IM BLICKPUNKT:
Internetkriminalität

Fast vier Millionen Deutsche sind schon einmal Opfer von Computer- oder Internetkriminalität geworden. Sieben Prozent aller Computernutzer ab 14 Jahren haben bereits einen finanziellen Schaden beispielsweise durch Viren, bei Online-Auktionen oder durch Datenmissbrauch beim Onlinebanking erlitten. Für die meisten Nutzerinnen und Nutzer gehört Sicherheitssoftware immer noch nicht zum Standard, so die Ergebnisse einer Studie im Auftrag des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) vom Juni 2008.

So wie Computer und Internet unseren Alltag durchdringen, so werden sie auch zum Medium für kriminelles Handeln. Die moderne Informationsgesellschaft bietet enorme Chancen, birgt aber auch Gefahren. Medienkompetente User wissen, wie sie sich dagegen schützen können.

IM BLICKPUNKT: Internetkriminalität beschreibt Erscheinungsformen und Aufkommen der Internetkriminalität, nennt Anlaufstellen, Informationsmöglichkeiten und Reaktionsmaßnahmen.

Staatskanzlei
des Landes Nordrhein-Westfalen

Was ist Internet-kriminalität?

Es mehren sich die Delikte rund um Computer und Internet. Ihr Spektrum ist groß und reicht von der unlauteren Werbung, Betrugsdelikten beim Anbieten von Waren und Dienstleistungen, Kreditkartenbetrug, dem illegalen Verkauf von Waffen, Medikamenten und Betäubungsmitteln über das Internet, Urheberrechtsverletzungen, der Verbreitung von illegaler Pornografie und extremistischer Propaganda bis hin zum Identitätsdiebstahl. Daneben finden ‚Einbrüche' auch in Computer und Datennetze statt. Das Ausspähen, Verändern oder Löschen von Daten ist oftmals die Folge.

Computer- und Internetkriminalität statistisch
Zur Einschätzung der Bedrohung durch Internetkriminalität lohnt ein Blick in den Bericht zur „Kriminalitätsentwicklung im Land Nordrhein-Westfalen Jahr 2007" (auch wenn dort eine andere Systematik der Datenerhebung angewendet, Computer- und Internetkriminalität getrennt ausgewiesen werden). Er wird alljährlich vom Landeskriminalamt herausgegeben.

Hintergrundinformation

Computerkriminalität und Internetkriminalität

Computerkriminalität umfasst Straftaten, für deren Ausführung ein Computer verwendet wird, beispielsweise also das Umgehen bzw. „Knacken" eines Kopierschutzes auf einer DVD mithilfe des Computers, um diese zu kopieren und eventuell weiterzuverkaufen.

Internetkriminalität umfasst Straftaten, die das Internet als Medium nutzen, um ‚klassische' Straftaten zu begehen, oder bei denen spezifische Internettechnologien für die Verübung von Straftaten genutzt werden. Beispiele für solche Straftaten sind der Missbrauch von Kontodaten, um illegal Geld von fremden Konten abzubuchen oder das Verkaufen von nichtexistenten Waren über fremde Accounts (z. B. eBay) in der Absicht, die potenziellen Käufer zu betrügen. Juristisch handelt es sich um unterschiedliche Tatbestände, praktisch jedoch sind die Übergänge fließend. Sie sind oftmals kaum voneinander abzugrenzen.

Die polizeiliche Kriminalstatistik (PKS) listet als Straftatbestände zur „**Computerkriminalität im engeren Sinne**" auf:

Delikt	Bekannt gewordene Fälle		Zu- bzw. Abnahme	
	2007	2006	absolut	in %
Computerbetrug	4 265	4 595	- 330	- 7,2
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	1 073	664	+ 409	+ 61,6
Datenveränderung / Computersabotage	977	576	+ 401	+ 69,6
Ausspähen von Daten	1 377	888	+ 489	+ 55,1
Betrug mittels rechtswidrig erlangter Debitkarten mit PIN (Geldausgabeautomaten)	6 145	6 928	- 783	- 11,3
Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	525	491	+ 34	+ 6,9
Softwarepiraterie (private Anwendung)	905	438	+ 467	+ 106,6
Softwarepiraterie (gewerbsmäßiges Handeln)	200	488	- 288	- 59,0
Computerkriminalität (insgesamt)	**15 467**	**15 068**	**+ 399**	**+ 2,7**

Die „**Computerkriminalität im weiteren Sinne**", insbesondere durch Nutzung von DV-Geräten und -Anwendungen, kann dieser Statistik nicht entnommen werden. Gleichwohl lässt sich sagen: Selbst wenn die Zahl der Delikte im Bereich der Computerkriminalität insgesamt leicht angestiegen ist, ist die Bedrohung immer noch gering. Die (manchmal von den Medien vermittelte) Bedrohungslage sollte nicht überschätzt werden, auch wenn Vorsicht angebracht ist.

Die Sonderkennung „Tatmittel Internet" wird in den Fällen angewandt, in denen das Medium Internet als Tatmittel verwendet wird. In der Regel sind das Betrugs- oder sogenannte Äußerungs- bzw. Verbreitungsdelikte. Hier wurden insgesamt 56.432 Straftaten erfasst, das sind 3,8 % der Gesamtkriminalität (2006: 60.501 Straftaten mit einem Anteil an der Gesamtkriminalität von 4,1 %). In 74,5 % der Fälle handelte es sich hierbei um Betrugsdelikte, in 10,7 % um Urheberrechtsverletzungen und in 5,4 % um Sexualdelikte (2006: 83,3 % Betrugsfälle, 7,2 % Straftaten gegen Urheberrechtsverletzungen, 2,9 % Sexualdelikte). Die Aufklärungsquote betrug 84,0 % (2006: 85,9 %).

Links

- Bericht zur Kriminalitätsentwicklung im Land Nordrhein-Westfalen für das Jahr 2007 (PKS):
  www1.polizei-nrw.de/lka/stepone/data/downloads/08/01/00/kriminalitaetsentwicklung_pks_nrw_2007.pdf
- Umfrage des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM):
  http://bitkom.org/de/presse/8477_53100.aspx

Klassische Gefahren auf neuen Wegen?

Wird das Internet bei der Verübung von Straftaten als Medium eingesetzt, kann man von klassischen Gefahren sprechen, auch wenn die Verbreitungsform manchmal den Umstand vergessen lässt, dass es sich hier um einen klassischen Straftatbestand „auf neuen Wegen“ handelt. Dazu zählen etwa die Verbreitung illegaler Inhalte, Betrug, Beleidigungen, Erpressungen, Fälschungen und Urheberrechtsverletzungen. Einige Bespiele sollen hier herausgegriffen werden, um hinter die oben genannten Zahlen zu blicken und sie inhaltlich durch aktuelle Phänomene zu illustrieren.

Illegale Netzinhalte

Für bestimmte Inhalte gilt ein absolutes Verbreitungsverbot. Handelt es sich um „Harte Pornographie“ (Gewalt-, Sodomie-, Kinderpornographie) nach §184 Abs. 3 StGB, „Volksverhetzung“ nach §130 StGB, oder „Gewaltverherrlichung und Aufstachelung zum Rassenhass“ nach §131 StGB, wird die Verbreitung strafrechtlich verfolgt.

Das bedeutet nicht, dass entsprechende Inhalte nicht über das Internet verbreitet werden. Sachdienliche Hinweise nimmt jede Polizeidienststelle entgegen. Problematisch ist hierbei auch die Vielzahl der Randfälle, wie etwa das Angebot an deutschsprachiger, rechtsextremer Propaganda im Internet. Unser aller Unterstützung ist hier gefragt.

Cyberbullying

Und wie verhält es sich mit den eher persönlichen Formen, mit Beleidigungen in Foren, Chats oder Gästebüchern? Teilweise hat sich hierfür auch der Begriff des Cyberbullying oder auch Flaming eingebürgert. Das Internet ist kein rechtsfreier Raum. Eine im Internet nachlesbare Beleidigung verletzt die gesetzlich garantierten Persönlichkeitsrechte ebenso wie eine verbal geäußerte Beleidigung und ist daher verboten. Datenschutzrechte sowie das Recht auf Schutz der eigenen Person werden grundsätzlich höher bewertet als das Recht auf freie Meinungsäußerung, woraus gegebenenfalls resultiert, dass die Löschung von Blog- oder Foreneinträgen notwendig wird.

Der rechtliche Schutz vor Verleumdungen bedeutet umgekehrt: Achtung bei emotionalen Reaktionen, insbesondere im Fall der Namensnennung. Schnell rutscht einem eine unbedachte Äußerung „über die Tastatur“ und ist mit Blick auf die dynamische Verbreitung im Web über Jahre hinweg recherchierbar. Wird hierbei eine Straftat unterstellt, hat man den Straftatbestand der „üblen Nachrede und Verleumdung“ gemäß § 186 und 187 des Strafgesetzbuches erfüllt. Dann droht eine Anzeige.

Achtung auch bei vermeintlich lustigen Fotos von privaten Anlässen, die als beleidigend eingestuft oder für den oder die Abgebildete(n) peinlich sein könnten. Nach § 22 des Kunsturhebergesetzes gilt: Bildnisse dürfen nur „mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden“. Das ungefragte Fotografieren einer Person stellt bereits einen Eingriff in das allgemeine Persönlichkeitsrecht dar. Wer ein solches Foto in einer Online-Foto-Community veröffentlicht, sollte sich absichern – oder von einer Veröffentlichung absehen.

Urheberrechtsverletzungen

Fotos und Filmausschnitte sind im Internet leicht zugänglich und werden daher gerne zu Illustrationszwecken genutzt. Urheberrechtsverletzungen sind daher fast an der Tagesordnung, denn Fotos und Filmausschnitte sind nahezu ohne Ausnahme urheberrechtlich geschützt, auch wenn die Nutzung kaum zu kontrollieren ist. Zudem gilt hier das Lichtbildschutzrecht, das vergleichsweise geringe Anforderungen an die

kreative Eigenleistung des Fotografen bzw. der Fotografin stellt.

Mittlerweile ist das „Zweite Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft“ in Kraft getreten - der sogenannte „Zweite Korb“. Das Umgehen technischer Schutzmaßnahmen ist demnach kein Kavaliersdelikt, sondern gesetzlich verboten. Gemeint sind Maßnahmen wie zum Beispiel digitale Wasserzeichen oder Kopierschutzvorrichtungen in beziehungsweise auf CDs, DVDs, Audio- und Videodateien sowie Bild- und Textdateien. Hinsichtlich der Musik- und Filmtauschbörsen im Internet gilt: Das Bereitstellen urheberrechtlich geschützter Werke (Musiktitel, Filme etc.) per Upload ist und bleibt illegal, sofern man nicht selbst der Rechteinhaber ist oder es sich um freie Inhalte handelt. Die Urheberrechtsnovelle unterstreicht zudem: Eine Privatkopie ist auch dann illegal, wenn die Vorlage rechtswidrig im Internet zum Download angeboten wurde, was für den Außenstehenden nicht so einfach zu durchschauen ist. Auch das Herunterladen aus einer illegalen Tauschbörse ist rechtswidrig und kann ebenso wie der Upload straf- und zivilrechtliche Sanktionen zur Folge haben. Selbst Links auf illegale Downloadangebote sind verboten.

Identitätsdiebstahl und (kein) Betrug

Häufig findet ein sogenannter Identitätsdiebstahl statt, um klassischen Betrug zu begehen. So ermitteln Betrüger beispielsweise die Kennwörter von Mitgliedern in Online-Auktionshäusern, etwa durch das Phishing oder das Ausspähen der Zugangsdaten. Sie bieten dann unter falschem Namen Waren an, über die sie gar nicht verfügen. Der Käufer überweist den Kaufbetrag, ohne im Anschluss eine Ware zu erhalten. Wenn der Betrug bemerkt wird, ist der „falsche“ Verkäufer dann häufig nicht mehr zu ermitteln, das Geld verschwunden; den Schaden müssen der Käufer und manchmal derjenige tragen, dessen Account ohne sein Wissen verwendet wurde.

Kein Betrug, sondern eher „randlegal“, sind die Methoden der „Online-Abzocker“, auch wenn die Betroffenen sich betrogen fühlen: Geworben wird mit Dienstleistungen, etwa Hausaufgabenhilfen, Persönlichkeitstest, IQ-Test, Berufswahlberatungen, kostenlosen SMS oder ähnlichen Angebote – häufig in Kombination mit Gratisgeschenken und Gewinnspielen. Man füllt ein Online-Formular mit seinen Daten aus, schickt es ab und hat – ohne es zu wollen – damit einer kostenpflichtigen Dienstleistung zugestimmt. Manchmal reicht dazu auch schon ein falscher Klick. Da hilft nur noch, von seinem Widerrufsrecht Gebrauch zu machen und sich eventuell an die Verbraucherzentrale zu wenden.

Problematisch ist auch der illegale Handel mit Konto- und Adressdaten: Wessen Kontoverbindung im Umlauf ist, der hatte vielleicht schon einmal mit widerrechtlichen Abbuchungen von seinem Bankkonto zu tun. Denn jeder, der im Besitz der Kontodaten ist, kann prinzipiell ohne Einzugsermächtigung Geld vom Konto abbuchen lassen.

Links

- Die Möglichkeit, online eine Anzeige zu erstatten: **https://service.polizei.nrw.de/egovernment/service/anzeige.html**
- jugendschutz.net überprüft Netzinhalte und kümmert sich um die Einhaltung des Jugendschutzes im Auftrag der Länder. Hinweise auf Verstöße werden online entgegen genommen: **www.jugendschutz.net/hotline/index.html**
- Die Handreichung „mekonet kompakt: Rechtsfragen in der digitalen Welt auf einen Blick“ erläutert, welche Bilder, Töne und Texte rechtlich geschützt sind und wann das Agieren im Netz Persönlichkeits- oder Urheberrechte verletzt. Die Broschüre gibt Tipps und benennt Anlaufstellen, die weiterführende Informationen bereithalten: **www.mekonet.de/doku/mnkompakt/mn_kompakt_recht.pdf**
- Das geballte Wissen der iRights.info-Website zum Urheberrecht in der digitalen Welt gibt es auch als Buch: „Urheberrecht im Alltag“ wurde in Zusammenarbeit mit der Bundeszentrale für Politische Bildung herausgegeben. Es ist als kostenloses Download-Angebot verfügbar: **www.irights.info/index.php?id=615**
- Die Verbraucherzentrale Nordrhein-Westfalen: **www.vz-nrw.de/UNIQ121819076915981/link270A.html**

Internetspezifische Gefahren

Dass Straftaten begangen werden, indem man unter falscher Identität agiert, ist nicht neu, nimmt mit Blick auf das Internet aber neue internetspezifische Formen an. Hier fällt die Grenzziehung schwer. Bei der Beurteilung der Internetkriminalität ist dies zu berücksichtigen. Gefahren entstehen durch die Anfälligkeit von Datennetzen, aber auch durch die Einbruchsmöglichkeiten in die „digitalen Privatsphären". Einige der wichtigsten internetspezifischen Gefahren:

- **Bots**: Unbefugte übernehmen mittels eingeschleuster Programme die Kontrolle über Rechner und machen sie zu (Ro)„Bots" oder „Zombies". Fortan verschicken die fremdgesteuerten PCs unbemerkt Werbe-E-Mails (Spam) oder attackieren andere Rechner so lange mit sinnlosen Anfragen, bis diese ihren Dienst versagen (Denial of Service-Attacke). Um die Intensität dieser Attacken zu steigern, werden die fremdgesteuerten PCs teils zu sogenannten Bot-Netzen verknüpft, die enorme Größen annehmen können.
- **Malware**: Schadhafte „Malware" sind Viren, Würmer und Trojaner. Viren verändern und löschen Programme und Dateien oder machen diese unbrauchbar. Sie „nisten" sich per E-Mail, beim Tausch von Datenträgern oder beim Herunterladen aus dem Internet ein. Würmer brauchen im Gegensatz zu Viren keinen „Wirt". Sie „klonen" sich selbst und verbreiten sich dann per E-Mail im Anhang weiter, etwa nach der Anmeldung in einem „infizierten" Online-Netzwerk. Würmer werden aber nur dann aktiv, wenn man sie herunterlädt oder anklickt. Trojaner „schleichen" sich unerkannt (als Teil eines vermeintlich nützlichen Programms) ein und treiben dann ihr Unwesen. Am gefährlichsten sind hier die „Backdoor-Trojaner", welche die totale Kontrolle des Computers von außen ermöglichen (s.o.). Dann hilft nur noch, ganz vom Netz zu gehen. Allerdings können sich Trojaner nicht selbstständig verbreiten.
- **Pharming**: Beim Pharming geht es um die Ausspähung von vertraulichen Daten, allerdings wird vom Opfer keine bewusste Mitwirkung an der Datenermittlung benötigt. Der Angriff erfolgt durch eine Manipulation des Systems, welches das Opfer zur Benutzung des Internets gebraucht, etwa indem Webseiten-Adressen einer Bankenwebseite gefälscht werden. Der ahnungslose Nutzer wird auf eine Seite umgeleitet, die der bekannten Bankwebseite täuschend ähnelt, gibt seine private PIN/TAN-Kombination auf „seiner" Bankenwebseite ein und damit in die Hände Dritter. Abbuchungen sind die Folge.
- **Phishing**: Gemeint sind alle Verfahren, bei denen versucht wird, mit Hilfe gefälschter E-Mails vertrauliche Zugangs- und Identifikationsdaten argloser Dritter auszuspähen. Mit diesen Daten wird dann – unter der Identität des Inhabers – im Online-Verkehr gehandelt. Waren werden angeboten und abkassiert, PIN/TAN-Kombinationen ermittelt und dazu genutzt, Transaktionen durchzuführen und noch anderes mehr.
- **Spyware**: Eine besondere Malware ist Spyware, die ebenfalls der Ausspähung von Daten dient. Spyware nennt man auf dem PC eingeschleuste kleine Programme, die gespeicherte Informationen und/oder das Surfverhalten des Nutzers ausspionieren und diese Daten unbemerkt weiter geben.
- **WLAN-Hacking**: Sogenannte „Wardriver" fahren mit dem Laptop auf dem Beifahrersitz durch die Straßen und suchen nach ungesicherten WLAN-Netzen, um Spam zu versenden oder illegale Tauschbörsen zu besuchen, um hier Musik oder Filme herunterzuladen. Einem Urteil des Oberlandesgerichts Düsseldorf zufolge haftet bei Missbrauch der- oder diejenige, die oder der sein privates Funknetzwerk nicht ausreichend absichert. Wer sein Funknetzwerk ausreichend verschlüsselt, ist auf der sicheren Seite und folgt der Sorgfaltspflicht beim Betrieb von lokalen Funknetzwerken.

Gefahrenabwehr und Schutzmaßnahmen

Was tun in Anbetracht von Betrügern, Kriminellen, schadhafter Software und Ausspähungsversuchen? Den Rechner vom Netz trennen? Überlegungen wie diese sind weitgehend unpraktikabel, auch wenn sie in Ausnahmen ergriffen werden.

Einige Verhaltensmaßregeln sind bei den internetspezifischen Gefahren bereits (implizit) angeklungen und sollen hier ergänzt werden – auch durch Empfehlungen zu technische Schutzmaßnahmen.

Verhaltensregeln

- Jede Verwendung fremder Bilder bedarf der Einwilligung des Rechteinhabers, die am besten schriftlich erfolgen sollte. Bei Bildern aus (kommerziellen) Fotobörsen ist das (erworbene) Nutzungsrecht zu beachten. Oftmals bleibt unbemerkt, dass sich der Umfang der erworbenen Lizenz zum Beispiel auf eine geringe Bildauflösung oder auch den ausschließlichen Gebrauch für Webseiten beschränkt.
- Medienkompetente User wissen um Datenschutz- und Urheberrechte und informieren sich über Neuerungen regelmäßig. Gehen Sie vorsichtig mit Ihrer Identität im Netz um und überlegen sorgfältig die Herausgabe persönlicher Daten im Sinne der Datensparsamkeit.
- Kontoauszüge sowie die Kreditkartenabrechnung sollten regelmäßig auf unberechtigte Abbuchungen überprüft werden. Mit dem Widerspruch bei der Bank informiert man am besten zugleich die Verbraucherzentrale und die Datenschutzbehörde.
- Speichern sie Passwörter möglichst nicht auf Ihrem PC und erneuern Sie sie in regelmäßigen Abständen. Achtung: Vornamen oder der Name eines Familienangehörigen sind für Kriminelle leicht nachzuvollziehen, ihre Verwendung daher ungeeignet.
- Informieren Sie sich regelmäßig über Entwicklungen im Bereich Soft- oder Hardware und vermeiden Sie, zweifelhafte Seiten anzusurfen, auch wenn das in der Praxis nicht immer einfach ist.

Links

- Microsoft hat gemeinsam mit der Universität München eine Webplattform namens IRBI (Internet Risk Behaviour Index) gestartet, die es Nutzern erlaubt, ihr Verhalten gegenüber potenziellen Internetgefahren zu testen: **www.irbi.de**
- Die kostenlose Broschüre „Computerkriminalität: So hilft die Polizei" der Landesinitiative secure-it.nrw benennt die wesentlichen Verhaltensregeln im Umgang mit dem eigenen Computer und zeigt, wie die Polizei im Schadensfall helfen kann: **www.secure-it.nrw.de/material/polizei.php**
- Die Arbeitsgruppe Identitätsschutz im Internet e.V. (a-i3) ist eine unabhängige, interdisziplinäre Organisation, die sich den Identitätsschutz im Internet zur Aufgabe gemacht hat. Sie wurde im Mai 2005 von Forschern der Ruhr-Universität Bochum sowie Praktikern aus dem Bereich der IT-Sicherheit gegründet und bietet unter anderem ein Servicetelefon sowie Warnungen vor aktuellen Phishing-E-Mails an: **https://www.a-i3.org/**

- Laden Sie keine Programme von Ihnen unbekannten Servern oder Seiten herunter und öffnen Sie keine Dateianhänge in unbekannten E-Mails. Programme wie Viren, Würmer und Trojaner gelangen entweder durch das unabsichtliche Herunterladen und Installieren von Software aus dem Internet oder durch das Öffnen verseuchter E-Mail-Dateianhänge auf den heimischen PC.
- Legen Sie für Newsgroups oder die Benutzung von Chatrooms weitere E-Mail-Adressen an. Das hilft auch, unerwünschte Spam-E-Mails zu kanalisieren.
- Sorgen Sie für den Notfall vor; erstellen Sie Backups und verwahren Sie die Originalsoftware und Key-Codes.

Technische Schutzmaßnahmen

- Die technischen Schutzmaßnahmen beginnen mit der Aktualität der verwendeten Software. Um Systemlücken zu schließen, bedarf es regelmäßiger Updates. Aber Achtung: Halten Sie Ihre Programme nur so aktuell wie nötig, nicht wie möglich. Nicht jedes Update ist automatisch besser als die vorherige Version und beseitigt jeden Mangel.
- Fast ebenso wichtig ist die passende Browsereinstellung. Dabei gibt es generell kein „richtig" und kein „falsch". Sie müssen bei der Wahl des Sicherheitsniveaus einen Kompromiss zwischen Funktionalität und Sicherheit finden.
- Der Einsatz von Antiviren-Software ist unerlässlich. Auch sie muss regelmäßig aktualisiert werden, sonst ist sie wirkungslos.
- Die Überwachung und Steuerung des Datenflusses in und aus dem Computer ist die Aufgabe von Firewalls (dt. „Brandschutzmauern"). Sie „stellen" sich zwischen den Computer und das Internet, überwachen den Datenverkehr und sind daher unbedingt zu empfehlen. Aber Achtung: Ihr Schutzumfang ist beschränkt und sollte komplettiert werden durch Firewalls in der Hardware, etwa im Router des WLAN-Zugangs. Wenn man sich bei der Konfiguration unsicher ist, sollte man einen Experten hinzuziehen.

Ausblick

Das Ansteigen der Internetkriminalität ist keineswegs eine ausgemachte Sache. Unser medienkompetentes Verhalten und technische Schutzmaßnahmen müssen ineinander greifen, dann ist das Surfen sicherer. Und die Gefahr sinkt, Opfer der Internetkriminalität zu werden, auch wenn es einen hundertprozentigen Schutz nicht geben kann. Die virtuelle Welt ist ein Abbild der realen Welt – im Guten, wie im Schlechten.

Impressum

Diese Broschüre ist mit Mitteln der Staatskanzlei Nordrhein-Westfalen entstanden. Sie kann kostenlos unter **www.media.nrw.de/medienkompetenz/imblickpunkt** heruntergeladen werden.

Redaktion:
ecmc Europäisches Zentrum für Medienkompetenz GmbH
Bergstr. 8 · 45770 Marl
Tel.: +49 (0)2365 9404-0 · Fax: +49 (0)2365 9404-29
E-Mail: info@ecmc.de · Internet: www.ecmc.de

Bildquellen:
streichholz / photocase.com (S. 1 u. 2), DMG07 / photocase.com (S. 1 u. 3), Tube / photocase.com (S. 1 u. 4)

Stand: November 2008