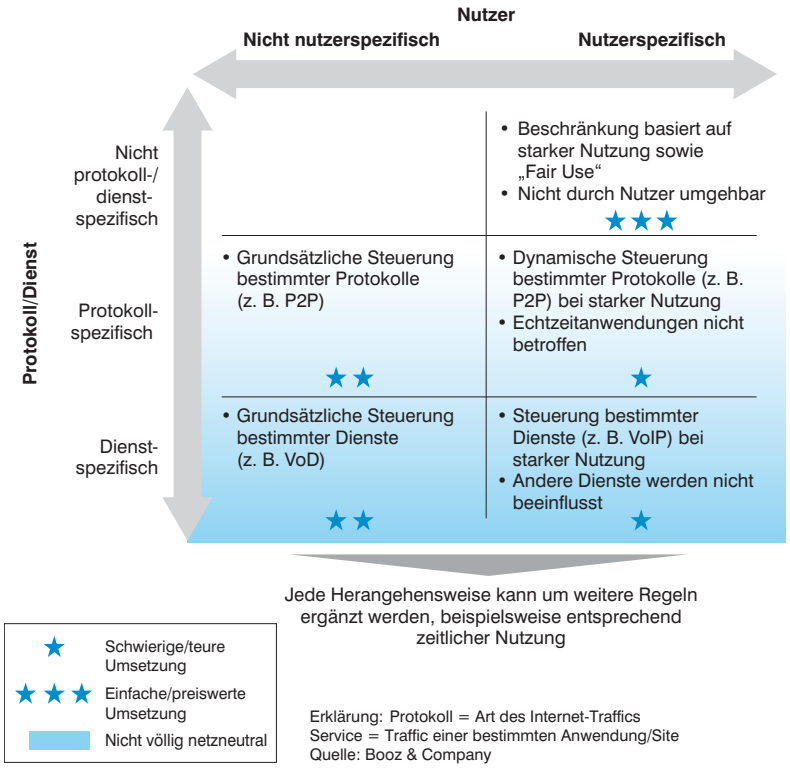
Die Traffic-Identifizierung kann demnach Nutzer-spezifisch erfolgen (über die IP-Adresse), Protokoll-spezifisch (durch Auswahl von Ports oder bei DPI zum Beispiel über das Mail-Protokoll) und/oder Service-spezifisch, also bezogen auf bestimmte Online-Dienste oder Anwendungen (etwa YouTube oder BitTorrent), erfolgen.

TRAFFIC-PRIORISIERUNG

Es gibt unterschiedliche Verfahren, die Priorität von Daten, und damit die Bandbreite, die sie belegen, zu senken. Einige können in jedem IP-Netz eingesetzt werden, während andere auf bestimmte Netze zugeschnitten sind. „Packet Cable Multimedia" (PCMM) beispielsweise ist eine spezifische QoS-Lösung nur für Kabelnetze.

Alle Techniken basieren auf der Verlangsamung des ausgewählten Traffics und reduzieren so den Datenfluss. In der Anwenderperspektive führt das Management von nicht zeitkritischem Datenverkehr höchstens zur Verlangsamung längerer Downloads. E-Mail und Browsing sind nicht betroffen.

Abb. 28: *Die Traffic-Shaping-Toolbox: Welcher Steuerungsmechanismus?*



Erklärung: Protokoll = Art des Internet-Traffics
Service = Traffic einer bestimmten Anwendung/Site
Quelle: Booz & Company

4. DATENSCHUTZ

Der Bereich Datenschutz befasst sich mit den Sicherheitsbefürchtungen von Personen im Bezug auf ihre digitalen Daten. Hier geht es um vier Ziele:

1. Verhindern, dass persönliche Daten öffentlich gemacht werden, ob versehentlich oder bewusst durch Verbraucher selbst (zum Beispiel in sozialen Netzen), durch Hacking oder durch sorglosen, nicht sicheren Datentransfer.

*Über jeden Bürger sind durchschnittlich 36 GB Daten bei Institutionen gespeichert. Das entspricht 80 Stunden Video oder 1 Million Seiten Text.**

2. Verhindern, dass persönliche Daten ohne Zustimmung kommerziell verwertet werden, etwa wenn in neuen marketingorientierten Geschäftsmodellen Informationen zu Personenstand oder Familie zur Generierung personalisierter Online-Werbung genutzt werden.

3. Schutz persönlicher Daten vor illegalen Zugriffen beispielsweise durch Spoofing und Phishing.

4. Verhinderung von Identitätsklau und Online-Betrug, also die Replizierung persönlicher Daten durch Kriminelle, um Geld oder andere Vorteile zu erlangen.

Datenschutz zielt im Wesentlichen auf zwei Bereiche: Erstens die unbeabsichtigte Veröffentlichung und zweitens die illegale Erlangung von Daten mit Methoden wie Phishing.

Virtuelle Realität: Auch im Second Life kann man auf Abwege geraten

2008 berichtete in Deutschland die Mutter eines 13-jährigen Mädchens von dessen plötzlichem Interesse an „Second Life“, einem Portal, in dem Besucher sich eine virtuelle Identität zulegen und ein neues, virtuelles Leben aufbauen können.

Das Mädchen bat seine Mutter um Geld, um „Linden-Dollars“, die Währung von Second Life, zu kaufen. Die Mutter verweigerte jede Unterstützung.

Erst Monate später fand sie heraus, dass sich ihre Tochter in einem „Erwachsenen-Club“ in Second Life zunächst als Stripperin und dann als virtuelle Prostituierte betätigt hatte. Sie wollte Linden-Dollars verdienen.

VERÖFFENTLICHUNG VON PERSONENDATEN

Im Internet ist eine starke Zunahme so genannter Social-Networking-Sites zu beobachten. Sie richten sich entweder an allgemeine Zielgruppen (wie Facebook) oder an Berufstätige (wie z. B. LinkedIn oder Xing). Solche Webseiten erfordern, speichern und publizieren immer größere Mengen von Nutzer-Informationen wie zum Beispiel Wohnort, Alter, Interessen oder Fotos. Zwar bieten die meisten eine Möglichkeit, den Zugriff auf die persönlichen Profile zu beschränken, doch in der Realität gibt die Hälfte der User sie uneingeschränkt frei. Auch viele andere Webseiten verlangen eine Anmeldung vor der Nutzung (Webmail-Portale) oder um alle Features nutzen zu können (viele Foren). Auch sie sammeln Nutzer- und Nutzungsdaten über ihre Besucher.

Missouri, USA, Mai 2008: „Cyberbullying“ könnte nach Selbstmord zum Straftatbestand werden

Nach dem Selbstmord einer 13-Jährigen, die von der Mutter eines Jungen aus ihrer Nachbarschaft online schikaniert worden war, wurde nun ein Gesetz vorgelegt, das „Cyberbullying“ hart bestraft – mit bis zu 2 Jahren Gefängnis.

Allerdings halten es viele für schwierig, zwischen einer Belästigung und „normalen“ Verhaltensweisen und Scherzen unter Jugendlichen zu unterscheiden. Auch die Methoden der Strafverfolgung werden kritisch gesehen.

Die Preisgabe solcher Informationen kann die persönliche Sicherheit gefährden und rufschädigend sein – man denke an die Gefahr des ID-Betrugs oder an Unternehmen, die die Angaben in Bewerbungen auf sozialen Netzen überprüfen oder in Online-Businessclubs nach passenden Kandidaten suchen. Sind die Daten erst einmal ins Netz gelangt, lassen sie sich kaum noch zurückziehen, da sie sich so einfach kopieren, verbreiten und abspeichern

*Internet-User wissen, dass sie Spuren im Netz hinterlassen: 47% „googeln“ nach Informationen über sich selbst. Doch 60% beunruhigt die Masse persönlicher Daten im Web nicht.***

* Quelle: IDC

**Quelle: Pew Internet & American Life Project

lassen. Neben den Verbrauchern selbst stellen auch Unternehmen ein Datenschutz-Risiko dar. Schon deshalb, weil sich digital gespeicherte Informationen bequemer verwalten, handhaben und austauschen lassen. Gleichzeitig ist auch die Gefahr der unbeabsichtigten Veröffentlichung ungleich höher, wie ein jüngster Fall in Großbritannien zeigt: Die britische Steuerbehörde musste sich bei den Kunden der Investmentbank UBS Laing & Cruickshank entschuldigen, nachdem vertrauliche Daten abhanden gekommen waren. Die Behörde hatte eine von der Bank übersandte CD-Rom verloren, die Adressen und Kontodaten von privaten Anlegern in staatlich geförderte Equity-Programme enthielt. Es handelte sich um den Fehler eines Mitarbeiters. Der Vorfall zeigt, wie real und wie hoch das Risiko ist.

*Selbst die CIA nutzt Facebook zur Rekrutierung neuer Mitarbeiter.****

Daneben lassen sich die umfassenden Kundendaten der Unternehmen aber auch auf ganz legale Weise verwerten. Ein so genannter „Customer Insight Superserver" wie der amerikanische Medienkonzern Meredith verkauft Auszüge seiner Datenbank mit Informationen über 85 Millionen US-Bürger – 6 von 10 Frauen und 8 von 10 Haushalten. Meredith hat inzwischen eigene Agenturen für Online-Werbung, die die wertvollen Informationen für Targeted Advertising verwerten.

PHISHING

Phishing-Attacken sind die häufigste Methode, illegal an persönliche Daten zu gelangen. Dazu geben sich die Täter als vertrauenswürdige Instanz aus, um dann sensible Informationen wie Namen, Passwörter und Kreditkartendaten auszuspähen. Die Opfer sind Endverbraucher. Die meisten Angriffe (über 65%) ahmen das Erscheinungsbild von E-Commerce-Sites wie eBay und PayPal nach.

Phishing ist die verbreitetste Methode, um an private Daten zu gelangen. 65% der Angriffe ahmen große E-Commerce-Sites nach.

Die Industrie sieht inzwischen Grund zur Besorgnis. Jeder erfolgreiche Angriff führt im Schnitt zu einem Verlust von 220 Dollar für die jeweilige Person. Und das Problem breitet sich rasant aus: 2007 wurden Monat für Monat 30.000 neue Phishing-Sites identifiziert.

Datenschutz-Probleme zu bewältigen, wird allerdings immer schwieriger, da viele unterschiedliche Organisationen – von Unternehmen (Banken, Einzelhandel) über Behörden bis hin zu sozialen Netzen – Personendaten in digitaler Form besitzen.

Außerdem ist die Definition von „persönlichen Daten" ein dynamisches Problem, das mit fortschreitender Technologisierung neu überdacht werden muss (zum Beispiel wird momentan heftig diskutiert, ob die IP-Adresse zu den persönlichen Daten gehört oder nicht). Ein weiterer wichtiger Punkt ist, auf welche Weise die Zustimmung zum Austausch der Daten gegeben werden kann. Hier werden zwei Methoden diskutiert: „Opt-in" und „Opt-out". Erstere erfordert eine aktive Bestätigung des Nutzers, dass er der Verwendung zustimmt. Die „Opt-out"-

Jeden Monat werden 30.000 neue Phishing-Sites entdeckt. Erfolgreiche Attacken kosten das Opfer im Schnitt 220 Dollar.

***Quelle: Wired 2007

Phishing: Prinzip und häufigste Verfahren

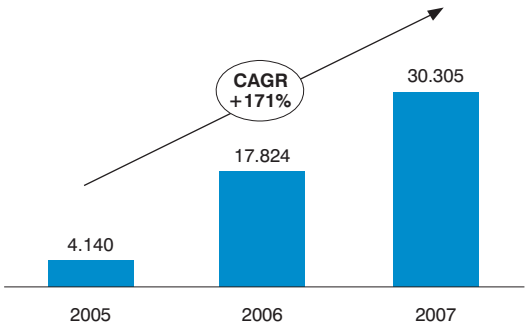
Phishing beginnt meist mit einer gefälschten E-Mail. Ihre Blockierung durch Spamfilter in Mail-Clients ist ziemlich effektiv, funktioniert aber nicht immer.

Früher waren Phishing-Mails leicht zu durchschauen – schlecht gemacht und voller Text- und Rechtschreibfehler. Inzwischen ist das Niveau stark gestiegen: Auch für erfahrene User sind die Nachrichten auf den ersten Blick kaum zu unterscheiden.

Die Hauptverfahren des Phishing sind:

- **Link-Manipulierung,** zum Beispiel „g00gle.com".
- **Website-Fälschung:** Die Seite sieht aus wie das Original, manchmal sogar die Adresse (möglich durch Lücken in der Browsersicherheit).

Abb. 29: *Durchschnittliche Anzahl neuer Phishing-Sites pro Monat (weltweit)*



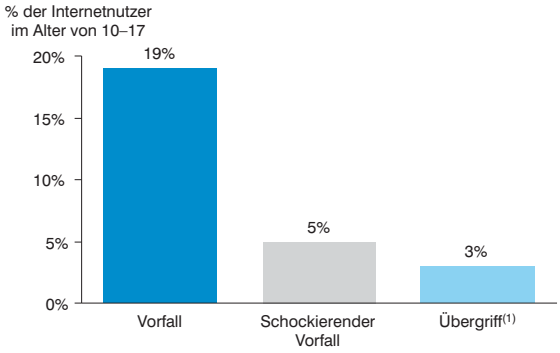
Quelle: PhishTank, APWG, NLC Fraud Center

Piraterie und Privatsphäre

USA, Mai 2008: Das Walter Reed Army Hospital veröffentlicht durch einen Sicherheitfehler Personendaten von über 1.000 Patienten. Die Daten befanden sich in einer einzigen Datei, die irrtümlich in einem Peer-toPeer(P2P)-System gepostet wurde.

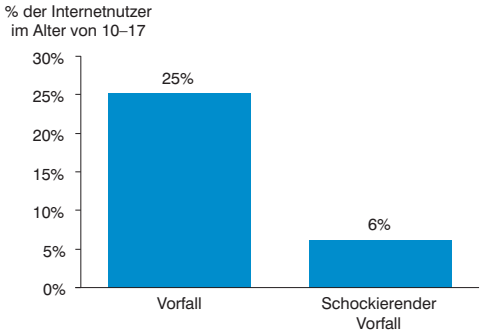
Es ist nicht die erste Sicherheitsverletzung durch Filesharing in P2P-Netzen, siehe ABN Amro und Pfizer. Auch wenn die meisten Unternehmen P2P strikt verbieten, sind sich einige Anwender des Risikos offenbar nicht bewusst.

Abb. 30: *Online-Belästigung von Kindern (USA 2006)*



(1) Als „Übergriff" gelten Versuche, nicht nur online, sondern auch per Telefon/Post oder persönlich mit dem Kind in Kontakt zu treten.
Quelle: Crimes Against Children Research Centre

Abb. 31: *Ungewollter Kontakt mit pornografischen Inhalten (USA 2006)*



Quelle: Crimes Against Children Research Centre

Methode ist bei Nutzern weniger beliebt, denn sie setzt voraus, dass die Erlaubnis als erteilt gilt, bis der Nutzer sie ausdrücklich entzieht. Dabei ist nicht immer klar, ob es überhaupt eine Wahlmöglichkeit gibt und wenn, wie man die Absage erteilen kann. Höhere Transparenz kann bei vielen Problemen bezüglich der Opt-in-/Opt-out-Alternative Abhilfe schaffen.

Bei einigen Formen der illegalen Datenerschleichung wie Phishing ist es relativ leicht festzustellen, dass eine Straftat begangen wurde. Doch sein grenzüberschreitender Charakter macht es schwierig, dieses Delikt zu überwachen und strafrechtlich zu verfolgen. Phishing-Attacken werden meist von Kriminellen verübt, die in einem anderen Land als das Opfer leben, während die betroffene Hardware sich oft in einem Drittland mit lockerer Datenschutzgesetzgebung befindet. Das macht es für die Polizei fast unmöglich, die Täter aufgrund lokaler Gesetzgebung zu verfolgen.

5. MINDERJÄHRIGENSCHUTZ

Minderjährigenschutz dient der Bewahrung junger Internet-User vor Online-Angriffen. Seine vier Hauptziele:

1. Schutz der Kinder vor unerwünschten Inhalten: Dies umfasst von der Darstellung von Sexualität und Gewalt bis zur Verführung Minderjähriger alle Inhalte, vor denen Eltern und Gesellschaft die Kinder schützen wollen (zum Beispiel Pornografie).

2. Verhinderung von „Bullying" und Schikanierung: Darunter versteht man Gewalttätigkeiten gegenüber Minderjährigen durch Peers oder Peer-Gruppen (zum Beispiel Onlinestellung von Prügel-Videos oder erniedrigenden Fotos).

3. Verhinderung von Online-Annäherungsversuchen („Grooming"): Wenn Erwachsene in Online-Umgebungen (zum Beispiel Chatrooms, sozialen Netzen) in böswilliger Absicht Beziehungen zu Kindern aufbauen.

4. Bekämpfung von Kinderpornografie: Beinhaltet sexuellen Missbrauch von Kindern in pornografischem Material (Foto, Video) und umfasst drei Handlungsfelder: a) Verfolgung der Konsumenten von Kinderpornografie, b) Verfolgung der Produzenten und Entfernung des Contents und c) Verhinderung des zufälligen Kontakts mit Kinderpornografie im Netz.

Der Beschäftigung mit dem Thema Minderjährigenschutz kommt eine besonders wichtige Funktion zu, denn es handelt sich wohl um den emotional am stärksten besetzten Bereich von Digital Confidence.

Minderjährigenschutz tut Not: 20% der britischen Jugendlichen waren online Annäherungsversuchen ausgesetzt, 25% obszönem Material.

Gleichzeitig ist die Bedrohung sehr real: 20% aller Jugendlichen waren schon einmal Annäherungsversuchen im Internet ausgesetzt und 25% sind mit obszönem Material in Kontakt gekommen (siehe Abb. 30 und 31). Im Juni 2008 veröffentlichte der Sydney Morning Herald im Zusammenhang mit einer Razzia unter Kinderpornografie-Konsumenten bestürzende Zahlen: 99 Bilder, die ein Hacker in eine „vertrauenswürdige europäische Website" eingeschmuggelt hatte, erhielten „in nur 76 Stunden unglaubliche 12 Millionen Hits, nachdem Pädophilen-Netze im Internet von der Existenz der Fotos erfahren und die URL verbreitet hatten".

Allerdings gibt es für die Industrie eine Reihe von Hürden bei der Bekämpfung. Viele Eltern stehen der Online-Welt unwissend gegenüber und sind sich der Fülle unerwünschter Inhalte ebenso wenig bewusst wie der Durchtriebenheit von Online-Praktiken wie Grooming und Bullying. Sie unternehmen daher nichts, um ihre Kinder zu überwachen und schützen, während diese online sind, was besonders dann nötig ist, wenn Pädophile in sozialen Netzen unterwegs sind.

*32% der Teenager in den USA haben schon erlebt, dass private Daten ohne ihre Einwilligung weiterverbreitet wurden.**

Darin liegt ein weiteres Problem der Bewältigung: Allzu häufig hängen die Risiken eng mit den reichhaltigen Funktionen der sozialen Netze, der Anonymität der Online-Welt und der Möglichkeit der Identitätsverschleierung zusammen. Genau genommen tragen also die Anbieter besonders reichhaltiger digitaler Welten selbst dazu bei, dass unerwünschte Aktivitäten auftreten und die Zukunftsfähigkeit des Internets bedrohen.

Um die Probleme im Zusammenhang mit dem Minderjährigenschutz anzugehen, müssen sie zunächst identifiziert und definiert werden. Jeder Stakeholder wird zustimmen, dass Kinderpornografie inakzeptabel ist und auf jeden Fall verhindert werden muss. Hinter der Frage steckt aber noch eine Menge Diskussionsbedarf, etwa Meinungsverschiedenheiten darüber, welche Inhalte für Minderjährige noch geeignet sind und welche auf jeden Fall verboten gehören – und dies alles vor dem Hintergrund der anhaltenden Debatte über die Gefährdung der freien Meinungsäußerung und Persönlichkeitsrechte.

6. VERMEIDUNG VON PIRATERIE UND DIEBSTAHL

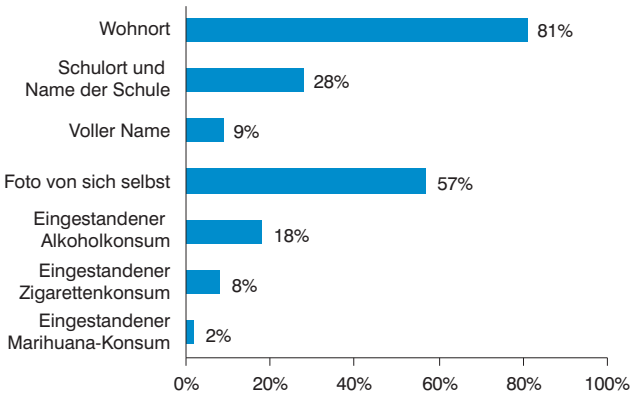
Durch Verhinderung von Piraterie und Diebstahl soll eine sichere Geschäftsumgebung für alle Beteiligten der digitalen Wirtschaft entstehen. Die beiden wesentlichen Ziele sind:

1. Bekämpfung des unerlaubten Austauschs von urheberrechtlich geschütztem Material – besonders der Austausch über Peer-to-Peer-Netze und ähnliche Anwendungen.

2. Schutz von E-Commerce-Transaktionen: Sicherstellen, dass die Beteiligten sich an allgemeine Geschäftspraktiken halten, also pünktlich zahlen und ordnungsgemäß liefern.

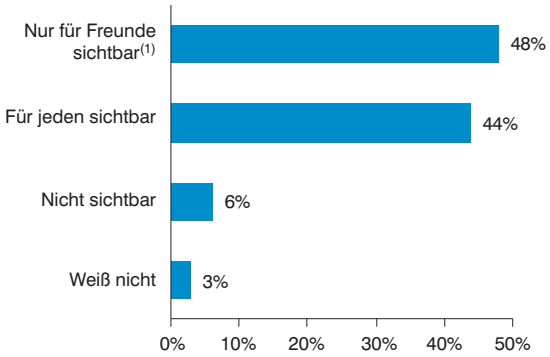
Für Unternehmen und Contentprovider ist das Vorhandensein von sicheren Vertriebsumgebungen eine der wichtigsten Voraussetzungen für die Produktion und Verfügbarkeit von Online-Content und das Entstehen von neuen, nachhaltig tragfähigen Online-Geschäftsmodellen. Daneben müssen E-Commerce-Plattformen wirksam vor Nichtzahlern und Nichtlieferungen geschützt werden. E-Commerce Anbieter müssen sicher

Abb. 32: *Profildaten junger Nutzer von sozialen Netzwerken (GB 2007)*



Quelle: Ofcom

Abb. 33: *Sichtbarkeit von Profilen in sozialen Netzwerken (GB 2007)*



(1) Bei sozialen Netzwerken sind „Freunde" alle zu einer „Freundesliste" hinzugefügten Personen. Es muss sich also weder um echte Freunde handeln noch um die Personen, für die sie sich ausgeben
Quelle: Ofcom

*Quelle: Pew Internet & American Life Project

Piraterie und Netzintegrität

Anfang 2007 wurde in Japans beliebtester Online-Tauschbörse „Winny“ ein ungewöhnliches und zerstörerisches Virus freigesetzt. Der Trojaner, der sich über die Anwender lustig machte, ihnen mit Polizei oder gar mit Mord drohte, löschte verschiedene Dateiformate und ersetzte sie durch populäre Comicfiguren, die vor den Gefahren von P2P warnten.

Ironie des Falles: In Japan ist das Schreiben von Viren nicht gesetzlich verboten. Der Autor des Trojaners, ein japanischer Student, wurde aber wegen Copyright-Verletzung verklagt, denn er hatte keine Genehmigung, die Comicfiguren in seine Malware einzubauen.

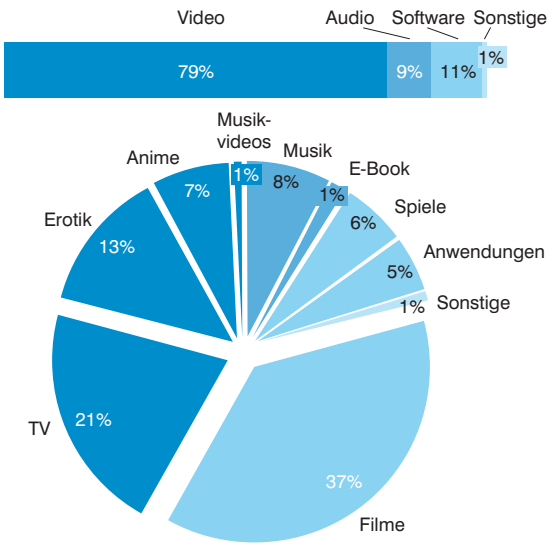
sein, dass Privat- und Geschäftskunden sich wie in der „Offline-Welt“ an bestimmte Geschäftspraktiken halten. Andererseits haben Privatkunden ein starkes Interesse daran, nicht durch die Nutzung von Anwendungen kriminalisiert zu werden, die ihnen über ihre Breitband-Leitung zugänglich sind, beispielweise beim Filesharing über ein P2P-System.

ONLINE-PIRATERIE: FILESHARING VON PEER ZU PEER

Mit dem Anwachsen der verfügbaren Bandbreiten und der zunehmenden Digitalisierung von Inhalten ist der Austausch von Content immer einfacher geworden. Seit den Zeiten von „Napster“ sind dutzende neue Filesharing-Systeme entstanden, die zum größten Teil P2P für die Verbreitung von Inhalten einsetzen.

*Quelle: Pew Internet & American Life Project

Abb. 34: *Verteilung von P2P-Content (Deutschland 2007)*



Quelle: ipoque

Heute machen P2P-Daten je nach Region zwischen 30 und über 60% des gesamten Internet-Traffics aus. In den Anfängen waren es vor allem Musikdateien, die ausgetauscht wurden, aber seit der Entwicklung von DSL wurde auch das Sharing von Bewegtbildern immer einfacher möglich. Heute macht Video 80% des Gesamtvolumens aus (siehe Abb. 34). Da sich die kommerziellen Angebote für P2P-Content-Distribution langsamer als erwartet entwickelten, wird allgemein angenommen, dass die meisten ausgetauschten Inhalte geschützt sind und das Hoch- und Herunterladen widerrechtlich geschieht.

*Filesharing ist für Rechteinhaber ein echtes Problem: In Deutschland entstehen 50% des Datenvolumens durch Peer-to-Peer-Traffic.**

Dass der IP-Traffic gerade durch P2P-Lösungen exponentiell anwächst, macht das Piraterie-Problem zum bestimmenden Faktor bei der Entwicklung innovativer Geschäftsmodelle und für die Entstehung künftiger digitaler und Online-Content-Angebote. Angesichts der aktuell aufkommenden Breitband-Produkte mit bis zu über 100 Mbit/s ist davon auszugehen, dass P2P-Traffic (legal und illegal) den größten Beitrag zum Anstieg der Datenströme leisten wird.

Um den Rechteinhabern zu ermöglichen, ihren digitalen Content effektiv zu schützen, wurde eine Reihe von Maßnahmen umgesetzt – mit unterschiedlichem Erfolg und öffentlichem Echo. Die digitale Rechteverwaltung DRM beispielsweise geriet wegen nicht transparenter Nutzerrechte in die Kritik von Politikern und Verbraucherschutzorganisationen. Die ISPs gerieten unter Druck, vorbeugende Maßnahmen gegen Copyright-Verletzungen zu treffen. Aufgrund des langjährigen Rechtsprinzips, das sie als „reine Durchleiter“ einstuft, sind Netzbetreiber und ISPs nicht verpflichtet, die Internet-Nutzung ihrer Kunden oder die im Netz ausgetauschten Inhalte zu überwachen. Es ist jedoch zu beobachten, dass Netzbetreiber und Internetprovider immer stärker freiwillige Verhaltenskodizes und Awareness-Kampagnen einsetzen, um Aufmerksamkeit zu erzeugen und den Sinn für die Werthaltigkeit intellektuellen Eigentums zu stärken – insbesondere bei der „Born Digital“-Generation, die davon ausgeht, dass Online-Content immer kostenlos sein sollte. Solche Kampagnen und Verhaltensweisen werden auch im Rahmen nationaler (Ko-)Regulierungsinitiativen diskutiert.

Zu den möglichen Maßnahmen gehören unter anderem: Die Überwachung durch Traffic-In-

P2P mit BitTorrent

BitTorrent ist ein weit verbreitetes, echtes P2P-Protokoll für den Austausch von Dateien. BitTorrent benötigt keinen zentralen Download-Server, als Koordinationspunkt fungiert lediglich ein „Tracker“ genannter Index-Server (normaler Web-/Fileserver). Ihm fallen zwei Aufgaben zu: Erstens die Verteilung der Torrent-Dateien (sie enthalten die Informationen über die Teile des Downloads) und zweitens die Führung einer Peer-Liste für jede Torrent-Datei (neu hinzukommende Nodes erhalten ein Verzeichnis von P2P-„Seeds“, mit denen sie sich verbinden können).*

Obwohl BitTorrent auch zum unerlaubten Tausch von Content eingesetzt wird, wachsen auch die kommerziellen Anwendungen ständig – allerdings nicht so schnell wie die illegale Nutzung. Einige Beispiele für den Einsatz von BitTorrent (Wikipedia und Pressemeldungen):

- Sub Pop Records (Musikdistribution), Vuze (Videodownloads).

- Podcast-Services verwenden neuerdings BitTorrent zur Verbreitung, vor allem unterstützt durch die Player-Software „Miro“.

- Der Datentransfer von Amazon S3 (eine Speicherlösung) basiert auf BitTorrent.

- „World of Warcraft“ setzt BitTorrent zur Distribution von Spiel-Updates ein (Dateien mit mehreren 100 MB).

- Distribution von Patches: Die INHOLLAND University verteilte in nur 4 Stunden 22 TB an Patches an 6.500 PCs – fast undenkbar in einer Client-Server-Umgebung (früher wurden 4 Tage dafür benötigt) — und reduzierte so die Zahl ihrer Download-Server von 22 auf 2.

Wegen seiner weiten Verbreitung lässt sich das Protokoll heute nicht mehr aus dem Internet „verbannnen“, wie manchmal gefordert wird (um Filesharing zu minimieren und Universitäten vor Strafverfolgung durch die Medienindustrie zu bewahren).

Direct Download Links (DDL): Alternative zum P2P-Filesharing

- Direct Download Links funktionieren wie normale Webserver, also ohne direkten Austausch von Daten zwischen Nutzern.

- Die Nutzer können einen Account anlegen und Dateien hochladen (mehrere 100 MB). Die Dateien sind nur über einen direkten Link zugänglich, der nur dem Nutzer bekannt ist (Server kann nicht nach Content durchsucht werden).

- Der Uploader macht den Link öffentlich (meist über ein externes Forum), sodass die Datei heruntergeladen werden kann.

- Nutzer ohne gebührenpflichtigen DDL-Account haben eingeschränkte Bandbreiten und Downloadvolumen. Außerdem müssen sie vor jedem Download warten (1 bis 2 Minuten vor dem ersten, länger bei den folgenden, volumenbasiert) und ein CAPCHA eingeben.

- Zu den beliebten DDL-Lösungen zählen Rapidsphere und MegaUpload. In Europa noch recht unbekannt, werden sie im Nahen Osten stark genutzt (hier sind 9% des Datenvolumens DDL-Traffic).

*Hinweis: BitTorrent kommt auch ganz ohne zentralen Tracker aus, wenn stattdessen verteilte „Hashtables“ eingesetzt werden (von vielen Implementierungen schon unterstützt). Das Ergebnis ist ein echtes serverloses P2P-System.

spektion (DPI) und/oder Filterung von Content; die Entfernung nach Abmahnung durch zuständige Behörden (für Netzbetreiber, die Content hosten); Einschränkung oder Blockierung des Zugriffs auf bestimmte Seiten oder Protokolle; Offenlegungspflicht von persönlichen Daten wie IP-Adressen für die Strafverfolgung; Anschreiben von Internet-Account-Inhabern, über deren Account unerlaubt Copyright-Material ausgetauscht wurde; Verweisen der Verbraucher an legale Plattformen für Content; bis hin zum zeitweisen Ausschluss illegaler Downloader vom Internet nach der so genannten „Three Strikes“-Regel („Beim 3. Mal bist du draußen“, auch: „Graduated Response“).

Alle diese Sicherheitsmaßnahmen werfen entscheidende Fragen auf – etwa wie man zu

Best Practices gelangt oder wie der Schutz vor Piraterie mit der bestehenden Haftungsgesetzgebung für „rein durchleitende“ Anbieter vereinbart werden kann und wie er sich mit fundamentalen Nutzerrrechten bezüglich Personendaten und Online-Verhalten sowie mit allgemeinen Ideen wie freies Internet, Informationsfreiheit und „Digital Inclusion“ verträgt. Das politische Klima in Europa scheint eher den Schutz der Nutzerrechte zu favorisieren, zumindest solange der User keinen kommerziellen Profit aus seinen Online-Transaktionen zieht. Downloader vom Internet auszuschließen, wird als unverhältnismäßig harte Strafe gesehen und widerspreche dem Ziel einer für alle zugänglichen Informationsgesellschaft. Die Einklagung von Copyright konzentriert sich auf das widerrechtliche Hochladen von geschützten Materialien, nicht auf den Download, der in vielen Staaten sogar legal ist. Hinzu kommt, dass Vorkehrungen wie Content-Filterung und DPI von den Betreibern hohe Investitionen verlangen. Hier bleibt die Frage, wem diese Kosten angelastet werden können und inwieweit der Werterhalt für die Content-Industrie konkret quantifizierbar ist und solchen Maßnahmen klar zugeordnet werden kann. Eine Studie der britischen Value Recognition Strategy Working Group von 2007 fand beispielsweise heraus, dass die Änderung des Verkaufsformats (wie die Zerteilung von CDs in einzelne Songs bei Apple iTunes) sowie der Preisdruck durch heruntergesetzte CDs in Supermärkten weit mehr zum Wertverlust in der britischen Musikindustrie beigetragen haben als P2P-Filesharing.

7. ZUSAMMENFASSUNG

Erst die Bedienung aller vier Säulen von Digital Confidence wird den nächsten Wachstumsschub im „Digital Life“ ermöglichen. Die von verschiedenen Stakeholdern bereits eingeleiteten Maßnahmen beweisen, dass die Problematik und der Handlungsbedarf allgemein anerkannt werden.

Doch die verschiedenen Parteien stehen dabei vor vielschichtigen Problemen. Beispielsweise gibt es in einer Reihe von Staaten tiefgreifende nationale Unterschiede, was die Rechtsprechung zu zentralen Fragestellungen angeht, während typische Online-Bedrohungen wie Phishing grenzüberschreitender Natur sind und bei der Strafverfolgung internationale Kooperation erfordern. Oft ist es schwierig oder unmöglich, die Täter zu finden oder zu bestrafen: Die Werkzeuge und Maßnahmen der „analogen“ Welt scheinen in den digitalen Umgebungen schlicht nicht zu greifen. Aufgrund der rasanten Weiterentwicklung von Technologien, gesellschaftlichem Verhalten und digitalen Möglichkeiten entstehen außerdem viele Grauzonen, gefördert vom kinderleichten Duplizieren digitaler Güter bis zur weltweiten Verfügbarkeit des Internets.

Die Industrie hat Digital Confidence als Top-Priorität erkannt, müht sich aber noch, effektive Ansätze zu finden.

Regulierer und staatliche Behörden sind aufgefordert, ihre eigene Position innerhalb von Digital Confidence zu definieren. Im Moment schwanken sie zwischen ultrastrenger Gesetzgebung, Verbraucheraufklärung und Philosophien der freien Marktregulierung. Eine zentrale Rolle wird auch internationalen Kooperationen und der Ratifizierung internationaler Abkommen zukommen, damit die nationalen Gesetzgebungen sich einander annähern und Verhaltensformen verbieten, die, obschon eindeutig illegal, nicht in allen Ländern vom Gesetz abgedeckt werden. So wurde in Großbritannien erst vor kurzem, im Mai 2008, eine Eingabe zur Schließung einer Gesetzeslücke gemacht, die Zeichnungen und computergenerierte Bilder von sexuellem Missbrauch an Kindern nicht unter Strafe stellte.

Die Industrie muss sich zwischen verschiedenen Graden der Intervention entscheiden. Dabei muss sie ihre Investitionskosten und die Anforderungen neuer Geschäftsmodelle im Blick haben, aber auch allgemeine politische Fragestellungen, das Bedürfnis nach innovativen Dienstleistungen und die Entwicklung von Netztopologien, die den Wünschen und Werten der „Born Digital“-Generation entgegenkommen. Die Online-Branche ist generell besorgt über zusätzliche haftungsrechtliche Verantwortlichkeiten und bedarf deshalb der Unterstützung durch zuständige Regierungsbehörden und Gesetzgeber. Wegen landes- und fallspezifischer Unterschiede kann es zwar beim Aufbau von Digital Confidence keine „One size fits all“-Lösung geben, aber aus den bisherigen Best Practices lässt sich einiges lernen. Das momentane Fehlen einheitlicher Strategien schadet letztendlich dem Verbraucher, der Transparenz und Hilfestellung bei den Risiken des digitalen Lebens vermisst – während die Unternehmen gefordert sind, zukunftssichere digitale Geschäftsmodelle zu entwickeln.

Die Definition der vier Säulen von Digital Confidence ermöglicht Unternehmen die Problemanalyse, Priorisierung und Umsetzung.

Die schwierigste Frage der Digital Confidence ist aber nicht, was getan werden muss, sondern wie und von wem. Hier müssen wirkungsvolle Aufgaben definiert und an die verantwortliche

Ebene vergeben weder. Die Frage ist also, welche Ebene betroffen ist: Verbraucher, Unternehmen, Regulierer? Und besonders: Wer muss die Maßnahme bezahlen?
Die von uns durchgeführten Befragungen weisen darauf hin, dass die Probleme weniger bei den technischen Lösungen liegen, als vielmehr in den grundlegenden unternehmenspolitischen Fragen: Sollte ein Unternehmen selbst bei der Blockierung unerwünschter Inhalte aktiv werden und dafür haftbar gemacht werden können? Wenn ja, wer entscheidet, was „unerwünscht“ und „illegal“ ist? Wo kann man die Linie ziehen? Wenn beispielsweise Kindesmissbrauch geblockt wird, wie steht es dann mit Rassismus?

Letzten Endes beruhen alle Probleme auf vielfältigen Interessen und widersetzen sich zu einfachen Lösungsansätzen. Die oben definierten vier Säulen der Digital Confidence strukturieren die Aktionsfelder nach ihren wichtigsten Aspekten und ermöglichen so eine umfassende Diskussion und effektives Handeln.

CONTENT FILTERING

Content-Filterung wird angewendet, um den Zugriff auf bestimmte Webseiten oder Seitenbereiche einzuschränken. Traffic-/Contentfilterung dient verschiedenen Aufgaben, beispielsweise:

- Ausfilterung von Spam-Mails.

- Abschottung von rechtswidrigen Inhalten wie Kinderpornografie oder urheberrechtlich geschütztem Material.

- Schutz Minderjähriger vor unerwünschten Inhalten.

Die Methode der Filterung richtet sich nach dem Anlass. Die Filterung kann im Enduser-Equipment vorgenommen werden (oft als Kindersicherung, da sie von den Erwachsenen leicht umgangen werden kann) oder netzbasiert sein (zum Beispiel Einschränkung oder Blockierung von unerlaubten Inhalten) oder eine Mischung aus beidem (Spam-Filterung: Mailserver blockiert Spam anhand von Blacklist, E-Mail-Client filtert den Rest inhaltsbasiert).

Für die netzbasierte Filterung gibt es eine Reihe von Methoden (siehe Abb. 35). Die am weitest verbreitete Implementierung ist DNS-basierte URL-Filterung[4]. In diesem Fall werden bestimmte Zugriffe auf die der IP-Adresse zugrundeliegende Domain anhand des Domainnamens gesperrt (Beispiel: „www.google.com“ wird blockiert, nicht aber „www.google.co.uk“, denn sie haben unterschiedliche Domainnamen). Ein solcher Filter kann sehr leicht von jedem Netzbetreiber implementiert werden und wirkt sich auf alle Kunden aus, die den DNS-Server des Anbieters benutzen. Allerdings kann er leicht umgangen werden, indem man über einen anderen, nicht mit Filtern versehenen DNS-Server geht. Außerdem erfordert diese Art der Filterung eine Blacklist mit indiziertem Content. Sehr geeignet ist sie vor allem für die Verhinderung unbeabsichtigter Zugriffe auf illegalen Content.

Aufwändigere Filter untersuchen den Inhalt eines Datenstroms und erkennen so, ob er gesperrt werden muss. Eine relativ einfache Variante ist die Erkennung von Spam-Mails, ein anderes die Kindersicherung vor obszönen Inhalten, die Webseiten nach Stichwörtern wie „Porno“ durchsucht und sperrt. Die höchst entwickelte Version stellen Filter für „Dynamic Content Fingerprinting“ dar. Sie können selbst Audio- und Video-Traffic analysieren und beispielsweise feststellen, ob Copyright-Material darunter ist. Ein weiteres Beispiel ist DPI. Die Technologie, auf der diese modernen Filtermethoden basieren, wird allerdings kontrovers diskutiert. DPI ermöglicht es, einzelne Datenströme „Buchstabe für Buchstabe“ zu durchleuchten, also möglicherweise auch persönliche E-Mails. Dies hat Anlass zu datenschutzrechtlichen Bedenken gegeben, da DPI personenbezogene Daten sammelt (angeschaute Webseiten, Suchverläufe) und als Möglichkeit zum unerlaubten Abfangen von Daten gilt.

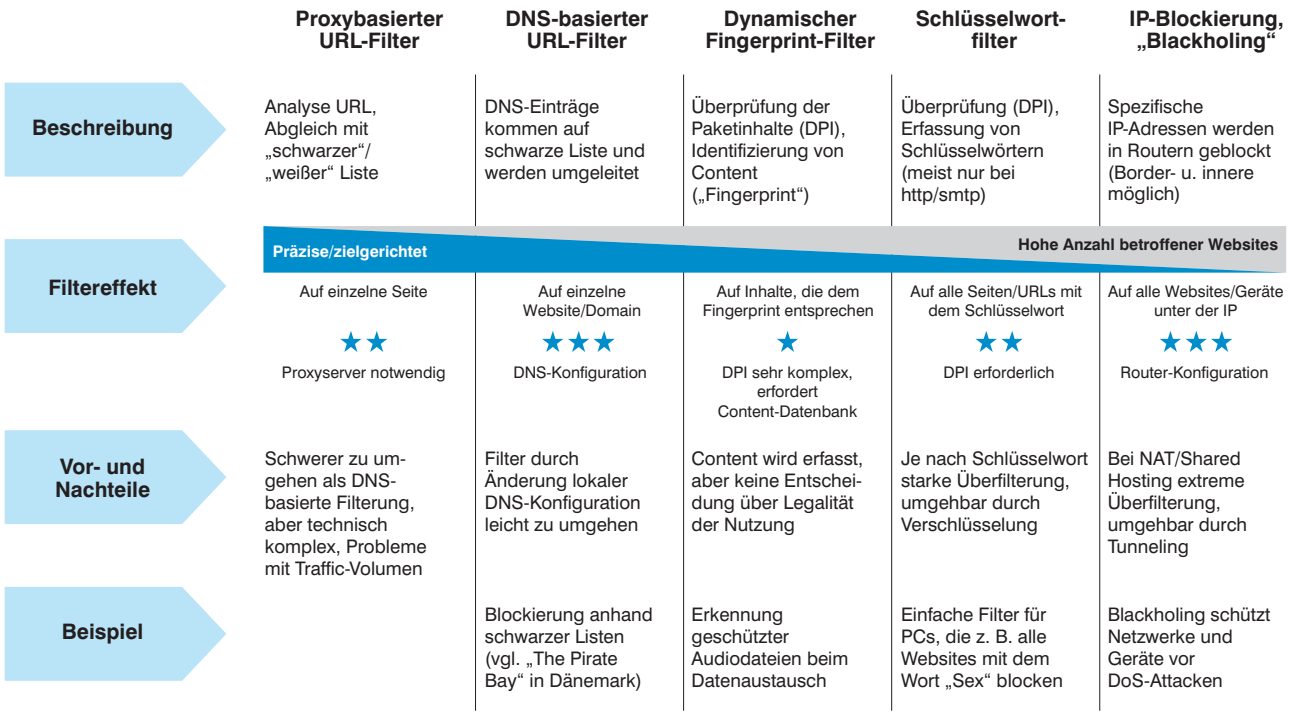
„Blackholing“ ist eine sehr einfache und effektive Filterung, hat aber entscheidende Nachteile. Eine spezifische IP-Adresse wird vollständig geblockt, an die Adresse gerichtete Pakete werden nicht weitergeleitet. Selbst für gewiefte Webuser ist diese Sperrung nur schwer zu umgehen. Doch da mehrere Systeme und Webseiten unter einer IP-Adresse liegen können, könnten hunderte andere Seiten und User als Kollateralschaden mit gesperrt werden („Overblocking“). Die Methode kommt daher nur zum Einsatz, wenn große

(4) DNS ist das „Domain Name System“, dass dem PC ermöglicht, den Server zu einer bestimmten Domain zu finden.

Netze in Gefahr sind oder die Bedrohung für die Nutzer sehr hoch ist.

Generell sind Filtermaßnahmen nur dann sinnvoll, wenn die Pflege und Aktualisierung der Content-Verzeichnisse konsequent umgesetzt wird. Wenn die „schwarzen Listen" jedoch zweckentfremdet werden oder die rechtswidrigen Inhalte nicht in angemessener Zeit entfernt werden, können sich rechtliche Probleme ergeben.

Abb. 35: *Toolbox – Filterung von Website Traffic*



Hinweis: Darstellung nicht erschöpfend, vgl. z. B. Möglichkeit der portbasierten Blockierung zusätzlich zur DNS-basierten Filterung, um die Umgehung zu erschweren.

Quelle: Booz & Company

★ Schwierige/teure Umsetzung

★★★ Einfache/preiswerte Umsetzung

IV. AKTUELLER DIGITAL-CONFIDENCE-ANSATZ: NOCH DEUTLICH VERBESSERUNGSFÄHIG

Um einen kohärenten Rahmen zur Sicherung von Digital Confidence zu entwickeln, ist ein Überblick über die Ansätze entscheidend, die von verschiedenen Stakeholdern verfolgt werden, um den immer drängenderen Herausforderungen zu begegnen.

Dazu soll eine Reihe von Fallstudien diskutiert werden, an denen sich Best (und Worst) Practices erkennen und Strategien für die Zukunft entwickeln lassen. Die Case-Studys werden ergänzt durch einen kurzen Überblick über die Prioritäten und Vorgehensweisen der Regulierer bei der Umsetzung von Digital Confidence.

1. FALLSTUDIEN: ERFOLG UND MISSERFOLG BEI DER SICHERSTELLUNG VON DIGITAL CONFIDENCE

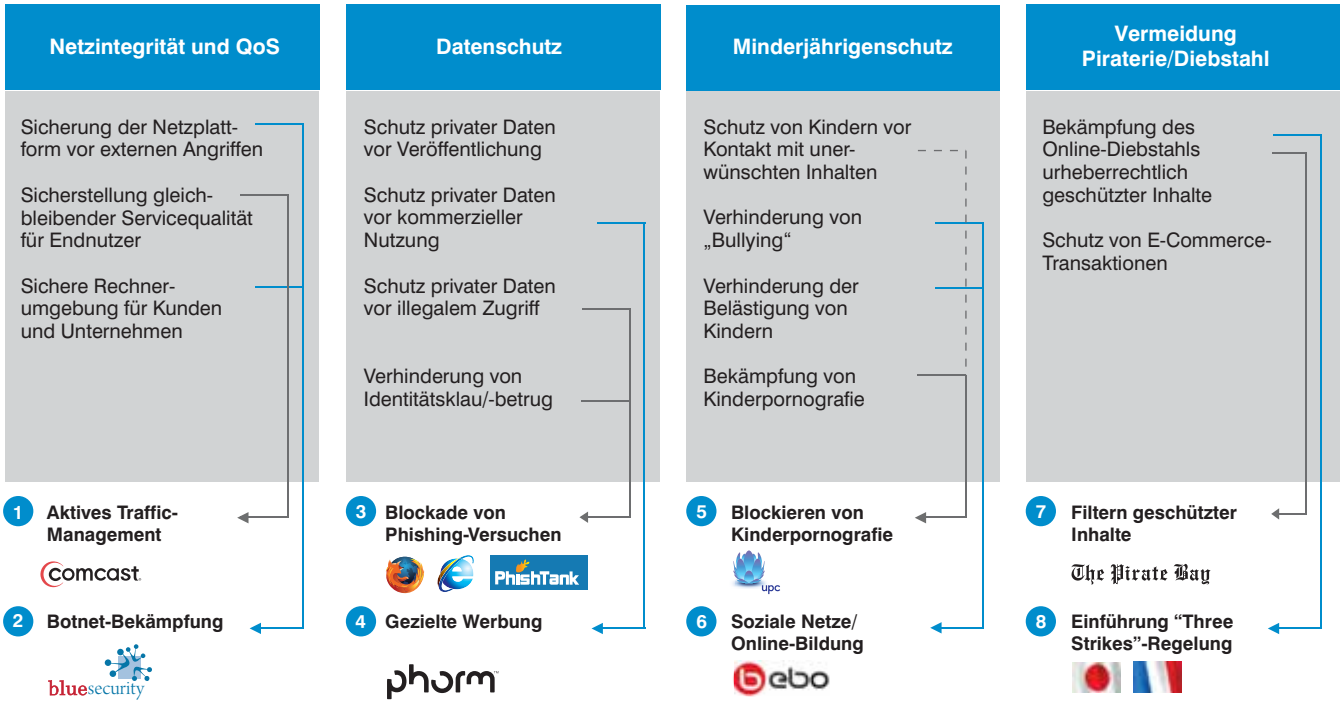
Die Identifizierung der Cases folgte entlang der vier Säulen von Digital Confidence: Netzintegrität und Quality of Service (QoS), Datenschutz, Minderjährigenschutz sowie Vermeidung von Piraterie und Diebstahl. Je Säule wurden zwei Fallbeispiele ausgesucht, um die Ziele in jedem Bereich so deutlich wie möglich zu machen und fundierte Schlüsse ziehen zu können (siehe Abb. 36).

- „Lernpotenzial".
- Zeitnähe.
- Geografische Verschiedenheit.

Wie in Kapitel III dargelegt, ist es von zentraler Bedeutung, welche Position ein Unternehmen in den einzelnen Bereichen von Digital Confidence einnimmt. Wie vorsorgend oder sogar vorschreibend muss oder will ich sein? Wie stark können die Maßnahmen eingreifen?

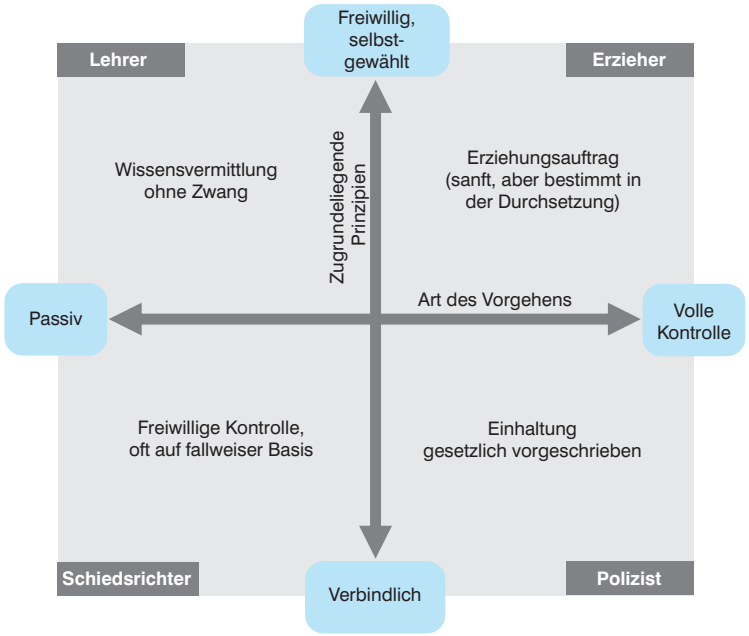
Zur Untersuchung der Fälle wurde eine allgemeine Positionierungs-Matrix für Digital Confidence entwickelt (siehe Abb. 37). In der

Abb. 36: *Aktuelle Konzepte – einige Beispiele*



Hinweis: Die Pfeilfarben dienen lediglich der Unterscheidbarkeit.
Durchgängige Linie = Hauptaspekt; gestrichelte Linie = Nebenaspekt

Abb. 37: *Positionen-Matrix zur Digital Confidence*



Matrix bildet die horizontale Achse die Art der Vorgehensweise ab (vom passiven „Hände weg"-Ansatz bis zur aktiven „vollen Kontrolle"). Die vertikale Achse differenziert die zugrundeliegenden Prinzipien. So ergeben sich vier Quadranten, die zugleich allgemeinen gesellschaftlichen Rollen entsprechen:

- Der Lehrer klärt die Nutzer so gut wie möglich über Angebote und Gefahren auf, verhängt aber normalerweise keine Sanktionen (vgl. Entwicklung von Lernmaterial zum Internet durch „Web Wise Kids").

- Auch der Erzieher klärt auf, führt aber anders als der Lehrer proaktive Maßnahmen durch, um die Nutzer zu schützen (vgl. Ausfiltern von Copyright-Material durch YouTube).

- Der Schiedsrichter vertraut auf freiwillige Regeln, die er fallbezogen durchsetzt, und setzt auf Richtlinien statt Aufklärung. Die Regeln basieren jedoch auf Absprachen (vgl. proaktive Abschottung von Kinderpornografie-Domains durch UPC [NL]).

- Der Polizist bevorzugt starke Sanktionen auf Basis gesetzlicher Regelungen. Er sorgt für die Ergreifung aller nötigen Maßnahmen und hält sich strikt an die Regeln, etwa das Totalverbot einer Aktivität (z. B. durch die „Beim 3. Mal bist du draußen"-Regel bei Copyright-Verletzungen).

FALLSTUDIE 1: AKTIVES TRAFFIC-MANAGEMENT

Problem: *Netzprovider verzeichnen eine zunehmende Bandbreiten-Auslastung und müssen Traffic steuern, um Datenstaus zu verhindern und die Qualität des Services zu gewährleisten.*
Risiko: *Zwar kann die Dienstgüte (QoS) in Spitzenzeiten leiden, doch nur immer Bandbreite nachzurüsten, wäre viel zu teuer und dennoch keine langfristige Lösung.*

Power-User konsumieren unverhältnismäßig viel Bandbreite – zum Nachteil durchschnittlicher Nutzer. Anwendungen wie Filesharing und Video-Streaming sind eben deutlich „bandbreitenhungriger" als normales Surfen im Web oder E-Mail. Diese ungleichmäßigen Nutzungsintensitäten führen in jedem Netz zu starken Spitzen in der Auslastung der Gesamtkapazität. Netzanbieter reagieren mit Investitionen in Next-Generation-Netze, um die verfügbare Bandbreite kontinuierlich an den Bedarf anzupassen. Doch damit alle Nutzer eine optimale QoS erleben, reicht Kapazitätssteigerung allein nicht aus: Die Gruppe der Power-User wird immer größer, ihr Bedarf an Bandbreite steigt ständig. Daher kann jede Nachrüstung des Netzes immer nur eine vorübergehende Lösung sein. Um eine „faire" Verteilung von Bandbreite und QoS für alle Nutzer zu gewährleisten, muss der Traffic zusätzlich gemanagt werden (siehe Abb. 38). Bei Flatrate-Tarifmodellen werden Nutzer mit hohem Verbrauch (steil ansteigende Kurve) von Nutzern mit geringem Verbrauch „subventioniert". Zum Vergleich: Wenn 10% der Power-Downloader per Traffic-Shaping gesteuert oder in eine höhere Nutzungsklasse umgezogen würden, würde sich die faire Verteilung der verfügbaren Kapazität unter allen Anwendern um fast 50% erhöhen.

Staffeltarife und Traffic-Management-Maßnahmen sind die beiden geeignetsten Gegenmaßnahmen. Eine Staffelung des Nutzungspreises kann Power-User dazu bringen, ihren Durchsatz zu verringern, indem Premium-Gebühren für das Herunterladen in Spitzenzeiten verlangt werden – insbesondere für datenintensive Nutzungsarten wie Filesharing. Solche Premium-Tarife haben einen doppelten Effekt: Erstens verlagern sie die Auslastung in weniger kritische Zeitbereiche und zweitens führen sie zu zusätzlichen Einnahmen, die zur Finanzierung von Infrastruktur-Erweiterungen eingesetzt werden können. Der kanadische Kabelbetreiber Rogers hat inzwischen solche Staffelgebühren eingeführt und in den USA prüft AT&T ein spezielles Pricing-Modell für BitTorrent-Traffic, das die Auswirkungen des

P2P-Verkehrs auf das Netz abmildern soll (das Unternehmen rechnet in den nächsten 3 Jahren mit einer Vervierfachung seines Datenvolumens). Währenddessen testet Time Warner ein Metering-basiertes Preissystem, mit dem die Kunden auf Grundlage ihrer Bandbreitennutzung abgerechnet werden.

Traffic-Management umfasst eine breite Palette von Netz-basierten Maßnahmen zur Steuerung des Datenflusses und Gewährleistung der Dienstgüte – zusätzlich zur Netzdimensionierung, die sich vor allem an der Spitzenauslastung orientiert. Die Maßnahmen reichen von der Durchsetzung von „Fair Use"-Grenzen über Formen des Traffic-Shaping bis zur Implementierung verschiedener Methoden der Traffic-Selektierung, die eine optimale QoS sichern (vgl. Kapitel III).

Die unterschiedlichen Ansätze zum aktiven Traffic Management lassen sich in einer thematisch angepassten Version der Positionierungs-Matrix darstellen (siehe Abb. 38). Ihre vertikale Achse fächert in diesem Fall die regulierenden Haltungen auf, die ein Netzbetreiber oder ISP bezüglich Traffic-Management einnehmen kann. Dabei bezeichnet der obere Pol eine Positionierung, die Anreize schafft, aber nicht in das Handeln der User eingreift, der untere eine forcierende Haltung, die auf User-Aktivität reagiert und konkrete Management-Maßnahmen ergreift. Die horizontale Achse zeigt an, wie spezifisch in den vorhandenen Traffic eingegriffen wird, das heißt, wie gezielt die technischen Maßnahmen sind. Beispielsweise differenziert dienstspezifisches Traffic-Shaping weit genauer zwischen verschiedenen Traffic-Arten als protokollspezifisches Shaping.

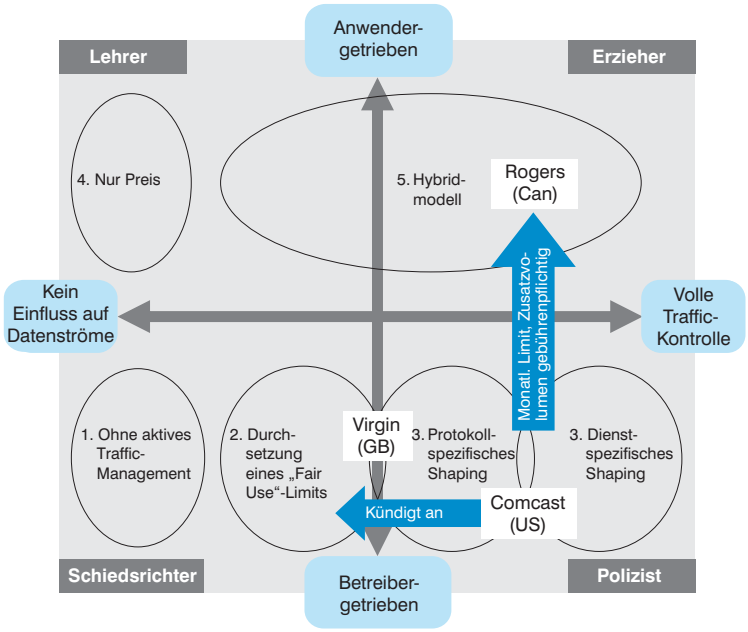
Einige Positionen in der Matrix sind realistischer als andere. Zum Beispiel ist ein allein auf Pricing basierender Ansatz wie im „Lehrer"-Quadranten beim momentanen Ungleichgewicht zwischen Bandbreitenangebot und -nachfrage kaum vorstellbar. Ohne technische Maßnahmen können die Anbieter den einwandfreien Netzbetrieb nicht garantieren.

Die Matrix lässt eine Reihe von aktuellen Best Practices erkennen: Comcast, einer der größten Kabelbetreiber in den Vereinigten Staaten, hatte aufgrund des Anwachsens von P2P-Systemen mit einer starken Traffic-Steigerung zu kämpfen. Unter diesem Druck verschärfte Comcast sein Traffic-Management und geriet in der Öffentlichkeit in heftige Kritik. Rogers in Kanada führte Nutzungspauschalen ein und erhob ab einer bestimmten Volumengrenze Zusatzgebühren (die Grenze lag bei bis zu 100 GB pro Monat). Dies ist ein Beispiel für ein hybrides Modell, bei dem Traffic-Management mit Preisstaffelung verknüpft wird. Virgin Media in Großbritannien ist ein Beispiel für einen Kabelbetreiber, der offen über seine Traffic-Management-Aktivitäten informiert.

*„Nicht gemanagte Netze führen zu erheblichen Qualitäts- und Verfügbarkeitseinbußen für alle Nutzer. Und das heißt auch: Die Kunden müssen für weniger Leistung immer mehr bezahlen, weil die Anbieter ihre Netze ständig ausbauen müssen, um mit dem massiven Anstieg an Bandbreiten-Konsum Schritt zu halten".**

*Kurt Dobbins, Arbor Networks

Abb. 38: *Digital-Confidence-Positionen zum aktiven Traffic-Management*



1. Nur wenige Netzbetreiber verwalten ihren Traffic nicht aktiv
   – Vorteil: Bei ausreichend Kapazität ist kein aktives Management erforderlich
   – Nachteil: Keine garantierte Servicequalität – Überlastung möglich
2. Netzbetreiber halten auf der Netzdimensionierung basierende „Fair Use"-Programme vor, um Spitzenlasten abzufedern
   – Bei Überschreitung des „Fair Use"-Limits können User auf eine höhere Bandbreite migriert werden
3. Einsatz von aktivem Traffic-Management, das allen Usern QoS garantiert
   – Aus Gründen der Netzneutralität ist ein nicht protokollspezifischer einem dienstspezifischen Ansatz vorzuziehen
4. Eine geschäftsrelevante Alternative des Bandbreiten-Managements ist die auslastungsbasierte Preisdifferenzierung
   – Vorteil: Steuerung über Marktanreiz, hält von exzessiver Nutzung ab
   – Nachteil: Weniger Nutzungskomfort – möglicher Wettbewerbsnachteil
5. Hybridmodelle („Additional Usage") verwenden Preisdifferenzierung, wenn bestimmtes Limit überschritten
   – Normalanwender profitiert von Flatrate-Preisen, nur Power-User zahlen Premiumnutzung

Comcast hatte Netz-Management-Maßnahmen ergriffen, die den P2P-Traffic durch BitTorrent zu stark reglementierte: Zwar waren BitTorrent-Downloads möglich, doch Nutzer berichteten, dass Uploads verzögert wurden und dass die Implementierung auch andere, mehr zeitkritische Anwendungen wie Lotus Notes beeinträchtigte. Beschwerden einzelner User erzeugten starke öffentliche Aufmerksamkeit und führten dazu, dass die FCC eine Untersuchung einleitete. Man warf dem Unternehmen ein irreführendes Serviceversprechen und Online-Betrug vor. Comcast packte die Probleme gründlich an. Es kooperierte mit BitTorrent und einigte sich auf eine Lösung: Comcast setzt eine nicht plattformspezifische Technik ein, die den P2P-Traffic höchstens bei absoluten Top-Usern verlangsamt. Auch von Vertretern der Netzneutralität erhielt die Lösung Zustimmung. Google nannte die Wahl eines nicht plattformspezifischen Ansatzes einen „Schritt in die richtige Richtung". Nur die FCC ließ sich nicht beruhigen und geißelte in einem Urteil die Praktiken, die Comcast schon hinter sich gelassen hatte.

*„Bei den heutigen Breitbandnetzen stellt sich nicht die Frage: ‚Managen ja oder nein?', sondern: ‚Wie?'"**

Akteure wie Virgin Media und Rogers machen keinen Hehl aus ihrem Traffic-Management. Die Akzeptanz scheint hoch.

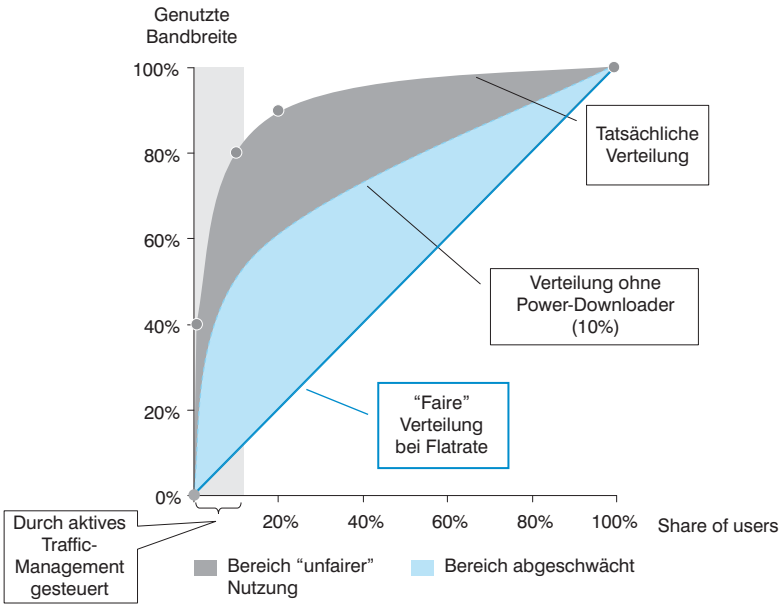
Obwohl die FCC den Bedarf für „angemessenes" Netz-Management durchaus anerkennt, warf die Behörde Comcast vor, auch ohne zwingenden Grund Internet-Traffic blockiert und die Verbraucher nicht darüber informiert zu haben. Im Juli 2008 beantragte der FCC-Vorsitzende die rechtliche Verfolgung: Comcast solle seine „Blockadepraxis" stoppen (wobei es sich eigentlich nur um eine Verzögerung handelte), Verbraucher darüber informieren, wie und in welchem Umfang die Praktiken angewendet werden und zukünftige Pläne für das Management des Netzs offenlegen. Die Klage stand im Zusammenhang mit einer Grundsatzerklärung der FCC vom September 2005, in der Prinzipien für ein „flächendeckendes, offenes, preiswertes und allgemein zugängliches" Breitband-Netz formuliert worden waren. Sie beruhen auf „angemessenem Netz-Management". Das FCC-Urteil scheint nicht viel mehr als eine Prinzipienerklärung zu sein (zumal Comcast wohl kaum finanziell belangt wird), die einen Präzedenzfall dafür schaffen will, wie „angemessenes" Management in der Praxis auszusehen hat.

Rogers führte die Premiumnutzungsgebühr im März 2008 ein. Je nach Tarif fällt pro Monat eine Zuzahlung von 1,25 bis 5 Dollar an. Bei mehreren Accounts zahlt der Kunde höchstens 25 Dollar. Die Einführung solcher nutzungsbasierten Preismodelle wird inzwischen von immer mehr Netzanbietern erwogen. Die Staffelung hat nur ein Problem: Sie könnte das wichtige Grundsatzversprechen der „Flatrate" unterminieren, das den Breitband-Massenmarkt erst möglich machte – sorgenfreies Surfen ohne Furcht vor Preisspitzen durch schwer kontrollierbaren Datendurchsatz. Rogers berücksichtigt dies über den 25-Dollar-Cap. Im Übrigen geht das Unternehmen offen und unverkrampft mit seinen Grundsätzen um. Auf der Website heißt es: „Unsere User können generell den Tarif ihren Bedürfnissen entsprechend wählen und akzeptieren dafür die Einhaltung einer monatlichen Volumengrenze. Sollten Sie doch einmal darüber liegen, können Sie Ihren Zusatzverbrauch entweder monatlich zuzahlen oder in einen Tarif wechseln, der Ihren Online-Anforderungen besser entspricht. Die Volumenmessung ergibt ein faires Bild, wie stark unsere Kunden den Service nutzen, und hilft uns, die Monatstarife für alle so niedrig wie möglich zu halten".

Ähnlich transparent geht auch die britische Virgin Media mit der Notwendigkeit von Traffic-Management und ihrer Form der Umsetzung um. Das Unternehmen setzt Traffic-Shaping zur Steuerung der obersten 3% der Power-User ein – und macht die Regeln auf der Webpräsenz öffentlich. Die Maßnahmen sind Bestandteil einer „Fair Use Policy", die die Dienstgüte für das Gros der Nutzer sichern soll. Auch Virgin Media denkt über die Einführung von Pricing-basierten Modellen nach. Traffic-

*Vint Cerf, Chief Internet Evangelist, Google

Abb. 39: *Bandbreitennutzung in verschiedenen Anwendergruppen*



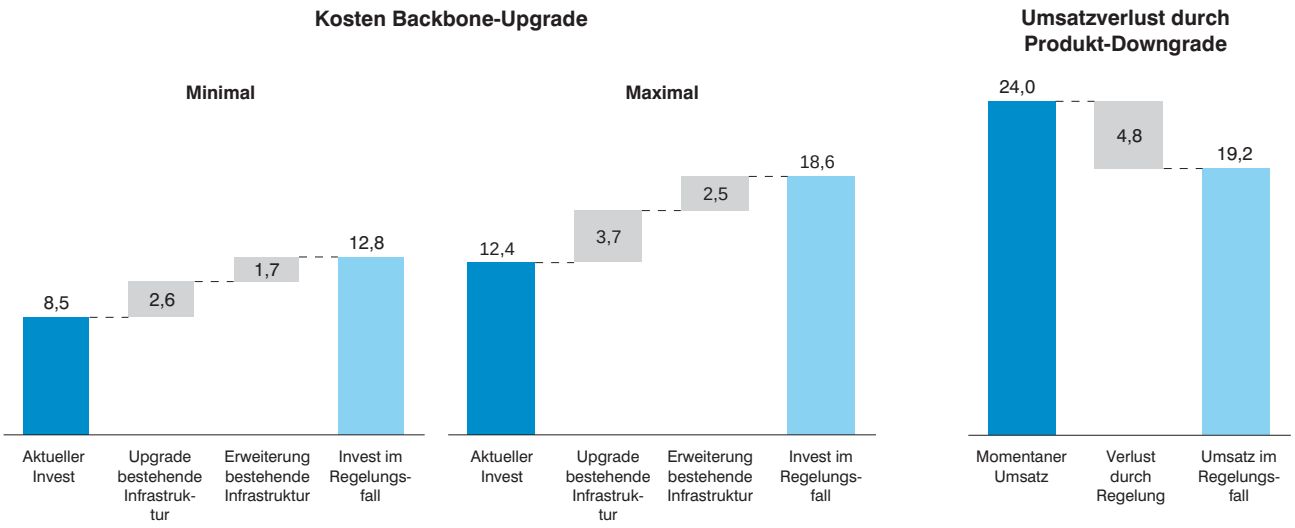
Quelle: Arbor Networks, Booz & Company-Analyse

AUSWIRKUNGEN BESTIMMTER MODELLE ZUR REGULIERUNG DER MINDEST-DIENSTGÜTE

Abb. 40: *Das Spektrum möglicher QoS-Regulierungen*

0. Kein Shaping erlaubt	1. Geringe QoS-Anforderungen	2. Mittlere QoS-Anforderungen	3. Hohe QoS-Anforderungen
• Netzneutralität kann als Möglichkeit interpretiert werden, kein Traffic-Shaping zu erlauben • Könnte mit anderen Optionen kombiniert werden, aber schwer umsetzbar	• Implementierung durch Anpassung bestehender Netzmanagement-Lösungen – Shaping nach Dienst/Protokoll – Mehr oder weniger aggressiv	• Z. B. Mindestbandbreite oder moderate Geschwindigkeitsanforderungen • Umsetzbar mit bestehender Infrastruktur und kleineren Updates – Backbone-Upgrades für mehr Bandbreite mit weniger Shaping – Zugangs-Upgrade (neues CPE)	• Hohe Anforderung an QoS (Mindestbandbreite sowie geringer Lag und Jitter) • Bestehendes Netz reicht nicht aus, Implementierung neuer Technologien erforderlich
• Zwei Optionen für Netzbetreiber, die kein Shaping anwenden: – Upgrade des Backbones – Downgrade der Produkte	• Kein Backbone- oder Zugangs-Upgrade nötig	• Backbone- oder Zugangs-Update für Teile des Netzes erforderlich • Unterschiedliche technische Restriktionen für DSL- und Kabelanbieter (Kabel mit Shared-Access-Netz ist z. B. bandbreitenstärker, neigt aber zu Datenstaus)	• Backbone- und Zugangs-Upgrades erforderlich (im Grunde Neuentwicklung des Netzes)
Produkt-Downgrade oder Netz-Upgrade	**Keine Upgrades**	**Netz-Upgrade**	**Netz-Rebuild**

Abb. 41: *Finanzielle Folgen einer europäischen „No Shaping"-Regulierung (Mrd. Euro)*



Hinweis: Europa = EU-27 + Norwegen + Schweiz
Hinweis: Hypothetisches Szenario, beruhend auf den Annahmen, dass Shaping in Europe verboten wird, zurzeit 20 % des Traffics reguliert werden und er jährlich um 67 % steigt. (Nicht berücksichtigt: mögliche Verteilung des Shapings zwischen Playern.)
Quelle: US BEA, Merrill Lynch, Ofcom, Unternehmensberichte, Booz & Company-Analyse

Management wird zunehmend Gegenstand von Untersuchungen durch Regulierungsbehörden. Das erwartete Urteil der FCC unterstreicht, dass für die Behörde bei der Definition eines „angemessenen“ Traffic-Managements der Verbraucherschutz einen hohen Stellenwert hat. Doch auch aus Sicht der Regulierer ist das Thema komplex. Abb. 40 und 41 illustrieren, welche wirtschaftlichen Auswirkungen ihre Entscheidungen haben könnten: Durch die Verhängung sehr strenger QoS-Vorschriften mit entsprechenden Einschränkungen der Durchführbarkeit von Traffic-Management würden hohe Zusatzkosten auf die europäischen Unternehmen zukommen – Kosten, die von den Netzbetreibern nicht absorbiert werden könnten, sodass der Endverbraucherpreis steigen würde. Letztendlich würde so der exzessive Gebrauch eines relativ kleinen Kundensegments zu einer allgemeinen Preiserhöhung führen. Daher sollte jegliche Regulierung im Bereich Traffic-Management sorgfältig abgewogen werden.

P4P trägt zur Entschärfung des P2P-Traffics bei und steigert das Nutzererlebnis

P4P oder „Proactive Network Provider Participation for P2P“ ist eine Initiative der Distributed Computing Industry Association (DCIA). Zu den Mitgliedern der Arbeitsgruppe gehören Branchenexperten wie AT&T, BitTorrent, Cisco, Joost, Pando, Telefonica, Verizon und Vuze.

P4P widmet sich zwei strategischen Zielen: 1) der Reduzierung des Backbone-Traffics und 2) der Senkung der Netzbetreiberkosten. Die technische Idee dahinter ist ein P2P-System (auf der Basis von BitTorrent), das Informationen über die Netztopologie nutzt, um Daten gezielt mit bestimmten Peers auszutauschen. Dazu hält der ISP zusätzliche Tracker vor, die die vorhandenen Peers nach dem optimalen Transferweg sortieren.

Ein weiteres neues Konzept ist Caching auf ISP-Ebene. Es ermöglicht die Reduzierung der Datenströme für Backhaul und Access: Clients müssen die Daten nur einmal in den Cache laden, von da an werden alle Netzabfragen aus dem Cache bedient. Erste Versuche mit Pando (BitTorrent-basiert) haben gezeigt, dass dies die Übertragungsgeschwindigkeit um 200 bis 800% erhöht und der Datenaustausch zwischen ISPs 40 bis 75% absinkt.

ERGEBNISSE AUF EINEN BLICK

Aus der Diskussion ergeben sich 5 Kernpunkte:

- Die Steuerung von Datenstaus und Kapazitätsengpässen gehört zu den zentralen Aufgaben jedes Netzbetreibers. Staffeltarife und Traffic-Management sind die geeignetsten Maßnahmen.

- Die Nutzung wird vermutlich parallel zur Bandbreitensteigerung durch Next-Generation-Netze ansteigen. Das macht das Problem noch dringender, denn es wird auch mehr datenintensive Anwendungen geben. Premium-Gebühren könnten helfen, die Kapazitäten auszugleichen und unter den Usern fairer zu verteilen.

- Zu einem gewissen Grad sind Traffic-Management-Maßnahmen immer erforderlich und zur Sicherung der QoS in verschiedenen Traffic-Typen vollkommen angemessen. Sie müssen nur offen kommuniziert werden, um die Serviceerwartungen mitzugestalten.

- Bei der Umsetzung des Managements ist die Debatte um Netzneutralität zu berücksichtigen. Protokollspezifische Implementierungen (wie im Fall BitTorrent) sind öffentlich scharf kritisiert worden. Nicht protokollspezifisches „Fair Use“-Management scheint daher am gerechtesten, wenn es sich nur auf unverhältnismäßige Nutzung bezieht und sich darauf beschränkt, aktuelle Überlastungen aufzulösen. Dieser Ansatz könnte die beste allgemeine QoS bieten, bei einem Interventionsgrad, der der Netzneutralität entspricht.

- Probleme im Bereich Traffic-Management lassen sich durch transparente, für alle Seiten akzeptable Vereinbarungen in den Griff bekommen, etwa zwischen Netzbetreibern und Application-Providern. Der Wettbewerbsgrad im Breitband-Markt sollte den Regulierungsbedarf bestimmen.

FALLSTUDIE 2: DIE BEKÄMPFUNG VON BOTNETS

Problem: Immer mehr Verbraucher-PCs sind von Bots infiziert, schädlicher Software, die von kriminellen „Bot Herders“ extern gesteuert wird. ISPs möchten Bots zum Schutz der Verbraucher aus dem Netz verbannen.
Risiko: Botnets sind der Ursprung der meisten digitalen Attacken wie Phishing, Spamming, Klickbetrug etc.

Botnets gelten als die schwerwiegendste Bedrohung der Netzintegrität durch kriminelle

Machenschaften. Es handelt sich um Gruppen von PCs in Haushalten, Firmen, Universitäten etc., die ohne das Wissen ihrer Besitzer in böswilliger Absicht von außen „ferngesteuert“ werden. Solche Netze können sich aus mehreren hunderttausend Computern zusammensetzen. Botnets eignen sich für verschiedene Zwecke, von Spamming über „Denial of Service“(DoS)-Attacken[5] bis zu Phishing und Klickbetrug. Beispiele aus der jüngsten Vergangenheit zeigen die verheerenden Auswirkungen Botnet-basierter DoS-Angriffe. Im April 2007 kam es in der estnischen Hauptstadt Tallin zunächst zu einer „manuellen“ DoS-Attacke, nachdem dort eine Statue aus der Sowjetzeit demontiert worden war. Blogger baten ihre Leser, bestimmte Services in Estland „anzupingen.” Ein „Ping“ ist ein Utility-Programm, das dazu dient, Testpakete an eine IP-Adresse zu schicken, um die Verfügbarkeit zu überprüfen. Normalerweise werden Pings zur Diagnose von Internet-Problemen abgesetzt, aber man kann sie auch zweckentfremden. Nachdem der Angriff erfolglos blieb, wurde ein Botnet „gemietet“ und eine echte DoS-Attacke gestartet. Ziele waren unter anderem die Websites der Regierung und des estnischen Parlaments, beinahe alle Ministerien, politische Parteien, drei der sechs großen Zeitungen des Landes, zwei der größten Banken sowie Unternehmen der Kommunikationsbranche. Der Angriff legte fast das gesamte digitale Leben eines Landes lahm, in dem immerhin 90% aller Bankvorgänge online getätigt werden.

*Eines der größten bekannten Botnets ist „Kraken“.**

Im April 2008 geriet Radio Free Europe, eine private, von den Vereinigten Staaten finanzierte Non-Profit-Organisation, unter massiven DoS-Beschuss. Mehrere osteuropäische Sites von Radio Free Europe wurden angegriffen, das heißt so mit fingierten Anfragen überschüttet, dass sämtliche Ressourcen davon belegt waren. Beide Angriffe waren politisch motiviert und wurden mit „gemieteten“ Botnets durchgeführt.

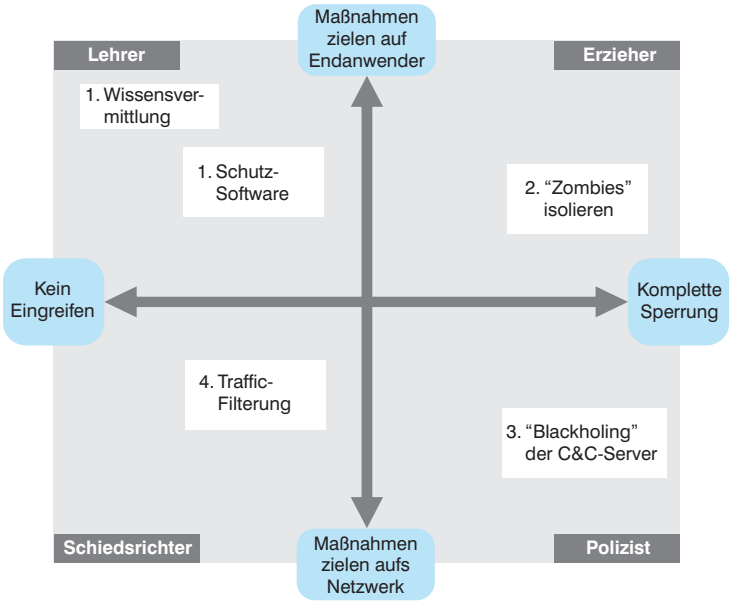
Da die meisten Anwendungen von Botnets rechtswidrig sind, kommt der polizeilichen Verfolgung bei ihrer Bekämpfung eine besondere Rolle zu. In den USA führte der FBI im Sommer 2007 die „Operation Bot Roast“ durch, bei der im ganzen Land rund 1 Million befallene Computer aufgespürt und zahlreiche Personen der Computer-/Cyberkriminalität angeklagt wurden. Andere Bekämpfungsstrategien neben der Strafverfolgung haben leider wenig Aussicht auf Erfolg. Eine Erstinfektion zu verhindern, ist am effektivsten, aber schwierig umzusetzen.

Die Ansätze einer „nicht polizeilichen“ Bekämpfung von Botnets lassen sich anhand einer thematisch angepassten Positionierungs-Matrix strukturieren (siehe Abb. 42). Dabei zeigt die vertikale Achse an, wo die Bekämpfung stattfindet: Auf der Verbraucher- oder der Netzseite. Die horizontale Achse gibt Aufschluss über den Grad der Intervention. Der linke Pol steht für den völligen Verzicht auf Eingriffe, der rechte für eine harte, interventionistische Position.

**500.000 infizierte PCs, 50 betroffene Fortune-500-Unternehmen.*

(5) In diesem Dokument wird durchgängig der Begriff „DoS“ verwendet. Genau genommen handelt es sich um „DDoS-Attacken“ („Distributed Denials of Service“, verteilte Dienstblockaden).

Abb. 42: *Digital-Confidence-Positionen zur Botnet-Bekämpfung*



1. Die meisten ISPs halten Informationen und Schutz-Software bereit
   - Vorteil: Kann bereits vor Bots schützen
   - Nachteil: Software-Schutz ist nicht 100% sicher und verlangt technische Vorkenntnisse
2. Separierung infizierter PCs vom Netz in einen „Walled Garden“ wird nur sehr begrenzt umgesetzt
   - Vorteil: „Garden“ verhindert Ausbreitung
   - Nachteil: Haftungsprobleme bei fälschlichem Verdacht, sehr serviceintensiv
3. „Blackholing“ meint im Prinzip das ausschließen von Servern vom Internet[1]
   - Vorteil: Sehr effektiv, besonders zur Bekämpfung älterer Botnets (oder von DoS-Attacken)
   - Nachteil: Extreme Maßnahme, da der Datenfluss komplett unterbunden wird
4. Filterung von Botnet-Traffic ist sehr effektiv, aber schwierig umzusetzen
   - Vorteil: Minimiert Bedrohung, ohne andere Bereiche zu sehr einzuschränken
   - Nachteil: Schwierig herauszufiltern, da kaum Unterschiede zu normalem Traffic

(1) Wird normalerweise nur für Control-Server und von DoS befallene Maschinen eingesetzt, nicht für infizierte PCs.

Aufklärung ist ein klares Beispiel für eine nicht sanktionierende und nutzerseitige Maßnahme: Die Verbraucher werden informiert, was Botnets sind und was man gegen sie tun kann. So hat etwa die European Network and Information Security Agency (ENISA) Verbraucherinformationen über Botnets, ihre Gefahren und mögliche Schutzmaßnahmen für Nutzer herausgebracht.

Eine andere Vorgehensweise, die in den „Lehrer"-Quadranten fällt, ist Software, die Computer vor einem Befall mit Bots bewahrt. Fast alle marktüblichen Antivirus- und Firewall-Produkte verfügen über Features zur Verhinderung der Infektion. Doch selbst die Hersteller solcher Programme sind nicht völlig immun: Blue Security, ein kleiner Anbieter von Sicherheitssoftware, fiel im Mai 2006 einer schweren DoS-Attacke zum Opfer und musste das Geschäft einstellen.

Blue Security hatte ein Anti-Spamming-Produkt entwickelt und auf den Markt gebracht, das als äußerst effektiv galt und ironischerweise selbst auf dem Botnet-Prinzip beruhte.(6) In der Folge wollten Spammer das Unternehmen durch Erpressung zur Aufgabe zwingen. Als Blue Security nicht darauf einging, kam es zu einem ersten DoS-Angriff auf die Server des Unternehmens – sie brachen zusammen. Die Admins leiteten den DNS-Eintrag auf TypePad um, einen der größten Blog-Hosts, der auch von Blue Security genutzt wurde. Wiederholte massive Attacken legten TypePad sowie Blue Securitys DNS-Provider Tucows lahm, beides große und viel frequentierte Websites. Nur durch eine konzertierte Aktion mehrerer Netzbetreiber und Serviceprovider konnte der Anschlag (mit Spitzenvolumina von über 3 GB pro Sekunde) abgewehrt und die beiden externen Seiten geschützt werden. Blue Security selbst war mehrere Tage lang offline. Zwei Wochen nach der ersten Attacke wurde das Anti-Spamming-Geschäft aufgegeben.

*„Blue-Security-CEO Eran Rehef über Spam-Bekämpfung: „Die Entscheidung liegt eindeutig bei der Politik. Die Spammer loszuwerden kostet 100 Mio. Dollar".**

Eine stärker nutzerzentrierte, aber interventionistische Möglichkeit besteht darin, die „Zombies", also die einzelnen Computer in einem Botnet, zu isolieren. Diese effektive, aber schwer zu bewerkstelligende Bekämpfungsmethode geht auf einen Vorschlag der Message Anti-Abuse Working Group (MAAWG) zurück. Infizierte Computer werden in einem „umzäunten Garten" mit Sicherheitsupdates und Desinfektionsmöglichkeiten vom Internet abgeschottet. Bis jetzt wurde dieses Verfahren nur sehr begrenzt eingesetzt, beispielsweise in großen privaten Netzen von Universitäten, da hier haftungsrechtliche Bedenken bestehen.

Als wirksamste Methode galt schon immer das Ausschalten („Blackholing") des Command-and-Control (C&C)-Servers eines Botnets. So gelang es schon 2004 dem norwegischen ISP-Monopolisten Telenor durch Stilllegung des C&C-Servers ein Botnet mit 10.000 Zombies unschädlich zu machen. Inzwischen haben die Bot Herder aber reagiert und verwenden zunehmend Netze ohne zentralen Server.

Zuletzt sei noch ein Netzseitiger, weniger tief eingreifender Ansatz zu erwähnt: Der Einsatz von Traffic-Filter-Technologien zur Bekämpfung von Botnets. Wie in anderen Anwendungsbereichen auch, dient die Filterung dazu, unerwünschte (Botnet-)Daten zu erkennen und die betreffenden IP-Pakete zu blockieren, sodass sie ihr Ziel nicht erreichen. Die Herausforderung ist jedoch, dass sich Botnet-Verkehr nur schlecht ausfiltern lässt, weil er starke Ähnlichkeit mit normalem Internet-Traffic aufweist. Viele ISPs und Netzbetreiber verfolgen derzeit eine vereinfachte Version dieses Ansatzes, indem sie allen Traffic blocken, der für Botnets typisch ist – allerdings mit dem Risiko, auch legitime Anwender auszugrenzen.

Darüber hinaus tun sich immer mehr IPSs mit den Strafverfolgern zusammen, überwachen Netzaktivitäten und informieren über Unregelmäßigkeiten. So konnte 2005 ein großes Botnet in den Niederlanden neutralisiert werden, nachdem der Provider XS4ALL den Behörden von „ungewöhnlichen Aktivitäten" in seinem Netz berichtete. Das Botnet bestand aus 1,5 Millionen Zombies. Drei Personen wurden angeklagt.

ERGEBNISSE AUF EINEN BLICK

Aus der Diskussion ergeben sich 7 Kernpunkte:

- Ihre Offenheit und Neutralität machen IP-Netze sehr leistungsstark, aber auch anfällig für „böse Absichten" wie das Betreiben von Botnets.

- Wegen ihrer Vielseitigkeit bei potenziellen Attacken sind Botnets eine Hauptgefahr für die Netzintegrität und damit für Netzbetreiber, Serviceprovider, Unternehmen und Verbraucher. Wie die Beispiele Estland und Radio Free Europe zeigen, sind viele Botnet-Aktivitäten politisch motiviert.

- Eine der schwerwiegendsten Angriffsarten ist die Denial-of-Service(DoS)-Attacke, durch die Seiten lahmgelegt und Unternehmen erpresst werden können. Alle großen DoS-Attacken der letzten Jahre gingen von Botnets aus.

*http://blogs.guardian.co.uk/technology/2006/05/17/spammers_kick_blue_frog_into_submission.html

(6) Sobald „Blue Frog" einen Spammer entdeckte, schickten alle mit Blue Frog arbeitenden Computer eine E-Mail an die Adresse – praktisch eine kleine DoS-Attacke auf den Urheber.

• Die behördliche Strafverfolgung spielt bei der Bekämpfung von Botnets eine wichtige Rolle. Um erfolgreich zu sein, bedarf es dabei der Mitarbeit anderer Stakeholder wie Netzbetreiber und ISPs.

• Aufklärung ist zwar nötig, aber wegen der Komplexität und Erklärungsbedürftigkeit des Themas nur begrenzt wirkungsvoll. Verbraucher können Infektionen nur schwer erkennen.

• Netzbetreiber müssen bei schweren Botnet-Attacken technische Gegenmaßnahmen treffen können. Da die Maßnahmen komplex sind und in das Verbraucherverhalten eingreifen, müssen die Betreiber mit allen Stakeholdern kooperieren, um die Eingriffe so gering wie möglich zu halten.

• Die Isolation von Zombies in „umzäunten Gärten" und die Zusammenarbeit mit Software-Herstellern zur Desinfektion von PCs sind vielversprechende Lösungen. Doch sie müssen möglichst nutzerfreundlich umgesetzt werden (mit minimalem Bedarf an Kundensupport und Opt-out-Möglichkeit für zu Unrecht Verdächtigte).

FALLSTUDIE 3: DIE BLOCKIERUNG VON PHISHING

Problem: Phishing-Mails werden zum Identitätsklau oder zu Betrugszwecken eingesetzt.
Risiko: Verbraucher können große Summen verlieren, zum Beispiel durch Diebstahl von Bankdaten. Die Authentizität der Mails ist oft schwer zu überprüfen.

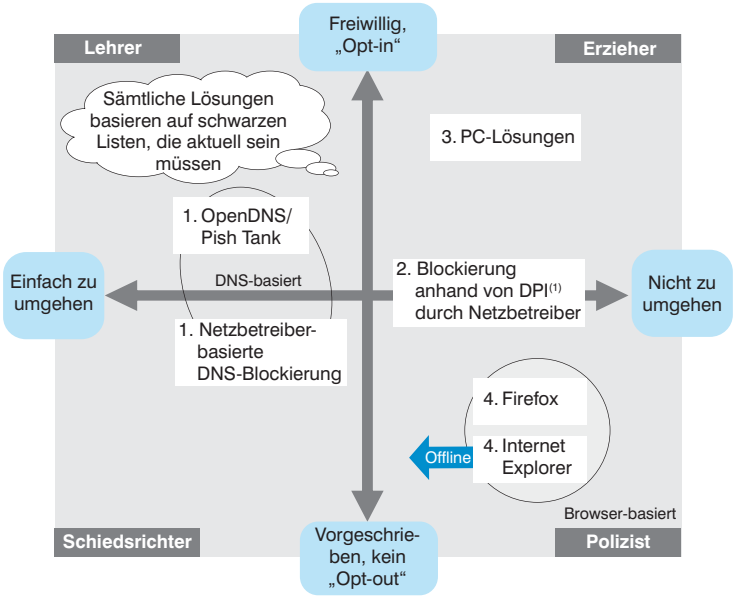
Phishing wird oft als eine der kritischsten und schnellstwachsenden Bedrohungen für den Datenschutz bezeichnet. Da es sich um ein äußerst komplexes Phänomen handelt, ist die notwendige Sicherstellung von Aufmerksamkeit und Wissen beim Verbraucher eine anspruchsvolle Aufgabe. Und die Herausforderung wächst, seit Phishing-Mails und -Webseiten immer professioneller auftreten und zunehmend schwierig von seriösen Angeboten zu unterscheiden sind – sogar für Experten, die wissen, wonach sie suchen müssen.

Kein Phishing-Filter bietet 100%ige Sicherheit.

Daher kann der Aufklärung nur eine begleitende Rolle bei der Verhinderung von Phishing-Schäden zukommen. Neben der noch konsequenteren Strafverfolgung von Personen und Firmen, die Phishing betreiben, besteht die wichtigste Gegenmaßnahme in der Blockierung der Angriffe mit technischen Mitteln.

Die verschiedenen Ansätze zur Phishing-Blockierung lassen sich mit der angepassten Positionierungs-Matrix zu Digital Confidence aufschlüsseln (siehe Abb. 43), wobei die vertikale

Abb. 43: *Digital-Confidence-Positionen zur Blockade von Phishing*



1 DNS-basierte Lösungen können bestimmte Domains auf dem DNS-Server des Netzbetreibers oder auf externen Servern blockieren
- Vorteil: Funktioniert bei allen Anwendungen (nicht nur bei Browser, sondern auch bei E-Mail etc.)
- Nachteil: Nur für URL-basiertes Phishing sinnvoll

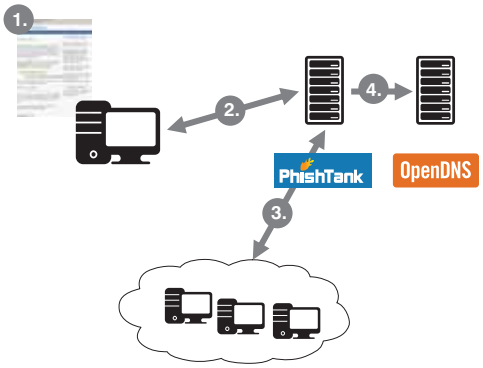
2 Deep Packet Inspection (DPI) beim Netzbetreiber prüft den Inhalt aller Pakete und leitet schädlichen Traffic um(1)
- Vorteil: Funktioniert für alle Anwendungen und viele Arten von Phishing-Angriffen
- Nachteil: Datenschutzbedenken, umgehbar durch Verschlüsselung

3 PC-basierte Sicherheitslösungen beinhalten für gewöhnlich auch einen Phishing-Filter
- Vorteil: Je nach Lösung Schutz sämtlicher Anwendungen möglich
- Nachteil: Muss installiert und konfiguriert werden

4 Aktuelle Browser können URLs mit Server-/ lokalen Blacklists abgleichen (auch heuristisch)
- Vorteil: Kaum Datenschutzbedenken (je nach Implementierung)
- Nachteil: Kein Schutz in anderen Anwendungen wie Mail oder älteren Browser-Versionen

(1) Zum Beispiel in Verbindung mit Werbung (Phorm).

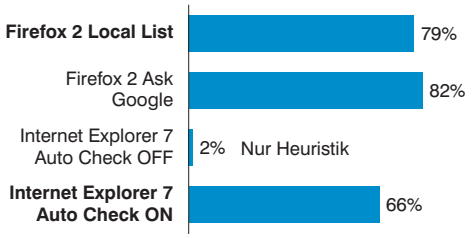
Abb. 44: *Blockierung von Phishing-Sites im Überblick*



1. Nach Eingang einer Phishing-E-Mail ruft der Nutzer die Website auf und **identifiziert die Phishing-Attacke anhand der E-Mail und der Website**
2. Der Nutzer leitet die URL als mögliche Quelle von Phishing an OpenDNS/PhishTank weiter
3. Die OpenDNS/PhishTank-Community verifiziert den Angriff
4. Domain kommt auf die schwarze Liste von PhishTank und wird in OpenDNS blockiert
5. Versuche, auf den Link zuzugreifen, werden blockiert

Quelle: OpenDNS.com, Phishtank.com

Abb. 45: *Wirksamkeit der browserbasierten Blockierung von Phishing (2006)*



Fett: Standardmodus
Quelle: Mozilla Foundation

Achse anzeigt, inwieweit der Nutzer sich freiwillig für eine Lösung entscheiden kann („Opt-in“) oder ob der der Schutz so lange aktiv ist, bis er sich dagegen ausspricht („Opt-out“). Die horizontale Achse zeigt den Grad der Umgehbarkeit der Lösung.

OpenDNS und FishTank sind Beispiele für ein Community-basiertes Vorgehen zur Identifizierung und Indizierung von Phishing-Sites (siehe Abb. 44). Dank der Größe der Community können Attacken sehr schnell, in weniger als 12 Stunden, entdeckt und überprüft werden. Dieser Ansatz verbindet sich mit DNS-Filterung und beruht auf der Möglichkeit, einzelne Domains gezielt zu blockieren. Dies kann entweder vom DNS-Server des ISPs geschehen oder von Drittservern. Die Methode hat den erheblichen Vorteil, dass sie für alle Anwendungen funktioniert, also nicht nur für Webtraffic via Browser, sondern beispielsweise auch für E-Mails. Sie ist jedoch nur bei URL-basiertem Phishing anwendbar, was sie auf rund 90% aller Attacken limitiert (10% verwenden IP-Adressen anstatt Domainnamen). Weitere potenzielle Hürden: Die DNS-basierte Blockierung kann, je nach verwendeter Lösung, eine Konfigurierung des Enduser-Equipments erfordern. Außerdem kann bei Blockierung durch den ISP „Overblocking“ zum ernsten Problem werden, wenn der Zugriff auf eine Seite eingeschränkt wird, die fälschlicherweise indiziert wurde.

Des Weiteren können ISPs auch DPI zur Blockierung von Phishing-Attacken einsetzen. DPI-Lösungen sind in der Lage, jedes Paket zu inspizieren, das im Netz unterwegs ist, und sie können bösartigen Traffic umleiten, also auch Traffic zu Webseiten, die auf „schwarzen Listen“ stehen. Dies funktioniert anwendungsübergreifend und ist daher bei den meisten Phishing-Attacken wirksam, ruft aber auch die einschlägigen Datenschutz-Bedenken bei DPI-Lösungen auf den Plan: Verbraucher könnten sich durch die so erzeugte höhere Transparenz verunsichert fühlen, selbst wenn die Daten sicher verwahrt und nicht für andere Zwecke genutzt werden. Der Einsatz von DPI zur Verhinderung von Phishing ist sehr effektiv und kann nur durch Verschlüsselung von Traffic umgangen werden (was bei Phishing-Angriffen selten der Fall ist).

Technologie ist der Schlüssel zur Phishing-Bekämpfung. Sie muss auf allen Ebenen greifen: Netz, PC und Browser.

Drittens kann man auch den Verbraucher-PC in den Mittelpunkt stellen. Viele der heutigen PC-basierten Sicherheitslösungen schließen einen Phishing-Filter mit ein, so wie die Sicherheits-Suites von Norton, McAfee, Sophos etc., die dem Verbraucher oft gleich vom ISP oder Netzbetreiber zur Verfügung gestellt werden. Diese Filter können sehr effektiv sein, denn je nach verwendeter Lösung sind sie für alle Applikationen wirksam und bieten daher einen guten Rundumschutz gegen Phishing. Ein Nachteil ist, dass sie stark von der Mitarbeit des Verbrauchers

Einwandfreies Blacklisting ist entscheidend: Nur indizierte Phishing-Sites werden blockiert.

abhängig sind, denn die Lösungen wollen installiert, konfiguriert und aktualisiert sein. Vor allem das regelmäßige Herunterladen der lokalen Blacklists ist für das einwandfreie Funktionieren der Filter entscheidend.

Nicht zuletzt kann Phishing-Blockierung auch im Browser-Layer durchgeführt werden. Aktuelle Versionen wie Internet Explorer 7 und Firefox 2 können URLs mit externen oder lokal gespeicherten schwarzen Listen abgleichen, um Phishing-Attacken zu erkennen und zu unterbinden. Auch heuristische Erkennungsmethoden sind möglich (zum Beispiel ausgehend von Mustern auf URLs, die bereits für Phishing benutzt wurden; diese Methode hat aber eine sehr geringe Erfolgsrate von nur 2%). Der Vorteil dieses Ansatzes ist, dass er keine größeren datenschutzrechtlichen Bedenken hervorruft, solange die Blockierung lokal erfolgt – etwa wie bei Firefox, der ein Verzeichnis von Phishing-Sites herunterlädt und sie automatisch überprüft. Eine Einschränkung besteht darin, dass die Browser-basierte Sperrung nicht gegen Angriffe auf andere Anwendungen wie zum Beispiel E-Mail hilft (derzeit nur ein geringfügiges Problem). Darüber hinaus ist sie anfällig für bösartige Software auf dem Anwender-System, zum Beispiel Bots (vgl. Kapitel III), die die Funktionen deaktivieren oder die Blacklist manipulieren.

Browser-basierte Phishing-Blockierung ist vor allem dann effektiv, wenn neue Browser verwendet werden. Ältere Versionen wie Internet Explorer 6 müssen mit Add-ons von Drittanbietern aufgerüstet werden (die meist auf ähnliche Blacklists zurückgreifen).

Bei allen vier Ansätzen sind schwarze Listen erforderlich – sonst weiß der Blocker nicht, was er blockieren soll. Letztendlich entscheidet der Inhalt dieser Verzeichnisse über den Erfolg der Maßnahme sowie über die generelle Akzeptanz von Anti-Phishing: Enthält eine Blacklist zu viele Einträge, kommt es zu „Overblocking", das heißt, es werden auch einwandfreie Seiten gesperrt (zum Beispiel wenn die wirkliche Log-in-Page zum Online-Banking versehentlich mit indiziert wurde). Wenn sie hingegen unvollständig ist oder zu selten aktualisiert wird, ist der Schutz mangelhaft und der Anbieter könnte haftbar gemacht werden.

ERGEBNISSE AUF EINEN BLICK

Aus der Diskussion ergeben sich 5 Kernpunkte:

- Da Phishing für Verbraucher kaum erklärbar ist, kann Aufklärung nur eingeschränkt wirksam sein. Ihr kommt eine begleitende Rolle zu.

- Die Blockierung der Phishing-Attacken ist eine zentrale Gegenmaßnahme. Die unterschiedlichen Ansätze haben jeweils Vor- und Nachteile bezüglich Effektivität, Abdeckung (wie viele Anwendungen sie schützen), Datenschutzbedenken und dem erforderlichen Engagement des Verbrauchers, die sorgfältig abgewogen werden müssen.

- Ausschlaggebend für alle Blocking-Strategien ist die Erstellung und Pflege von schwarzen Listen, die zu blockierende Phishing-Sites abbilden. Heute werden mehrere umfassende Verzeichnisse angeboten (zum Beispiel von Google, PhishTank) und eingesetzt.

- Browserbasierte Lösungen sind heute besonders wichtig, da sie dem Nutzer die größtmögliche Interaktivität garantieren und im Angriffsfall auch nahtlos Informationen mit einschließen. Ein großes Problem sind ältere Browser, die noch keine Schutzmechanismen enthalten. Hier muss die Software-Industrie mit den ISPs zusammenarbeiten, um die aktuellsten Browserversionen zu pushen.

- Den meisten Erfolg versprechen Lösungen, die dem (erfahrenen) User eine Möglichkeit zum Opt-out und zum Überstimmen der Blockierung lassen, falls beispielsweise Content zu unrecht indiziert wurde. Diese Ansätze müssen ebenfalls die Privatsphäre achten und keine Datenschutzbedenken aufkommen lassen (zum Beispiel lokale Blacklists).

FALLSTUDIE 4: TARGETED ADVERTISING

Problem: Bei der Nutzung des Internets entstehen viele Verhaltensdaten, die die Wirtschaft für die gezielte Kundenwerbung einsetzen möchte.

Risiko/Vorteil: Datenschutzbedenken bei Verbrauchern, aber auch deutlich relevantere Werbung (und entsprechend mehr Umsatz).

Mit dem Web 2.0 entstanden viele neue Services auf der Grundlage von sozialen Netzen. Beste Beispiele: Facebook und MySpace. Bei vielen von ihnen brachen die Mitglieder- und Userzahlen alle Rekorde – in der Regel auch deshalb, weil sie für die Verbraucher kostenlos angeboten werden. Trotzdem steigt der Druck auf die Anbieter, diese Dienstleistungen in Zukunft auch finanziell zu verwerten. Es ist zu erwarten, dass Werbung, und hier besonders die gezielte, kontextbezogene Nutzeransprache (Targeted Advertising), bei der Monetarisierung von

Web-2.0-Services eine zentrale Rolle spielen wird. Wie unsere Marktanalyse zeigt, wird kein anderes Segment der digitalen Welt so schnell wachsen wie die Werbeeinnahmen (vgl. Kapitel II). Große Internet-Player wie Google und Yahoo! haben schon begonnen, daraus Kapital zu schlagen: Werbung ist ihre einzige Einnahmequelle. Es ist also nicht überraschend, dass es in diesem Bereich in letzter Zeit große Umwälzungen gegeben hat. Google kaufte im April 2007 für 3,1 Mio. Dollar DoubleClick, einen der führenden Online-Marketer. Im Juli 2007 kaufte AOL den Behavioral-Ad-Spezialisten Tacoda. Und Yahoo! erwarb im September 2007 Blue Lithium, Anbieter Performance-gesteuerter Werbemittel. Daneben setzen auch Netzanbieter zunehmend auf werbebasierte Geschäftsmodelle, um ihre Wachstumsambitionen zu realisieren.

Wenn es richtig gehandhabt wird, kann Targeted Advertising ein „Win-Win" für Verbraucher und Industrie sein: Die Werbung wird relevanter und damit weniger lästig, die Ansprache ist gezielter und dadurch kosteneffizienter.

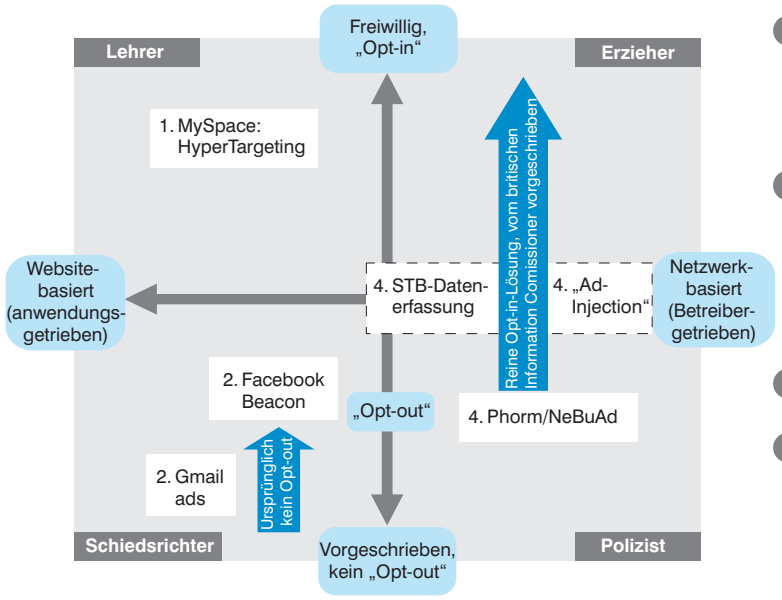
Die wirtschaftlichen Zusammenhänge liegen auf der Hand: Junge Konsumentengruppen verbringen immer mehr Zeit im Web. Außerdem macht das Internet dem Werbetreibenden zusätzliche Informationen verfügbar: Wofür interessiert sich der Verbraucher? Wo wohnt er? Einige dieser Informationen werden auf Plattformen wie Facebook offen ausgetauscht, andere erhält man durch Sammeln von Verhaltensdaten.

Die meisten, wenn nicht alle, neuen Geschäftsmodelle beruhen auf einer extensiven Datensammlung, was dazu geführt hat, dass einige jüngste Entwicklungen Datenschutz-Bedenken hervorgerufen haben. So veranstaltete in den USA die Federal Trade Commission (FTC) im November 2007 eine Tagung zum Thema „Online Behavioral Advertising" mit spezieller Betonung der Datenschutzproblematik und ging danach mit eigenen „Online Behavioral Advertising Principles" an die Öffentlichkeit.

Aus Sicht der Digital Confidence lassen sich die Wachstumstreiber und Lösungskonzepte des Targeted Advertising in einer thematisch angepassten Version der Positionierungs-Matrix anordnen (siehe Abb. 46). Die horizontale Achse differenziert, ob Werbung Website-/Applikations-basiert ist (von Internet-Akteuren wie sozialen Netzen) oder Netz-getrieben (von Kabelbetreiber oder ISPs). Die vertikale Achse zeigt an, inwieweit der Anwender selbst bestimmen kann, ob seine Daten zu Werbezwecken genutzt werden oder nicht. Die Möglichkeiten reichen von „Opt-in", der völlig freien Entscheidung, bis zu „No Opt-out", also der automatischen Verwendung, solange der Nutzer keinen expliziten Einwand erhebt.

Es gibt vier verschiedene Beispiele für die Umsetzung von Targeted Advertising. MySpace testet eine Lösung, die als besonders „Opt-in"-

Abb. 46: *Digital-Confidence-Positionen zur gezielten Werbung*



1. HyperTargeting von MySpace kategorisiert Nutzer anhand ihrer angegebenen Interessen und sendet sie mit entsprechender Werbung
   - Werbetreibende wählen die Kategorien
   - Noch in der Testphase, aber schon jetzt Datenschutzdiskussion
2. Facebook Beacon führt Facebook mit anderen Websites zusammen (Aktivitäten dort werden an Facebook weitergeleitet)
   - Ursprünglich Erweiterung von „Facebook Stories", kann jedoch für personalisierte Werbung eingesetzt werden
   - Starke Datenschutzdiskussion nach Einführung mit Gerichtsverfahren gegen Partner-Websites („Harris vs. Blockbuster")
3. Google Mail passt Werbung dem Inhalt von E-Mails an (automatisierte Content-Erkennung)
4. Ansätze der Netzbetreiber analysieren alle Nutzer-Aktivitäten im Web (Adserving für Partner-Sites oder „Injection" in alle Sites(1))
   - Datenschutzbedenken, da zur Profilerstellung der gesamte Datenverkehr inspiziert wird
   - Nach Test von BT ohne Zustimmungsmöglichkeit forderte das ICO (GB) Phorm-Implementierungen nach britischem Recht mit „Opt-in"

(1) Aktuelle Lösungen sind auf Adserving ausgerichtet.

freundlich gilt. Hingegen startete Facebook mit „Facebook Beacon“ 2007 eine Anwendung, die ganz ohne Zustimmung der Nutzer auskommen sollte und nur auf massiven öffentlichen Druck in eine „Opt-out“-Lösung umgewandelt wurde. Ein Beispiel für die erfolgreiche Umsetzung von kontextbezogener Werbung ist Gmail: Bei seinem kostenlosen E-Mail-Angebot analysiert Google den Inhalt von E-Mails, um in der Schnittstelle gezielt Anzeigen platzieren zu können. Dies ist integraler Bestandteil der Dienstleistung, die Nutzer müssen zustimmen, dass sie Werbung anhand ihres E-Mail-Verkehrs erhalten. Doch dem Erfolg nach zu urteilen nehmen Gmail-User daran nicht viel Anstoß. Dennoch hat Gmail beim Launch 2004 zunächst heftige Datenschutz-Debatten ausgelöst. Die Vorwürfe reichten von der unbefristeten Speicherung von Daten bis zur unbefugten Durchleuchtung von E-Mails Dritter.

85% aller User möchten nicht, dass ihnen Werbung gezeigt wird, die von früher besuchten Websites abgeleitet ist.

Die „HyperTargeting“-Lösung von MySpace kategorisiert Anwender nach den Interessen auf ihrem öffentlichen Profil (über 100 Kategorien). Werbetreibende können passend zu ihrer Kampagne die Zielkategorien frei wählen. Bei Vorabtests erreichte MySpace damit eine „Click-through“-Steigerung von 300% (die Anzeigen wurden dreimal so häufig angeklickt wie zuvor) und einen 50%igen Anstieg des Tausenderkontaktpreises oder „cost per mille“ (CPM). CPM ist die Standardeinheit zur Berechnung von Werbepreisen nach der Anzahl von Zielgruppenkontakten. Auch wenn es sich bisher nur um Tests handelt, wurden die datenschutzrechtlichen Konsequenzen schon intensiv diskutiert. Doch mit der Entscheidung für eine „Opt-in“-Lösung zeigt MySpace ganz offensichtlich Respekt für die Belange der Anwender.

Mehrere Partner zogen sich von Facebook Beacon zurück, nachdem sie gemerkt hatten, dass kein Opt-out bestand.

Im Gegensatz dazu war Facebook Beacon seit dem Start mit 44 Partner-Sites im November 2007 als allgemeingültiges Angebot ohne vorherige Zustimmung geplant. Es band Facebook in sämtliche Partner-Sites ein und ermöglichte den Austausch umfassender Datensammlungen und Profile, solange der Facebook-User eingeloggt war. Ursprünglich als Erweiterung für „Facebook Stories“ gedacht („Dein Freund hat sich das Video XYZ auf Joost angeschaut“), eignet sich Beacon auch für Targeted Advertising. Nach der Einführung wurden Bedenken über die Datensicherheit laut und einige teilnehmende Unternehmen wurden angeklagt. Daher entschloss sich Facebook schon im Dezember 2007 für eine Opt-out-Möglichkeit.

Am Beispiel Gmail fällt auf, wie mit potenziellen Unsicherheiten offen umgegangen werden kann. Auf der Website macht Google in einem ausführlichen Text klar, welche Vorteile kontextbezogene Werbung für den Verbraucher hat: „Google meint, das unsere User größeren Nutzen aus gezielte Botschaften ziehen als aus zufälligen Pop-ups und irrelevanten Banner-Ads.” Gmail löst wahrscheinlich auch deswegen weniger Kontroversen aus, weil die Nutzer die Werbung nach eigenen Aussagen als hilfreich empfinden und die Daten restriktiv eingesetzt werden, das heißt auf den betreffenden Nutzer und die Gmail-Anwendung beschränkt bleiben.

„Phorm“ und „NebuAd“ sind netzbasierte Lösungen für Targeted Advertising, die alle Surfaktivitäten von Internet-Usern analysieren und die gezielte Platzierung von Online-Werbung erlauben. Phorm soll in Kürze bei großen Netzanbietern wie BT und Virgin in Großbritannien probeweise an den Start gehen. Es verwendet DPI zur Untersuchung der Netzaktivitäten, inspiziert also den gesamten Traffic und leitet daraus Profile ab.

Die hochentwickelten Monitoring-Fähigkeiten von DPI selbst bei der Erkennung von anonymisiertem Traffic für Targeted-Advertising-Zwecke haben die Aufmerksamkeit und Kontrolle seitens der Regulierer heraufbeschworen. Die Einführung solcher Dienste in einigen Märkten hat zu starken Medienreaktionen und zu Kritik durch die Anwender geführt, insbesondere wegen der Art und Weise, wie die Technologie von den Netzbetreibern getestet wurde – beziehungsweise versucht wurde zu testen: So begann BT einen Pre-Trial von Phorm-basiertem Targeted Advertising zunächst, ohne seine Kunden darüber zu informieren. Dies rief das britische Information Commissioner’s Office (ICO) auf den Plan, das verlangte, die für den Test relevanten Kunden über die Technologie aufzuklären und ihre Zustimmung durch ein aktives „Opt-in“ einzuholen, wobei eine Aufkündigung jederzeit möglich sein sollte.

Charter Communications, der viertgrößte Kabelbetreiber der USA, stellte seine Versuche mit Targeted Advertising schon nach einem Monat wieder ein. Auch wenn Q&As auf der Internetseite des Unternehmens für eine gewisse Transparenz gesorgt hatten, waren die Anwen-

der vom angekündigten kommunikativen Zusatznutzen („enhanced browsing experience“) nicht zu überzeugen. Außerdem wendeten sie sich gegen den Einsatz von DPI, der als zu invasiv empfunden wurde, und befürchteten trotz gegenteiliger Versicherungen eine Zweckentfremdung der Profile. Nicht zuletzt war den Nutzern die angebotene Opt-out-Lösung zu umständlich: Sie sollten ein Formular ausfüllen und ein Cookie akzeptieren. (Nach einer Cookie-Bereinigung oder einem Browserwechsel wäre das Targeted Advertising allerdings wieder aktiviert gewesen – bis zum nächsten Opt-out per Formular).

Neben Lösungen wie Phorm kann netzbasierte kontextbezogene Werbung auch über Set-Top-Boxen in Zusammenhang mit Ad-Injection platziert werden. Dies eröffnet auch DTV-Plattformen den Zugang zu Community-artigen Funktionen (wie kumulierten User-Ratings), plattformübergreifenden Promotion-Aktionen und gezielterer Werbung. Dabei kann die STB als Schnittstelle für interaktive Botschaften genutzt werden, beispielsweise für auf die Sehgewohnheiten abgestimmte VoD-Angebote („Sie haben schon 10 Dokumentarfilme über die afrikanische Tierwelt angeschaut. Würden Sie gern eine Dokumentation über Löwen herunterladen?“). Ein solcher Ansatz basiert auf der Sammlung von Zapping- und Programmdaten.

ERGEBNISSE AUF EINEN BLICK

Aus der Diskussion ergeben sich 6 Kernpunkte:

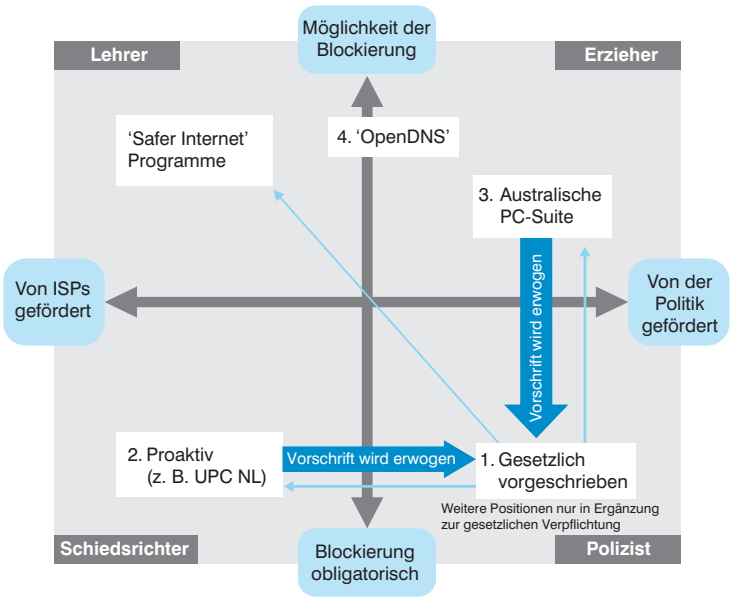
- Targeted Advertising ist deutlich auf dem Vormarsch, begünstigt von einigen zentralen Faktoren: Breitband als Massenphänomen, Verfügbarkeit von hochentwickelten Internet-Monitoring-Technologien und Bedarf an neuen Geschäftsmodellen zur Verwertung neuer Web-2.0-Services und -Plattformen.

- Targeted Advertising wird bei der Finanzierung innovativer Dienstleistungen eine Schlüsselstellung einnehmen, insbesondere bei der Verwertung von Web-2.0-Services und -Applikationen. Bei richtiger Handhabung hat auch der Verbraucher einen Mehrwert (siehe Gmail).

- Wegen der reichhaltigen Daten, die auf sozialen Netzen ausgetauscht werden, eignen sie sich besonders für Targeted Advertising. Netzanwender sind erst dabei, die Möglichkeiten zu erkennen.

- Frühe Ansätze im Targeted Advertising mit DPI und anderen Technologien haben in der Öffentlichkeit und den Medien für großes Aufsehen gesorgt und stießen häufig auf Datenschutz-Bedenken oder Ablehnung.

Abb. 47: *Digital-Confidence-Positionen zur Blockierung von Kinderpornografie*

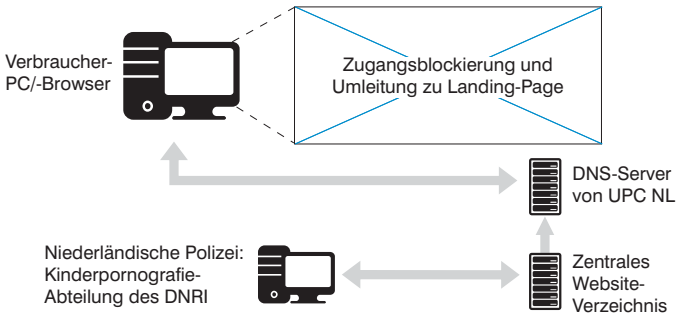


1. Standardposition von ISPs: Inhalte nur blockieren, falls gesetzlich vorgeschrieben
   - Plus: Basisschutz gewährleistet
   - Minus: Kein zusätzlicher Schutz möglich
2. Proaktive ISPs blockieren bestimmte Angebote auch ohne gesetzliche Verpflichtung
   - Plus: Verhindert ungewollten/zufälligen Zugang
   - Minus: Fließende Grenze zwischen Schutz und Zensur, wenn Dritte Blacklists zweckendfremden
3. Entwicklung einer PC-basierten Lösung für Eltern durch die australische Regierung
   - Plus: Anwender können sich aktiv schützen
   - Minus: Installation und Konfiguration erfordern Spezialwissen, hoher Preis, nicht Hacker-sicher
4. „OpenDNS“-Lösungen sind anbieter-getrieben und überlassen Nutzern die Auswahl von zu blockierenden Kategorien
   - Plus: ISPs nicht für Content verantwortlich
   - Minus: Kein gleichmäßiger Schutz – abhängig von persönlicher Initiative und Vorlieben

• Um die allgemeine Nutzerakzeptanz zu erreichen, genügt es nicht, die Datenschutzvorschriften einzuhalten. Der Schlüssel ist transparente Information über geplante Targeted-Advertising-Initiativen und die klare Kommunikation des Zusatznutzens für die Anwender („What's in it for me?").

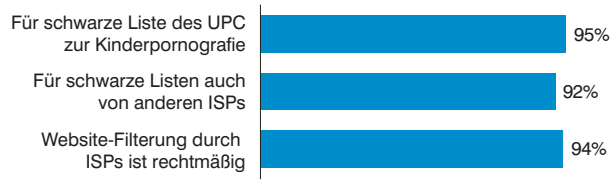
• An bereits erfolgten Einführungen lässt sich zeigen, dass fehlende Transparenz zur Erzwingung von Opt-in-Modellen führen kann. Einfach zu bedienende, klar kommunizierte Opt-out-Tools werden aber offenbar akzeptiert, vor allem, wenn sie mit einem echten (kostenlosen?) Mehrwert verbunden sind, wie der Fall Gmail zeigt.

Abb. 48: *Blockierung von Kinderpornografie – technische Umsetzung*



Hinweis: Techn. Lösung vereinfacht.
Quelle: UPC

Abb. 49: *Blockierung von Kinderpornografie in der öffentlichen Meinung*



Quelle: NSS-Befragung (n = 600)

FALLSTUDIE 5: BLOCKIERUNG VON KINDERPORNOGRAPHIE

Problem: Sperrung von Websites, die den sexuellen Missbrauch von Kindern zeigen (mehrere tausend Sites).
Risiko: Die Gefahr, unbeabsichtigt auf Kinderpornografie-Seiten zu gelangen, ist gering, sie sind aber auffindbar. Die Opfer werden schwer geschädigt.

Inhalte, die den sexuellen Missbrauch von Kindern darstellen, sind in den meisten Ländern der Welt verboten (mit Unterschieden in der Abgrenzung von „Kindern" und „Jugendlichen" im Bereich zwischen 14 bis 18 Jahren). Dennoch werden sie im Internet auf Tausenden von Seiten angeboten.

Die Bekämpfung konzentriert sich auf die strafrechtliche Verfolgung derjenigen, die für die Existenz von Kinderpornografie verantwortlich sind: Ihre Konsumenten zum einen, Produzenten zum anderen. Diese Aufgabe kann nur von den Strafverfolgungsbehörden geleistet werden, die dabei aber, soweit erforderlich und gesetzlich vertretbar, durch andere Stakeholder (zum Beispiel Netzanbieter) unterstützt werden können. Die Politik ist dabei, ihr Engagement in diesem Bereich zu verstärken: Vor einigen Monaten, im Mai 2008, stellte der US-Senat für die nächsten 8 Jahre insgesamt 1 Mrd. Dollar für ein entschiedenes Vorgehen gegen Kinderpornografie bereit.

*In den Vereinigten Staaten werden jährlich über 1.500 Personen wegen Besitz von Kinderpornografie aus dem Netz festgenommen. Die meisten besitzen mehrere hundert Fotos von Kindern zwischen 6 und 12 Jahren.**

Auf der anderen Seite fällt die Aufgabe, Internetnutzer vom versehentlichen Kontakt mit diesen pornografischen Inhalten zu schützen, vor allem in das Ressort der Netzanbieter. Doch das ist leichter gesagt als getan, denn das Thema ist vielschichtig und kontrovers: Erstens setzen sich blockierende Unternehmen Zensurvorwürfen und Haftungsansprüchen aus, zweitens ist eine wasserdichte Blockade fast unmöglich, da sämtliche zur Verfügung stehenden Techniken auch außer Kraft gesetzt werden können.

Die heutige Rechtsprechung deckt nicht alle Probleme sexuellen Missbrauchs im Internet ab.

Ein Problem ist, dass Verbot und Sperrung eine einheitliche Definition von Kinderpornografie voraussetzen. In der Praxis hat sich gezeigt, dass hier eine Grauzone zwischen Pornografie und Kunst besteht. Außerdem müssen die Definitionskriterien eindeutig einklagbar sein. Ob aber ein Jugendlicher, der in einem obszönen Kontext gezeigt wird, Opfer von Kinderpornografie ist (das heißt, ob die kritische Altersgrenze des jeweiligen Landes unterschritten ist), ist meist nur schwer oder gar nicht feststellbar. Außerdem werfen Bilder, die mit Bildbearbeitungssoftware erstellt und manipuliert wurden, (juristische) Probleme ganz anderer Art auf, die bei der Schaffung der meisten Gesetze noch gänzlich unbekannt waren.

Die verschiedenen Ansätze bei der Blockierung von Kinderpornografie lassen sich eben-

*National Centre for Missing & Exploited Children

falls anhand der Positionierungs-Matrix für Digital Confidence verdeutlichen (siehe Abb. 47). Hierbei differenziert die vertikale Achse, ob die Sperrung optional (das heißt dem Nutzer überlassen), freiwillig (vom Netzbetreiber selbst auferlegt) oder obligatorisch ist, während die horizontale Achse anzeigt, ob Netzbetreiber oder Regulierer die treibende Kraft hinter der Blockierung sind.

Bisher ist die dominante Methode, die über juristisch verfügte Blockaden hinausgeht, die freiwillige Filterung obszöner Inhalte anhand von Verzeichnissen verbotener Inhalte, die von Dritten erstellt, gepflegt und geprüft werden. ISPs stehen einer solchen Filterung meist zögerlich gegenüber, schließlich kommt ihnen als „reine Durchleiter" nicht die Rolle zu, Internet-Freiheiten zu beschränken. Darüber hinaus möchten sie nicht dafür belangt werden, wenn aus Versehen legaler Content mitgeblockt wird. Falls Filterung eingesetzt wird – ob freiwillig oder unter Strafandrohung –, sollte es rechtliche Instanzen geben, die unabhängig kontrollieren, ob die zu filternden Inhalte unter bestehendem Recht tatsächlich illegal sind.

Ein herausragendes Beispiel für das proaktive Engagement eines ISPs ist die Anti-Kinderpornografie-Kampagne der niederländischen UPC. Seit Anfang 2007 kooperiert UPC mit dem niederländischen Justizministerium und der Polizei, die über 3.000 missbräuchliche Websites indiziert haben, und erschwert den Zugang zu diesen Seiten über eine Landingpage mit dem Text: „Sie versuchen, auf eine indizierte Website zuzugreifen." Mit dieser Lösung wird mehrere tausend Mal pro Monat der versehentliche Kontakt mit Kinderpornografie verhindert.

Technisch versierte User (auch Kinder) können die meisten PC-basierten Filter problemlos umgehen.

Die Öffentlichkeit reagierte äußerst positiv auf die Initiative. In einer diesbezüglichen Umfrage gaben 95% der Befragten an, sie seien für die Blockierung von kinderpornografischen Inhalten, 94% meinten, die Netzbetreiber sollten generell unerwünschte Seiten herausfiltern. Die zweite Zahl scheint sehr hoch, doch das könnte darauf zurückzuführen sein, dass die Frage vor dem Hintergrund des sexuellen Missbrauchs von Kindern statt in einem neutralen Kontext gestellt wurde. Auch die Mehrzahl der Presseberichte (63%) war positiv. Im niederländischen Parlament gab es darüber hinaus eine Debatte über die Wirksamkeit von DNS-Filterung und die Tatsache, dass die Filter nicht von allen ISPs eingesetzt werden. Die Regierung wurde aufgefordert, die Möglichkeiten einer verordneten, potenziell noch tiefer eingreifenden Filterung bei allen niederländischen ISPs zu prüfen.

Der große Vorteil von freiwilligen, ISP-geführten Maßnahmen ist, dass sie umfassenden Schutz bieten können, sofern sie von starken Institutionen unterstützt werden, die die Nachteile einer zu langsamen oder nicht ausreichend informierten Gesetzgebung ausgleichen. Aus Sicht der Netzanbieter und ISPs ergibt sich allerdings das Problem, dass sie danach auch für weitere Blockierungswünsche in anderen Bereichen herangezogen werden könnten – ein schleichender Übergang zur Zensur und zu haftungsrechtlichen Problemen. Zwei Beispiele: Im Juli 2007 unternahm die schwedische Polizei den Versuch, den größten BitTorrent-Tracker der Welt, The Pirate Bay, in ein Verzeichnis von Kinderpornografie-Seiten aufzunehmen. In Dänemark ordnete ein Gericht an, eine DNS-basierte Pornografie-Liste um zwei populäre Musik-Download-Portale zu erweitern (das russische AllofMP3.com und ebenfalls The Pirate Bay) und provozierte damit die Ausbreitung von Überbrückungs-Tricks, die die Wirksamkeit des ursprünglichen Filters untergraben.

Ein anderer Ansatz war in Australien zu beobachten. Seit 2007 erwägt die australische Regierung eine Doppelstrategie, durch die zum einen die ISPs zur Filterung gezwungen werden sollen. Zumindest dieser Teil des Projekts verlief im Sande, nachdem eine Reihe erfolgloser Feldversuche ergeben hatte, dass sich die Filterlösungen anscheinend nicht auf große ISPs skalieren ließen. Darüber hinaus herrscht große politische Uneinigkeit über die Art und Qualität der Inhalte, die in eine entsprechende schwarze Liste der Australian Communications and Media Authority (ACMA) aufgenommen werden sollen.

Als zweiten Teil der Strategie entwickelte man NetAlert, ein Filterprogramm mit dem Motto „Protecting Australian Families Online", das auch die Sperrung von Kinderpornografie zulässt. NetAlert ist eine PC-basierte Lösung, vergleichbar mit vielen kommerziellen Produkten. Sie stellt den mündigen, verantwortungsvollen Konsumenten in den Mittelpunkt, verlangt aber auch ein gewisses Maß an Eigeninitiative und Sachkenntnis. Da viele Nutzer technisch nicht ausreichend versiert sind, erwies sich die Lösung als schwer umsetzbar (seit dem Roll-out sind nur einige hundert Implementierungen erfolgt), während sie für Experten einfach zu umgehen ist. Es heißt, ein Teenager habe den 84 Mio. AUD teuren Filter binnen 30 Minuten geknackt.

Das australische Beispiel zeigt: Keine Filtermethode ist 100%ig gegen eine willkürliche Um-

Bestehende Kinderpornografie-Blacklists und OpenDNS-Kooperation

In Großbritannien haben ISPs eine URL-basierte Filterung eingeführt, die mittlerweile von 96% der privatern Breitbandkunden genutzt werden kann. Die URL-Liste wird von der Internet Watch Foundation (IWF) bereitgestellt und enthält mehrere tausend URLs sowie durchschnittlich 250 bis 300 Domainnamen von Websites, die sexuellen Missbrauch an Kindern mit Fotos und Videos kommerzialisieren. Bei der Hotline der IWF kümmern sich 6 Mitarbeiter um eingehende Meldungen, das Aufspüren und Überprüfen von Inhalten und die Führung der URL-Liste. Die Liste wird zweimal täglich aktualisiert und auch die beteiligten ISPs müssen ihre Filter entsprechend anpassen – mindestens alle 24 Stunden. Die IWF macht ihr Verzeichnis auch anderen Hotlines zugänglich (bisher in Dänemark, Australien und Korea), wobei in den einzelnen Ländern noch einmal geprüft wird, ob die Aufstellung der lokalen Gesetzgebung entspricht.

In den USA einigten sich Verizon, Sprint, Time Warner Cable, AT&T und AOL im Juni/Juli 2008 auf eine Blockierung aller Websites und Newsgroups, die Kinderpornografie propagieren. Sie verpflichteten sich zur Anwendung der schwarzen Liste des National Center for Missing and Exploited Children. Ziel der Übereinkunft war es, die Verbreitung und Auffindung des Materials im Netz extrem zu erschweren. Dabei war man sich der Unmöglichkeit eines totalen Stopps bewusst: Bestimmte Drittfirmen bieten ihren Kunden einen bezahlten Privatzugang zu Newsgroups an und sorgen dafür, dass ihre Aktivitäten selbst vom eigenen ISP nicht erkannt werden. Eine Bibliothek mit 11.400 illegalen Bildern wurde erstellt, die es den Ermittlern erlaubte, tausende Bilddateien gleichzeitig zu durchsuchen. Über ihren „Hash-Wert“ – eine Art elektronischer Fingerabdruck – konnten Dateien gleichen Inhalts überall im Netz identifiziert werden.

www.nystopchildporn.com, eine Initiative des New Yorker Justiz-Chefs Andrew Cuomo, informiert darüber, welche ISPs sich vertraglich bereiterklärt haben, gegen Kinderpornografie auf ihren Servern vorzugehen.

gehung geschützt. Zudem spielt in jedem Fall die Qualität der schwarzen Listen eine entscheidende Rolle: Wie und von wem sie beaufsichtigt, gepflegt/aktualisiert und durchgesetzt werden. Wie schnell das indizierte Material dann entfernt wird, ist eine weitere Frage. Berichten zufolge dauert es bei normalen „Notice & Takedown“-Verfahren im Schnitt 30 Tage, bis die gemeldeten pornografischen Inhalte aus dem Netz verschwinden. Nationale Hotlines stehen vor dem Problem, nicht schnell genug internationale Unterstützung (durch Interpol oder Eurojust) zu erhalten, um Hosting-Anbieter zur Entfernung der Inhalte zu zwingen, nachdem sie innerhalb ihrer Jurisdiktion über Verstöße informiert wurden. Nach Angaben der britischen Internet Watch Foundation waren 2% der identifizierten kommerziellen Kinderpornografie-Seiten auch ein Jahr später noch aktiv.

Das Fehlen einer 100% sicheren Lösung, unterschiedliche Qualitäten der Indizierung, verschiedene Vollstreckungsstandards: All diese Faktoren spielen bei der Frage eine Rolle, ob eine verordnete ISP-Filterung angebracht ist.

Die Filterung von Kinderpornografie durch ISPs und Carrier könnte auch der erste Schritt zur Zensur sein.

Nicht zuletzt können Systeme zur Blockierung von Kinderpornografie auch ganz auf Verbraucher-Empowerment beruhen. Ein Vorzeigebeispiel für einen solchen Ansatz ist die Lösung von OpenDNS[7]. Dabei handelt es sich um einen kostenlos zugänglichen DNS-Server, der über ein Web-Interface die Auswahl zu blockierender Kategorien ermöglicht. Wenn versucht wird, auf gesperrte Inhalte zuzugreifen, leitet der Server den Nutzer auf eine Landingpage um. Den Verbrauchern auf diese Weise selbst die Verantwortung zu überlassen, bietet immense Vorteile: Da sie freiwillig entscheiden, was sie sehen oder blocken möchten (natürlich nur innerhalb des rechtlichen Rahmens), sind Zensur- und Haftungsprobleme vom Tisch. Dabei minimieren einfache netzbasierte Lösungen das erforderliche Nutzer-Know-how und sind auch für „Normalverbraucher“ problemlos einsetzbar. Im Vergleich zu Proxyservern oder Desktop-Systemen kommen DNS-Server mit viel weniger Konfiguration aus. Trotzdem müssen den Verbrauchern geeignete, einfach zu bedienende Tools zur Verfügung gestellt werden. Außerdem müssen die Register blockierter Seitenentsprechend gemanagt werden, idealerweise auf Ebene der Industrie.

(7) Hinweis: OpenDNS ist auf http://www.opendns.com frei zugänglich. Wir erwähnen die OpenDNS-Lösung mehrmals als Referenz, da sie von allen Lesern dieser Studie kostenlos getestet werden kann.

ERGEBNISSE AUF EINEN BLICK
Aus der Diskussion ergeben sich die folgenden acht Kernpunkte:

• Die Blockierung von Kinderpornografie gilt allgemein als moralisch gerechtfertigt und wünschenswert. Bei anderen unerwünschten Inhalten (Rassismus, „Bombenbastler“) gehen die Meinungen auseinander, vor allem in Bezug auf Meinungsfreiheit.

• Die Ausweitung von Blacklists auf andere Angebote, etwa illegale Musikseiten, die, anders als sexueller Missbrauch, nicht allgemein geächtet sind, bewirkt meist das Gegenteil: Es kommt zur massenweisen Verbreitung von Tricks zur Überbrückung der Filter.

• Auch in rechtlicher Hinsicht gibt die Umsetzung Probleme auf, da die einzelnen Rechtsprechungen von unterschiedlichen Tatbeständen ausgehen. Internationale Abkommen zur Schaffung einheitlicher Gesetzesgrundlagen – wie die Übereinkunft des Europarats zum Schutz von Kindern gegen sexuelle Ausbeutung und sexuellen Missbrauch (2007) – wurden bis jetzt nicht flächendeckend umgesetzt.

• Ein konzertierter internationaler Ansatz zur Strafverfolgung ist gefragt, um die Entfernung indizierter Seiten zu beschleunigen.

• Die Erwartungen an die Filterwirkung müssen gedämpft werden. Kein Filter bietet eine 100%ige Lösung. Netzbasierte Systeme verhindern lediglich den unbeabsichtigten Kontakt mit missbräuchlichen Inhalten – ein wichtiges Argument gegen die gesetzlich vorgeschriebene Filterung.

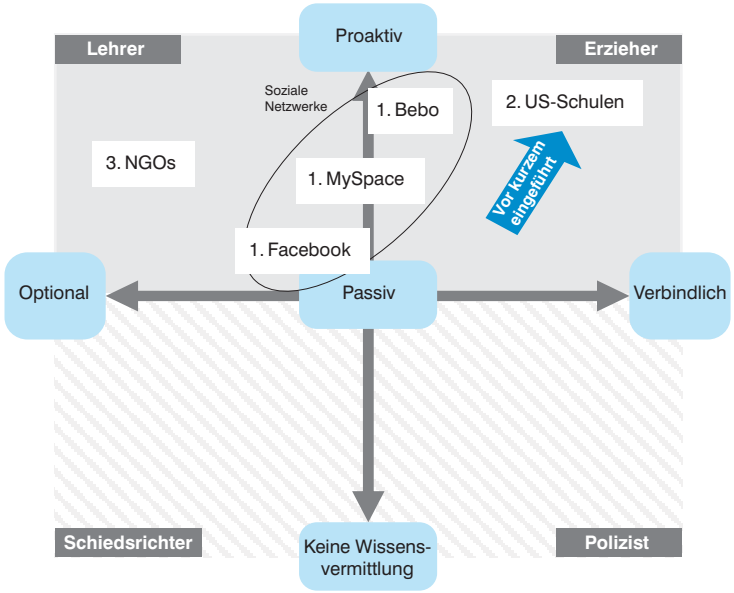
• Engagement für die Blockierung von Pornografie zieht immer starke Zensurbefürchtungen und Kontroversen über Haftung und nationale Unterschiede nach sich.

• Für Netzbetreiber und ISPs zeichnen sich zwei Lösungen ab:

– In Ländern ohne ausreichendes unabhängiges Blacklisting: Selbsthilfe des Verbrauchers (zum Beispiel durch breite Förderung von OpenDNS-artigen Systemen) und Aufklärung über die Funktion und Leistung solcher Lösungen.

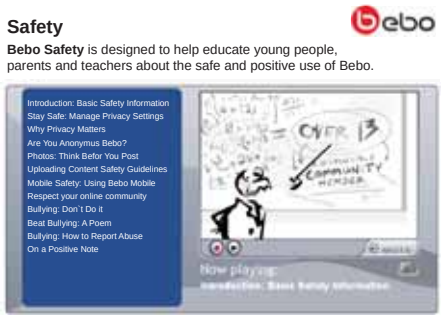
– In Ländern mit bestehender Indizierung durch Drittanbieter: Die Branche muss entscheiden, wie viel Kontrolle sie freiwillig ausübt. Auf der niedrigsten Interventionsstufe könnte mit DNS-basierter Filterung begonnen werden. Der Übergang zur URL-basierten Filterung empfiehlt sich nur, wenn angemessene, rechtsgeprüfte Listen existieren.

Abb. 50: *Digital-Confidence-Positionen zu sozialen Netzwerken/Online-Erziehung*



1. Websites sozialer Netzwerke warnen vor Gefahren beim Datenaustausch und zu vertrauensseligem Verhalten
   - Bebo: sehr jung und interaktiv, sehr restriktive Standard-einstellungen
   - MySpace und Facebook haben ältere Zielgruppen und sind standardmäßig weniger restriktiv
2. US-Schulen starten speziellen Unterricht zum Thema Internet und soziale Netzwerke
   - Schwerpunkt auf Gefahren in sozialen Netzwerken (z. B. Belästigung, Beleidigung)
   - Pflichtfach z. B. in Virginia
   - Unterstützt von NGOs, die Schulungsmaterial entwickeln (z. B. „Web Wise Kids“)
3. NGOs wie ConnectSafely informieren Kinder, Eltern und Lehrer über die Gefahren im Internet

Abb. 51: *Vermittlung von Wissen über soziale Netzwerke bei Bebo*



- Info-Video zu sozialen Netzwerken mit Fokus auf möglichen Gefahren für die Zielgruppe Kinder (Comic-Stil)
- Informationsmaterial für Lehrer und Eltern
- Kooperation mit relevanten NGOs bei der Entwicklung von Schulungsmaterialien

• Um die Ausweitung der Filterung auf andere Bereiche zu vermeiden, sollten die Indizierungsstellen idealerweise von den staatlichen Strafverfolgungsbehörden unabhängig sein. Die britische Internet Watch Foundation ist ein gutes Beispiel für eine solche Organisationsform.

FALLSTUDIE 6: SOZIALE NETZE UND AUFKLÄRUNG MINDERJÄHRIGER

Problem: Kindern und Jugendlichen ist nicht bewusst, welche Gefahren Online-Interaktionen (beispielsweise in sozialen Netzen) mit sich bringen können: „Grooming", Annäherungsversuche etc.

Risiko: Durch den hohen Anonymitätsgrad ist das Risiko im Internet stärker als in der realen Welt (Kinder lernen, dass sie nicht mit Fremden reden sollen, aber wer ist im Internet ein „Fremder"?).

Neben der Blockierung von pornografischen Seiten (und gegebenenfalls anderer schädlicher Inhalte) ist ein zweiter wichtiger Ansatz des Minderjährigenschutzes die Aufklärung über Funktionen und Gefahren des Internets, damit Kinder und Jugendliche selbstständig zu ihrer Sicherheit beitragen können.

Internetgestützte soziale Interaktionen haben, parallel zu ihrem rapiden Wachstum, soziale Probleme geschaffen, die vorher nicht bekannt waren: „Bullying" (Mobbing durch Gleichaltrige), Annäherungsversuche und Verführung Minderjähriger, aber auch der allgemein laxe Umgang mit persönlichen Daten.

Internet-Stakeholder halten umfassendes Informationsmaterial für Kinder und Erwachsene bereit.

Hier allein auf die Hilfe der „klassischen Erziehungsberechtigten" zu setzen, scheint zu viel verlangt. Je mehr sich unerfahrene Eltern und Bildungsträger mit den digitalen Welten auseinandersetzen müssen, desto dringender benötigen sie doppelte Unterstützung:

1. Eltern und Schulen müssen befähigt werden (oder sich selbst befähigen), den Erwartungen an Erziehung und Bildung gerecht zu werden.

2. Andere Organisationen – ISPs, Netzwerbetreiber und Web-2.0-Unternehmen wie Social-Networking-Plattformen – müssen in den Erziehungsauftrag eingebunden werden.

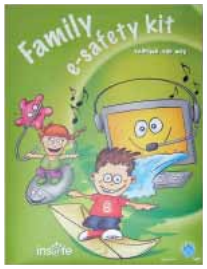
Die unterschiedlichen Ansätze zu einer solchen Erziehung lassen sich in einer adaptierten Version der Positionierungs-Matrix für Digital Confidence anschaulich machen (siehe Abb. 50). Dabei stellt die vertikale Achse das Ausmaß des Engagements dar (die Untere Hälfte hat nur theoretischen Wert, da „Keine Erziehung" keine Option ist). Die horizontale Achse gibt den Grad der Ermessensfreiheit an, das heißt, ob die Erziehungsmaßnahme ein offenes Angebot oder eine Verpflichtung darstellt.

Soziale Netze erfordern deutlich stärker als bisher eine Aufklärung der Nutzer. Alle beteiligten Akteure müssen dies anerkennen und mit wirksamen Lösungen unterstützen.

Zunächst fällt auf, dass soziale Netze sich stark für die Aufklärung ihrer Nutzer engagieren, wie am Beispiel von Bebo, MySpace und Facebook zu erkennen ist. Auf der Skala „Angebot-Verpflichtung" nehmen alle drei eine ähnliche, mittlere Position ein. Deutliche Unterschiede bestehen beim Aktivitätsniveau der Vorbeugung.

Bebo ist stark auf Kinder und Jugendliche zugeschnitten und geht das Thema Anwender-Erziehung entsprechend proaktiv an. Beispielsweise bietet das Unternehmen ein Informationsvideo zu den Gefahren von Social Networking an, das sich in seinem unterhaltsamen und intuitiven Comic-Stil speziell an Kinder wendet. Außerdem hält Bebo Aufklärungsmaterial für Eltern und Lehrer bereit, das gemeinsam mit verschiedenen NGOs entwickelt wird.

Facebook ist zurückhaltender mit seinen Aufklärungsmaßnahmen, vermutlich weil die Zielgruppe aus erfahrenen, ein wenig älteren



Usern besteht. Das Portal bietet einen Einführungstext mit fünf Sicherheitstipps sowie FAQs, die sich an Nutzer, aber auch an Eltern richten. Meist geht es um Beschwerdeprozeduren.

Daneben haben inzwischen auch amerikanische Schulen begonnen, spezielle Kurse zu den Themen Internet und Social Networking zu veranstalten. In Virginia ist der Internet-Sicherheits-Unterricht an den Highschools schon Pflicht.

Das Hauptgewicht liegt auf den Risiken in sozialen Netzen und hier besonders auf Belästigung und Annäherungsversuchen. Der Unterricht stützt sich auf Material, das von der gemeinnützigen Organisation „Web Wise Kids" entwickelt wurde.Darüber hinaus engagieren sich zahlreiche weitere NGOs in der Aufklärung über das Internet und Community-Portale, viele mit deutlichem Fokus auf Minderjährigen.

Entsprechend dem allgemeinen Run auf soziale Netze hat das Thema „Sicherheit beim Knüpfen von Online-Kontakten" jetzt auch seinen eigenen Ort im Web 2.0: „ConnectSafely" hat sich zum einzigen Ziel gesetzt, der „Diskussion über sicheres soziales Verhalten in festen und mobilen Netzen" ein Forum zu bieten.

„Web Wise Kids" nennt sich eine große amerikanische NGO, die sich mit allen Formen von Sicherheitsgefahren im Internet auseinandersetzt. Dazu wurden unter anderem Computerspiele entwickelt, die Kinder über onlinegerechtes Verhalten und Probleme wie Online-Belästigung, Angriffe von Pädophilen und illegale Downloads aufklären. Die Organisation stellt Unterrichtsmaterialien für Schulen bereit und spricht auf ihrer Homepage alle Beteiligten gezielt an, von Eltern und Kindern über Lehrer bis hin zu Strafverfolgungsbehörden.

In unserer Region wird die Bewusstseinsbildung von „InSafe" vorangetrieben, einem Netz mit Länderzentralen in ganz Europa. Vorbildlich ist das Projekt des „Family e-Safety Kit", das Anfang 2008 veröffentlicht wurde. Es stellt Themen der Online-Sicherheit so dar, dass es von Eltern und Kindern gemeinsam gelesen werden kann.

Eltern erwarten, dass vor allem die Schulen über das Internet aufklären.

Trotz vieler positiver Beispiele kann die Entwicklung mit dem rasanten Anstieg von Internet- und Social-Networking-Aktivitäten Minderjähriger kaum Schritt halten. Wie wir gesehen haben, gibt es schon heute zahlreiche gute Initiativen. Aber jetzt bedarf es einer noch stärkeren Kollaboration zwischen den einzelnen Stakeholdern, um Erfahrungen, Best Practices und Lernformate, die sich bewährt haben, zu bündeln – nicht zuletzt, um den notwendigen Invest des Einzelnen möglichst gering zu halten.

Insbesondere die Aufnahme des Themas in die Schulkurrikula steht erst am Anfang. Umfragen zeigen, dass Eltern sich die Schulen als wichtigste Aufklärer in Sachen Internetsicherheit wünschen. Interessanterweise folgen aber schon an zweiter Stelle der „ISP oder Telefonanbieter." Obwohl Software-Hersteller nur von 7% erwähnt werden, wäre die mögliche Integration von Lern- und Aufklärungsangeboten in Nutzerschnittstellen (Betriebssysteme, Browser etc.) ein logischer Schritt, um mehr Nutzer interaktiv zu erreichen.

Abb. 52: *Informationskanäle für Eltern (Großbritannien 2006)*

Quelle: Eurobarometer

ERGEBNISSE AUF EINEN BLICK

Aus der Diskussion ergeben sich 6 Kernpunkte:

- Minderjährige über die Möglichkeiten und Gefahren im Internet und besonders in sozialen Netzen zu unterrichten, wird zur immer dringenderen Aufgabe.

- Soziale Netze versuchen, ihre Nutzer zu informieren, allerdings auf freiwilliger Basis. Deshalb muss die Öffentlichkeit sie beobachten und ergänzende Maßnahmen treffen.

- Eltern erwarten von Schulen und ISPs einen entscheidenden Erziehungsbeitrag – eine wertvolle Chance für beide Gruppen, ihr Profil zu schärfen und ihr Engagement weiter zu intensivieren.

• NGOs sind bereits vielfältig aktiv geworden. Sie sollten diese Aktivitäten künftig gemeinsam mit anderen bündeln und großflächige Kooperationen anstreben, besonders mit Schulen.

• ISPs im Team mit NGOs können eine sehr gute Kombination darstellen, um ein großes Publikum mit Online- und Offline-Information zu erreichen.

• Alle Bildungsangebote müssen auf die spezifischen (Alters-)Gruppen im Netz zugeschnitten sein. So benötigen heranwachsende „Born Digitals" keinen technischen Nachhilfeunterricht, aber Aufklärung über die Gefahren beim laxen Umgang mit persönlichen Daten und Online-Profilen. Kinder brauchen einfache, interaktiv vermittelte Leitsätze, während Eltern sich über das konkrete Online-Verhalten ihrer Kinder informieren können müssen, damit sie die ersten Symptome von Gefahren wie Belästigung, Annäherungs- und Verführungsversuche sofort erkennen.

FALLSTUDIE 7: AUSFILTERN VON COPYRIGHT-INHALTEN

Problem: Im Internet zirkuliert massenhaft raubkopierter Audio und Video-Content, während die Content-Industrie unter Druck steht, profitable digitale Geschäftsmodelle zu entwickeln.

Risiko: Netzbetreiber müssen den Zugang zu bestimmten Angeboten einschränken, was aber möglicherweise geltendem Recht widerspricht und das Nutzererlebnis im Internet limitiert.

Die starke Zunahme von Filesharing-Protokollen und –Plattformen in Kombination mit gestiegenen Verbindungsgeschwindigkeiten hat die Bekämpfung von Online-Piraterie zur größten Herausforderung für die Inhaber von Rechten und für die Regulierer gemacht.

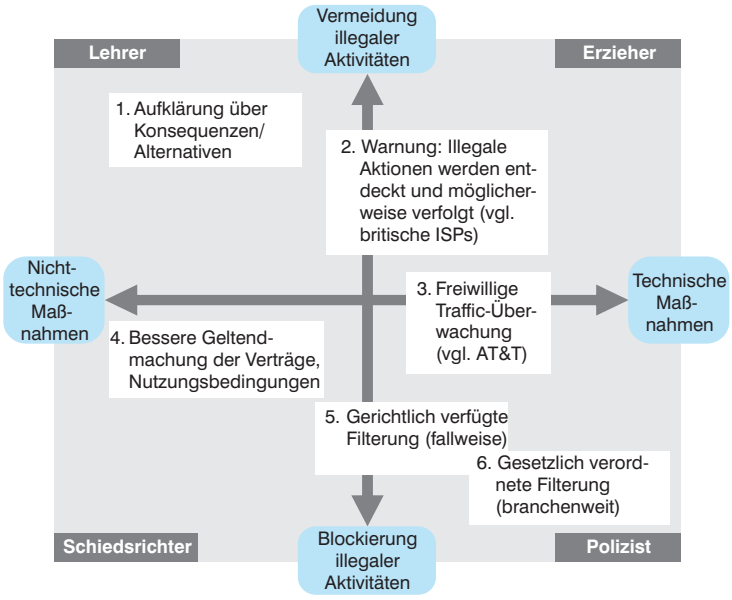
In letzter Zeit hat sich die Aufmerksamkeit des Gesetzgebers zunehmend den Netzanbietern und ISPs zugewandt, wodurch sich die Branche gezwungen sieht, selbst eine proaktivere Haltung einzunehmen. Dabei wird sowohl über technische Maßnahmen nachgedacht (beispielsweise Deep Packet Inspection, verschiedene Arten der netzbasierten Filterung, Digital Fingerprinting durch Hosting-Anbieter oder Watermarking durch Content-provider) als auch über nichttechnische (wie die Abmahnung von Kunden, die als Raubkopierer identifiziert wurden), vgl. Fallstudie 8.

*„Ein Internet-Provider, der seine Copyright-Immunität aufgibt, ist wie ein Astronaut, der sich auf dem Mond seinen Raumanzug auszieht".**

Im EU-Recht gelten Netzbetreiber und ISPs als „reine Durchleiter", sie sind nicht generell dazu verpflichtet, die Datenströme in ihren Netzen zu überwachen. Nur von ihnen selbst gehosteten illegalen Content müssen sie entfernen, wenn sie dazu aufgefordert werden. Der Idee, mit Internet-Filterung selbst zur Bekämpfung von Copyright-Verstößen beizutragen, stehen sie skeptisch gegenüber. Der Grund: Die meisten Filtertechnologien tun entweder zu viel des Guten („Overblocking") und setzen die Netzbetreiber damit Haftungsansprüchen aus – wenn beispielsweise legale Inhalte als „Kollateralschaden" mit gesperrt oder rechtmäßige

*Dr. jur. Tim Wu, Columbia University

Abb. 53: *Digital-Confidence-Positionierung zum Ausfiltern von urheberrechtlich geschützten Inhalten*



1. ISPs informieren Kunden über die entstehenden Schäden durch Urheberrechtsverletzung und nennen Alternativen
2. Von Rechteinhabern informiert, warnen ISPs die Kunden, dass ihr Internetanschluss für illegales Filesharing/ Downloading missbraucht wird und dies rechtliche Folgen haben kann
3. Die freiwillige Überwachung der Datenströme durch ISPs kann zu „Big Brother"-Vorwürfen und Rechtsunsicherheit für den ISP führen
4. ISPs können gegenüber Straftätern ihre Nutzungsbedingungen stärker geltend machen, in dem sie z. B. Kunden abmahnen
5. Mit gerichtlicher Genehmigung können ISPs den Zugang zu bestimmten Seiten einschränken oder sperren
6. Die Politik könnte den Einsatz von Filtern in der gesamten ISP-Branche anordnen

Verwendungen, die urheber- und informationsrechtlich erlaubt sind, eingeschränkt werden. Oder sie „unterblocken“, weil Raubkopierer und neue Technologien den Filter immer umgehen können. Das macht es zu einer schwierigen Herausforderung, die richtige freiwillige oder gar gesetzlich vorgeschriebene Lösung zu finden. Für einen Netzbetreiber oder ISP kann es zudem schwierig (bis unmöglich) sein, ein legales von einem illegalen Angebot zu unterscheiden, wenn beide exakt dieselbe Datei offerieren. Es gibt also keine „One size fits all“-Lösung und keine 100% wirksame Methode.

Zudem existiert, anders als in der Debatte um die Filterung von Kinderpornografie, kein allgemeiner politischer oder öffentlicher Wille, potenzielles Overblocking und damit die Einschränkung grundlegender Internet-Freiheiten zu tolerieren, um die kommerziellen Interessen eines einzelnen Stakeholders zu schützen – so legitim diese auch sein mögen. Als AT&T im Januar 2008 ankündigte, künftig seinen gesamten Traffic auf mögliche Verstöße gegen den amerikanischen Schutz geistigen Eigentums hin zu überwachen, brachte dies dem Unternehmen heftige Verbraucherschelte und den Vorwurf ein, mit „Big Brother“-Praktiken zu arbeiten. Auch der Umstand, dass der Carrier freiwillig seine Immunität in Copyrightfragen aufgibt, wenn er selbst entscheidet, welche Daten über sein Netz gehen, wurde kontrovers diskutiert.

Daher wird die Muss-Filterung meist nur von einzelnen Gerichten verhängt, jeweils bezogen auf einen konkreten Fall.

Anhand der thematisch adaptierten Digital-Confidence-Matrix lassen sich die Positionen zur Filterung – als eine von mehreren Formen des Vorgehens gegen unerlaubtes Filesharing – in zwei Dimensionen darstellen (siehe Abb. 53). Die vertikale Achse gibt an, wie stark eingegriffen wird, um den Datenaustausch zu unterbinden, von der Abmahnung der Nutzer bis zur Sperrung durch Filterung. Die horizontale Achse differenziert zwischen nichttechnischen Maßnahmen zur Disziplinierung der Nutzer bis hin zum Einsatz von Technologie gegen illegale Filesharer und Downloader. Hier nimmt die Filterung entweder die Rolle des „Schiedsrichters“ ein, etwa wenn ein ISP nach einem Gerichtsbeschluss den Zugang zu einer P2P-Seite sperrt, oder die des „Polizisten“, wenn ein ganzer ISP-Sektor gesetzlich verpflichtet wird, Filter zu installieren.

In den letzten Jahren hat sich besonders „The Pirate Bay“ (TPB) zum Zankapfel in diesem Bereich entwickelt. TPB ist einer der weltweit größten BitTorrent-Tracker und Suchanbieter für Torrents und steht im Ruf, große Mengen geschütztes Material, zum Beispiel raubkopierte Filme, in Umlauf zu bringen. Mehrere ISPs, darunter die dänische Tele 2, sahen sich gezwungen, den Zugang zu TPB zu sperren (vgl.

Abb. 54: *The Pirate Bay – aktuelle Entwicklung*

- 1 Mio. Torrents
- 12 Mio. Peers (simultan aktive Verbindungen)
- 2,5 Mio. registrierte Nutzer

- Mai 2006: Polizeirazzia bei TPB
  - Server und andere Ausrüstung werden konfisziert
  - Gründer werden verhört, aber nicht angeklagt
  - Angeblich war MPAA treibende Kraft hinter der Razzia
  - Im Juni 2006 ist TBP wieder online
- Juli 2007: Schweden will TPB auf Kinderpornografie-Blacklist setzen
  - Hätte den Zugang von Schweden aus verhindert
  - Zurückgenommen, da Pornografie-Vorwürfe nie bewiesen werden konnten
- September 2007: Geheime E-Mails von MediaDefender zeigen, dass Medienkonzerne Hacker für DoS-Attacken gegen TPB engagiert hatten
- Januar 2008: Den TPB-Betreibern wird „Mithilfe zu Urheberrechtsverstößen“ vorgeworfen
- Februar 2008: Die dänische Tele2 wird aufgefordert, Kunden von TPB zu trennen
  - IFPI behauptet, Tele2 würde über den Zugang zu TPB das Copyright verletzen
  - Einspruch – verstößt nach Tele2 gegen europäisches Gesetz, da das Kopieren in Routern durch die Infosoc-Richtlinie ausdrücklich erlaubt ist (Artikel 5.1)
  - Traffic aus Dänemark nimmt aufgrund der öffentlichen Diskussion um 12 % zu
- März 2008: Schwedische ISPs von IFPI zu TPB-Blockade verklagt
  - Telia Sonera widersetzt sich, da das Ausspionieren der Kunden nicht rechtens sei
  - Das Unternehmen sei für die Transaktionen seiner Kunden nicht verantwortlich
- April 2008: TPB verklagt IFPI auf Schadensersatz für entgangenen Tele2-Traffic

Quelle: Zeitungsartikel, The Pirate Bay, Wikipedia

die Darstellung Abb. 54). Aber die forcierte Blockade steht vor einem zweifachen Problem: Dem der technischen Machbarkeit und dem der rechtlichen Grundlage. Auf der technischen Seite lässt sich der Zugang zwar mittels DNS-Routing einschränken – aber entweder finden die Nutzer Wege, dies zu umgehen, oder, wie in Dänemark geschehen, der Anbieter (TPB) stellt einen anderen Domainnamen zur Verfügung, der auf die Seite verweist. Alternativ könnte man die IP-Adresse von TPB „blackholen". Dies gilt aber als extrem invasiv, da auch andere Angebote unter der gleichen Adresse ausgeschaltet würden (und eine Umgehung immer noch möglich wäre).

Im März 2008 wollten Presseberichten zufolge vier Musikkonzerne die ehemals staatliche Gesellschaft Eircom dazu zwingen, den illegalen Musik-Download durch Internet-User zu stoppen – der erste Fall in Irland, in dem ein ISP für das Verhalten seiner Kunden verantwortlich gemacht werden sollte, statt wie bisher die Straftäter einzeln zu verfolgen. Vorausgegangen war ein Gerichtsentscheid in Belgien vom Juni 2007, in dem der führende belgische ISP Scarlet angewiesen wurde, innerhalb von 6 Monaten eine Filterlösung einzurichten. Dies führte zu einer intensiven Diskussion, ob man Netzbetreibern solche Maßnahmen vorschreiben darf oder nicht.

Die Frage, ob avancierte Filtertechnologien im Kampf gegen Datenpiraterie zum festen Bestandteil der Netzmanagement-Toolbox von Netzbetreibern gemacht werden sollten, bestimmte zuletzt auch die amerikanische Debatte über die Neutralität des Internets. Rechteinhaber wie MPAA und NBC verlangten von den Carriern, künftig proaktiver vorzugehen und Bandbreiten-Management-Tools gegen die Verbreitung von Raubkopien einzusetzen. Ihrer Meinung nach sollte Netzneutralität den Schutz geistigen Eigentums fördern und die Entwicklung innovativer Filter- und Erkennungstechnologien, mit denen sich raubkopierter Content aufspüren lässt, nicht behindern. Verbraucherschutzorganisationen waren allerdings der Ansicht, dies grenze an Zensur.

ERGEBNISSE AUF EINEN BLICK

Aus der Diskussion ergeben sich die folgenden Kernpunkte:

- Der Entscheidung, selbst proaktiv ihren Internet-Traffic zu überwachen, um Piraterie zu bekämpfen, stehen ISPs generell zögerlich gegenüber: Eine aktive Rolle impliziert, dass sie in den Datenfluss eingreifen und damit ihren Status als „reine Durchleiter" verlieren, der ihnen die Immunität in Copyrightfragen sichert, und sie sich somit haftungsrechtlichen Ansprüchen aussetzen.

- Content-Filterung ist sowohl technisch als auch rechtlich schwierig umzusetzen. Sie führt mit großer Wahrscheinlichkeit zur Überbeziehungsweise Unterblockierung von Copyright-Inhalten und zur Beeinträchtigung des „Fair Use". Im Unterschied zur Filterung von Kinderpornografie gibt es unserer Kenntnis nach keine unabhängigen Institutionen, die dezidiert P2P-Blacklists verfügbar machen, überprüfen und aktualisieren. Zudem können automatisierte Filtertechnologien wie Fingerprinting zwar geschützten Content markieren, aber keine verlässliche Aussage treffen, ob die Verwendung tatsächlich illegal ist oder unter eine Ausnahmeregelung fällt. Letztendlich stellt sich die Grundsatzfrage, ob der Netzbetreiber für den Schutz von Urheberrechten verantwortlich ist. Die damit verbundenen Kosten würden sich in höhere Kosten für die eigene Dienstleistung niederschlagen.

- In den wenigen Fällen, in denen Netzwerbetreiber die proaktive Filterung ihres Traffics angekündigt haben, rief dies aufgrund der invasiven netzbasierten Filtertechnologien (Deep Packet Inspection etc.) harsche Verbraucherkritik und Datenschutzbedenken hervor. Außerdem besteht das Risiko eines Wettbewerbsnachteils gegenüber nicht filternden Marktteilnehmern.

- Im Unterschied zur Kinderpornografie-Debatte gibt es für die Filterung zur Wahrung der rein kommerziellen Interessen eines einzigen Stakeholders bei gleichzeitiger Einschränkung grundlegender Internet-Freiheiten keine breite politische oder öffentliche Unterstützung.

- Die netzbasierte Filterung wird kritisiert, weil sie verschiedene Arten von Traffic und Diensten unterschiedlich behandelt und damit gegen die Netzneutralität verstößt. Die Technologien würden die legitime Nutzung und die freie Meinungsäußerung einschränken, Innovationen verhindern und dabei das eigentliche Problem nicht lösen. Hingegen machen sich die Rechteinhaber für die Netzneutralität stark, um geistiges Eigentum zu schützen und die Entwicklung ausgereifter Technologien zur Filterung und Content-Erkennung zu unterstützen.

- Auch Verbraucheraufklärung ist wichtig, hat aber ihre Grenzen: Die meisten Nutzer wissen sehr wohl, was sie tun.

FALLSTUDIE 8: EINFÜHRUNG DER „THREE STRIKES“-REGEL

Problem: Im Bestreben, Datenpiraterie zu bekämpfen, befürworten die Medienkonzerne die Einführung einer „Three Strikes“-Regel: Internetnutzern, die das Copyright verletzen, wird nach dem dritten Vorfall der Anschluss gesperrt.

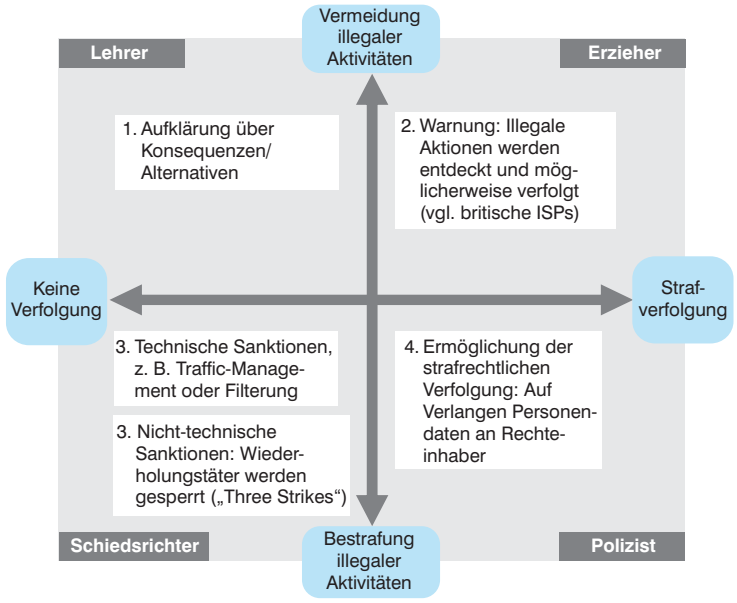
Risiko: Die Einführung der Regel würde möglicherweise tausende User vom Internet ausschließen, was sowohl die Persönlichkeitsrechte als auch das Wachstum digitaler Märkte bedroht.

Neben technischen Modellen zur Bekämpfung digitaler Copyright-Verletzungen wird derzeit in der EU, den USA und Japan auch eine Reihe von nichttechnischen Lösungen auf ISP- und Netzbetreiber-Ebene diskutiert. Die meiste Beachtung fand dabei eine Regelung nach dem Sport-Motto „Three strikes and you’re out“ („Beim 3. Mal bist du draußen“), für die sich Rechteinhaber in allen drei Regionen starkgemacht haben. Es ist die Idee, hartnäckige Wiederholungstäter vom Internet auszuschließen – und daneben über ein wirksames Abschreckungsinstrument zu verfügen, das Nutzer von vornherein von Copyright-Verstößen abhält.

Im Vergleich zur gezielten Blockierung von Angeboten wie „The Pirate Bay“, die lediglich die Möglichkeit für (potenziell rechtswidriges) Filesharing schaffen, oder verglichen mit der Ausfilterung von Copyright-Material, ist die Gefahr groß, über das Ziel hinauszuschießen, wenn man individuelle Nutzer „bloß“ wegen Copyright-Verletzungen aus dem Netz verbannen will. Es ist die Frage, ob die Geschäftsinteressen einer einzelnen Branche Grund genug sein können, um Personen vollständig aus der digitalen Welt auszuschließen. Ebenfalls fraglich ist, ob den Netzbetreibern eine solche Rolle überhaupt zukommt. Jemand den Internetzugang zu entziehen, ist eine drakonische Strafe, die unter Umständen erst dann verhängt werden sollte, nachdem sämtliche anderen Rechtsmittel ausgeschöpft sind. Wenn Netzbetreiber sich aufgrund von Beweisen der Rechteinhaber für eine Anschlusssperrung entscheiden, machen sich private Akteure zu Richtern in eigener Sache. Charles Dunstone, CEO von Carstone Warehouse, erklärt denn auch: „Unsere Position ist ganz klar. Wir sind nur das Kabel, das den Zugang zum Internet ermöglicht. Wir kontrollieren weder das Internet noch das, was unsere User im Internet tun. Ich kann mir keine Situation vorstellen, in der wir freiwillig einen Kundenaccount sperren, nur weil von Dritten ein Fehlverhalten unterstellt wird.“

Auch die „Three Strikes“-Regel bewegt sich in einem Umfeld möglicher Reaktionen auf die Verfolgung von unerlaubtem Filesharing (vgl. Fallstudie 7). Die Position des „Lehrers“ wäre es, den Nutzer lediglich auf den Schaden hinzuweisen, der durch illegale Downloads oder das unerlaubte Filesharing rechtlich geschützter Inhalte entsteht, und ihn auf alternative, legale Angebote hinzuweisen (siehe Abb. 55). Auf der nächst

Abb. 55: *Digital-Confidence-Positionierung zur „Three Strikes“-Regel*



1. ISPs informieren Kunden über die entstehenden Schäden von Urheberrechtsverletzungen und nennen Alternativen
2. Von Rechteinhabern informiert, warnen ISPs ihre Kunden, dass ihr Internetanschluss für illegales Filesharing/ Downloading missbraucht wird und dies rechtliche Folgen haben kann
3. ISP sind (per Gesetz oder Co-Regulierung) verpflichtet, gegenüber Straftätern ihre Nutzungsbedingungen geltend zu machen und direkt aktiv zu werden:
   - Anwendung technischer Maßnahmen wie Traffic-Management und Filter
   - Anwendung nichttechnischer Maßnahmen, z. B. (zweitweise) Sperrung des Netzzugangs
   - Die „Three Strikes“-Regel kombiniert Warnhinweise mit einem Ausschlussverfahren
4. ISPs sind gesetzlich verpflichtet, auf Wunsch des Rechteinhabers Personendaten zur IP-Adresse zu offenbaren, auch ohne Gerichtsbeschluss
   - Abgleich mit bestehender Datenschutzgesetzgebung nötig

Hinweis: Vgl. Case 7 für eine eingehende Diskussion der Filterung von Copyright-Material.

höheren Stufe der Intervention entspräche es dem „erzieherischen“ Ansatz, dass der Netzbetreiber individuelle Teilnehmer aufgrund von Informationen der Rechteinhaber proaktiv verwarnt, dass ein über den Internetaccount der Person verbundener Computer zum Download oder Austausch geschützter Inhalte genutzt wird. Dem Nutzer wird klar gemacht, dass dies einer Copyrightverletzung gleichkommt, was juristische Schritte des Rechteinhabers nach sich ziehen kann. In diesem Rahmen könnte auch auf Sicherheitssoftware hingewiesen werden, mit der sich illegale Downloads über den Account künftig ausschließen lassen. So könnten die Netzanbieter ihre eigene Haftung minimieren und gleichzeitig dem Nutzer zu verstehen geben, dass ihn die Anonymität des Internets nicht völlig unsichtbar macht.

Dieser Ansatz wird derzeit von sechs führenden ISPs in Großbritannien umgesetzt. Nach einem ersten Probelauf von Virgin Media und der British Phonographic Industry (BPI), bei dem die Wirksamkeit schriftlicher Abmahnungen getestet wurde, kam es im Juli 2008 zu einer koregulierenden Lösung auf Basis eines Memorandum of Understanding unter Mitwirkung des Regulierers Ofcom. Das MoU zielt lediglich auf die Schaffung eines branchenweiten Handlungsrahmens zur Bekämpfung des rechtswidrigen Gebrauchs von P2P-Technologie, nicht auf das Problem kommerzieller Piraterie. Unterzeichnet haben es BPI und MPAA als Vertreter der Content-Industrie, Virgin Media, BSkyB, BT, Orange, Tiscali und Carphone Warehouse auf Seiten der ISPs sowie drei verantwortliche Ministerien. Die beteiligten ISPs erklärten sich zu einem 3-monatigen Trial bereit, bei dem zunächst wöchentlich 1.000 Kunden nach entsprechenden Hinweisen der Musikrechte-Inhaber eine Abmahnung erhalten. Außerdem wollen sie einen Code of Practice ausarbeiten, der – vorbehaltlich der Zustimmung des Ofcom – Richtlinien für die Beweisführung, Maßnahmen gegen vermutliche Täter, Wiederholungstäter und Kriminelle, Wege der Entschädigung zu Unrecht Verdächtigter sowie Beschwerdekanäle für die Verbraucher definiert. Bisher gehen die britischen ISPs nicht so weit, Kunden eine Anschlusssperrung anzudrohen, doch jede Abmahnung ist von einer schriftlichen Warnung der BPI begleitet, die für den Fall fortdauernder unerlaubter Aktivitäten eine Zugangssperrung und die gerichtliche Vorladung in Aussicht stellt. Maßnahmen gegen Wiederholungstäter, die auf die Mahnbriefe nicht reagieren, müssen noch diskutiert werden. Zu den vorgeschlagenen Lösungen gehören technische Maßnahmen wie Traffic-Management und Filterung sowie die Kennzeichnung von Content zur leichteren Identifikation.

Dieser dritte Ansatz – spezifische Filterung von Copyright-Material oder Filesharing-Seiten – wurde im vorigen Case schon eingehend dargestellt.

Die am stärksten interventionistische Methode – Abschaltung – wird momentan breit diskutiert und wird sogar in einigen Ländern im Rahmen einer „Beim 3. Mal bist du draußen“-Regelung schon eingeführt. In Frankreich wurde ein entsprechender Vorschlag als „Olivennes-Vertrag“ bekannt (nach Denis Olivennes, CEO des großen französischen Medien-Einzelhändlers FNAC und Vorsitzender der Anti-Piraterie-Kommission, die den Vertrag erarbeitete und dem französischen Präsidenten Sarkozy vorlegte). Nach den Instruktionen der neu eingerichteten Anti-Piraterie-Behörde HADOPI, die Benachrichtigungen der Rechteinhaber über Verstöße prüft und weiterleitet, müssten die ISPs Warnungen aussprechen und Sanktionen verhängen. Sie würden sich verpflichten, verdächtigen Nutzern zunächst eine Abmahnung per E-Mail zu schicken. Kommt es zu keiner Reaktion und fortwährenden Copyright-Verletzungen, wird eine Woche später eine zweite Abmahnung als registriertes Einschreiben verschickt. Wenn der Nutzer immer noch nicht reagiert und seine Aktivitäten fortsetzt, wird der Account 15 Tage lang gesperrt. Falls der Missbrauch nach dieser Frist weitergeht, kann der Zugang bis zu 1 Jahr lang gesperrt werden.

*Guy Bono, Mitglied des Europäischen Parlaments: „In diesem Punkt widerspreche ich aufs Schärfste der Position einiger Mitgliedsstaaten. Deren repressive Maßnahmen werden ihnen von Industrien diktiert, die es verabsäumt haben, ihre Geschäftsmodelle auf die Erfordernisse der Informationsgesellschaft umzustellen. Das Sperren des Internetanschlusses steht in keinem Verhältnis zu den Zielen. Es ist eine gewaltige Sanktion mit gravierenden Auswirkungen in einer Gesellschaft, die Netzzugang als ein Grundrecht zur sozialen Inklusion ansieht“.**

*„Englands sechs größte Internetprovider haben ein von der Regierung vorgelegtes Abkommen zur Bekämpfung von illegalem Musik-Filesharing unterzeichnet. Mit einer Reihe von Maßnahmen werden die sechs Provider – BT, Virgin Media, Orange, Tiscali, Sky und Carphone Warehouse – künftig gegen überführte Filesharer vorgehen. Berichten zufolge stehen die ISPs der von der BPI favorisierten ‚Three strikes and you‘re out‘-Lösung skeptisch gegenüber, durch die auch die Kappung von DSL-Anschlüssen möglich würde“.***

Doch im allgemeinen herrscht noch große Unklarheit darüber, wie die „Three Strikes“-Regel umgesetzt werden kann, beispielsweise über die Dauer der Sperrung von Anschlüssen, den unklaren Überwachungsprozess (Frankreich erwägt ein landesweites Täter-Register), länderspezifische Zuständigkeitsdiskussionen (insbesondere, ob Netzbetreiber und ISPs alle Verstöße selbst aufspüren oder nur auf Benachrich-

*http://www.cablefo-rum.co.uk/article/397/european-parliament-rejects-3-strikes-rule-is-vm-listening

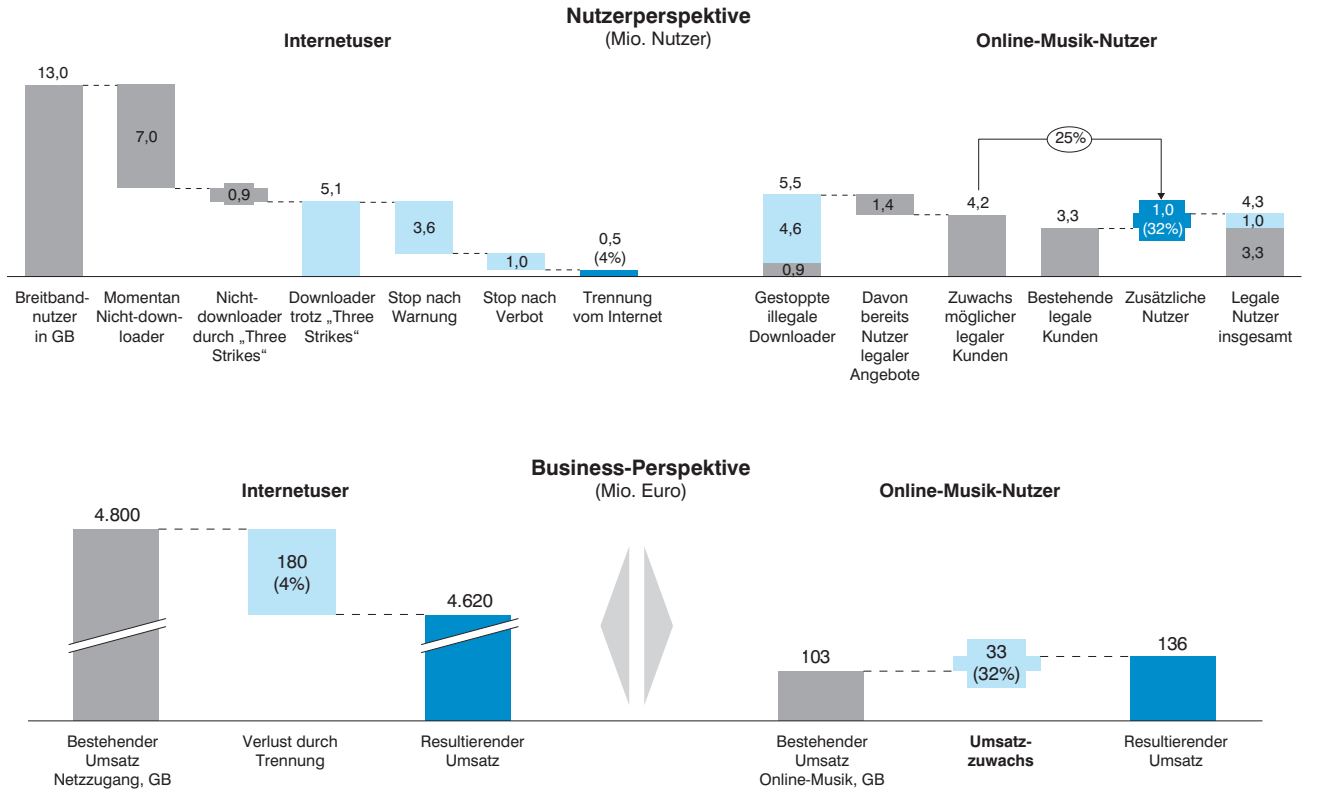
**BBC News vom 24. Juli 2008

tigung der Copyright-Eigner eingreifen müssen), haftungsrechtliche Probleme und nicht zuletzt über die Frage, wer die Umsetzung bezahlt.

Die einzelnen Staaten haben sehr unterschiedliche Positionen zum „Three Strikes"-Konzept. Frankreich scheint mit seiner Formulierung eines Gesetzesvorschlags, der im Herbst 2008 im Parlament diskutiert werden soll, am weitesten vorn zu stehen. Die Kooperation der großen ISPs wurde über einen „Deal" sichergestellt, bei dem im Gegenzug DRM-freie Musikdateien zum legalen Download angeboten werden. Großbritannien schien Frankreich zunächst folgen zu wollen und dachte Anfang 2008 über eine Einführung nach, für den Fall, dass sich ISPs und Rechteinhaber nicht einigen würden. Doch im weiter oben behandelten MoU wird die Anschlusssperrung als von den Vertragsparteien zu diskutierende Maßnahme nicht mehr erwähnt. Der britische Ansatz ist an die Verpflichtung aller Beteiligten gekoppelt, mehr attraktive kommerzielle Content-Angebote als Alternative zu unerlaubtem Filesharing verfügbar zu machen (Abonnements, On-Demand, legale Filesharing-Portale etc.). In Japan haben sich die vier großen ISP-Verbände auf Druck der Regierung und der Content-Industrie zur Umsetzung von „Three Strikes" entschlossen. Die Europäische Union hat das Konzept im April 2008 zurückgewiesen, im Rahmen der Verabschiedung eines Reports zur Förderung der Kulturindustrien Europas.

Nicht zuletzt zählt „Three Strikes" auch zu den möglichen technologisch umzusetzenden Aufträgen an die ISPs, die im Rahmen des Anti-Counterfeiting Trade Agreement (ACTA) der G8 diskutiert werden. Es soll noch vor Ende 2008 finalisiert werden. ACTA dient vor allem der Modernisierung der Rechtsbasis im Bezug auf P2P und neue Entwicklungen im Internet. Zwar sind die Verhandlungen nicht öffentlich, doch inoffiziellen Informationen nach gehören sowohl „Three Strikes" als auch die gesetzlich vorgeschriebene Filterung zu den Agendapunkten.
Ein Aspekt, der in der öffentlichen Diskussion oft übersehen wird, sind die Gesamtschäden, die der digitalen Wirtschaft durch das massenweise „Abklemmen" von Internet-Kunden drohen. Die Auswirkungen müssen noch ganzheitlicher untersucht werden. So ergab eine umfassende Sensitivitätsanalyse für Großbritannien, dass die Einführung von „Three Strikes" die Sperrung von 500.000 Nutzern und Umsatzeinbußen der Netzbetreiber von 180 Mio. € zur Folge haben könnte (siehe Abb. 56). Zum Vergleich: Die

Abb. 56: *Umsetzung von „Three Strikes" in GB – Grobe Sensitivitätsanalyse*



Quelle: Zeitungsberichte, Europäische Kommission

Musikindustrie rechnet im günstigsten Fall mit einem Umsatzplus von 33 Mio. € – ihre Einbußen von rund 150 Mio. € wären wahrscheinlich nur ein Bruchteil dessen, was andere Stakeholder verlieren würden, etwa durch Abnahme des E-Commerce-Volumens.

Neben der Tatsache, dass User vom digitalen Leben ausgeschlossen werden, macht vor allem der mögliche finanzielle Schaden der gesamten digitalen Wirtschaft das „Three Strikes"-Konzept zu einem problematischen Ansatz, wenn es um die angemessene Bekämpfung von Piraterie geht.

ERGEBNISSE IM ÜBERBLICK

Aus der Diskussion ergeben sich 4 Kernpunkte:

- Mit dem „Three Strikes"-System erreicht der Kampf gegen Copyrightverletzungen sein nächstes Level an Interventionismus – mit dem Risiko, über das Ziel hinauszuschießen, sollten die Folgen nicht sorgfältig abgewogen werden.

- Es ist sehr zweifelhaft, ob die Geschäftsinteressen einer einzelnen Branche den Ausschluss von Einzelpersonen vom digitalen Leben rechtfertigen, erst recht, wenn man an die Umsetzungskosten und Opportunity-Verluste anderer Stakeholder denkt.

- Die öffentliche Debatte um „Three Strikes" konzentriert sich auf die Angemessenheit der Maßnahme. Andere Faktoren, wie die Schwierigkeiten bei der Erkennung von Copyright-Material und die ganzheitlichen Auswirkungen, werden noch zu sehr vernachlässigt.

- In den einzelnen Regionen haben Politik und Netzbetreiber unterschiedlich agiert. Das Europäische Parlament fordert in seinem Beschluss zu den „Kulturindustrien Europas" vom April 2008 eine stärkere Zusammenarbeit von Content-Eignern und Netzbetreibern und verurteilt Maßnahmen, durch die nicht profitorientierte Nutzer kriminalisiert werden, ausdrücklich als falschen Weg bei der Piraterie-Bekämpfung. Mit deutlichem Wink nach Frankreich rief das Parlament dazu auf, alle Maßnahmen zu vermeiden, „die mit Persönlichkeits- und Menschenrechten sowie mit den Prinzipien Angemessenheit, Wirksamkeit und Abschreckung nicht vereinbar sind, wie die Sperrung von Internetanschlüssen."

2. DIE AGENDA DER REGULIERER

Die unterschiedlichen Rechtsprechungs- und Regulierungs-Aktivitäten auf EU- und Länderebene lassen sich in 6 Themenschwerpunkte gliedern:

- Aktivitäten zur Überarbeitung der bestehenden Gesetzgebung, die Anbieter elektronischer Kommunikationsnetze und -Dienstleistungen betrifft.

- Aktivitäten im Zusammenhang mit der Neuinterpretation bestehender Rechte wie z. B. der EU-Datenschutzrichtlinie.

- Aktivitäten zur Förderung branchenübergreifender Kooperationen.

- Co-Sponsoring-Programme.

- Gesetzgebungsinitiativen in einzelnen Ländern.

- Aktivitäten zur Förderung der internationalen Koordination.

2.1 ANPASSUNG VON RAHMENBEDINGUNGEN UND RECHTSPRECHUNG

Im November 2007 legte die Europäische Kommission einen Vorschlag zur „Novellierung des europäischen Rechtsrahmens" für Anbieter elektronischer Kommunikationsinfrastrukturen und -Dienstleistungen vor. Die Kommision geht davon aus, dass die darin gemachten Empfehlungen bis Ende 2009 in geltendes Recht umgesetzt werden.

Vor dem Hintergrund der steigenden Bedrohung durch Spam, Spyware, Viren und Phishing-Attacken soll die Gesetzesnovelle die bestehenden Datennetze stärken und frühere Gesetze ergänzen, die bestimmte Handlungen unter Strafe stellen. Im Hinblick auf Digital Confidence sind die Ziele vor allem:

- Stärkung der Verbraucherinformation und der Regressmöglichkeiten im Zusammenhang mit Datensicherheit und „E-Privacy". Beispielsweise sollen Netzbetreiber und ISPs gesetzlich verpflichtet werden, Sicherheitsverletzungen zu melden.

- Verbesserung des Nutzererlebnisses durch die Förderung eines ungehinderten Zugangs zu digitalen und Online-Services, z. B. durch die Stärkung der nationalen Regulierer bei der Festsetzung von Mindestanforderungen an die Service-Qualität.

Speziell zum Thema Netzsicherheit und Datenschutz enthält die Novelle folgende Vorschläge:

• Verbraucher werden von ISPs informiert, falls ihre persönlichen Daten aufgrund von Sicherheitsverletzungen gefährdet sind.

• Betreiber und Regulierer werden für die Sicherheit und Integrität von Netzen und Dienstleistungen stärker in die Verantwortung genommen.

• Die Umsetzungs- und Strafverfolgungsmöglichkeiten der zuständigen Behörden werden erweitert, speziell im Kampf gegen Spam.

• Die Anwendung von EU-Recht auf Datensammlungs- und -erkennungseinrichtungen soll geklärt werden.

Im Bezug auf die künftige Sicherung des Zugangs zu hochwertigen digitalen und Online-Services empfiehlt die Novelle:

• Nationale Regulierungsbehörden dürfen Mindestanforderungen zur Dienstgüte an die Netzanbieter stellen, basierend auf Standards, die auf EU-Level entwickelt wurden.

Ziel ist es, Qualitätsverlusten und Traffic-Verzögerungen vorzubeugen, die eine Grundkonnektivität der Verbraucher bedrohen würden. Nach Angaben der EU-Kommissarin für Informationsgesellschaft und Medien Viviane Reding werde es aber immer noch Freiräume für Traffic-Steuerung und -Shaping zur Optimierung der Nutzung geben, allerdings unter dem Vorbehalt, dass dies transparent, angemessen und nicht diskriminierend geschehe.

Der Novellierungsvorschlag beschäftigt sich auch mit der Unabhängigkeit der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) mit Sitz auf Kreta, die 2004 im Hinblick auf die immer größere geschäftskritische Bedeutung von ITC gegründet wurde. Die Agentur engagiert sich unter anderem durch Best-Practice-Vergleiche und die Entwicklung von Standards zur Risikominimierung für den Erhalt betrieblicher Kontinuität im Fall von Infrastruktur-übergreifenden Störungen wie bösartigen Angriffen und kritischem Datenverlust. Sie hat sich bereits zu vielen Themen geäußert, beispielsweise zu Sicherheitsproblemen in sozialen Netzen, Botnets und reputationsbasierten Systemen. Zweifel aufgreifend im Hinblick auf die Frage der effizienten operativen Unterstützung von Unternehmen durch die ENISA hat die Kommission empfohlen, die Agentur mit einer neuen, noch zu etablierenden europäischen Regulierungsbehörde zu verschmelzen. Da dieser Vorschlag jedoch sehr kontrovers aufgenommen wurde, ist derzeit unklar, ob sie aufgelöst wird oder unabhängig bleibt. Die EU hat jedenfalls entschieden, dass das Mandat der ENISA bis 2011 erhalten bleibt, bis die europäische Regulierungsbehörde, so sie denn gegründet wird, ihre Aufgaben übernimmt.

2.2 NEUINTERPRETATION BESTEHENDER RECHTE

Die fortlaufende Neuinterpretation bestehender Rechtsgrundsätze ist gerade im Bereich Datenschutz ein vorherrschendes Thema. Die aktuellen Entwicklungen bei Web-2.0-Diensten und den damit verbundenen Geschäftsmodellen – Viral Marketing, Suchtechnologien, soziale Netze etc. – machen es schwierig, Grundprinzipien wie Transparenz, informierte Einwilligung, Zweckbeschränkung und Berichtigungsanspruch aufrechtzuerhalten, die in der EU-Datenschutzrichtlinie von 1995 niedergelegt sind.

Die Anwendbarkeit existierender Rechtsprinzipien der Datenschutzrichtlinie auf neue technologische Entwicklungen wird kontinuierlich durch die Artikel-29-Datenschutzgruppe geprüft. Vor kurzem legte die Gruppe eine Stellungnahme zu datenschutzrechtlichen Problemen von Suchmaschinen vor. Zentrales Ergebnis war, dass die EU-Richtlinie grundsätzlich auf die Verarbeitung persönlicher Daten durch Suchdienste anwendbar ist. Demnach müssen die Anbieter persönliche Daten löschen oder irreversibel anonymisieren, sobald sie nicht mehr ausdrücklich für den legalen Zweck gebraucht werden, für den sie erhoben wurden. Außerdem müssen sie das Setzen und die Speicherdauer von Cookies jederzeit rechtfertigen können. Jede geplante Weiterleitung von Anwenderdaten oder Anreicherung des Nutzerprofils bedarf der Zustimmung. Opt-outs von Website-Herausgebern sind zu respektieren und Aufforderungen seitens der Nutzer zum Nachladen/Aktualisieren von Caches sind sofort Folge zu leisten. Für Aufsehen sorgte vor allem, dass die EU-Experten IP-Adressen als persönliche Daten werten.

Auch künftig zählt die Gewährleistung des Datenschutzes bei neuen Technologien zu den Prioritäten der Datenschutzgruppe, etwa bei sozialen Netzen (hier besonders Angebote für Kinder und Jugendliche), Behavioral Targeting, Data-Mining (online und offline) und Online-Broadcasting.

2.3 FÖRDERUNG VON KOOPERATIONEN

Im Hinblick auf die rasante Veränderung der Märkte, Geschäftsmodelle und Technologien werden konzertierte Anstrengungen der Stakeholder inzwischen rein legislativen Ansätzen vorgezogen. Für die bessere Bekämpfung der Piraterie von Copyright-geschütztem Material plant die Kommission, mit der sogenannten „Content Online Platform" ein Diskussions- und Kooperationsforum für alle Beteiligten einzurichten, das auch Verbrauchermeinungen breiten Raum gewährt.

Aufbauend auf ihr Communiqué „Creative Content Online in the Single Market" (2008), plant die Kommission außerdem die Förderung von Verhaltenskodizes zwischen Netzzugangs-/Serviceprovidern, Rechteinhabern und Konsumenten, um das Copyright angemessen zu schützen und eine enge Zusammenarbeit bei der Bekämpfung von Piraterie und unerlaubtem Filesharing zu gewährleisten.

2.4 SPONSORING-INITIATIVEN ZUR DIGITAL CONFIDENCE

Anfang 2008 stellte die Europäische Kommission ihr neues „Safer Internet"-Programm vor, das die Online-Sicherheit von Kindern erhöhen soll. Es baut auf die gleichnamige Initiative aus dem Jahr 2005 auf und umfasst auch jüngste Entwicklungen der Web-2.0-Ära, zum Beispiel soziale Netze. Das Programm bietet die Kofinanzierung von Maßnahmen, die folgenden Zielsetzungen entsprechen:

- Schaffung nationaler Kontaktstellen zur Meldung von rechtswidrigen und schädlichen Inhalten und Verhaltensweisen, insbesondere sexuellem Missbrauch von Kindern und Grooming.

- Förderung freiwilliger Regulierung in diesem Bereich sowie der Motivation von Kindern, bei der Online-Sicherheit aktiv mitzuwirken.

- Bewusstseinsbildung bei Kindern, Eltern und Lehrern und Unterstützung von Beratungsstellen, die Sicherheitstipps geben.

- Einrichtung einer Wissensbasis zum Umgang mit neuen Technologien und den verbundenen Risiken durch Vernetzung von Wissenschaftlern mit Expertise über Online-Kinderschutz auf europäischer Ebene.

Die Vorschläge greifen auch Empfehlungen auf, die im Februar 2008 während eines europäischen Jugendforums im Rahmen des Safer Internet Day von Kindern gemacht wurden. Das neue „Safer Internet"-Programm (2009–2013) soll 2009 verabschiedet werden, die Kofinanzierung von Projekten beginnt voraussichtlich 2010.

Beispiele für Projekte, die unter der „Safer Internet"-Initiative 2005 finanziert wurden, sind „Insafe" (Projekt für einen sicheren und positiven Umgang mit dem Internet durch den positiven Umgang mit dem Internet durch den Austausch von Best Practices, Informationen und Ressourcen zwischen Unternehmen, Schulen und Familien) und „INHOPE" (Support von weltweiten Internet-Hotlines zur Meldung von illegalem Content wie Kinderpornografie, vgl. die Diskussion des Minderjährigenschutzes in Kapitel IV-1).

2.5 INITIATIVEN AUF NATIONALER EBENE

In einzelnen Ländern lassen sich erhebliche Unterschiede im Umgang mit den Bedrohungen der Digital Confidence beobachten. Besonders deutlich sind sie beim Kampf gegen Piraterie. Frankreich verfolgt mit dem „Olivennes-Vertrag" den Ansatz, illegale Downloader mit einer „Three strikes and you're out"-Regel zeitweilig vom Internet auszuschließen, und bildet damit ein Ende des Spektrums nationaler Initiativen. Der auf ISP-Selbstregulierung basierende „Notice & Takedown"-Ansatz (Informieren und Entfernen) der Niederlande repräsentiert das andere Ende. Gleichzeitig stellt die in Frankreich erwogene Verfolgung von Downloadern die Umkehrung dessen dar, was in den USA geplant ist: Dort sind es die Uploader, nicht die Downloader, die zum Ziel von „Notice & Takedown"-Verfahren werden sollen. Zwar ist das Hochladen Copyright-geschützter Werke auch in Frankreich verboten, doch das französische Modell bietet keine rechtliche Handhabe zur technischen Verfolgung von Uploadern. Der Olivennes-Vertrag verpflichtet ISPs, eine Content-Erkennung zu implementieren (Fingerprinting und/oder Watermarking) und im Falle von Verstößen eine Regulierungsbehörde zu benachrichtigen, die dann Maßnahmen gegen die Nutzer ergreift.

Im Januar 2008 entschied der Europäische Gerichtshof in einem Verfahren über den Schutz geistigen Eigentums, dass die EU-Richtlinien zu Datenschutz und E-Privacy den Netzbetreibern nicht vorschreiben, persönliche Daten von Copyright-Verletzern offenzulegen, um den Rechteinhabern die Strafverfolgung in einem

BEISPIELE FÜR AKTUELLE REGULIERUNGSDEBATTEN

Japan: „Richtlinien für Traffic-Shaping", Mai 2008

In Japan, das wegen seiner Übertragungsgeschwindigkeiten und dem hohen Grad des NGN-Roll-outs als einer der fortschrittlichsten Märkte der Welt gilt, haben im Mai 2008 vier IuK-Industrieverbände (Japan Internet Providers Association, Telecommunications Carriers Association, Telecom Service Association, Japan Cable and Telecommunications Association) „Richtlinien für Traffic-Shaping" verabschiedet. Nach einer Studie des japanischen Kommunikations-Ministeriums vom November 2007 hatten 40% der japanischen ISPs eine eigene Bandbreitenregulierung eingeführt.

Nachdem P2P-Filesharing auch in Japan zu heftigen Traffic-Steigerungen geführt hat, sollen die Richtlinien die Geschwindigkeits-Drosselung bei Power-Usern regulieren. Sie werden vom Interior & Communications Ministry überwacht und etablieren Mindeststandards für Traffic-Shaping, die von den ISPs jeweils durch eigene Maßnahmen ausgestaltet und ergänzt werden. Die Befolgung ist freiwillig: Die Richtlinien beschreiben lediglich einen „sicheren Hafen" legaler Verhaltensweisen.

Die Richtlinien besagen, dass die ISPs das Volumenwachstum prinzipiell durch Aufrüstung ihrer Infrastruktur abfedern sollten. Die Begrenzung der Übertragungsgeschwindigkeit sei nur im Ausnahmefall zu erwägen, beispielsweise bei Usern, die bestimmte Software wie P2P-Anwendungen stark nutzen, oder bei Anwendern, die riesige Datenmengen hochladen und damit eine bestimmte Obergrenze überschreiten, sofern sie dadurch einen Großteil des Netzs belegen und die Kommunikation anderer Nutzer behindern. In diesem Fall müssen die ISPs die Nutzer jedoch über die Einschränkung informieren.

Die Mindeststandards beziehen sich auf 1) die Ausführlichkeit, mit der die Regulierung im Nutzervertrag ausgewiesen werden muss, 2) Mindestanforderungen zur Durchführung von Traffic-Shaping und 3) die relevanten Rechtsgrundlagen.

Die Richtlinien beschreiben vor allem die rechtliche Basis für die Einschränkung der Bandbreite bei bestimmten Applikationen oder bei Nutzern, die das Netz zum Nachteil normaler Anwender unverhältnismäßig stark belasten.

Dabei wird anerkannt, dass es im Zusammenhang mit DPI, das zum Packet-Shaping eingesetzt wird, Datenschutzbedenken gibt („Kommunikationsgeheimnis"), die bestimmte Formen der Nutzerzustimmung verlangen. Gleichzeitig ist aber auch eine Möglichkeit der Außerkraftsetzung dieser Anforderungen vorgesehen, falls ein „rechtlich vertretbarer" Grund für die Anwendung von Packet-Shaping vorliegt.

Die in den Richtlinien genannten Beispiele für rechtlich vertretbare Maßnahmen – entweder die Einschränkung einer bestimmten Anwendung oder eines Power-Users – orientieren sich an den Kriterien 1) Legitimität des Zwecks, 2) Handlungsbedarf und 3) Rechtmäßigkeit der Mittel.

Dabei erheben die Beispiele keinen Anspruch auf Vollständigkeit, da man davon ausgeht, dass sich die Maßnahmen noch weiter entwickeln werden. Die Richtlinien sind entsprechend weit gefasst und auf den stabilen Netzbetrieb ausgerichtet.

Die Richtlinien empfehlen eine umfassende Bekanntmachung von Packet-Shaping-Maßnahmen (im Gegensatz zur Einholung der Nutzerzustimmung), die für die Enduser, Nicht-Enduser und andere (vor allem nachgelagerten) ISPs klar nachvollziehbar sein muss.

GB: „Voluntary Code of Practice – Broadband Speeds", Ofcom, Mai 2008

In Großbritannien werben die Breitband-Internetprovider heute mit so genannten „Headlight"-Volumen, die maximal über das Netz transportiert werden können. Je nach verwendeter Technologie, Infrastruktur und Umgebung lassen sie sich vom einzelnen User aber kaum jemals erreichen.

Ein neuer Code of Practice fordert jetzt von den Netzanbietern eine akkurate Einschätzung ihrer maximalen Übertragungsgeschwindigkeiten. Außerdem verlangt er die Offenlegung von Traffic-Shaping und diesbezüglicher interner Regeln (betroffene Protokolle und Anwendungen, „Fair Use"-Grenzen etc.).

Ofcom wird die Breitband-Geschwindigkeiten weiter im Auge behalten und stellt schon jetzt fest, dass sie erheblich von den angegebenen Maximalgeschwindigkeiten abweichen. In Zukunft könnten auch Durchschnittsgeschwindigkeiten in den Code aufgenommen werden.

Zivilprozess zu ermöglichen. In diesem Fall hatte der spanische Rechteverwerter Promusicae von einem Gericht verlangt, die Telefónica zur Herausgabe der Identität und Adressen von Kunden zu zwingen, die den P2P-Service Kazaa zu unerlaubtem Filesharing genutzt hatten. Wie schon beim Kulturindustrien-Beschluss des Europäischen Parlaments wurde bei der Frage, ob grundlegende Bürgerrechte oder (geistiges) Eigentum geschützt werden sollten, im Sinne des Bürgerrechts entschieden, in diesem Fall zugunsten des Schutzes von Personendaten.

Frankreich hat für seine EU-Präsidentschaft im zweiten Halbjahr 2008 angekündigt, es werde nicht Ziel seiner IPR-Politik sein, eine exakte Kopie des Olivennes-Vertrags auf europäischer Ebene zu forcieren. Stattdessen will die französische Präsidentschaft alle Stakeholder an einen Tisch bitten und Verhandlungen fördern.

Schließlich gehört die „Three Strikes"-Regel auch zu den Regulierungsvorschlägen, die momentan auf Ebene der G8 diskutiert werden. Das Anti-Counterfeiting Trade Agreement (ACTA), das die G8-Staaten bis Ende 2008 verabschieden wollen, könnte „Three Strikes" neben gesetzlich vorgeschriebener ISP-Filterung enthalten. Die Maßnahme ist der Versuch einer Antwort auf P2P und andere neue Herausforderungen im Internet und dient dem Kampf gegen Piraterie und der Ergreifung entsprechender gesetzlicher Maßnahmen.

Militärische Botnets im Informationskrieg

Im Mai 2008 machte Colonel Charles W. Williamson III. den Vorschlag, die Air Force solle ihr eigenes Zombie-Netz aufbauen, um damit DoS-Angriffe gegen Feinde durchzuführen. Er empfahl die absichtliche Installation von Bots auf nicht geheimen Computern und in Behörden und Verwaltungen.

Andere Militärs schlugen sogar vor, Bots auf bestehenden Sicherheitssystemen einzusetzen und nicht mehr gebrauchte Computer für eine „Bot-Armee" zu recyceln.

Die zivilen Kommentatoren von Wired sprachen von der „irrsinnigsten Idee der Army seit der Gay-Bombe". Andererseits lässt sich die Durchschlagskraft von DoS-Attacken nicht leugnen: In Russland brachten Hacker vor kurzem fast sämtliche Webseiten von Kernkraftwerken zum Absturz.

Quelle: Wired, Darkreading

2.6 INTERNATIONALE KOORDINATION

Nach den DoS-Attacken auf Estland (siehe Fallstudie 6) einigte sich der NATO-Gipfel in Bukarest Anfang April 2008 auf eine gemeinsame Strategie zur Cyber-Verteidigung und auf die Einrichtung einer Behörde, der die Aufgabe zukommt, die „politischen und technischen" Abwehrmaßnahmen der NATO zu koordinieren.

Außer einer zentralen Institution erfordert ein wirklich gesamteuropäischer Ansatz bei der Verhinderung und Bekämpfung von Online-Angriffen aber auch Strukturen auf Länderebene, vergleichbar etwa mit dem U.S. Computer Emergency Readiness Team (US-CERT): Diese Partnerschaft zwischen dem Department of Homeland Security und dem öffentlichen und privaten Sektor wurde 2003 ins Leben gerufen, um die Netzinfrastrukturen des Landes zu schützen. Sie koordiniert seitdem landesweit die Verteidigung gegen Cyber-Attacken. Derzeit besitzen nur wenige europäische Staaten ähnliche Strukturen. Die EU-Kommissarin für Informationsgesellschaft und Medien, Viviane Reding, hat angekündigt, dass die Europäische Kommission Anfang 2009 ein Communiqué zum Schutz kritischer Telekommunikationsinfrastrukturen vorlegen wird. Ziel sei es, die Vorbereitung und Response-Zeit auf Cyber-Attacken auf europäischer Ebene zu verbessern. Die Kommissarin unterstrich die Bedeutung technischer Entwicklungen, man dürfe aber nicht die Aufklärung der Bürger über Möglichkeiten und Risiken der Informationsgesellschaft aus den Augen verlieren. Diese Haltung scheint auf große Unterstützung in der Industrie zu treffen.

2.7 FAZIT

Die wichtigsten rechtlichen Grundlagen zur Minimierung der Digital-Confidence-Risiken sind größtenteils bereits etabliert, doch zugleich ist es notwendig, bestehende Regulierungskonzepte ständig zu überprüfen und sie im Hinblick auf neue Technologien, Märkte und Nutzungsrealitäten neu zu interpretieren. Die grenzübergreifende Problematik der Digital-Confidence-Bedrohungen erfordert vor allem eine enge internationale (legislative) Zusammenarbeit, ein stärkeres Bewusstsein für die Dringlichkeit des Handlungsbedarfs und die Bereithaltung entsprechender Ressourcen zur Schaffung von Abwehrstrukturen und Public-private-Partnerships durch Regierungen und zuständige Behörden. In der Politik und im Bereich Regulierung scheint der Trend weg von einseitiger Gesetzgebung hin zu mehr Stakeholder-Beteiligung und Koregulierung zu gehen – übrigens nicht nur in Europa, sondern aufgrund des Drucks der FCC inzwischen auch in den USA. Dies erfordert jedoch gleichzeitig eine kontinuierliche Überprüfung

der Angemessenheit aller Regulierungsaktivitäten, ganz besonders jedoch stark interventionistischer Praktiken (wie der „Three Strikes"-Regel oder der obligatorischen Netz-Filterung), die grundlegende Internet-Freiheiten und Verbraucherrechte (z. B. Datenschutz) einschränken und angestammte Rechtsverbindlichkeiten der Industrie untergraben.

Doch die Industrie hat die Chance, ihr Profil in diesem Bereich zu schärfen und durch Aufklärung und Empowerment der Verbraucher deren Vertrauen in neue digitale und Online-Services zu stärken. Ergänzend zu Industrie-geführten Corporate-Responsibility-Initiativen ist bei der Durchsetzung die verstärkte Zusammenarbeit der einzelnen Sektoren untereinander und mit Regierungs- und Regulierungsorganisationen gefragt, um eine solide rechtliche Basis für unterschiedliche Interventionsgrade zu garantieren. Beispiele hierfür sind die verschieden starken Filter- und Blockierungsmaßnahmen, bei denen die Netzbetreiber haftungsrechtlich abgesichert sein müssen. Auf dem Gebiet der Netzsicherheit könnten Public-private-Partnerships ein guter Weg sein, um die effektive Sammlung von oft hochsensiblen und vertraulichen Daten zu gewährleisten, die einen Beitrag zur kohärenten Bekämpfung leisten.

V. RISK-BENEFIT-ANALYSE: DIGITAL CONFIDENCE ZAHLT SICH AUS

Wie in den vorhergehenden Kapiteln deutlich wurde, sind die Herausforderungen von Digital Confidence vielschichtig. Digitales Vertrauen ist nicht nur ein wichtiger „Feel good, feel safe"-Faktor für die Verbraucher, sondern hat darüber hinaus eine hohe Bedeutung für die Wirtschaft. So verursacht beispielsweise Online-Piraterie allein in Europa Verluste von mehreren Milliarden €. Jeder Schlüsselbereich von Digital Confidence erfordert die Abwägung gesellschaftlicher und vor allem finanzieller Vor- und Nachteile. Ein besonders restriktiver Schutz persönlicher Verbraucherdaten kann Geschäftsmodelle, die auf gezielter Verbraucheransprache beruhen, gefährden – und damit einen künftigen Online-Werbemarkt von 57 Mrd. € im Jahr 2012. Dabei ist es wichtig, festzuhalten, dass schon heute eine Vielzahl innovativer und nützlicher Online-Dienste wie Routenplaner oder Stadtpläne nur deshalb kostenlos für ein Massenpublikum verfügbar sind, weil sie über Werbung finanziert werden. Solche Angebote könnten künftig unter Druck geraten, während Neuentwicklungen ganz auf der Strecke bleiben könnten.

Um ein gemeinsames Vorgehen zu gewährleisten, das zum einen Wertschöpfung ermöglicht und zum anderen den Verbrauchererwartungen an die Industrie in allen Bereichen von Digital Confidence entspricht, müssen für alle Stakeholder der digitalen Wirtschaft Rollen und Verantwortlichkeiten definiert werden. Diese Rollen sollten die Lasten fair verteilen und dem Anteil der jeweiligen Stakeholder an der Wertschöpfungskette proportional entsprechen. Dabei ist es selbstverständlich, dass die Netzbetreiber als wichtige Wachstums-Enabler – sowohl als Carrier wie auch als Provider von Internet- und Digitalangeboten über ihr Netz – nach wie vor eine zentrale und starke Position bei der Schaffung von Digital Confidence einnehmen müssen. Ihr Kerngeschäft des „Durchleiters" steht letztendlich genauso auf dem Spiel wie künftige Umsätze aus Online-Handel und Mehrwertdiensten.

So würde zum Beispiel eine „Three strikes and you're out"-Regel, wie sie von den Content-Eignern und ihren Verbänden befürwortet wird, von den Netzanbietern verlangen, dass sie die Nutzung von Copyright-Material in ihren Netzen überwachen und kontrollieren. Ein solcher Ansatz könnte aber allein die digitale Wirtschaft Großbritanniens mit unmittelbaren Umsatzverlusten von insgesamt rund 150 Mio. € pro Jahr konfrontieren – ganz zu schweigen von den Konsequenzen für den Verbraucherdatenschutz.

Um die ökonomischen Auswirkungen eines Gelingens oder Scheiterns von Digital Confidence darzustellen, haben wir in dieser Studie die digitale Wirtschaft Europas mit ihren aktuellen und vor allem zukünftigen Umsatzmöglichkeiten ganzheitlich betrachtet, um die Auswirkungen einer starken oder schwachen Entwicklung von Digital Confidence konkret beziffern zu können. Bisherige Studien und Berichte haben sich nur mit Einzelansätzen im Bereich Digital Confidence befasst, wobei jede von eigenen Annahmen ausging und auf eine begrenzte Region bezogen war. Alle diese Daten wurden für unsere Einschätzung herangezogen und zum Aufbau eines umfassenden und kohärenten Modells für ganz Europa und sämtliche Digital-Confidence-Maßnahmen genutzt.

An Digital Confidence zu scheitern, wäre teuer: Ein Marktwert von 124 Mrd. € im Jahr 2012 – 1% des europäischen BIP – steht auf dem Spiel.

Mit der folgenden Risk-Benefit-Analyse geben wir einen genauen Überblick darüber, welche Digital-Confidence-Säulen den größten Einfluss auf die wirtschaftliche Entwicklung haben werden. Die Analyse berechnet die Auswirkungen von zwei alternativen Szenarien auf den Umsatz im Vergleich zu einem neutralen Base Case. Sie trifft genaue Aussagen darüber, welche Umsatzströme der Digital Economy von Störungen des digitalen Vertrauens betroffen sein würden, und ermöglicht der Wirtschaft damit die klare Einschätzung der finanziellen Anreize für die Entwicklung von Digital-Confidence-Lösungen. Mit dem Verständnis dieser Zusammenhänge wird es auch Politik und Regulierern möglich, die Bestrebungen der Industrie in Bereichen zu unterstützen, in denen es nicht so sehr um finanzielle, sondern um gesamtgesellschaftliche Interessen geht.

Grundlage war ein Market-Sizing zur Ermittlung der Studien-Baseline. Es basiert auf einer Vielzahl von Statistiken und Forecasts, einem Abgleich unter Booz & Company-Experten, den Ergebnissen von über 50 Interviews mit Branchenexperten sowie die genaue Untersuchung von Best Practices und Brancheneinschätzungen.

Nach der detaillierten Auswertung der erhobenen Daten wurden die Haupttreiber der Analyse identifiziert und zum Ausgangspunkt der Modellentwicklung gemacht. Das Modell wurde iterativ entwickelt, wobei die Variabilität der Treiber in Sensitivitätsanalysen erfasst wurde. Das stabilisierte Ergebnis der Modellierung wurde schließlich in kohärente Szenarien überführt, was eine Gesamtbetrachtung der Up- und Downside des Digital-Confidence-Case erst möglich macht.

1. FINANCIAL SUMMARY: RISIKEN DES „WORST CASE" SIND GRÖSSER ALS DIE BENEFITS

Als Referenzpunkt veranschlagen wir die europäische[8] digitale Wirtschaft im Jahr 2012 mit einem Gesamtumsatzvolumen von 436 Mrd. € in den vier Kategorien Netzzugang, Handel, Content und Werbung bei einem jährlichen Wachstum (CAGR) von insgesamt 18% (2007–2012).

Datenschutz und Netzintegrität/QoS sind die wirtschaftlich einflussreichsten Faktoren.

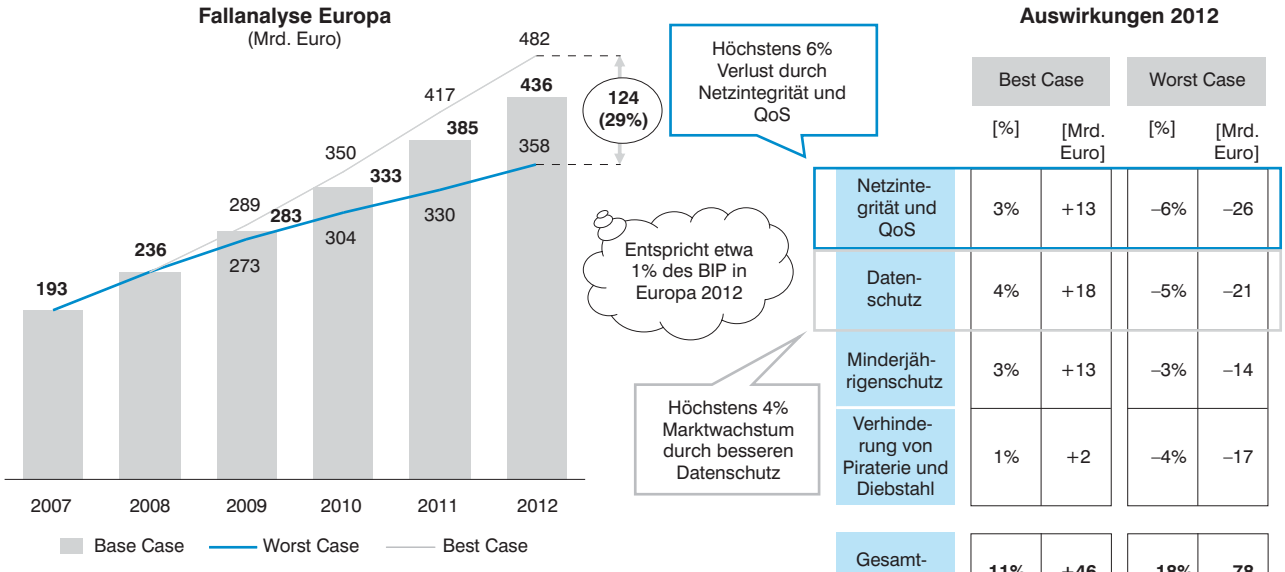
Das Worst-Case-Szenario, nämlich das Scheitern von Digital Confidence an einer zu großen „Divergenzsituation" innerhalb der Branchen, birgt ein weit größeres Risiko als das bestmögliche Szenario, dass wir als „One direction" bezeichnen, Benefits aufweist. Während sich die Downside auf 78 Mrd. € beläuft, beträgt die Upside nur 46 Mrd. €. Beide Zahlen addieren sich zu einem Umsatz-Delta von 124 Mrd. €, was ungefähr 1% des europäischen BIP entspricht – mit entsprechenden Auswirkungen auf Investitions- und Beschäftigungsimpulse.

(8) Unter Europa verstehen wir in diesem Kontext die EU-27 zuzüglich Norwegen und der Schweiz.

Dieser Value at Stake illustriert den potenziellen Wertverlust im gesamten Ökosystem Digitalwirtschaft, von den Konsumenten über Werbetreibende und Contentprovider bis zu den Netzbetreibern. Im schlimmsten Fall wird es im Vergleich zum Best Case weniger User geben, die kleinere Umsätze generieren. Und auch wenn diese Umsätze nicht ganz verloren wären (eine Abwanderung von Amazon käme zum Beispiel dem stationären Buchhandel zugute), so könnten einige Geschäftsmodelle und ihre Umsätze vor dem Totalverlust stehen (zum Beispiel Internetauktionshäuser, die nur sehr schwer in die Offline-Welt zu überführen sind).

Zwei Digital-Confidence-Säulen haben, quer durch sämtliche Umsatzkategorien, den größten wirtschaftlichen Einfluss: Zum einen der Datenschutz, der sich auf die Unsicherheiten bei den Verbrauchern über die Sicherheit digitaler Daten bezieht. Im Worst-Case-Szenario sind die Verbraucher weniger bereit, persönliche Informationen Dritten zur Verfügung zu stellen. Damit setzen Sie die innovativen Werbemodelle unter Druck, in die Online-Marketer und digitale Wirtschaft große Hoffnungen setzen – nicht nur, weil sie zum Eckpfeiler vieler B2C-Geschäftsmodelle werden könnten, sondern auch, weil sie Verbrauchern konkrete Vorteile bringen, beispielsweise durch gezieltere Information bei Kaufentscheidungen. Darüber hinaus könnten Konsumenten bei fehlendem Vertrauen in den Umgang mit ihren Daten weniger geneigt sein, online Waren und digitale Inhalte zu kaufen. Die zweite Säule mit direktem signifi-

Abb. 57: *Der Effekt von Digital Confidence – Indikative Sensitivitätsanalyse*



Hinweis: Geschätztes BIP Europas 2012: 12,5–13,5 Billionen Euro (EU-27 + Norwegen + Schweiz)
Quelle: Europäische Union, Booz & Company-Analyse

kanten Einfluss auf Umsätze ist die Dienstgüte (Quality of Service, QoS), also der Schutz der Technologieplattformen zur Gewährleistung optimaler Anbindung an das „Digital Life“. Nur bei entsprechendem Management können die Netze dem Endverbraucher eine QoS bieten, mit der er von der ganzen Reichhaltigkeit des digitalen Lebens profitieren kann, von VoIP-Telefonie über Surfen im Internet und Multimedia-Dienstleistungen bis zu Video on Demand. Damit beeinflussen Netzintegrität und QoS direkt die Nutzungsintensität und die Nutzerzahlen in allen Umsatzkategorien.

Die Einführung von Services mit höherer Interaktivität und größerem Bedarf an Bandbreite ist ein Prüfstein für Digital Confidence.

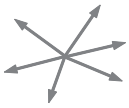
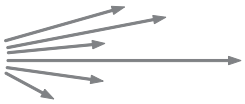
Die weiteren Digital-Confidence-Säulen sind zwar ebenfalls bedeutend, üben aber einen geringeren wirtschaftlichen Einfluss aus, da sie sich nur auf bestimmte Umsatzkategorien beziehen. Die Verhinderung von Diebstahl und Piraterie betrifft zum Beispiel vor allem die Content-Eigner, des Weiteren besteht noch ein beträchtliches Risiko für den Bereich E-Commerce, falls Kunden von Online-Angeboten auf traditionelle Medien (wie CD/DVD) ausweichen. Der Schutz Minderjähriger hat indirekte Folgen für die Nutzung, insofern Eltern kontrollieren, wie häufig ihre Kinder im Internet sind und Kinder und Jugendliche selbst von bestimmten Angeboten (zum Beispiel sozialen Netzen) Abstand nehmen, weil sie ständig von Negativerfahrungen hören.

2. DIGITAL-CONFIDENCE-SZENARIEN – VON DIVERGENZ BIS KONVERGENZ

Die zur Darstellung der möglichen Auswirkung von Digital Confidence entwickelten Szenarien beruhen allgemein auf aktuellen Einschätzungen der Online-Wirtschaft und speziell auf einer Reihe von Fallbeispielen, die illustrieren, welche Maßnahmen gegen die dringendsten Probleme bereits getroffen wurden. Die drei Szenarien mit ihren unterschiedlichen Merkmalen wurden jeweils durch ein übergreifendes Motto charakterisiert.

„Business as usual“ ist der Start- und Referenzpunkt der Analyse. In diesem Szenario folgt die Industrie ihrem einmal eingeschlagenen Weg und erreicht nur graduelle Verbesserungen in bestimmten Bereichen und Prozessen, wobei sich

Abb. 58: *Der Effekt von Digital Confidence – Mögliche Szenarien im Überblick*

	Worst-Case-Szenario	Base-Case-Szenario	Best-Case-Szenario
Motto	„Divergenzsituation“ – verschiedene Maßnahmen im Einsatz 	„Business as usual“ – Maßnahmen mehr oder weniger synchron 	„One Direction“ – Konvergenz bei allen Stakeholdern 
Netzintegrität u. QoS	• Unkoordinierte Nutzung führt zu Datenstaus und schlechtem Nutzungserlebnis	• Gelegentliche Datenstaus besonders in Spitzenzeiten; sie erfordern zunehmenden Managementaufwand von den Netzbetreibern	• Erheblich größere Bandbreiten als heute und zuverlässig gutes Anwendungserlebnis
Datenschutz	• Konsumenten geben immer mehr Informationen preis: Profiling-Risiken	• Mehr Transparenz über Datennutzung, aber keine signifikante Verbesserung bei Phishing und ID-Klau	• Information, Transparenz und effektive Opt-in-/Opt-out-Möglichkeiten fördern die Bereitschaft zur Datenübermittlung (z. B. neue Werbeformen)
Minderjährigenschutz	• Lückenhafte Aufklärungsinitiativen zu Internet-Gefahren für Erwachsene und Kinder	• Fortsetzung bestehender Informations- und Filterstrategien führt zu leichten Prozessverbesserungen	• Konsequentere Aufklärung von Kindern und Erwachsenen durch alle Anbieter • Diszipliniertere Nutzung durch Minderjährige und soziale Netzwerke
Piraterie/ Diebstahl	• Fortgesetzte Piraterie und damit einhergehend weniger legale Content-Angebote	• Hoher Anteil von unerlaubtem Filesharing und Download geschützter Daten	• Bessere DRM-Lösungen für traditionelle Geschäftsmodelle
Position Regulator	• Keine stimmige Vision, Tendenz zur Überregulierung (z. B. QoS- und Datenschutzanforderungen)	• Meist Konzentration auf dringendstes Problem, besonders bei divergierenden Interessen (Datenschutz, Minderjährigenschutz), gelegentlich einseitige Interventionen wie „Three Strikes“	• Unterstützt den „One Direction“-Ansatz voll, regt von der Industrie verantwortete, kollaborative Steuerung an

die Stakeholder mehr oder weniger untereinander abstimmen. Aufklärungs- und Erziehungsmaßnahmen bleiben auf dem jetzigen Stand, die Transparenz bei der Datenverwertung steigt langsam an, aber es gibt keine Durchbrüche bei der Bekämpfung von Phishing und Malware. Durch relativ wirksames Management ist die QoS, abgesehen von gelegentlichen Überlastungen, akzeptabel. Die Probleme bei der Eindämmung von Copyrightverletzungen bleiben die gleichen (Piraterie-Schäden auf heutigem Niveau sind Teil des Base Case).

„One direction" bezeichnet den günstigsten Fall: Ein Szenario, in dem sich die Industrie auf einen abgestimmten Ansatz zur Bildung von Digital Confidence geeinigt hat und in dem alle Akteure konsequent einer gemeinsamen Vision folgen. Die Aufklärungsangebote haben sich durchgehend verbessert, oft in enger Zusammenarbeit verschiedener Stakeholder, und ein besseres Verständnis der Verbraucher über Stärken und Schwächen von Targeted Advertising führt zu dessen nachhaltigem Wachstum. Mit einer breiten Palette von anerkannten Maßnahmen gelingt es den Netzbetreibern und Serviceprovidern, eine äußerst zuverlässige QoS mit höheren Geschwindigkeiten als heute anzubieten. Unerlaubtes Filesharing nimmt ab, weil sich das Bewusstsein der Verbraucher gewandelt hat und bequeme Alternativangebote, gepaart mit neuen Geschäftsmodellen, entstehen.

Die „Divergenzsituation" wäre der schlimmste Fall für die Digitale Wirtschaft, da sie das Wachstum des „Digital Life" nachhaltig beeinträchtigen würde. In einem solchen Szenario operieren die Akteure unabhängig voneinander. Das Fehlen einer gemeinsamen Vision führt zu einer Vielzahl von inkonsequent gehandhabten Maßnahmen. Es gibt nur wenige, oft widersprüchliche Initiativen zum Schutz von Minderjährigen in digitalen Umgebungen und da die Verbraucher immer wieder ärgerliche Datenschutzverstöße erleben, entsteht eine generelle Skepsis gegenüber dem digitalen Leben. Unkontrolliertes Traffic-Management führt zu häufigen Beeinträchtigungen der QoS und zu Beschwerden über mangelnde Netzneutralität. Copyright-Probleme steigen rapide an und die allgemeine Krise der Content-Industrie sorgt auch in der digitalen Welt für das Verschwinden legaler Content-Angebote.

Fast 80 Mrd. € E-Commerce-Einkünfte wären 2012 bei fehlender Digital Confidence gefährdet.

Der wesentliche Unterschied zwischen diesen Szenarien besteht im Grad der Koordination von Digital-Confidence-Ansätzen zwischen den Akteuren der Industrie. „Koordination" soll nicht bedeuten, dass alle Beteiligten stets das Gleiche tun. Gemeint ist vielmehr der Grad der Bereitschaft, in die gleiche Richtung zu arbeiten und sich branchenweit über die Prioritäten und die sich daraus ergebende Verantwortung für den einzelnen Stakeholder abzustimmen.

Ein höherer Grad von geteilter Verantwortung – wie im Best Case dargestellt – resultiert in einer verbesserten Umsetzung von Digital Confidence auf allen vier Säulen des Modells und unterstützt so die Intensivierung der Nutzung und die Steigerung der Erträge.

3. WICHTIGE UMSATZTREIBER: WERBUNG UND CONTENT SIND AM STÄRKSTEN VON DIGITAL CONFIDENCE ABHÄNGIG

Die Umsatzkategorien Content und Werbung wären von unzureichender Digital Confidence am meisten bedroht.

Der Bereich Content reagiert am sensibelsten auf Defizite der Digital Confidence. Das ist schon an den wirtschaftlichen Auswirkungen von Videopiraterie (online und offline) deutlich zu erkennen. Die Motion Picture Association of America (MPAA) schätzt, das 2007 ein weltweiter Verlust von 18 Mrd. Dollar durch Filmpiraterie entstanden ist, wobei nur die direkten Schäden, nicht die möglicherweise noch größeren indirekten Folgen für die Wirtschaft berücksichtigt wurden. Bei potenziellen Verlusten von 31% müssen sich Konsumenten wie Unternehmen darauf verlassen können, dass Online-Content-Plattformen die Interessen der Content-Eigner wahren und gleichzeitig eine sichere Umgebung für sensible Daten bieten (Nutzungsprotokolle, Kreditkarten-Aufzeichnungen etc.). Da Content außerdem häufig echtzeitgebunden ist (wie der BBC iPlayer und andere Streaming-Video-Lösungen), ist die Qualität der zugrundeliegenden Infrastruktur entscheidend: Die Möglichkeit für Umsatz und Umsatzsteigerungen wird also weiterhin stark von der Qualität der angebotenen Netze abhängen. Hierfür werden Netzbetreiber und Contentprovider ein Modell finden müssen, mit dem sie Kosten und Benefits gerecht verteilen können. Nur so können Anreize für Infrastruktur-Investitionen geschaffen werden, um das Internet zu einem Massenmarkt für Content-Delivery zu

E-Commerce, Content und Werbung sind dem Risiko fehlender Digital Confidence am stärksten ausgesetzt.

entwickeln. Im besten Fall können so 4 Mrd. € zusätzlich generiert werden, im ungünstigsten drohen 6 Mrd. € Verlust.
Auch der Werbemarkt ist stark vom digitalen Vertrauen der Konsumenten abhängig, denn die Werbetreibenden werden ihre Budgets nur dann weiterhin von traditionellen auf digitale Umgebungen verlagern, wenn Nutzung und Online-Zeiten sich weiter erhöhen. Für die Werbung beträgt die Upside 9 Mrd. € und die Downside 14 Mrd. €. Und das heißt: Im Worst-Case-Szenario wären fast 25% des Werbemarkts bedroht.

In absoluten Zahlen geht der E-Commerce das größte Digital-Confidence-Risiko ein, denn der Online-Einzelhandel repräsentiert bei weitem die größte Umsatzkategorie. Hier beträgt der Worst Case 52 Mrd. €, die günstigste Schätzung gerade mal die Hälfte. Insgesamt gesehen ist die Branche jedoch weniger betroffen, da das Vertrauen in etablierte Akteure (wie Amazon) schon jetzt recht hoch ist. Außerdem ist bei den physisch versendeten Waren das Fulfillment nicht Internet-abhängig.

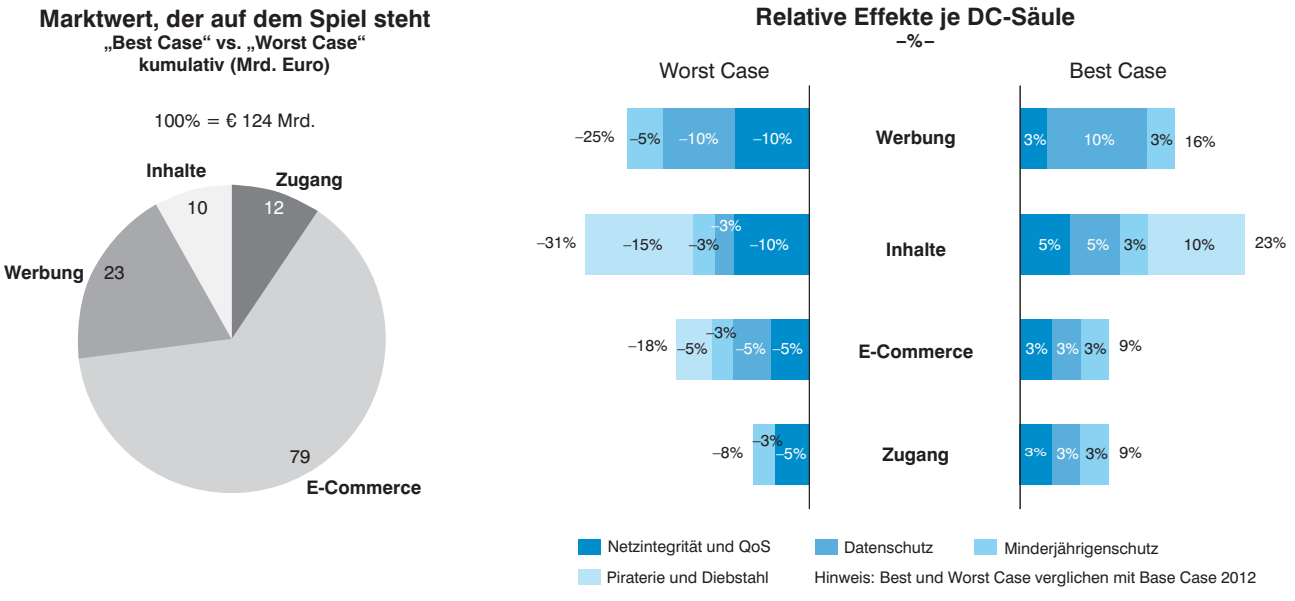
Als grundlegende Leistung ist Netzzugang die Umsatzkategorie, die am wenigsten von Digital-Confidence-Fragen beeinflusst wird. Allerdings sind hier auch die Wachstumserwartungen am geringsten, da Breitband-Anschlüsse immer mehr zum selbstverständlichen Massengut werden. Erfolg oder Scheitern digitalen Vertrauens werden die Nutzerzahlen wohl nicht dramatisch verändern und so betragen Upside und Downside jeweils 6 Mrd. €. Abb. 58 gibt einen Überblick über die verschiedenen Szenarien und ihre Auswirkungen.

4. FAZIT

Selbst bei rein wirtschaftlicher Betrachtung und wenn man die breiteren gesellschaftlichen Aspekte für den Moment außer Acht lässt, hat die Digital Economy erhebliche Vorteile, wenn sie bestimmte Bereiche der Digital Confidence konsequent anspricht, um zumindest das Worst-Case-Szenario zu vermeiden und im Idealfall die bestmögliche Gewinnsituation anzustreben. Dabei ist der Bereich Datenschutz besonders – aber nicht nur – wegen seiner Relevanz für innovative Werbemodelle („Targeted Advertising“) wirtschaftlich interessant. Netzintegrität und Quality of Service sind wichtig, um das ständig expandierende Content- und Bewegtbild-Angebot im Internet voll zu unterstützen.
Der Bereich Piraterie und Diebstahl ist sowohl für die Inhaber von Content-Rechten als auch für Online-Händler relevant. Aber neben der offensichtlichen wirtschaftlichen Bedeutung für den Schutz bestehender Rechte und die Einführung innovativer digitaler und internetbasierter Content-Modelle besteht hier auch ein anderes beträchtliches Risiko: Nutzer könnten ihren Konsum auf Offline-Kanäle verschieben, ein Wechsel der für viele neue Geschäftsmodelle (zum Beispiel Online-Auktionen) nicht möglich ist.

Die Netzbetreiber müssen auch weiterhin eine starke Position innehaben, schließlich ist ihre Leistung eine der Grundvoraussetzungen für die oben genannten Wachstumstreiber. Der Grad der Netzintegrität übt einen wesentlichen wirtschaftlichen Einfluss aus, selbst wenn das Kerngeschäft der Betreiber – Netzzugang – zunächst am wenigsten von den Risiken und Benefits von Digital Confidence betroffen scheint.

Abb. 59: *Der Effekt von Digital Confidence – Wachstumsbereiche und Säulen*



VI. DIGITAL CONFIDENCE: DER AKTIONS- UND HANDLUNGSRAHMEN

1. DIE INDUSTRIE MUSS FÜHREN

Europas digitale Wirtschaft hat eine realistische, optimistische Wachstumsperspektive, seit Web-2.0-typische Angebote, die auf der Funktionalität, Ubiquität und Kapazität von Breitbandverbindungen beruhen, zum Mainstream geworden sind. Doch die Abwanderung auf neue Zugangsnetze, eine starke Vermehrung komplexer Netztechnologien und die immer selbstbewusster auftretende „Born Digital"-Generation könnten sich im Ökosystem der digitalen Wirtschaft störend auswirken. Der Paradigmenwechsel stellt die gesamte Industrie, aber auch Entscheidungsträger und Regulierer vor große Herausforderungen. Das Vertrauen, das Kunden in das Geschäftsverhalten und die Sicherheit von Dienstleistungen und Netzen der Service- und Plattformanbieter, aber auch in die Durchsetzbarkeit von Verbraucherschutzmaßnahmen seitens Gesetzgebern und Aufsichtsbehörden setzen, entwickelt sich momentan zur wichtigsten Voraussetzung für die erfolgreiche Ausschöpfung des digitalen Wachstumspotenzials.

Die Industrie befindet sich in Bezug auf die zukünftige Entwicklung des digitalen Lebens an einem Wendepunkt. Die Kosten-Nutzen-Analyse zeigt, welche finanziellen Auswirkungen Digital Confidence auf die Industrie hat. Ein Marktvolumen von 124 Mrd. Euro steht auf dem Spiel – hier besteht ganz klar ein wirtschatlich getriebener Handlungsbedarf. Ungeachtet der finanziellen Anreize stellt die Schaffung von Digital Confidence jedoch auch eine soziale Verantwortung dar, zumal Verbraucher, Regulierer und die Gesellschaft insgesamt von Problematik betroffen sind.

Die Fallstudien im vorliegenden Bericht bestätigen, dass verschiedene Stakeholder aus der Industrie bereits intensiv an Lösungen arbeiten. Bei diesen Maßnahmen handelt es sich allerdings größtenteils um Reaktionen auf die aktuelle Problematik, geboren aus der Notwendigkeit, die Forderungen der Verbraucher, Medien und Regulierer zu erfüllen, insbesondere vor dem Hintergrund bekannt gewordener Zwischenfälle, bei denen es zu erheblichen Datenschutz- und Sicherheitsverletzungen oder anderen Vertrauensbrüchen kam. Solche Vertrauensbrüche wurden bisher unter anderem durch folgende Umstände begünstigt:

- Nichterfüllung von Erwartungen an die Dienstleistungsqualität, etwa durch nicht einhaltbare Versprechungen, vor allem wenn die Leistungsfähigkeit nicht unter der Kontrolle des Netzbetreibers liegt – so etwa im Fall US-amerikanischer ISPs, die den Eindruck vermittelten, dass über ihr Netz keine Inhalte zugänglich sind, die mit sexuellem Kindesmissbrauch einhergehen. Ein anderes Beispiel betrifft Nutzer, die beim Einsatz von Netzmanagement-Technologien eine Verschlechterung populärer daten- und damit bandbreitenintensiver Dienste wie P2P File-sharing-Seiten feststellen.

- Nichterfüllte Erwartungen im Bezug auf die Effizienz von Filtertechnologien im Fall von Inhalten, die mit sexuellem Kindesmissbrauch einhergehen.

- Einsatz von intrusiven Internet-Überwachungstechnologien zu kommerziellen Zwecken.

Ungeachtet der Vielfalt und Komplexität aktueller Ansätze zeichnen sich folgende Leitlinien für Best Practices zur Verbraucherakzeptanz ab:

- Verbraucher akzeptieren vor allem transparente und unaufdringliche Maßnahmen – Netzbetreiber, Content- und Plattform-Anbieter müssen gemeinsam mit dem Regulierer auf eine solche Kommunikation hinarbeiten.

- Die Verbraucher sind besorgt darüber, wie Netzbetreiber und ISPs ihre digitalen Daten handhaben und überwachen. Klare Aussagen und konsequente, zuverlässige Rahmenbedingungen haben hier oberste Priorität.

- Verbraucher wollen selbst Kontrolle über das Risiko, dem sie sich aussetzen – dazu brauchen sie Zugang zu den entsprechenden Tools, Opt-in-/Opt-out-Möglichkeiten und angemessene Informationen.

- Verbraucher akzeptieren Maßnahmen, wenn diese die Qualität der Services sichern. Auch

wenn dies aktives Traffic-Management bedeutet, sind sie dazu bereit, vorausgesetzt die Nutzungsbedingungen werden offen kommuniziert, die Preismodelle sind fair und transparent und die Zugangsstrukturen diskriminierungsfrei.

Fallstudien zeigen zudem die hohe Komplexität, die mit der erfolgreichen Sicherstellung von Digital Confidence einhergeht. Selbst Lösungen, die in bester Absicht den Fokus darauf setzen, bestimmten Verhaltensweisen durch die Blockierung oder Filterung von Inhalten vorzugreifen, können eine Gefährdung von Persönlichkeitsrechten und Netzneutralität bedeuten. Lösungen, die auf die Aufklärung und Stärkung der Verbraucher abzielen, damit diese die Risiken begreifen und die Verantwortung für Maßnahmen zur Minimierung dieser Risiken übernehmen, erfordern von der Branche ein hohes Maß an Engagement, um ein entsprechendes Bewusstsein aufzubauen. Die Software-Tools zur Unterstützung beider Ansätze sind bereits verfügbar, doch bisher fehlt es an einer gemeinsamen Definition von Standards und Richtlinien in Bezug auf unerwünschte Inhalte.

Nur die Beachtung aller vier Säulen von Digital Confidence ermöglicht den nächsten Wachstumsschub im „Digital Life".

Um dafür zu sorgen, dass die Digital-Confidence-Problematik mit ihrer zunehmend umfassenden und internationalen Dimension weltweit mit einer einheitlichen Lösung beantwortet wird, ist ein ganzheitlicher Ansatz erforderlich, der branchenweit umgesetzt wird. Nur so kann in Bezug auf die Risiken und Nutzen des digitalen Lebens ein ausreichendes Maß an Transparenz und Hilfestellung für die Verbraucher erreicht werden.

Jede der vier Säulen von Digital Confidence ist sehr komplex, nicht nur was Gefahren und Lösungen angeht, sondern auch in Bezug auf die unterschiedlichen Positionen und Interessen der Stakeholder.

Die Problematik wird im Folgenden hauptsächlich aus der Sicht des Netzbetreibers dargestellt. Seine empfohlene Positionierung in Bezug auf Digital Confidence wird definiert, um anschließend die geeigneten Maßnahmen im Detail darzustellen. Danach wird die Diskussion zurück auf die Ebene der gesamten Branche gebracht, wobei die Auswirkungen für die anderen Stakeholder, insbesondere die Regulierer, erläutert werden.

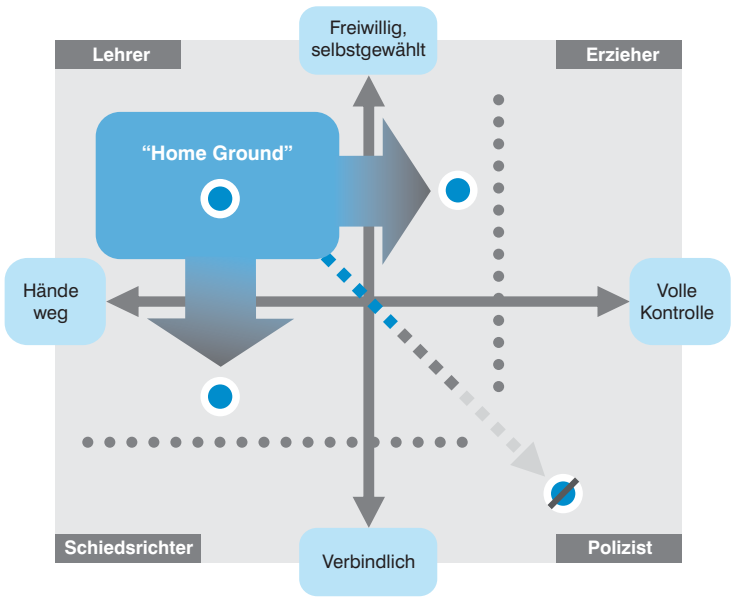
2. NETZBETREIBER UND ISPS BRAUCHEN EINE KLARE POSITION ZU DIGITAL CONFIDENCE

Das generelle Selbstverständnis von Netzbetreibern und ISPs spielt im Zusammenhang mit der Definition des Beteiligungsgrades bei der Umsetzung proaktiver Digital-Confidence-Strategien eine entscheidende Rolle: Sie müssen sich der Frage stellen, ob sie sich als „reine Durchleiter" sehen, die lediglich Infrastrukturen verfügbar machen, oder ob sie sich aktiv an der Festlegung von Regeln zur Benutzung dieser Infrastrukturen und an der Überwachung dieser Regeln beteiligen wollen.

Auf diese Frage gibt es jedoch keine eindeutige Antwort, denn die Position eines Netzbetreibers oder ISPs ist je nach Betrachtung der einzelnen Digital-Confidence-Säulen oft ganz unterschiedlich.

Die Digital Confidence Positionierungs-Matrix dient als Struktur, mit der sich Positionen sowohl für die einzelnen Säulen von Digital Confidence als auch für das Konzept insgesamt bestimmen lassen. Die vertikale Achse differenziert die zugrunde liegenden Prinzipien mit den zwei Polen „freiwillig" und „obligatorisch". Die horizontale Achse differenziert die Art der Vorgehensweise, vom passiven „Hände weg"-Ansatz bis zur aktiven „vollen Kontrolle". Die sich ergebenden vier Quadranten entsprechen auf symbolhafte Weise bestimmten archetypischen gesellschaftlichen Rollen. Der Lehrer klärt die Nutzer so gut wie möglich über Angebote und Gefahren auf, verhängt aber normalerweise keine Sanktionen. Auch der Erziehungsberechtigte klärt über Gefahren und Maßnahmen auf, führt aber im Gegensatz zum Lehrer proaktive Maßnahmen durch, falls er es für notwendig

Abb. 60: *Positionierung – „Home Ground" für Netzbetreiber*



erachtet. Der Schiedsrichter vertraut auf freiwillige Regeln, die er fallbezogen durchsetzt und setzt auf Richtlinien statt auf Aufklärung; die Regeln basieren auf Absprachen. Der Polizist bevorzugt naturgemäß starke Sanktionen und ergreift alle notwendigen Maßnahmen auf Basis klarer Regeln, um beispielsweise sämtliche illegalen Aktivitäten zu blockieren.

Auf der Grundlage unserer Untersuchungen und Branchenkenntnisse sind wir, gestützt durch unser Befragungsprogramm, zu der Erkenntnis gelangt, dass die angestammte Position der ISPs, der „Home Ground", bisher im oberen linken Quadranten liegt – also bei der Rolle des Lehrers. Die Merkmale, die mit diesem Quadranten verbunden werden, entsprechen dem ursprünglichen Selbstverständnis eines Netzbetreibers: Sein Kerngeschäftszweck besteht nach wie vor darin, ein sicheres, zuverlässiges und leistungsstarkes Datennetz für den Internetverkehr zur Verfügung zu stellen, ohne Einflussnahme auf die Daten, die über sein Netz ausgetauscht werden. Daraus lässt sich die Rolle eines Lehrers ableiten, der Verbraucher auf die Digital-Confidence-Problematik aufmerksam macht und ihnen zugleich Werkzeuge an die Hand gibt, um diese Probleme auf Basis eines „Hände weg"-Ansatzes selbst zu lösen. Diese Positionierung reduziert Risiken und Verantwortlichkeiten in Bezug auf Probleme, für die der ISP nicht primär verantwortlich ist. Im Allgemeinen wäre der ISP nicht für die Definition von Digital-Confidence-Standards und die Überwachung ihrer Einhaltung verantwortlich, beispielsweise für die strafrechtliche Verfolgung von Urheberrechtsverstößen. Unsere Analyse zeigt jedoch, dass dies nicht ausreicht. Da ein signifikanter Anteil des künftigen Wachstums mit einer ansteigenden Nutzung bestehender und neuer digitaler bzw. Online-Mehrwertdienste verbunden ist, wird das Maß an Vertrauen, das Verbraucher ihrem Provider entgegen bringen, zur entscheidenden Vorbedingung für Wachstum und Erfolg im digitalen Markt. Für einen ISP reicht es nicht mehr aus, nur auf Aufklärung, Corporate-Responsibility-Programme und die Einhaltung gesetzlicher Vorschriften zu setzen, um die Akzeptanz und das Vertrauen der Nutzer zu erhalten. Den Gesetzgebern gelingt es oft nur mühsam, mit der Geschwindigkeit und der Tragweite der Entwicklungen Schritt zu halten, etwa im Bereich neuer Technologien zur Überwachung des Internetverkehrs oder steigender Sicherheitsrisiken in Verbindung mit zunehmend raffinierten Cyber-Straftaten, die Auswirkungen auf digitales Vertrauen haben. Erfolgreiche Unternehmen geben sich daher nicht mit der Befolgung der Gesetze zufrieden. Sie handeln vorausschauend und entwickeln eigene Digital-Confidence-Prinzipien:

- Sie arbeiten mit vertrauensbildenden Verfahren und Protokollen.

- Sie sind in ihrer Kundenkommunikation so offen und transparent wie möglich.

- Sie bemühen sich noch intensiver, Verbraucher aufzuklären und zu stärken, um ihre Interessen in der digitalen Welt selbst zu schützen.

- Sie befolgen den stufenweisen proaktiven Ansatz des E3 Paradigmas: Erst aufklären (Educate), dann stärken (Empower) und nur wenn nötig gezielt durchgreifen (Enforce).

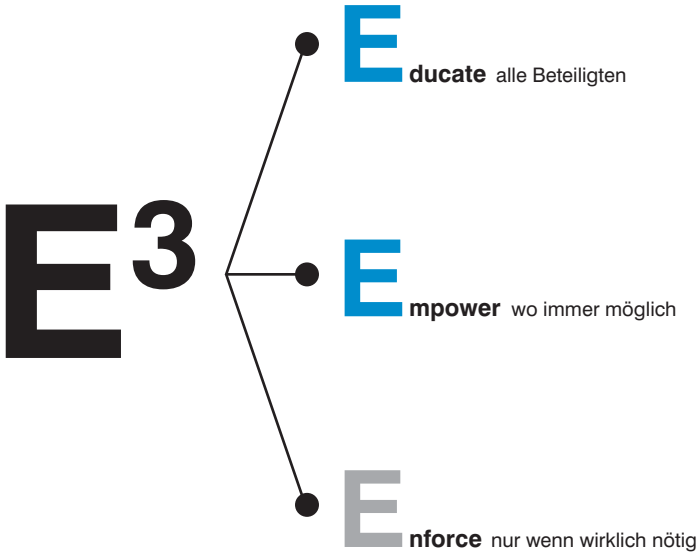
Netzbetreiber und ISPs müssen die Branchenagenda proaktiv gestalten, indem sie Lösungen und Ansätze entwickeln, die zu einer Neupositionierung führen, bei der sie gezielt und selektiv (auch) die Rolle eines Erziehungsberechtigten und Schiedsrichters einnehmen.

Netzbetreiber und ISPs können sich aus verschiedenen Gründen veranlasst sehen, ihre bisherige Positionierung zu ändern. Erstens könnten strategische oder geschäftliche Gründe einen Netzbetreiber dazu bringen, seine bisherige Position aufzugeben, etwa um das Wohlwollen der Verbraucher zu sichern. Falls beispielsweise Eltern mit den Maßnahmen zum Schutz ihrer Kinder zufrieden sind, werden sie ihnen erlauben, das Internet häufiger zu nutzen. Zudem ist Traffic-Management von strategischem Wert, denn es sorgt dafür, dass nicht nur die Power-User, sondern alle Kunden von Investitionen in neue Zugangsnetze mit höheren Bandbreiten profitieren. Die Fähigkeit eines Netzbetreibers, den Nutzern dauerhaft eine hohe Servicequalität und optimale Breitbandnutzung zu bieten, wird sich als entscheidender Wettbewerbsvorteil im aktuellen Infrastruktur-Wettkampf erweisen.

Die Industrie sollte dem E³-Paradigma folgen: Educate, Empower, Enforce.

Zweitens kann die Gefahr einer unverhältnismäßig eingreifenden Regulierung durch die Förderung einer besseren Selbstkontrolle und Zusammenarbeit innerhalb der Branche verhindert werden. Ein Beispiel dafür liefert Großbritannien, wo die führenden ISPs mit dem Verband der britischen Tonträgerindustrie BPI kooperieren, um Verbraucher aktiv anzusprechen und vor Piraterie zu warnen. In den USA einigte sich Comcast in konstruktiver Weise mit BitTorrent auf eine für beide Seiten akzeptable

Abb. 61: *Das E³-Modell*



Verfahrensweise in Bezug auf Traffic-Management von P2P Traffic.

ISPs sollten jedoch äußerst vorsichtig sein, wenn sie Rollen außerhalb ihres primären Verantwortungsbereichs übernehmen. Entscheidungen, die ihre starke Position als reiner Infrastrukturanbieter unterminieren und sie unkontrollierbarer Haftbarkeit aussetzen, sind letztendlich nicht dazu angetan, digitales Vertrauen zu fördern - während bei den Endverbrauchern falsche Erwartungen geweckt würden, ganz zu schweigen von den negativen Signalen an Investoren und Aktionäre.

ISPs sollten soweit möglich vermeiden, die Rolle des Polizisten zu übernehmen, außer sie sind rechtlich dazu befugt. Die Rolle des Polizisten stellt einen stark eingreifenden Ansatz dar, der die Verbraucherakzeptanz negativ beeinflussen würde. Falls sie rechtlich befugt sind, haben Netzbetreiber und ISPs nicht nur eine tatsächliche Verpflichtung, diese Rolle zu übernehmen, sondern sind bei der Ausübung dieser Rolle auch haftungsrechtlich geschützt. Wenn sie beispielsweise gesetzlich befugt sind, bestimmte Internetseiten aufgrund von inhaltlichen Bedenken zu blockieren, setzen sie sich weniger dem Risiko aus, wegen Verstößen gegen Urheberrechte, Persönlichkeitsrechte, Meinungsfreiheit oder Netzneutralität angeklagt zu werden.

Zusammengefasst lässt sich diese Positionierung als klares Paradigma formulieren:
E3 - Educate (Aufklären), Empower (Stärken), Enforce (Durchgreifen). Die Positionierung in der Matrix bestimmt, in welchem Ausmaß diese Rollen im Falle des Netzbetreibers erfüllt werden.

3. CALL TO ACTION FÜR NETZBETREIBER: FÜNF SCHLÜSSELINITIATIVEN ZUR DIGITAL CONFIDENCE

Das E3-Paradigma definiert in zusammengefasster Form Handlungsoptionen für Netzbetreiber und ISPs, ist jedoch ebenso auf alle anderen Stakeholder im Digital Life anwendbar.

Educate (Aufklären): Netzbetreiber und ISPs sollten ihren Kunden die Gefahren der digitalen Welt verständlich machen und ihnen das erforderliche Wissen vermitteln, damit sie mit diesen Gefahren umgehen und das Internet sicher nutzen können. Strategien sollten den Endnutzern klar und transparent kommuniziert werden. Dazu gehört auch Transparenz in Bezug auf die Strategie des Unternehmens im Bereich Digital Confidence.

Empower (Stärken): Netzbetreiber und ISPs sollten ihre Kunden soweit wie möglich in die Lage versetzen, digitale Bedrohungen und Probleme selbst zu kontrollieren, beispielsweise durch einen Opt-In- oder Opt-Out-Ansatz zur Blockierung unerwünschter Inhalte. Vor allem sollten Netzbetreiber und ISPs Kunden solche Prozesse und Tools zur Verfügung stellen und Dritte darin unterstützen, diese Tools und Dienste zu entwickeln.

Enforce (Durchgreifen): Netzbetreiber und ISPs sollten proaktiv eingreifen, um das Nutzerverhalten zu steuern; vor allem bei speziellem öffentlichen Interesse ist diese Maßnahme wichtig zu Erhaltung von Digital Confidence. ISPs sollten in solchen Fällen eine branchenweite einheitliche Umsetzung anstreben und sich über Best Practices austauschen.

Die starke Betonung von Nutzeraufklärung und Nutzerstärkung berücksichtigt auf effiziente Weise Veränderungen in der Selbstauffassung der Verbraucher und in ihrer Vorgehensweise, sich zu informieren und Probleme zu lösen. Eine kürzlich durchgeführte Studie (Edelman's Trust Barometer 2008), bei der die junge europäische Meinungselite im Alter von 24 bis 34 – die sogenannten „Info-entials" – analysiert wurde, kam zu dem Schluss, dass diese Zielgruppe bei der Sammlung von Informationen ganz anders vorgehen als die älteren Meinungsführer: Sie nutzen zahlreiche verschiedene Informationsquellen und ihre Ansichten sind durch kontinuierliche Mitwirkung, Reflektion und Meinungsaustausch geprägt. Als selbständige Nutzer sind die "Info-entials" nicht nur offen für Aufklärung und Stärkung, sondern verlangen sogar danach. Die Studie fand heraus, dass die "Info-entials", wenngleich sie sich traditionell durch eine zynische Einstellung zum Marktgeschehen auszeichnen, heute ein vergleichs-

weise hohes Vertrauen zu Anbietern haben. Die Informationsquellen, denen die "Info-entials" in den meisten EU-Ländern das größte Vertrauen entgegen bringen, sind "Leute wie du und ich" sowie NGOs. Netzbetreiber und ISPs können dieses Wissen nicht nur nutzen, um digitales Vertrauen aufzubauen, sondern auch für klassische Kundenbindungsmaßnahmen.

Aufbauend auf dieser allgemeinen Leitlinie wird eine unternehmensorientierte Sichtweise eingenommen, um konkrete Maßnahmen abzuleiten und zu spezifizieren. Relevante Maßnahmen wurden auf fünf Handlungsebenen definiert:

1. RICHTLINIEN UND VERFAHREN

Jeder Netzbetreiber und ISP sollte ein Positionspapier vorhalten, das seine Strategie und Position für jede der Digital-Confidence-Säulen definiert. Auf dieser Grundlage müssen Digital-Confidence-Richtlinien vier Bereiche adressieren: Traffic-Management und andere technologische Maßnahmen zur Sicherstellung der Dienstequalität, Datenschutz, Minderjährigenschutz und Verhinderung von Piraterie. Das Positionspapier muss präzise genug formuliert sein, um konkrete Hilfestellung zu den mit den Einzelproblemen verbundenen prinzipiellen Fragestellungen zu bieten – etwa dazu, wie ein Unternehmen den Konflikt zwischen unerwünschten Inhalten und Meinungsfreiheit ausbalanciert.

In einem weiteren Schritt gilt es, diese Richtlinien in den Kernprozessen des Unternehmens zu verankern. Dies hat in den meisten Fällen direkten Einfluss auf die Produktentwicklung der Netzbetreiber, beispielsweise um sicherzustellen, dass Produkte und Services den Standards entsprechen.

Darüber hinaus müssen Netzbetreiber ihre Digital-Confidence-Richtlinien und -Prozeduren regelmäßig aktualisieren, indem sie sie juristischen, politischen und technischen Überprüfungen unterziehen.

Aus allen in diesem Bericht analysierten Fällen lässt sich eine sehr wichtige Lehre ziehen: Digital Confidence bedeutet Vertrauen, und Vertrauen entsteht durch offene Kommunikation. Transparenz zahlt sich aus. Deshalb sollten Unternehmen die angewendeten Richtlinien und die damit verfolgten Ziele – einschließlich geschäftlicher Ziele – deutlich kommunizieren. Die Erfahrung zeigt, dass die Verbraucherakzeptanz generell hoch ist, wenn Regeln und die damit verfolgten Ziele offen kommuniziert werden – etwa im Fall des E-Mail-Angebots „Gmail" von Google, bei dem gezielte Werbung eingesetzt wird. So entsteht ein Dialog mit dem Verbraucher, der sogar entscheidend zur Optimierung der Angebote beitragen kann.

2. GOVERNANCE

Die Digital-Confidence-Problematik ist nicht nur sehr komplex, sondern auch äußerst sensibel und funktionsübergreifend. Häufig erfordert sie die Definition von grundlegenden Positionen, etwa zur Frage, wie mit sexuellem Missbrauch im Internet umgegangen werden soll. Jeder Fehler kann enorm ruf- und ergebnisschädigend sein. Daher ist es besonders wichtig, dem Thema die gebührende Aufmerksamkeit auf höchster Managementebene zu widmen. Digital Confidence sollte tief in den Organisationsstrukturen verankert sein, beispielsweise durch den Einsatz eines Digital Confidence-Lenkungsausschusses unter der Leitung erfahrener Führungskräfte, der die Planung und Umsetzung aller damit verbundenen Aktivitäten beaufsichtigt.

3. TECHNOLOGIE

Da unterstützende Technologien für Digital Confidence bereits in großer Anzahl vorhanden sind, haben nun Entscheidungen zur individuellen Positionierung, zur Ausgestaltung von Richtlinien und zum Aufbau der Organisation oberste Priorität. Dennoch werden die meisten Netzbetreiber um gewisse technologische Investitionen nicht herumkommen, wenn sie zukunftssicher bleiben wollen. Diese Investitionen sind nötig, um sicherzustellen, dass die Servicequalität trotz steigendem Multimedia-Traffic dauerhaft aufrecht erhalten werden kann. Bei Investitionsentscheidungen werden die Netzbetreiber zwischen den Vorteilen von Kapazitätserweiterungen und aktivem Traffic-Management, beispielsweise durch Staffelpreise und technische Lösungen, abwägen müssen. Netzbetreiber sind gut beraten, gemeinsam mit den Contentprovidern ihre Netze für Multimedia-Datenströme fit zu machen und neue Technologien wie Peer-to-Peer-Caching (vgl. Ansätze der P4P Initiative) oder Content-Delivery-Netze zu integrieren.

Sie müssen die Regulierer davon überzeugen, dass sie sich der Problematik in angemessener Weise annehmen.

Ein weiterer entscheidender Risikobereich betrifft momentan die technische Ausrüstung der Endnutzer. Ihre Geräte sind im Allgemeinen nur schlecht gegen Bedrohungen wie Viren, Botnets und andere Formen von Malware geschützt. Softwarelösungen sind zwar schon vorhanden, doch Netzbetreiber und ISPs müssen Kunden noch stärker als bisher ermutigen, sie auch einzusetzen. Daneben müssen sie Tools und Lösungen anbieten, die es den Kunden ermög-

lichen, den Grad des Risikos selbst zu bestimmen (etwa durch eine Opt-in-/Opt-out-Möglichkeit).
Das erfordert zugleich einen Wechsel der Gangart: Es wird nicht mehr ausreichen, entsprechende Programme zum kostenlosen Download anzubieten. Vielmehr müssen Netzbetreiber und ISPs die Installation aktiv vorantreiben (gegebenenfalls auch beim Kunden vor Ort) und die Anzahl ständig überwachen (im Wesentlichen dadurch, dass sie sich in Bezug auf ihre Rolle neu positionieren und weniger als Lehrer, sondern mehr als Erziehungsberechtigter agieren).

4. AUFKLÄRUNG DER VERBRAUCHER

ISPs sowie Betreiber von Kabel- und Telekommunikations-Netzen sollten gemeinsam mit NGOs gezielte Programme entwickeln und eigene angemessene Aufklärungsinitiativen durchführen, beispielsweise Informationskampagnen auf ihren eigenen Internetseiten.

Die Programme müssen alle Bedrohungen im Zusammenhang mit Datennutzung und -veröffentlichung, kontextbezogener Werbung, Piraterie und Online-Verhalten allgemein abdecken, einschließlich „Bullying“, sexuellen Missbrauch und unzulässige Inhalte.

Bei der Aufklärung sollten gezielt Botschaften eingesetzt werden, die auf spezifische Nutzergruppen zugeschnitten sind, einschließlich Eltern und Kinder: Bei den Elternprogrammen sollte die Beaufsichtigung der Aktivitäten der Kinder und die Schaffung eines Bewusstseins für die Gefahren im Mittelpunkt stehen, wobei auch die verfügbaren Werkzeuge vorgestellt werden, mit denen Eltern die Online-Umgebung ihrer Kinder kontrollieren und mitgestalten können. Die Aufklärung von Kindern sollte den Fokus auf die Erkennung und den Umgang mit Bedrohungen setzen.

5. REGULIERUNG

Im Rahmen der proaktiven Vertrauensbildung kommt Netzbetreibern die Aufgabe zu, Regulierer auf Handlungsfelder hinzuweisen, die eindeutig nicht im Verantwortungsbereich der Infrastrukturprovider liegen (wie z. B. die Indizierung von illegalem Content oder Strafverfolgung). Die Regulierer sollten ihrerseits keine vorschnellen Maßnahmen ergreifen, solange die Verhältnismäßigkeit im Einzelfall nicht gewährleistet werden kann. Der Regulierer sollte nur dann direkt eingreifen, wenn die Verbraucherinteressen ernsthaft gefährdet sind.

Im Gegenzug muss die Industrie unter Beweis stellen, dass es ihr mit Digital Confidence ernst ist, indem sie in Eigeninitiative entsprechende kohärente Lösungen entwickelt. Diese Lösungen sollten von allen Playern unterstützt werden, wobei die Kosten der Umsetzung proportional zum wirtschaftlichen Nutzen aufzuteilen sind. Die Regulierer sollten die Industrie darin unterstützen, solche Lösungen zu entwickeln, etwa durch Förderung von Kooperationen mit Stakeholdern und finanzielle Unterstützungsprogramme. Dabei sollten sie die Kräfte des Wettbewerbs zum Vorteil der Verbraucher walten lassen, statt sie zu regulieren. Tatsächlich kann Regulierung, selbst wenn sie in guter Absicht erfolgt, vom Verbraucherstandpunkt aus kontraproduktiv sein und wirtschaftlichen Schaden verursachen, wie die Modellrechnung zur QoS-Regulierung zeigt.

Bei der Umsetzung der Maßnahmen auf diesen fünf Handlungsebenen sind Netzbetreiber und ISPs allgemein gut beraten, auf möglichst breiter Front mit NGOs zusammenzuarbeiten. Viele Aspekte können effektiver angesprochen werden, wenn ein Provider gemeinsam mit einer NGO aktiv wird, denn das garantiert Neutralität und branchenweite Akzeptanz durch den guten Ruf der gemeinnützigen Organisation. Jüngste Umfragen zeigen, dass NGOs im Verbrauchervertrauen ganz oben liegen.

4. AUSWIRKUNGEN AUF ANDERE STAKEHOLDER

Die Position des Netzbetreibers hat natürlich auch Einfluss auf die anderen Stakeholder im Ökosystem des digitalen Lebens. Die zwei wichtigsten Gruppen sind folgende:

- Verbraucher.

- Andere Anbieter entlang der digitalen Wertschöpfungskette (einschließlich Contentprovider, Software- und Anwendungsentwickler sowie Distributoren, beispielsweise E-Shops).

VERBRAUCHER

Die Verbraucher müssen begreifen, dass der Einsatz des gesunden Menschenverstands in der Online-Welt genauso selbstverständlich erfolgen sollte wie in allen anderen Lebensbereichen. Zudem müssen sie den Umgang mit den verbraucherorientierten Lösungen erlernen, die von Netzbetreibern, ISPs und anderen Organisationen entwickelt werden, um den Verbrauchern zu ermöglichen, die Bedrohungen des digitalen Lebens selbst zu

Verbraucher müssen lernen, mit den von der Industrie zur Verfügung gestellten Ressourcen umzugehen.

erkennen und zu kontrollieren. Um diesen Anforderungen gerecht zu werden, sollten die Verbraucher Aufklärungsangebote von öffentlichen Stellen nutzen (etwa von Schulen, Universitäten oder Behörden).

ANBIETER VON URHEBERRECHTLICH GESCHÜTZTEN INHALTEN SOLLTEN IHRE AGENDA AUF ZWEI HAUPTWEGEN VORANTREIBEN

Die Eigentümer von Inhalten sollten dafür Sorge tragen, dass Copyright-Material ausreichend geschützt ist. Die Musikindustrie kämpft seit Jahren mit dem Problem, das die von ihr entwickelten Geschäftsmodelle keine ausreichende Kontrolle zur Vermeidung von Piraterie beinhalten. Aufgrund der Verfügbarkeit höherer Bandbreiten und moderner Kompressionstechnologien betrifft diese Problematik inzwischen auch die Film- und Fernsehbranche. Eigentümer von Inhalten müssen gemeinsam Lösungen entwickeln, um den Wert der ihnen gehörenden Inhalte angemessen zu schützen. Um dieses Ziel zu erreichen, müssen sie Lösungen zum Copyright-Schutz auf Branchenebene entwickeln. Die Content-Industrie kann sich nicht einzig und allein darauf verlassen, dass die Netzbetreiber Inhalte in ihrem Auftrag schützen. Zudem sind Verbraucher weniger geneigt, Lösungen von Internetanbietern zu akzeptieren (z. B. die Filterung oder Blockierung von Inhalten), wenn diese nur aufgrund von geschäftlichen Interessen verfügbar gemacht werden, wie es etwa bei Maßnahmen zur Vermeidung von Piraterie der Fall ist. Lösungen, die auch einen moralischen oder gesellschaftlichen Aspekt haben, werden von Verbrauchern dagegen eher akzeptiert (z. B. die Blockierung von kinderpornografischen Inhalten). Lösungen zur Pirateriebekämpfung müssen innovative Geschäftsmodelle ebenso umfassen wie unterstützende Technologien für das Management digitaler Rechte.

INTERNETINDUSTRIE UND ANDERE STAKEHOLDER SOLLTEN KOOPERIEREN

E-Commerce-Unternehmen sollten gemeinsam mit Netzbetreibern und ISPs Aufklärungsprogramme zu Themen von beiderseitigem Interesse (z. B. Phishing) entwickeln. Die Zielsetzung solcher Programme muss darin bestehen, das Vertrauen der Verbraucher zu erhöhen, indem ihnen ein noch umfassenderes Wissen über die Gefahren und Probleme der digitalen Welt vermittelt wird. Zudem müssen den Verbrauchern die Werkzeuge zur Bekämpfung dieser Gefahren zur Verfügung gestellt werden. Zusammen mit Software- und Anwendungsentwicklern können Netzbetreiber und ISPs effiziente Lösungen und Maßnahmen entwickeln, wie zum Beispiel OpenDNS/PhishTank einschließlich der geforderten Blacklists.

5. PRIORITÄTEN FÜR REGULIERER

Die wichtigsten rechtlichen Grundlagen zur Minimierung der Digital-Confidence-Risiken sind größtenteils bereits etabliert, doch zugleich ist es notwendig, bestehende Regulierungskonzepte ständig zu überprüfen und sie an neue Technologien, Märkte und Nutzungsrealitäten anzupassen. Die grenzübergreifende Problematik der Digital-Confidence-Bedrohungen erfordert vor allem eine enge internationale (legislative) Zusammenarbeit, ein stärkeres Bewusstsein für die Dringlichkeit des Handlungsbedarfs und die Bereithaltung entsprechender Ressourcen zur Schaffung von Abwehrstrukturen und Public-private-Partnerships durch Regierungen und zuständigen Behörden. In der Politik und im Bereich Regulierung scheint der Trend weg von einseitiger Gesetzgebung hin zu mehr Stakeholder-Beteiligung und Koregulierung zu gehen – übrigens nicht nur in Europa, sondern aufgrund des Drucks der FCC inzwischen auch in den USA. Dies erfordert jedoch gleichzeitig eine kontinuierliche Überprüfung der Angemessenheit aller Regulierungsaktivitäten, ganz besonders jedoch der stark interventionistischen Praktiken (wie der „Three Strikes“-Regel oder Bestrebungen, eine obligatorische Netz-Filterung durchzusetzen), die grundlegende Internet-Freiheiten und Verbraucherrechte (z. B. Datenschutz) einschränken und angestammte Rechtsverbindlichkeiten der Industrie unterminieren.

Regulierer müssen nicht nur die Rollen der Netzbetreiber und ISPs kennen, sondern auch die Auswirkungen einer Regulierung auf diese Rollen.

In anderen Fällen, wie etwa der Durchsetzung strenger QoS-Anforderungen, könnte eine eingreifende Regulierung unbeabsichtigte Folgen für die Industrie haben, zum Beispiel einen deutlichen Anstieg der Kosten für Netz-Upgrades, die letztlich auf die Konsumenten weitergewälzt werden würden. Daher sollten Regulierer insbesondere die Verflechtungen zwischen den einzelnen Digital-Confidence-Bereichen und deren Bedeutung für die verschiedenen Stakeholder berücksichtigen und entsprechend ausgewogene Entscheidungen fällen.

Bei der Sicherung von Digital Confidence spielen die Regulierer zweifellos eine entscheidende Rolle. Angesichts der hohen Komplexität der Digital-Confidence-Problematik könnten die

Regulierer durch die Förderung der Zusammenarbeit aller beteiligten Parteien einen wichtigen Beitrag leisten. Die Analysen dieser Studie zeigen, dass folgende Bereiche die besondere Aufmerksamkeit der Regulierer erfordern:

Die Umsetzung von Regeln ohne Berücksichtigung sämtlicher Folgen kann hohe Umsatzverluste für alle Stakeholder bedeuten.

- Anregung der Netzbetreiber und ISPs zur Ausgestaltung von Digital-Confidence-Leitlinien und -Prozeduren sowie Verhaltenskodex-basierter Selbstkontrolle auf Seiten der Industrie, insbesondere in Bereichen, in denen eine stärker eingreifende Regulierung (z. B. zum Traffic-Management) negative wirtschaftliche Auswirkungen haben oder Verbraucherrechte bedrohen würde (z. B. „Three Strikes“ oder „Beim 3. Mal bist du draußen“-Regel).

- Erwägung von Maßnahmen zur Begrenzung des rechtlichen und (in einigen Fällen) Image-Risikos, das Netzbetreiber und ISPs mit der Einführung von Digital-Confidence-Strategien und -Maßnahmen eingehen – etwa durch Vorantreiben der Entwicklung und branchenweiten Einführung eines Registers verbotener Seiten zum Schutz Minderjähriger oder durch Harmonisierung der momentan noch verstreuten europäischen Ansätze zu einer international koordinierten Vorgehensweise beim Minderjährigenschutz.

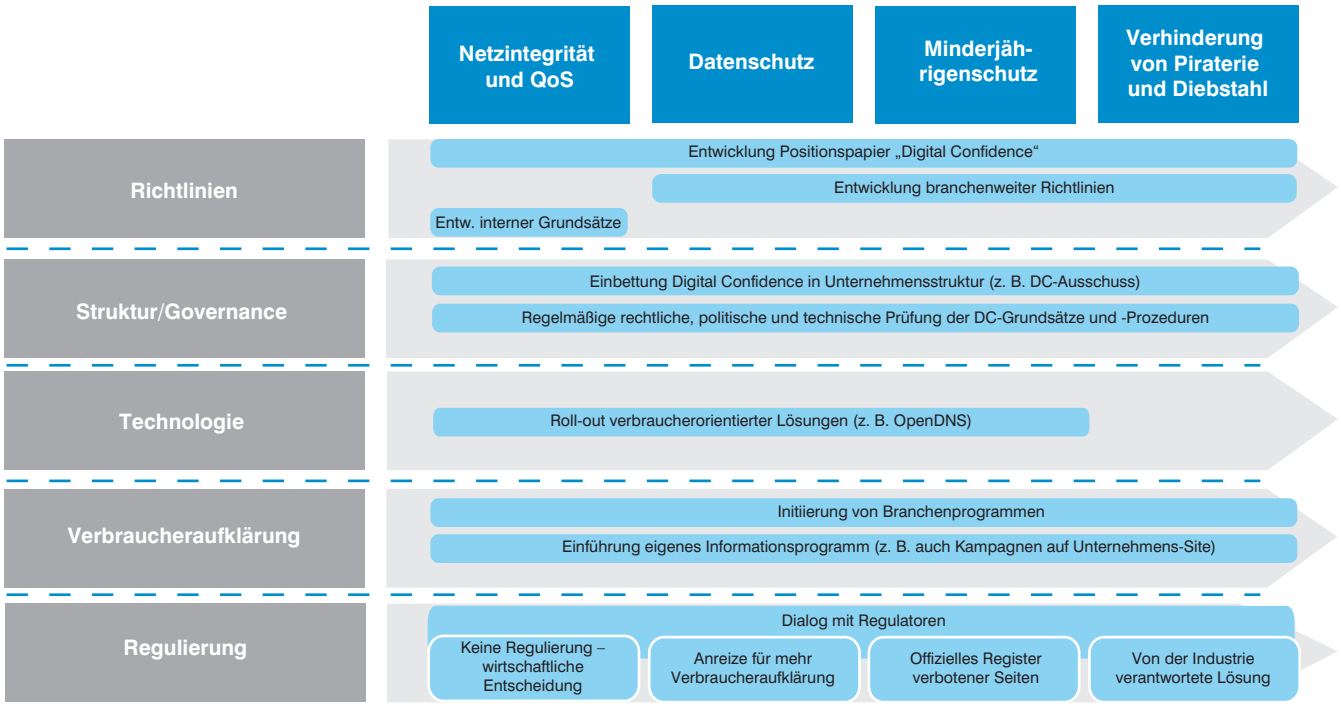
- Schaffung von Anreizen für die Branche, sich aktiver um die Aufklärung der Verbraucher zu bemühen, zum Beispiel durch die Bereitstellung finanzieller Mittel und Gründung von Dachinitiativen, die Skaleneffekte ermöglichen, etwa auf Basis der beim Safer Internet Programme gemachten Erfahrungen.

- Verstärkung der Bemühungen um internationale Zusammenarbeit bei der Entwicklung globaler Lösungen oder Lösungsrahmen für originär globale Probleme, z. B. beim Copyright-Schutz.

Als Fazit lässt sich sagen: Die erfolgreiche Umsetzung von Digital Confidence bedeutet nicht unbedingt einen hohen Investitionsaufwand. Ein Scheitern würde die Branche jedoch teuer zu stehen kommen. Natürlich ist die erfolgreiche Umsetzung von Digital-Confidence-Programmen keine leichte Aufgabe und durchaus mit Kosten verbunden. Zahlreiche CEOs werden zu Recht der Ansicht sein, dass ihre Unternehmen schon längst viele der oben vorgeschlagenen Maßnahmen ergriffen haben. Doch in den meisten Fällen wird dieses Engagement nicht ausreichen. Bei Digital Confidence geht es um mehr, als Informationsmaterial zum Download bereitzuhalten. Es geht darum, mit den führenden Institutionen in diesem Bereich – private und öffentliche – auf Top-Management-Ebene in Dialog zu treten, um klare und aufmerksamkeitsstarke Kampagnen zu initiieren. Dazu müssen Investitionen getätigt und möglicherweise ganz neue Fähigkeiten in den Unternehmen entwickelt und verankert werden. Digitales Vertrauen entsteht nicht allein dadurch, umfangreiche Datenschutzerklärungen vorzuhalten. Es entsteht durch ein gewandeltes Bewusstsein, wie Unternehmen mit dem Thema umgehen und wie es intern, aber auch gegenüber Kunden und der Gesellschaft kommuniziert wird. Kurz: Digital Confidence braucht Führung von oben, um auf breiter Front erfolgreich zu sein.

Die enorme Bedeutung der Problematik steht außer Frage. Die Bewältigung dieser komplexen Herausforderung wird noch sehr viel Zeit beanspruchen und keiner der involvierten Stakeholder wird in der Lage sein, die Probleme ganz allein zu lösen. Digital Confidence muss von der gesamten Branche getragen werden und erfordert eine aktive Beteiligung der wichtigsten Stakeholder auf der Grundlage eines gemeinsamen Handlungs- und Aktionsrahmens mit klar verteilten Rollen und Verantwortlichkeiten. Nur so kann digitales Vertrauen wirklich gewährleistet werden und für alle Akteure in der digitalen Welt einen echten Mehrwert schaffen.

Abb. 62: *Prioritäten in den einzelnen Handlungsfeldern*



Hinweis: DC = Digital Confidence

DIE AUTOREN DER STUDIE

Thomas Künstner
Vice President
thomas.kuenstner@booz.com
+49 211 3890 143

Michael Fischer
Principal
michael.fischer@booz.com
+49 211 3890 168

John Ward
Senior Associate
john.ward@booz.com
+44 20 7393 3782

Martin F. Brunner
Senior Associate
martin.brunner@booz.com
+49 30 88705 842

Florian Pötscher
Senior Consultant
florian.poetscher@booz.com
+43 1 51822 900

BOOZ & COMPANY WORLDWIDE OFFICES

Asia

Beijing
Hong Kong
Seoul
Shanghai
Taipei
Tokyo

Australia, New Zealand, and Southeast Asia

Adelaide
Auckland
Bangkok
Brisbane
Canberra
Jakarta
Kuala Lumpur
Melbourne
Sydney

Europe

Amsterdam
Berlin
Copenhagen
Dublin
Düsseldorf
Frankfurt
Helsinki
London
Madrid
Milan
Moscow
Munich
Oslo
Paris
Rome
Stockholm
Stuttgart
Vienna
Warsaw
Zurich

Middle East

Abu Dhabi
Beirut
Cairo
Dubai
Riyadh

North America

Atlanta
Chicago
Cleveland
Dallas
Detroit
Florham Park
Houston
Los Angeles
McLean
Mexico City
New York City
Parsippany
San Francisco

South America

Buenos Aires
Rio de Janeiro
Santiago
São Paulo

09/08 Printed in Germany