



Ein Projekt im Rahmen
des Aktionsplans
„Gut leben im Alter“
der Landesregierung.



verbraucherzentrale

Rheinland-Pfalz

Silver Surfer –

SICHER ONLINE IM ALTER
Mobiles Internet & Smart-Technologien

weitere Kooperationspartner:



Wie man diese Broschüre benutzt

Die Broschüre „Silver Surfer – Mobiles Internet & Smart-Technologien“ dient als Lernbegleitmaterial zur Seminarreihe „Silver Surfer – Sicher online im Alter“. Die Module in dieser Broschüre entsprechen den Inhalten der Schulungen. Darüber hinaus bietet das Werk viele Informationen rund um das Thema Internet. Es soll gleichzeitig als Nachschlagemöglichkeit dienen. Begriffe, die mit einem Pfeil ➔ markiert sind, werden am Ende der Broschüre in einem Glossar erneut aufgegriffen und näher erläutert.

In der Broschüre finden sich unterschiedliche Symbole:



Übung: Dieses Symbol weist auf Übungen hin, die zu dem entsprechenden Thema im Kurs behandelt werden.



Weiterführendes: Das entsprechende Thema wird an einer anderen Stelle der Broschüre erneut aufgegriffen und umfangreicher dargestellt.



Link: Auf der Internetseite www.silversurfer-rlp.de sind Links zu weiterführenden Informationen und anderen Internetquellen zu finden.



Lernbuch: Das Buchsymbol verweist auf umfangreiche Informationen im bereits erschienenen Lernbuch „Silver Surfer – Sicher online im Alter“. Mehr dazu finden Sie auf unserer Internetseite www.silversurfer-rlp.de.

Auf der Website www.silversurfer-rlp.de finden sich aktuelle Informationen, Seminartermine, Videos und weiterführende Links.

Alle Informationen der vorliegenden Broschüre haben wir nach bestem Wissen und Gewissen geprüft. Wir freuen uns stets über kritische Anmerkungen, die helfen, diese Broschüre noch besser zu machen. Sollte Ihnen etwas auffallen, zögern Sie nicht, uns zu kontaktieren: pressmar@mkn-online.de

Um einen für die Leserinnen und Leser besseren Textfluss zu erhalten, wird im folgenden Text auf die jeweils weibliche Form verzichtet. In diesem generischen Verständnis sind Frauen immer mit angesprochen.

Vorwort

Seit 2011 gibt es in Rheinland-Pfalz das Projekt „Silver Surfer – Sicher online im Alter“. In Kursen, Fortbildungen, Workshops und Tagungen im ganzen Land lernen Seniorinnen und Senioren seither, wie sie sich im Internet selbstbewusst und sicher bewegen können. Über 2.500 Menschen haben seither an den Veranstaltungen teilgenommen. Ein großer Erfolg, der uns anspornt, auch in Zukunft die Medienkompetenz älterer Menschen zu stärken.

Die neue Broschüre richtet den Blick auf zwei aktuelle Entwicklungen: das mobile Internet und Smart-Technologien. Smartphones, Tablets und Smart-TVs nehmen im Alltag von Menschen jeden Alters einen immer größeren Stellenwert ein. Wie ein roter Faden zieht sich dabei die Nutzung von Internetdiensten als verbindendes Element durch die Gerätschaften. Kleine Anwendungen, sogenannte Apps, machen Smart-Technologien äußerst flexibel und auf die Bedürfnisse von Nutzern individuell abstimmbare. Durch die Mobilisierung von Endgeräten mittels WLAN und Mobilfunk ist die Verfügbarkeit von Internetdiensten zunehmend entkoppelt von einem bestimmten Standort. All diese Entwicklungen bringen viele Veränderungen in den (Medien-)Alltag von Menschen. Denn der Wandel birgt viele Chancen, aber auch Risiken. Die neue Broschüre „Mobiles Internet und Smart-Technologien“ möchte über diese Themen aufklären. Die Entwicklung mobiler Technologien beginnt gerade erst. In Zukunft werden neue Anwendungen zu neuen Herausforderungen für Daten- und Verbraucherschutz führen. Dies stellt auch den Bildungsbereich vor neue Aufgaben. Die kontinuierliche Transformation der digitalen Welt zeigt, dass digitaler Verbraucherschutz und lebenslanges Lernen eine Daueraufgabe sind. Dies beweist auch das Ergebnis des 3. Verbraucherdialogs der Landesregierung zum Thema mobile Bezahlverfahren. Dort wurde deutlich, wie wichtig es ist, dass Politik, Wirtschaft und Verbraucherschutz bei Fragen der Sicherheit von Zahlungen und beim Datenschutz an einem Strang ziehen.



Renate Pepper



Ulrike von der Lühe

Ein großer Dank gebührt dem Silver-Surfer-Netzwerk. Ohne den engagierten Einsatz der Mitarbeiterinnen und Mitarbeitern des Medien-KompetenzNetzwerks Mainz-Rheinhessen und der Verbraucherzentrale Rheinland-Pfalz wäre das Projekt bislang nicht so erfolgreich verlaufen. Ohne die Mitwirkung des Verbands der Volkshochschulen von Rheinland-Pfalz hätten die Kurse nicht im ganzen Land stattfinden können. Danksagen möchten wir auch den Mitarbeiterinnen und Mitarbeitern des rheinland-pfälzischen Landesdatenschutzbeauftragten für ihre Unterstützung rund um das große Thema Datenschutz. Ein besonderer Dank gilt dem Ministerium der Justiz und für Verbraucherschutz Rheinland-Pfalz, durch dessen finanzielle Unterstützung das vorliegende Werk realisiert werden konnte.

Mainz, Mai 2014

Renate Pepper

Direktorin der Landeszentrale für Medien und Kommunikation (LMK)
Rheinland-Pfalz

Ulrike von der Lühe

Vorstand Verbraucherzentrale Rheinland-Pfalz

Inhaltsverzeichnis

MODUL 1

Das mobile Internet	5
1. Grundlegende Strukturen und Unterschiede von mobilen und heimischen Netzwerken	6
2. Internet über das Mobilfunknetz	7
3. Heimisches Netzwerk via DSL oder Kabel	11

MODUL 2

Was das mobile Internet mit sich bringt	15
1. Betriebssysteme und Apps	15
2. Cloud-Computing als Grundlage des mobilen Internets	17
3. Meine Daten und Datenschutzrechte im mobilen Internet	20
4. „Mobile Payment“ – einfacher bezahlen	25

MODUL 3

Blick in die Zukunft des Internets	29
1. Die Palette „smarter“ Endgeräte	29
2. Der gläserne Verbraucher – Herausforderung für den Verbraucherschutz	31
3. Big Data	35
4. Web 3.0 – das Netz wird intelligent	37

Glossar	41
----------------------	-----------

Stichwortverzeichnis	43
-----------------------------------	-----------

Autoren	44
----------------------	-----------

Silver Tipps – sicher online!

Im Sommer 2014 startet „Silver Tipps“, das unabhängige Serviceportal für ältere Onlinerinnen und Onliner. Gefördert von der Stiftung MedienKompetenz Forum Südwest bereitet hier die Initiative Medienintelligenz der Johannes Gutenberg-Universität Mainz die Themen Datenschutz, Internetsicherheit und Verbrauchertipps gemeinsam mit den Partnern SWR, den Verbraucherzentralen und dem MedienKompetenzNetzwerk Mainz-Rhein Hessen auf.



www.silver-tipps.de

Das mobile Internet

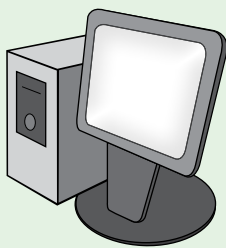
| FLORIAN PRESSMAR & JEANINE WEIN

MODUL
01

Egal ob unterwegs in Bus und Bahn, beim Wochenendausflug oder Bummel durch die Stadt – durch mobile Endgeräte wie Smartphones sind die Möglichkeiten des Internets heutzutage von überall aus nutzbar. Welche Besonderheiten das mobile Internet mit sich bringt, zeigt dieses Modul auf.

Lange Zeit hatte man nur vom heimischen Computer aus einen Zugang ins weltweite Datennetz – weil zu Hause der dafür erforderliche Telefonanschluss lag. Internet von unterwegs, zum Beispiel mit dem Handy, war zwar auch vor einigen Jahren schon möglich, wegen der damals hohen Entgelte war es aber unbezahlbar. Heute ist das ganz anders. Nach Angaben des IT-Branchenverbands BITKOM besitzen schon 40 Prozent aller Handynutzer ab 14 Jahren ein sogenanntes Smartphone, Tendenz steigend.

Desktop-PC



- stationär
- Internetnutzung via Heimnetzwerk möglich

Laptop



- klein & tragbar
- Internetnutzung via Heimnetzwerk möglich
- Internetnutzung unterwegs via Hotspot möglich


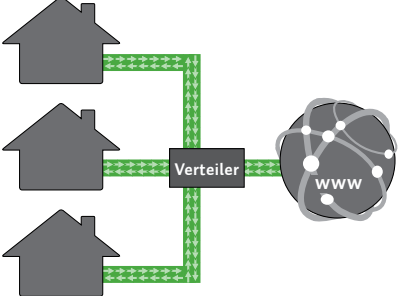
Smartphone/Tablet-PC



- zum Mitnehmen geeignet
- verschiedene Arten der Internetnutzung möglich
 - Heimnetzwerk
 - Hotspot
 - Mobilfunknetz (⇒ 3G-/4G-Modul nötig)

1. Grundlegende Strukturen und Unterschiede von mobilen und heimischen Netzwerken

Um das mobile Netz optimal nutzen zu können, sind ein paar grundlegende Unterscheidungen wichtig, zunächst die zwischen dem heimischen Netzwerk und dem Mobilfunknetz.

Mobiles Internet via Mobilfunknetz	Heimisches Netzwerk via DSL oder Kabel
	
<p>Eigenschaften:</p> <ul style="list-style-type: none"> • Vertrag mit Mobilfunkanbieter nötig • ⇒ Datenpakete werden über das Mobilfunknetz übertragen 	<p>Eigenschaften:</p> <ul style="list-style-type: none"> • Vertrag mit Telefonanbieter oder Kabelnetzbetreiber nötig • auch als sogenannter Hotspot (manchmal auch als WLAN oder ⇒ Wi-Fi bezeichnet) in Cafés, Restaurants etc. verfügbar (teilweise gegen Gebühr)
<p>Vorteile:</p> <ul style="list-style-type: none"> • ortsunabhängig das Internet nutzen • nützlich vor allem mit mobilen Endgeräten wie Smartphones und Tablets • spezielle Anwendungen wie Navigation möglich 	<p>Vorteile:</p> <ul style="list-style-type: none"> • schnelle Geschwindigkeiten • meist feste Flatrate-Tarife ohne ⇒ Drosselung der Geschwindigkeit • Verbindung mehrerer Geräte im Heimnetzwerk möglich
<p>Nachteile:</p> <ul style="list-style-type: none"> • kein flächendeckender Empfang, da an Mobilfunknetz gekoppelt • unterschiedliche Geschwindigkeiten je nach Technik, Anbieter und Region • häufig Volumentarife, die mit einer ⇒ Drosselung der Geschwindigkeit oder zusätzlichen Kosten verbunden sind 	<p>Nachteile:</p> <ul style="list-style-type: none"> • ortsgebunden

2. Internet über das Mobilfunknetz

Schon in den 1990er-Jahren konnte man mit Handys auf das Internet zugreifen – aber aufgrund der geringen Geschwindigkeit, des kleinen Handybildschirms und der immensen Kosten war das Surfen auf diesem Weg lange Zeit alles andere als ein Vergnügen. Vor allem zwei Entwicklungen waren nötig, um den Zugriff auf das Internet über das Mobilfunknetz massentauglich zu machen:


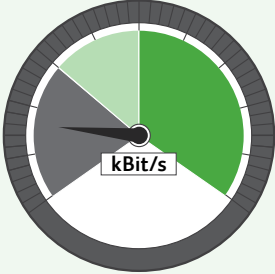

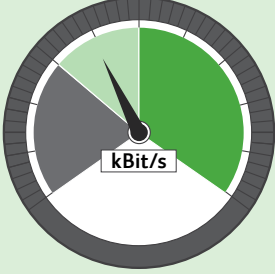

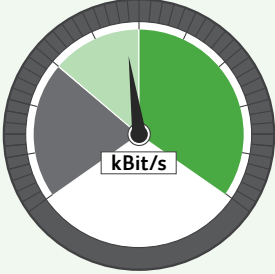

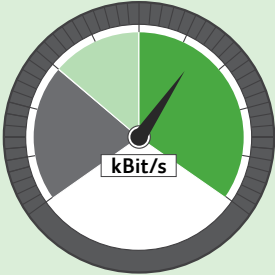

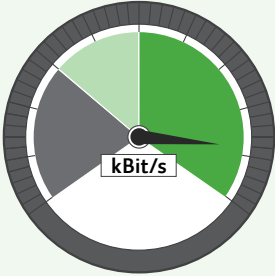
- 1) Mobilfunkbetreiber mussten ihre Mobilfunknetze auf neuere Standards umstellen, die größere Datenmengen und Übertragungsgeschwindigkeiten erlaubten, und die Flächenabdeckung verbessern.
- 2) Smartphones mit großen Bildschirmen und einfacher Bedienung über Berührung mussten entwickelt werden.

Aktuell setzen sich Smartphones und Tablets mit dazugehörigen mobilen Internetverbindungen verstärkt auf dem Markt durch. Es ist zu erwarten, dass auch aufgrund der stetig besser werdenden Mobilfunkverbindungen immer mehr dieser Geräte Einzug in die Haushalte der Menschen in Deutschland halten werden. Da jedoch der Stand des Netzausbaus je nach Anbieter und Region erheblich variiert, gibt es aktuell sehr unterschiedliche Geschwindigkeiten, mit denen man unterwegs mit Smartphone oder Tablet-PC surfen kann. Ein entsprechendes Kürzel ist im Display des Geräts zu sehen.

Jedes Kürzel steht für einen bestimmten Mobilfunkstandard und damit verbunden einer maximalen Datenübertragungsgeschwindigkeit. Hierbei gilt die Regel, dass neuere Standards schnellere Übertragungen von Daten im Mobilfunknetz ermöglichen. Aber welche Standards erlauben welche Geschwindigkeiten? Die wichtigsten sind in der folgenden Tabelle aufgelistet.



**ÜBERTRAGUNGS-
GESCHWINDIGKEITEN**

Standard/ Abkürzung	Erklärung	Geschwindigkeit
GPRS oder G 	<p>GPRS ist ein älterer Übertragungsstandard, der von allen aufgeführten Verbindungen die langsamste Datenübertragungsgeschwindigkeit zulässt. Extrem lange Ladezeiten für Internetinhalte sind die Folge. GPRS beruht auf dem ersten globalen und erstmals volldigitalen Mobilfunkstandard GSM. Im Vergleich zu früheren analogen Funknetzen werden diese Standards auch als 2. Generation, deshalb auch 2G, des Mobilfunks bezeichnet.</p>	
EDGE oder E 	<p>EDGE ist ein Mobilfunkstandard, der einen Zwischenschritt zwischen GPRS und UMTS darstellt. Im Wesentlichen wird bei EDGE das vorhandene GPRS-System genutzt und modifiziert, wodurch eine höhere Geschwindigkeit erreicht werden kann.</p>	
UMTS oder 3G 	<p>Der UMTS-Standard wird auch als 3. Generation des Mobilfunks und deshalb auch 3G bezeichnet. Er stellt einen Durchbruch in Sachen Datenübertragungsgeschwindigkeit mittels Mobilfunknetzen dar, so kann man beispielsweise mit UMTS auch Videos mobil anschauen.</p>	
HSDPA/ HSPA+ oder H/H+ 	<p>HSDPA und HSPA+ sind der Turbo für den UMTS-Übertragungsstandard und ermöglichen potenziell Geschwindigkeiten wie beim heimischen DSL. Sie stellen damit einen Zwischenschritt zwischen UMTS und LTE dar.</p>	
LTE 	<p>LTE ist die 4. Generation, auch 4G, der Mobilfunkstandards, die sehr große Datenübertragungsgeschwindigkeiten zulässt. So kann es auch als Ersatz zu einem heimischen Kabel- oder DSL-Anschluss infrage kommen – jedoch nur in den Regionen, in denen LTE bereits ausgebaut ist. Um LTE nutzen zu können, müssen mobile Endgeräte LTE-fähig sein.</p>	

Alle Übertragungsstandards sind Kinder ihrer Zeit. Das heißt, dass mit den Anforderungen des Nutzers auch die Datenübertragungswege breiter geworden sind. Heute sind die Übertragungsgeschwindigkeiten in der mobilen Datenübertragung vergleichsweise hoch. Dennoch erreichen Funknetzwerke in den seltensten Fällen ihre volle Geschwindigkeit. Enge Bebauung, Umwelteinflüsse oder hohe Abstände zu den Funkmasten können die Geschwindigkeit beeinträchtigen. Deshalb sind Nutzer von heimischen Anschlüssen via DSL oder Kabel in Sachen Geschwindigkeit und Preis nach wie vor klar im Vorteil.

Flatrates und Volumentarife

Dass das Internet über das Mobilfunknetz massentauglich geworden ist, hängt nicht zuletzt auch damit zusammen, dass Pauschaltarife, also Flatrates, für die Internetnutzung populärer geworden sind. Bei Flatrates bezahlt man seinem Mobilfunkanbieter meist monatlich einen festen Betrag, in dem das Versenden und Empfangen unbegrenzt vieler ➔ Datenpakete enthalten ist. Zusätzliche Kosten entstehen bei einer Flatrate in der Regel nicht. Doch bei Vertragsabschluss lohnt ein Blick ins Kleingedruckte. Oft ist da von einer Beschränkung oder Drosselung der Geschwindigkeit die Rede. Konkret bedeutet das: Ein bestimmtes Datenvolumen, also eine bestimmte Menge an Datenpaketen, wird mit der beworbenen hohen Geschwindigkeit übertragen. Ist dieses aufgebraucht, verringert sich die Geschwindigkeit meist erheblich. Dadurch verlängern sich beispielsweise Ladezeiten von Internetseiten, im Extremfall kann es sogar sein, dass einige Dienste wie das Anschauen von Videos im Internet bei einer gedrosselten Bandbreite gar nicht mehr möglich sind.

Je nach Anbieter sind Pakete zwischen 200 MB und 500 MB gängig: Wenn das Volumen aufgebraucht ist, wird gedrosselt. Für Vielsurfer werden auch größere Pakete angeboten.

Von den Flatrates zu unterscheiden sind mobile Datentarife auf Volumenbasis. Bei diesen Volumentarifen richten sich die Kosten nach der Menge der Daten, die verschickt oder empfangen werden. Ist das Freivolumen aufgebracht, entstehen zusätzliche Kosten. Es gibt Tarife mit einer bestimmten Kostenobergrenze, also einer Art Preisdeckelung.

! TIPP

Smartphones, zum Teil auch Tablet-PCs, sind für die mobile Internetnutzung vorgesehen. Ab Werk sind sie so voreingestellt, dass im Hintergrund, manchmal auch unbemerkt vom Besitzer, Daten übertragen werden. Beim Kauf eines solchen Geräts sollten Sie also auch die entsprechende Flatrate besitzen. Mit einem herkömmlichen Vertrag wird die Internetnutzung meist nach Volumen abgerechnet und kann sehr teuer werden.

Smartphones im Ausland

E-Mails abrufen, Navigationsfunktionen nutzen oder Flugzeiten online heraussuchen – die Funktionen eines Smartphones sind vielseitig und oft sehr nützlich. Im Ausland ist jedoch Vorsicht geboten bei der Nutzung des eigenen Smartphones. Auch wenn eine Internetflatrate besteht, so gilt diese in der Regel nur innerhalb Deutschlands. Sobald man sich im Ausland befindet, verbindet sich das Smartphone mit einem ausländischen Anbieter, und dabei gelten entsprechende ➤ Roaming-Tarife. Diese sind zwar in den letzten Jahren stetig gesunken und sinken noch immer, dennoch können hier unerwartet hohe Kosten entstehen.

Nach einer schrittweisen Herabsetzung der Roamingentgelte innerhalb der Europäischen Union arbeitet die Europäische Kommission jetzt daran, diese Entgelte für Anrufe, SMS und mobiles Internet ganz abzuschaffen. Als endgültiger Zeitpunkt ist das Jahr 2016 im Gespräch. Sicher ist die Abschaffung noch nicht.

! TIPP

Schutz vor ausufernden Kosten beim Roaming bietet die automatische Deckelung. Sie führt von sich aus zu einer Trennung der Mobilfunkverbindung, wenn Kosten in Höhe von 59,50 Euro entstanden sind. Seit 2012 gilt die Datenkostenbremse weltweit, sofern technisch eine Echtzeitüberwachung möglich ist. In jedem Fall müssen die Nutzer bei der Einreise in das Nicht-EU-Land über die Kosten informiert werden und auch darüber, dass eine die Datenkostenbremse in einem Land nicht zur Verfügung steht.

Um gänzlich zu verhindern, dass das Smartphone unbeabsichtigt im ausländischen Netz Daten über das Mobilfunknetz versendet und empfängt, lässt sich in den Einstellungen das „Daten-Roaming“ ausschalten. Die Nutzung von WLAN, beispielsweise bei Hotspots, ist weiterhin möglich.

3. Heimisches Netzwerk via DSL oder Kabel

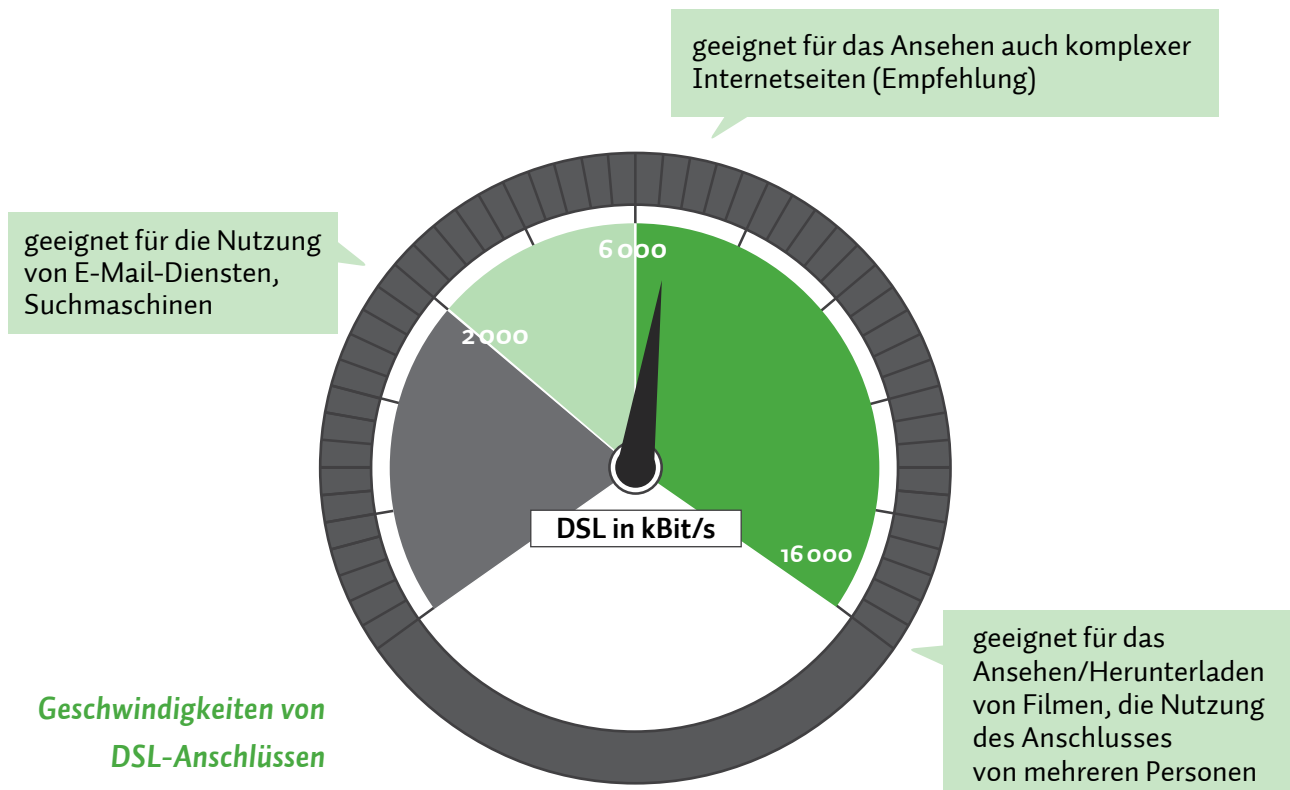
Da die mobile Internetnutzung wie beschrieben noch mit einigen Besonderheiten und zum Teil auch Nachteilen einhergeht, nutzen viele Menschen als heimische Anschlüsse DSL oder Kabel, die in Sachen Geschwindigkeit und Preis nach wie vor klar im Vorteil sind. Diese Anschlüsse laufen meist über den Telefon- oder Kabelnetzanbieter, der seinerseits häufig die notwendigen Geräte zur Verfügung stellt, um den Weg ins Netz zu ermöglichen. Der Unterschied zwischen Kabel und DSL besteht in der Art der Datenübertragung: Bei DSL wird das Telefonnetz, bei Internet über den Kabelanschluss das Kabelnetz genutzt. Am weitesten verbreitet sind DSL-Anschlüsse, die es in verschiedenen Bandbreiten gibt. Die Bandbreite gibt die „Geschwindigkeit“ an, mit der Datenpakete über das Internet übertragen werden.

Generell gilt: Je niedriger die Bandbreite, desto langsamer ist man im Internet unterwegs!

Welche Bandbreite ein Anschluss hat, hängt davon ab, was der Anbieter technisch an einem bestimmten Ort liefern kann, und natürlich davon, wie viel man für den Anschluss bezahlen möchte. Welche Bandbreiten welche Nutzungsmöglichkeiten eröffnen, zeigt die folgende Abbildung.



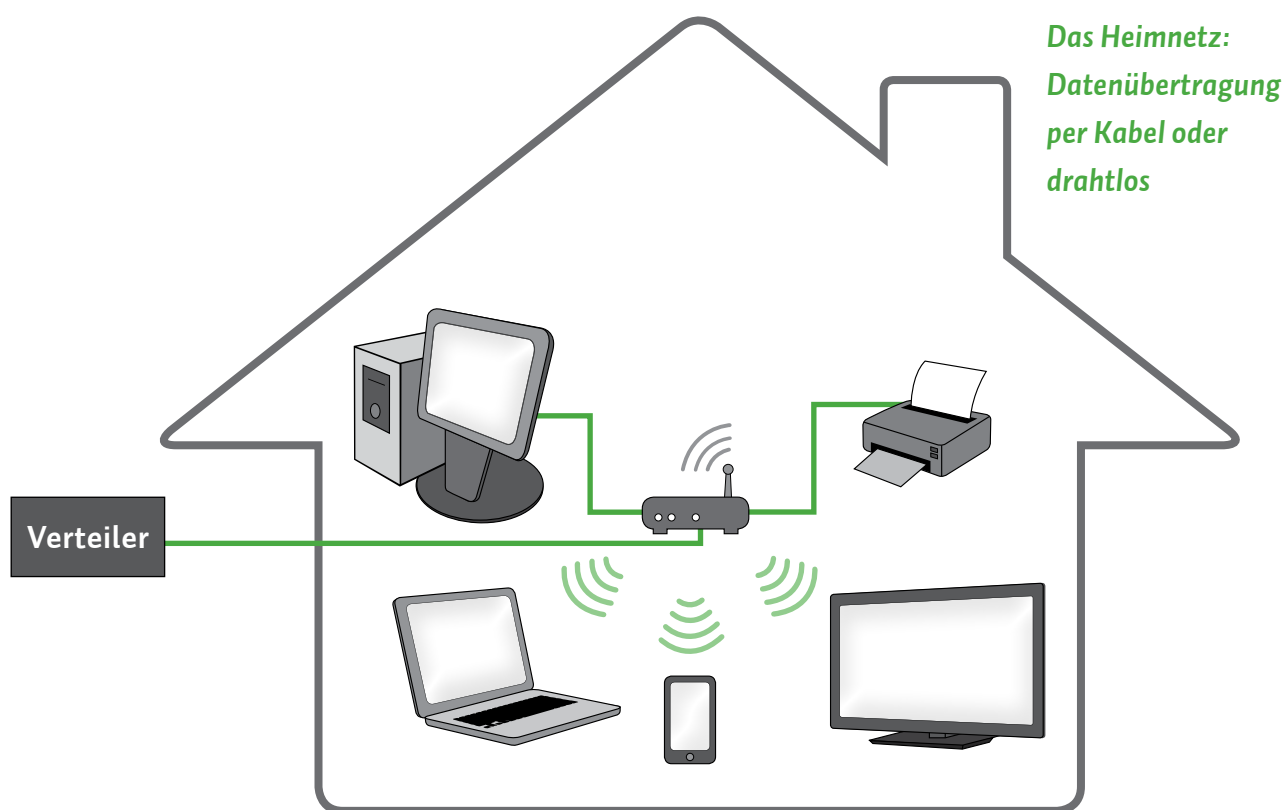
**GESCHWINDIGKEITS-
TEST**



Die Bandbreite wird in kBit/s oder mBit/s angegeben.
 $1000 \text{ kBit/s} = 1 \text{ mBit/s}$

Ob DSL oder Kabel: Zuhause steht dann meist ein sogenannter Router, der die ankommenden Datenpakete auf verschiedene Geräte verteilt, zum Beispiel zum Laptop, dem Stand-PC und zum Netzwerkdrucker, aber auch zum internetfähigen Smart-TV und zum Tablet-PC. Der Router ist also das Herzstück des Heimnetzwerks, da er eine Verbindung von mehreren Geräten zu Hause erst ermöglicht. Oft spricht man auch von einem lokalen Netzwerk, um eine Abgrenzung zum weltweiten Internet vorzunehmen.

Um die aus dem Internet ankommenden Datenpakete an die verschiedenen Geräte im Heimnetzwerk zu verteilen, stehen dem Router grundsätzlich zwei Übertragungswege zur Verfügung. Zum einen können Router und Gerät durch ein Netzkabel miteinander verbunden und die Daten per Verbindungskabel transportiert werden. Zum anderen können die Daten auch drahtlos, also per Funk übertragen werden. Um diesen Unterschied deutlich zu machen, gibt es die zwei Abkürzungen LAN und WLAN. LAN steht für den englischen Begriff Local Area Network, meint also das lokale (Heim-)Netzwerk. WLAN steht für Wireless Local Area Network und bezeichnet damit die drahtlose Version des heimischen Netzwerks.



Voraussetzung für eine drahtlose Datenübertragung ist natürlich, dass sowohl der Router als auch das entsprechende Gerät WLAN-fähig sind. Heute sind fast alle PCs, Laptops und Smartphones mit der Möglichkeit der WLAN-Nutzung ausgestattet. Ältere Computermodelle lassen sich zum Teil mit separaten WLAN-Karten oder -Sticks nachrüsten. Drucker und Multifunktionsgeräte können oft gegen Aufpreis in einer WLAN-fähigen Ausstattung gekauft werden. Bei der drahtlosen Übertragung spielt die Entfernung zum Router eine wichtige Rolle. Je weiter man sich vom Signalursprung entfernt, desto schwächer wird das Signal. Deshalb ist WLAN auf einen bestimmten Radius rund um den Router begrenzt, zum Beispiel im eigenen Haus oder der eigenen Wohnung.

! TIPP

Ihren heimischen Anschluss sollten Sie vor fremden Zugriffen schützen. Wie Sie Ihr WLAN absichern, können Sie im Lernbuch „Silver Surfer – Sicher online im Alter“ nachlesen.

Hotspots

Manche Städte und Gemeinden, aber auch Hotels, Cafés, Bibliotheken und Restaurants, bieten ebenfalls lokale Netzwerke zur Nutzung an. Entweder sie geben ihren Gästen einen Zugangscode, mithilfe dessen sie sich in das Netzwerk einwählen können, oder sie öffnen das Netzwerk prinzipiell für alle und setzen kein Passwort. Oft spricht man hier auch von (WLAN-)Hotspots, manchmal auch von Wi-Fi. Solche Hotspots können kostenfrei sein, oder der Betreiber erhebt ein Entgelt für die Nutzung.

TIPP

In einem Café oder auf einem öffentlichen Platz weiß man nicht genau, wer sich noch alles mit seinem Gerät im Netzwerk befindet, ob der Datenfunk mitgeschnitten wird und vor allem auch welche Absichten die anderen Nutzer haben. Aus diesem Grund sollten Sie in öffentlichen WLANs keine sensiblen Daten übertragen: Onlinebanking und ähnlich sensible Anwendungen gehören ausschließlich ins heimische Netzwerk, um niemanden zum „Lauschen“ einzuladen.

Hotspots funktionieren im Prinzip ähnlich wie das eigene heimische Netzwerk via DSL oder Kabel. Hat man zu Hause einen Router mit WLAN, können prinzipiell auch Freunde und Bekannte mit den entsprechenden Zugangsdaten ihre Geräte in das Netzwerk einwählen, wenn Sie sich im Funkradius des Routers befinden. ||

Was das mobile Internet mit sich bringt

MODUL
02

| HELMUT EIERMANN, CHRISTIAN GOLLNER & BARBARA STEINHÖFEL

Um in die Welt des mobilen Internets einzutauchen, steht eine Vielzahl an internetfähigen mobilen Geräten zur Auswahl. Welche das sind und welche technischen Besonderheiten die mobilen Alltagshelfer haben, zeigt dieses Modul auf. Mit vielen neuen Möglichkeiten kommen aber auch neue Gefahren, vor allem beim Schutz persönlicher Daten. Mit den hier genannten Hintergrundinformationen und Tipps für mehr Sicherheit ist man gegen Datenverlust und Angriffe gut gerüstet.

1. Betriebssysteme und Apps

Mobile Endgeräte wie Smartphones und Tablets sind kleine Computer, die genau wie PC und Laptop ein Betriebssystem benötigen. Allerdings sind dies spezielle Betriebssysteme, die auch als OS bezeichnet werden, abgekürzt vom englischen Begriff für Betriebssystem: Operating System. Die Hersteller der Smartphones und Tablets verwenden unterschiedliche Betriebssysteme.

Die bekanntesten sind:

- iOS von Apple
- Android, entwickelt von der Open Handset Alliance (ein Unternehmenszusammenschluss unter der Leitung von Google)
- Windows Phone von Microsoft sowie die Vorgängerversion Windows Mobile
- BlackBerry OS von RIM





Silver Surfer – Lernbuch :
„HANDY, SMARTPHONE
UND CO.“

Apps

App steht für „**A**pplication“ und bedeutet nichts anderes als Anwendung. Apps sind kleine Programme, die auf dem Smartphone oder Tablet installiert werden können. Sie erweitern die Funktionen eines Smartphones um nützliche Eigenschaften. Am Gerät können damit zum Beispiel Spiele gespielt oder Landkarten angesehen werden. Durch Apps für die Sicherheit von Systemen, wie zum Beispiel einem Antivirenschanner, kann man sich vor kriminellen Angreifern schützen.

Generell werden Apps über Vertriebsplattformen angeboten und können von dort je nach Vorgabe des Herstellers kostenlos oder kostenpflichtig heruntergeladen werden.

Beispiele für bekannte Anbietershops:

- App Store von Apple (⇒ iTunes)
- Google Play Store für Android
- Windows Phone Store von Microsoft
(früher: Windows Phone Marketplace)
- BlackBerry AppWorld

Um Apps herunterladen zu können, muss man sich in dem entsprechenden Shop registrieren und ein Nutzerkonto anlegen. Da einige Apps Geld kosten, muss man sich auch entscheiden, wie man die Apps bezahlen möchte.

Viele Apps sind kostenlos, aber nicht unbedingt umsonst. Zahlreiche Apps sind sehr neugierig und greifen vom Smartphone oder Tablet Daten ab. Zudem muss man bei kostenlosen Apps mit lästigen Werbeeinblendungen leben.

Oft wird auch zunächst eine kostenlose „Lite“-Version der App angeboten, die in ihrer Funktionalität eingeschränkt ist. Will man alle Funktionen nutzen, muss man die Premiumversion kostenpflichtig erwerben. Diese Premiumversion kann direkt aus der Lite-Version der App heraus bestellt werden, das nennt man dann In-App-Kauf.

In-App-Käufe sind auch bei vielen Spiele-Apps möglich, hier erwirbt man zum Beispiel zusätzliches Zubehör oder weitere Spielerunden.



TIPP

Oft hört man auch den Begriff Widget. Widgets sind kleine Programme, die auf dem Startbildschirm des Smartphones oder Tablets platziert werden können. Da sie „live“ Daten liefern, kann man sich mit ihnen beispielsweise über das aktuelle Wetter informieren oder anstehende Termine anzeigen lassen.

2. Cloud-Computing als Grundlage des mobilen Internets

Bisher war es üblich, dass man seine Daten wie Fotos, Musik oder Dokumente auf einzelnen Geräten wie Computer oder Laptop speichert. Das Problem an der Sache: Sobald man mehrere Geräte hat, muss man die Daten umständlich von einem zum anderen kopieren. Auch von unterwegs kann man nur auf die Daten zugreifen, die auf dem jeweils mitgeführten Gerät vorhanden sind.

So entstand der Bedarf nach einer Speichermöglichkeit, auf die von überall aus zugegriffen werden kann. Hier kommen Clouds ins Spiel, was übersetzt „Wolken“ bedeutet. Das Praktische am sogenannten Cloud-Computing ist nicht nur, dass man mit unterschiedlichsten Endgeräten auf seine Daten zugreifen kann, sondern dass es auch von überall aus funktioniert – und zwar über das Internet.

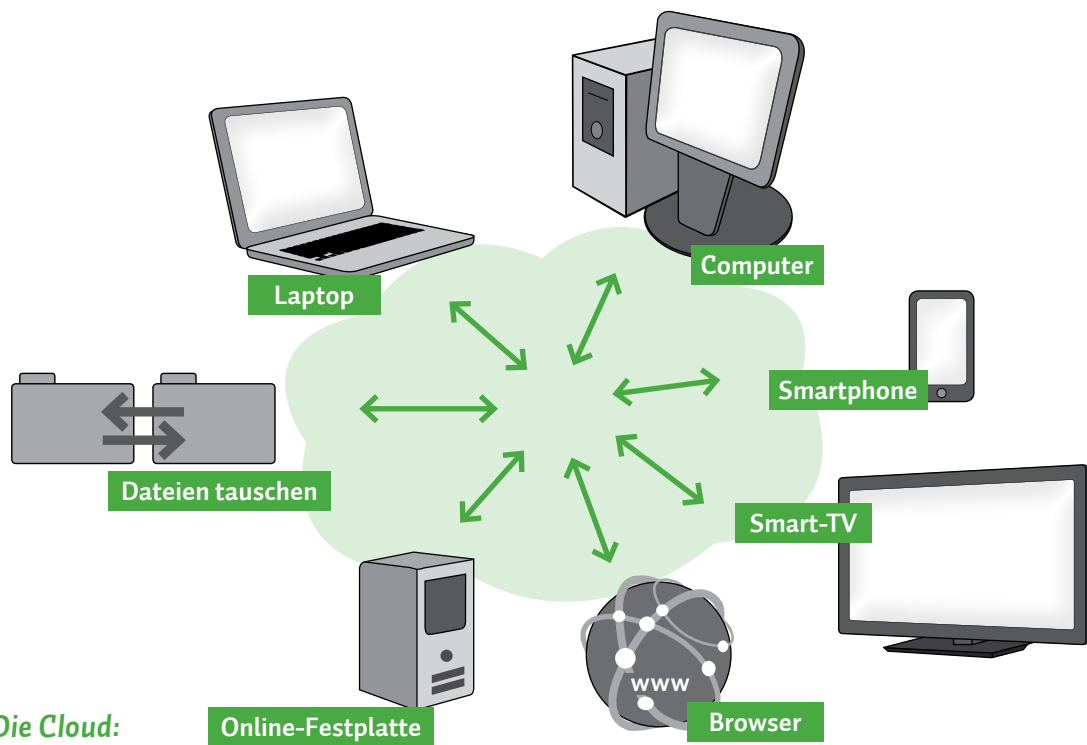
Die Anbieter solcher Cloud-Dienste stellen ihren Benutzern dafür Speicherplatz im eigenen Rechnersystem zur Verfügung. Der Benutzer meldet sich beim Anbieter an und kann dann von seinem Computer, Laptop, Smartphone oder Tablet auf seinen persönlichen Speicherplatz zugreifen.

Doch was einen so innovativen Namen hat, ist gar nicht so neu. Früher nannte man das Webspacer oder Online-Speicher. Jeder, der schon einmal eine E-Mail in einem Internetbrowser gelesen oder geschrieben hat, hat bereits einmal eine (Daten-)Wolke genutzt. Wie jeder Cloud-Dienst greift auch das E-Mail-Konto auf Speicherplatz im Internet zurück.

Allerdings sollte man darauf achten, wie umfangreich die Daten sind. Zum einen bieten kostenlose Cloud-Dienste meist nur einen begrenzten Speicherplatz an, und zum anderen benötigt das Kopieren von großen Datenmengen auch bei einer schnellen Internetverbindung viel Zeit. Ein funktionierender Internetzugang ist also Voraussetzung für die Nutzung einer Cloud. In Gebieten mit schlechter Mobilfunkversorgung kann eine unzuverlässige Verbindung zu Cloud-Diensten die Freude an der Nutzung erheblich mindern.



Modul 1:
„DAS MOBILE INTERNET“



*Die Cloud:
Datenzugriff von überall*

Zusätzlich ist bei allen Cloud-Diensten eine Registrierung erforderlich beziehungsweise ein Nutzerkonto bei dem entsprechenden Anbieter.

Es gibt die unterschiedlichsten Anbieter und Angebote. Ein deutscher Cloud-Anbieter ist die Telekom Deutschland GmbH. Andere bekannte Anbieter, in der Regel mit Sitz in den USA, sind Amazon, Apple, Google, Microsoft oder Dropbox. Die Hersteller von Betriebssystemen wie Windows oder Android bauen Zugriffsmöglichkeiten für die von ihnen betriebenen Clouds schon jetzt in ihre Produkte ein, sodass keine Zusatzsoftware notwendig ist. Wer seinen Cloud-Speicher auch mit seinem Tablet oder Smartphone nutzen möchte, muss bei der Auswahl darauf achten, ob es passende Apps gibt.

Allerdings birgt die Cloud auch Gefahren, denn oft weiß man nicht, wo sich die Daten genau befinden und wer alles darauf Zugriff hat.

EXKURS: VERSCHLÜSSELN VON DATEN

Nicht jeder möchte, dass Dritte die Daten in der Cloud oder auf dem Weg dorthin auslesen können. Daher sollte man die Daten verschlüsseln.

Bei der Verschlüsselung werden digitale Daten, also zum Beispiel Texte oder Bilder, mittels mathematischer Verfahren für Dritte unleserlich gemacht. Entschlüsseln kann die Daten bei sicheren Verschlüsselungsverfahren nur derjenige, der die richtigen digitalen Schlüssel besitzt. Für die Verschlüsselung benötigt man spezielle Programme, die kostenpflichtig und zum Teil auch kostenlos erhältlich sind. Um die Daten jedoch auf allen gewünschten Endgeräten nutzen zu können, muss das entsprechende Verschlüsselungsprogramm auf allen Geräten installiert sein. Man sollte also darauf achten, dass das Verschlüsselungsprogramm auch auf mobilen Endgeräten wie Smartphones oder Tablets funktioniert.

Worauf man bei der Auswahl eines Cloud-Dienstes achten sollte

Cloud-Nutzer sollten darauf achten, dass die Cloud so transparent und sicher wie möglich gestaltet ist. Das bedeutet, dass der Verbraucher darüber informiert wird:

- wo (Land, Region) sich welche Daten von ihm befinden,
- welche Subunternehmer noch eingeschaltet werden,
- wer Zugriff auf die Daten hat und
- welche Rechte und Pflichten der Cloud-Anbieter und welche der Cloud-Nutzer hat.



APPS – NEUGIERIGE DATENSAMMLER

3. Meine Daten und Datenschutzrechte im mobilen Internet

Mobile Geräte wissen sehr viel über ihre Nutzer, und häufig werden diese Daten weitergegeben. Vor allem die Werbewirtschaft hat Interesse an Daten wie dem aktuellen Standort des Gerätes, dem Kommunikationsverhalten seiner Nutzer oder den Informationen in den Adressbüchern. Diese und andere Daten geben mobile Geräte häufig preis, oft ohne dass ihre Besitzer dies wissen. Auf der Grundlage der gesammelten Daten wird Werbung ganz genau auf die Bedürfnisse der Menschen zugeschnitten. Zudem versuchen Kriminelle, sensible Bankdaten auszuspähen, um damit Zugriff auf fremde Konten zu erhalten.

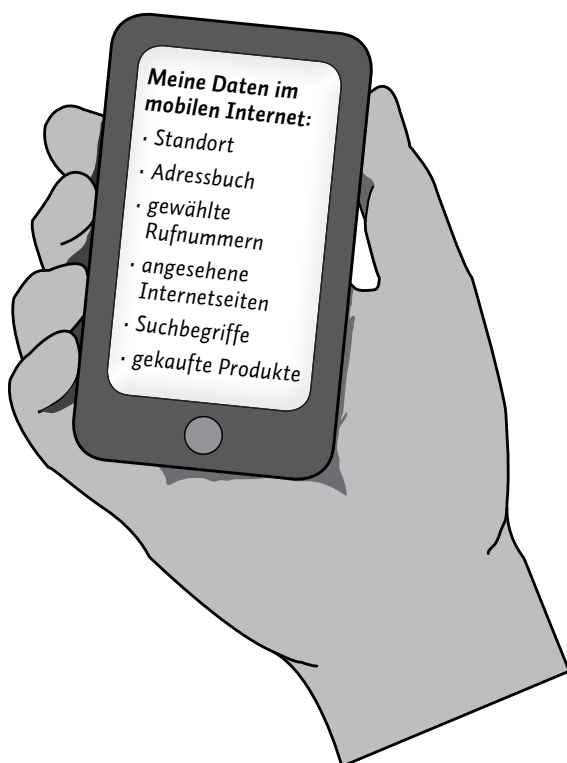
Gegen die Gefahren für die eigenen Daten kann man sich allerdings schützen. Nutzer sollten die technischen Möglichkeiten, die einer Datenweitergabe entgegenwirken, im Blick haben. Zudem bestehen Datenschutzrechte, mit denen man die Kontrolle über die eigenen Daten behält.

Was mobile Geräte alles wissen

Die neuen digitalen Alleskönner Smartphone und Tablet können sehr genau verzeichnen, wie und wo ein Nutzer das Gerät verwendet. Der eingebaute ➔ GPS-Chip ermöglicht dem Gerät, mittels Satelliten seinen Standort exakt zu bestimmen, und auch die Information über die empfangbaren Funknetzwerke erlaubt die Ortung des Gerätes und damit seines Besitzers. Wird der Standort in regelmäßigen Abständen ermittelt, kann nachvollzogen werden, welche Orte ein Nutzer gerne aufsucht.

Das Gerät weiß zudem, wie häufig, wann und wie lange mit bestimmten Personen aus dem Telefonbuch telefoniert wurde. Es kann auch verzeichnen und speichern, wer anruft. Im Internet eingegebene Suchbegriffe und aufgerufene Seiten können gesammelt werden, ebenso wie die persönlichen Interessen und Vorlieben, die in einem sozialen Netzwerk wie Facebook oder Google+ eingetragen werden.

Die Informationen werden teilweise an die Hersteller von Geräten oder Programmen weitergesandt. Warum wird dies gemacht? Zum einen können die Unternehmen ihre Produkte mit solchen Daten verbessern, zum anderen aber, und das ist viel wichtiger, lassen sich solche Daten durch ihre Verknüpfung zu Profilen für Werbung verwenden.



Smartphones –
kleine Geräte für riesige
Datenmengen

Mobile Geräte beziehungsweise die Anbieter der installierten Apps können mit der Kenntnis der persönlichen Daten tiefe Einblicke in die Privatsphäre der Nutzer nehmen. Wer die Neugierde und Sammelleidenenschaft seines Smartphones oder Tablets verringern möchte, kann dies zum Beispiel durch Anpassung der Datenschutzeinstellungen tun.

Einstellungsoptionen findet man sowohl in den Betriebssystemen als auch in den Apps. Hier kann man als Nutzer entscheiden, welches Programm auf welche Daten Zugriff hat und inwieweit diese zu Marketingzwecken verwendet werden können.

! TIPP

Wenn Sie sichergehen wollen, dass sich Geräte nicht unkontrolliert orten beziehungsweise orten lassen, sollten Sie darauf achten, dass die Funktionen ⇒ GPS (Satellitenortung), WLAN (drahtlose Netzwerkverbindung) und der Datenaustausch über die Funktechnik ⇒ Bluetooth nur dann eingeschaltet sind, wenn Sie sie wirklich benötigen.

Rechte des Verbrauchers

Die Anbieter von Betriebssystemen und Apps dürfen mit den Daten auf mobilen Geräten nicht nach freiem Belieben verfahren. Die Erhebung, Speicherung und Nutzung von Daten, die sich auf eine Person beziehen, sind nur dann zulässig, wenn diese zuvor eingewilligt hat. Wer die Kontrolle behalten will, sollte sich mit den Datenschutzbestimmungen der Betriebssysteme und Apps vertraut machen. Denn durch Bestätigung der Bestimmungen durch Fingertipp wird die abgefragte Einwilligung erteilt.

Häufig, aber nicht immer, lassen sich bestimmte Datenübertragungen nachträglich über die Einstellungen unterbinden. Die Datenschutzbestimmungen können sich jedoch jederzeit ändern.

TIPP

Das deutsche und das europäische Datenschutzrecht gibt Verbrauchern ein Recht auf Löschung von Daten und auf Auskunft über alle gespeicherten Informationen. Setzen Sie sich bei Fragen am besten direkt mit den Unternehmen in Verbindung. Bei Problemen können die Aufsichtsbehörden für den Datenschutz weiterhelfen, also die Datenschutzbeauftragten des Bundes und der Länder.

Bezahlen mit den eigenen Daten

Viele Apps für mobile Geräte werden völlig kostenfrei angeboten. Tatsächlich wird bei der Installation solcher Programme kein Entgelt berechnet. Die „Bezahlung“ erfolgt auf andere Weise.

Kostenlose Apps finanzieren sich üblicherweise durch Werbeeinblendungen, die sich am Verhalten der Nutzer und ihren Gewohnheiten ausrichten. Aus den gesammelten Daten lassen sich Konsumwünsche ablesen, wodurch Werbung gezielter platziert und deswegen teurer verkauft werden kann. In diesem Zusammenhang kann es passieren, dass sich der Hersteller eines kostenlosen Spielprogramms die Einwilligung geben lässt, dass er auf die Standortdaten und auf das im Gerät hinterlegte Adressbuch Zugriff nehmen darf. Dies geschieht auch dann, wenn dies zum Funktionieren der App gar nicht notwendig wäre.

Kaum eine App lässt sich installieren, ohne dass Nutzer zuvor eine Fülle von Zugriffsrechten hinnehmen sollen. Und die Nutzung und Weitergabe der auf diese Weise gewonnenen Daten ist oftmals in Nutzungsbedingungen versteckt, die man mit der Installation der App stillschweigend akzeptiert.

Vielfach kann eine App gar nicht erst installiert werden, ohne dass eine breite Einwilligung gegeben wird. Auch die Datenschutzeinstellungen erlauben dann oft keine nachträglichen Änderungen zum Umfang der Datennutzung.



APP-BERECHTIGUNGEN

! TIPP

Fragen Sie sich beim Installieren einer App, warum eine App Zugriff auf bestimmte Daten des Smartphones braucht. Eine Taschenlampen-App muss beispielsweise keinen Zugriff auf das Telefonbuch beanspruchen, um funktionsfähig zu sein. In solchen Fällen empfiehlt sich die Suche nach einer anderen App oder gar der Verzicht der Installation.

Kriminelle greifen nach Daten

Mobile Geräte werden in einem immer größeren Ausmaß zum Ziel von Kriminellen. Mit technischen Tricks versuchen sie, sensible Daten auszuspähen oder Smartphones und Tablets fernzusteuern. All das dient dem Ziel, die Kreditkarten oder Bankkonten der Betroffenen zu eigenen Gunsten zu belasten.

Vor solchen kriminellen Zugriffen schützt – wie auch am heimischen PC – eine Sicherheitssoftware. Solche Programme sind von unterschiedlichen Anbietern entweder kostenlos oder kostenpflichtig in den App-Anbietershops zu erhalten. Diese erkennen Schadsoftware, mit der Geräte manipuliert werden sollen, recht zuverlässig. Neben der Einrichtung einer Sicherheitssoftware sollten Sie Programme grundsätzlich nur aus dem offiziellen Anbietershop des Geräteherstellers beziehen. Bei Quellen außerhalb der überwachten Bereiche ist die Gefahr, Schadsoftware zu erhalten, besonders groß.



Silver Surfer – Lernbuch:
„VORSICHT, VIREN!“

Die Kriminellen nutzen Schwachstellen in der Gerätesoftware bewusst aus. Deswegen sollte man das Betriebssystem und die Programme immer auf dem neusten Stand halten. ➔ Updates der Hersteller machen die Geräte sicherer.

Wer Kreditkartenzahlungen oder Bankgeschäfte unmittelbar am mobilen Gerät durchführt, sollte die Kontoauszüge aufmerksam auf unerwünschte Abbuchungen untersuchen. Unregelmäßigkeiten sollten der zuständigen Bank sofort mitgeteilt werden.



Weitere Informationen:

**LINKLISTE
„SMARTPHONES UND
APPS – DATENSCHUTZ“**



Weitere Informationen:

**LINKLISTE
„SMARTPHONES UND
APPS – VERBRAUCHER-
SCHUTZ“**

TIPP

Wichtige Datenschutztipps für die Nutzung von Apps:

- Verwenden Sie nur Apps aus sicheren Quellen, also den Anbieter-shops der Gerätehersteller.
- Machen Sie sich mit den besonderen Datenschutzbestimmungen einer App vertraut. Beachten Sie, dass diese sich jederzeit ändern können.
- Nutzen Sie die Datenschutzeinstellungen, um ungewollte Datenübertragungen einzuschränken; Bluetooth, GPS und WLAN sollten nur aktiviert sein, wenn sie benötigt werden.
- Achten Sie darauf, welche Daten Sie auf Ihrem Smartphone gespeichert und abrufbar haben.
- Schützen Sie Ihre Daten durch Verschlüsselung, Passwort und gegebenenfalls die Löschfunktion nach Verlust.
- Löschen Sie Ihre Daten, bevor Sie das Smartphone zur Reparatur geben oder verkaufen.
- Virenschutz ist beim Smartphone unbedingt zu empfehlen – auch wenn sein Schutz nicht dem beim heimischen PC entspricht.
- Führen Sie Sicherheitsupdates durch und aktualisieren Sie regelmäßig das Betriebssystem.
- Sie können sich an den Anbieter von Diensten wenden, der Ihre Daten verwaltet, und Auskunft über die gespeicherten Daten fordern.

Quelle: Auszug aus der Checkliste des Informationsangebots „Smartphones und Apps – Spione in der Hosentasche“, www.mjv.rlp.de/smartphones

4. „Mobile Payment“ – einfacher bezahlen

Der Begriff Mobile Payment bedeutet zu Deutsch mobiles Bezahlen. Dahinter stehen zahlreiche technische Verfahren, mit deren Hilfe Verbraucher mit ihrem mobilen Gerät oder speziellen Karten bezahlen können. Nach Vorstellung der Anbieter der Systeme sollen diese Techniken das Bargeld vor allem bei Kleinbeträgen einmal vollständig ersetzen. Ein Vorteil von Mobile-Payment-Technologien ist die geringe Zeit, die ein Bezahlvorgang damit benötigt. Die Bezahlung ist weniger aufwendig als die Nutzung einer Giro- oder Kreditkarte.

Immer mehr Händler entscheiden sich, ihren Kunden das mobile Bezahlen zu ermöglichen. Doch der Markt für mobile Bezahlösungen ist noch sehr unübersichtlich, da sich bislang keine verbreiteten Standards herausgebildet haben. Derzeit können einzelne mobile Bezahl-systeme nur bei wenigen Unternehmen genutzt werden.

Wie funktioniert das mobile Bezahlen?

Die neuen Bezahlmöglichkeiten funktionieren kaum anders als die Bezahlung mit einer Geldkarte oder der Girokarte, die auch Maestro-Karte genannt wird und die frühere EC-Karte ersetzt. Der wesentliche Unterschied besteht in der Neuerung, dass beim mobilen Bezahlen keinerlei Kontakt mehr zwischen dem Datenträger und dem Lesegerät bestehen muss. Alle zur Abwicklung erforderlichen Daten werden in der Regel über Funkwellen übertragen. Die Daten, die früher auf der Bankkarte gespeichert waren, werden nun meist mithilfe des Smartphones an den Händler weitergereicht.

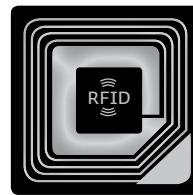
Im Einzelhandel stehen vermehrt Lesegeräte an den Kassen bereit, die die erforderlichen Codenummern von den Geräten auslesen können. Dabei werden die Informationen entweder direkt per Funk zwischen dem Lesegerät an der Kasse und dem Smartphone auf kurzer Strecke ausgetauscht oder über das Internet verschickt.

Wer das mobile Bezahlen mit einem Smartphone nutzen möchte, muss sich zunächst bei einem Anbieter einer solchen Methode anmelden. Registrierung und Nutzung können mit Kosten verbunden sein. Teilweise müssen Verbraucher zur Bonitätsprüfung in eine Schufa-Abfrage einwilligen.

Ganz ohne Smartphone kommt die Bezahlung mit einer speziellen funkfähigen Giro- oder Kreditkarte aus. Viele Verbraucher besitzen eine solche Karte schon jetzt, da Sparkassen und andere Kreditinstitute diese bereits seit geraumer Zeit ausgeben.

Technik des mobilen Bezahlens

Die Datenübertragung zwischen Smartphone beziehungsweise Funkkarte und dem Kassenterminal wird durch den Funkstandard NFC ermöglicht. Diese Abkürzung steht für „near field communication“, bedeutet also wörtlich übersetzt Nahfeldkommunikation. Karten und Geräte müssen zur Übertragung nur für einen kurzen Moment zusammengehalten werden. Oft benötigt das Auslösen einer Zahlung nicht die Eingabe einer PIN, also einer persönlichen Identifikationsnummer, was den Vorgang beschleunigt. In den Karten und Geräten verbergen sich Computerchips, die über eine Miniatur-Antenne verfügen.



*Schematische Darstellung eines RFID-Transponders
mit auslesbarem Chip in der Mitte*

Ob eine Karte oder ein Smartphone NFC-fähig ist, ist anhand dieser Kennzeichen zu erkennen:



Markierung auf Karten



Markierung auf Geräten

Die NFC-Funktion eines Smartphones lässt sich nur in Verbindung mit einer speziellen App mit Bezahlungsfunktion eines Finanzdienstleisters nutzen. Das Programm nimmt auf den eingebauten NFC-Chip Zugriff und steuert die Datenweitergabe an ein Lesegerät.

Verbreitete Systeme und ihre Anbieter sind:

- Girogo der deutschen Sparkassen,
- PayPass des Kreditkartenunternehmens MasterCard,
- Paywave des Kreditkartenanbieters Visa und
- PayPal mit seiner App.

Teilweise bieten Einzelhändler eine eigene Bezahlösung für das Smartphone an, die die NFC-Technik nicht verwendet. Zur Nutzung muss eine besondere App heruntergeladen werden. An der Kasse wird nur ein Bestätigungscode angegeben, oder man fotografiert über die Bezahl-App einen ➔ QR-Code, eine Art Strichcode, der die Bezahlinformationen enthält.

Auch Zahlungen von einem Smartphone zu einem anderen sind möglich. Diese Anwendungen eignen sich vor allem für den privaten Bereich oder den Flohmarkt, benötigen aber ebenfalls besondere Apps.

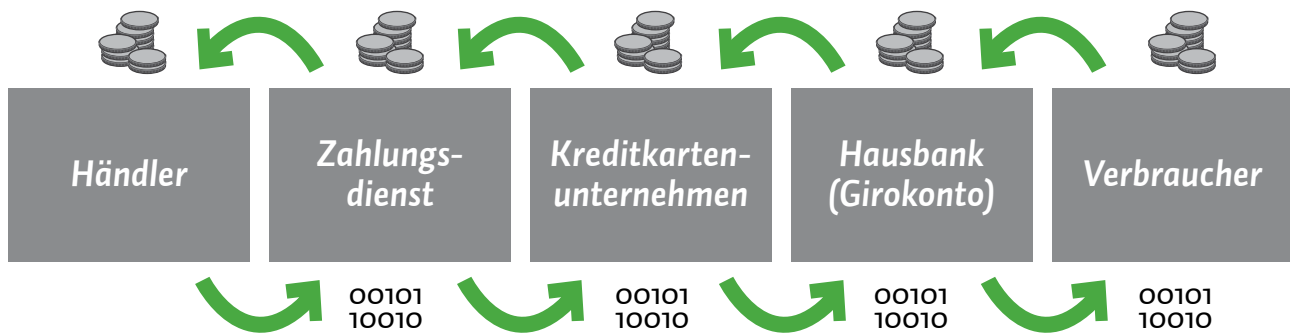
Eine besondere Funktion bieten **E-Wallets**, zu Deutsch elektronische Geldbeutel. Dies sind Apps, in denen Karten ganz unterschiedlichen Typs hinterlegt und beim Bezahlen genutzt werden können. Neben Kreditkarten können dort zum Beispiel Mitgliedskarten und Karten aus Kundenbindungsprogrammen wie Payback oder DeutschlandCard eingepflegt und gemeinsam verwendet werden.

Abrechnung

Die Abrechnung im Mobile Payment ist häufig kompliziert nachzuvollziehen. Je mehr Unternehmen an einem mobilen Bezahlvorgang beteiligt sind, desto unübersichtlicher wird der Geldfluss. Im Mobile Payment fließt das Geld nicht direkt zwischen Kunde und Händler, sondern über meist mehrere Finanzdienstleister. Am Ende eines Zahlungsvorgangs wird in aller Regel das Girokonto des Benutzers im Wege des Lastschriftverfahrens belastet. Bei manchen Bezahlssystemen erscheinen die Beträge zunächst auf der Telefon- oder Kreditkartenabrechnung.



ERFAHRUNGSAUSTAUSCH



Beispiel für einen Geld- und Informationsfluss im Mobile Payment

Wie steht es mit der Sicherheit?

Kein technisches System ist absolut sicher. Die Gefahr für das Auslösen ungewollter Transaktionen oder für Zugriffe von Kriminellen ist wegen der zahlreichen Schutzmaßnahmen vonseiten der Anbieter derzeit als gering einzustufen. Dennoch sollten Nutzer von Mobile Payment ihre Kontoauszüge stets sorgfältig auf mögliche unberechtigte Abbuchungen prüfen. Auf dem mobilen Gerät, über das mobile Bezahlvorgänge abgewickelt werden, sollte eine Schutzsoftware gegen Viren und Trojaner eingesetzt werden.

Worauf man achten sollte

Wer sich einem mobilen Bezahlssystem anschließen möchte, hat die Wahl unter einer Reihe von Anbietern. Solange noch zahlreiche konkurrierende Systeme am Markt bestehen, sollte jener Anbieter den Vorzug erhalten, dessen System dort genutzt werden kann, wo man regelmäßig einkauft. Zu beachten ist auch, dass nicht alle Systeme überall im Ausland nutzbar sind. Girogo der Sparkassen zum Beispiel kann nur innerhalb Deutschlands verwendet werden.

Die Informationen aus den Bezahlvorgängen geben Details zum Konsumverhalten preis. Bei Abschluss eines Nutzungsvertrages sollte anhand der Datenschutzbestimmungen geklärt werden, dass diese Daten nicht zu Marketingzwecken, sondern nur zur Abwicklung der Bezahlvorgänge verwendet werden. ||

Blick in die Zukunft des Internets

MODUL
03

| CHRISTIAN GOLLNER & BARBARA STEINHÖFEL

Heutzutage werden nicht nur Uhren und Brillen „smart“, sondern auch das Internet. Welche Eigenschaften die mobilen Alltagshelfer haben und wie die Zukunft des Internets aussehen könnte, zeigt dieses Modul auf. Smart-Technologien sollen das Leben der Verbraucher einfacher machen – das birgt Chancen, aber auch so manches Risiko. Verbraucher können gläsern werden, wenn Daten über die Gerätenutzung unkontrolliert gesammelt und ausgewertet werden. Die massenhafte Erfassung solcher Informationen in anonymer Form kann die Menschen in Wissenschaft und Forschung aber auch weiterbringen.

1. Die Palette „smarter“ Endgeräte

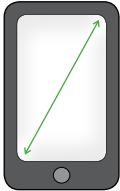
Smartphones und Tablets gehören heute zum Alltag vieler Verbraucher. Die Palette der angebotenen Geräte ist groß, und die Unterschiede sind auf den ersten Blick nicht immer ersichtlich. Wenn man sich heute mit mobilen Endgeräten befasst, spricht man aber längst nicht mehr nur von Smartphones und Tablets. Ob Brille oder Uhr – viele dieser Alltagsgegenstände werden langsam ebenfalls „smart“. Smart bedeutet in diesem Zusammenhang „intelligent“ oder „schlau“. Schläuer als die alten Geräte sind sie wegen ihrer ununterbrochenen Verbindung zum Internet, ihrer starken Rechenleistung und den immer häufiger verbauten Sensoren, zum Beispiel zum Messen des Pulsschlags.



Smartphone
bis 4,5 Zoll



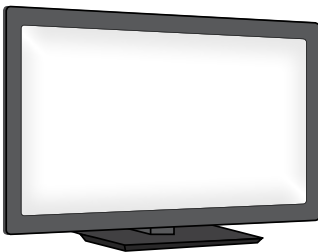
Phablet
4,5–7 Zoll



Tablet
7–10,1 Zoll

Smartphone & Tablet

Das klassische Smartphone hat ein Display mit einer Diagonalen von bis zu 4,5 Zoll. Die sogenannten Smartlets oder Phablets sind – wie die Namen andeuten – Mischformen aus Smartphones und Tablets und haben einen größeren Bildschirm als ein Smartphone, sind aber kleiner als Tablets. Die Bildschirmdiagonale beträgt zwischen 4,5 und sieben Zoll. Ist das Display zwischen sieben und 10,1 Zoll groß, spricht man von einem Tablet.



Smart-TV

Wenn man sich heute einen neuen Fernseher anschafft, holt man sich wahrscheinlich ein sogenanntes Smart-TV ins Haus. Smart-TV, manchmal auch Hybrid-TV oder HbbTV genannt, ist die Bezeichnung für Fernsehgeräte, die internetfähig sind. Man kann zahlreiche Zusatzangebote nutzen, zum Beispiel die Mediatheken der Fernsehsender, und auch im Internet surfen. Außerdem kann man mit dem smarten Fernsehgerät auf Fotos zugreifen, die auf einem PC gespeichert sind. Auch Videotelefonie ist am Fernseher möglich.



Smartwatch

Noch recht neu auf dem Markt sind Smartwatches, also smarte Armbanduhren. Diese Uhren haben ein kleines Display von meist rund 1,5 Zoll. Sie verbinden sich per ➔ Bluetooth mit einem Smartphone, und über entsprechende Apps kann man sich an der Uhr dann zum Beispiel den Terminplaner, E-Mails oder auch Statusmeldungen aus sozialen Netzwerken anzeigen lassen. Mit einigen Modellen kann man auch direkt telefonieren, Fotos schießen oder den Puls messen.



Smart-Brille

Die neuste Entwicklung sind sogenannte Smart-Brillen. Mithilfe dieser Datenbrillen wird ein Bild ins Sichtfeld des Trägers projiziert. So kann man Daten lesen, Nachrichten empfangen oder sich den Weg weisen lassen. Über eine eingebaute Kamera kann die Brille auch die Umgebung wahrnehmen und so etwa das gerade Gesehene erklären.

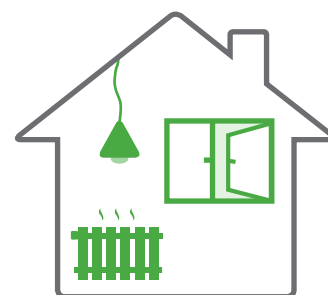
Smart-Kamera

Von einem Hersteller gibt es auch bereits eine smarte Kamera, die genau wie ein Smartphone und alle anderen smarten Geräte über ein Betriebssystem und eine Internetverbindung verfügt. So ist es möglich, Fotos zum Beispiel direkt zu verschicken oder in einem sozialen Netzwerk zu veröffentlichen.



Smarthome

Auch an den Begriff Smarthome sollte man sich schon mal gewöhnen. Dazu gehört die Vernetzung beispielsweise von Schließanlagen, Lampen, Jalousien, Heizung oder Alarmanlagen. Über entsprechende Apps können dann via Smartphone oder Tablet die Jalousien geöffnet oder geschlossen, die Lampen ein- oder ausgeschaltet und die Heizung reguliert werden. Auch sicherheitstechnisch ist diese Idee nicht uninteressant. So gibt es Lösungen in Kombination mit Bewegungsmeldern und Webcams. Wenn das Smartphone sich meldet, hat jemand das Grundstück betreten und den Bewegungsmelder aktiviert. Eine SMS informiert darüber, ob sich der Einbrecher schon im Haus oder noch auf dem Grundstück befindet. Per Webcam kann man nun via Smartphone verfolgen, was ein möglicher Einbrecher so anstellt.



SMARTHOME

2. Der gläserne Verbraucher – Herausforderung für den Verbraucherschutz

Nicht mehr nur im Berufsleben spielt moderne Technik eine immer wichtiger werdende Rolle. Auch der Alltag von Verbrauchern wird immer stärker von Technik begleitet. Der Trend geht hin zur Vernetzung aller nur erdenklichen Anwendungen: So könnte bald die Heizung des Zuhauses über die Konsole des Autos gesteuert werden oder der leere Kühlschrank automatisch Milch und Käse bestellen.

Vernetzte Technik kann nur dann reibungslos funktionieren, wenn die Geräte untereinander über verschiedene Wege wie zum Beispiel das Internet frei „kommunizieren“ können. Der Inhalt dieser Kommunikation enthält jedoch höchst sensible Daten zur persönlichen Lebensführung. Diese Daten müssen geschützt werden, da ihre Offenlegung einen Eingriff in die Privatsphäre bedeutet und weil Verbraucher dadurch gegenüber Unternehmen Nachteile erleiden können.

Die totale Erfassung und Vernetzung

Smarte Technologien können Menschen dabei helfen, ihren Alltag schneller und einfacher zu bewältigen. Die meisten smarten Geräte verfügen über zahlreiche Sensoren, mit denen sie Informationen aus der Umwelt aufnehmen und verarbeiten können. Zum Beispiel erfassen die Geräte satellitengenau ihre Position und können mithilfe einer eingebauten Kamera und dem internen Mikrofon sogar „sehen“ und „hören“.

Hier einige Beispiele: Das Smartphone kann Bewegung messen und versteht gesprochene Sprache immer besser. Sensoren für Heizungssysteme sind in der Lage, die Anwesenheit von Menschen in bestimmten Räumen zu erkennen, Spielekonsolen können Körpergesten wahrnehmen und interpretieren, Fitnesssysteme messen die Herzfrequenz und zählen die Schritte, der Fernseher speichert, welche Sendungen angesehen wurden. Das alltägliche Leben wird digital gespiegelt. Die smarten Geräte erhalten tiefe Einblicke in das Privatleben. Manchmal sogar tiefere Einblicke, als enge Familienangehörige erhalten würden.

Die Vernetzung der Sensoren und Erfassungssysteme ist Voraussetzung für das Funktionieren smarterer Technologien, doch die anfallenden Informationen können auch zu Zwecken der Werbung genutzt werden. Schon heute findet die Kommerzialisierung von Informationen über den Alltag, also eine wirtschaftliche Verwertung, statt. Verbraucher bemerken dies zum Beispiel immer dann, wenn ihnen im Internet wiederholt Werbung für genau jene Produkte angezeigt wird, die sie sich gerade erst oder vor ein paar Tagen angesehen haben.

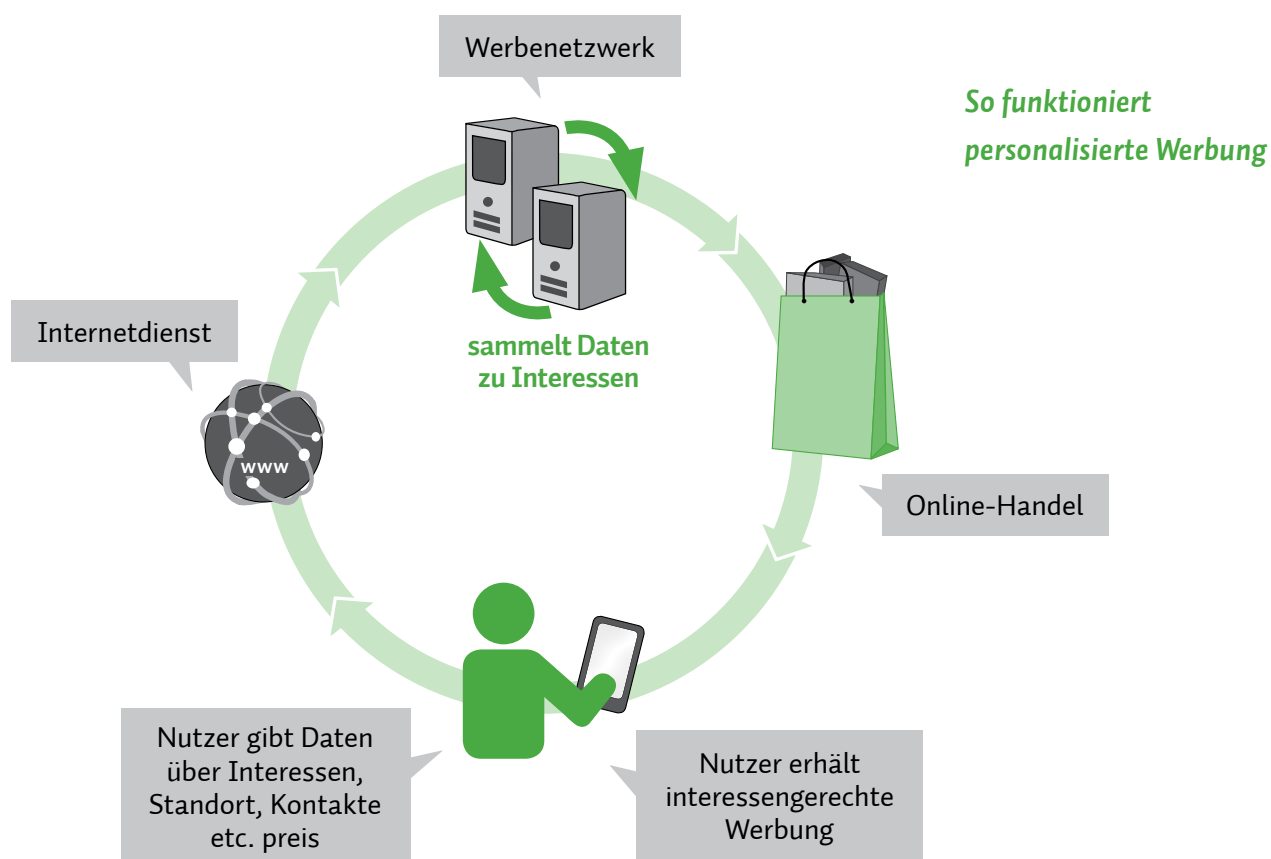
Wer hat Zugriff auf die Daten?

Grundsätzlich unterstehen personenbezogene Daten dem Datenschutzrecht. Eine Verwendung von Daten, die über den reinen Vertragszweck hinausgeht, bedarf nach deutschem und europäischem Recht in aller Regel einer gesonderten Einwilligung. Für Marketingzwecke ist die Datennutzung ohne Einwilligung gar nicht erlaubt.

Verbraucher haben sich mittlerweile schon daran gewöhnt, dass sie beim Abschluss von Verträgen mit einer ganzen Reihe von datenschutzrelevanten Erklärungen konfrontiert werden. Im Kleingedruckten verstecken sich die erforderlichen Einwilligungserklärungen, die Werbung aufgrund der nutzungs- und verhaltensabhängigen Daten aus smarten Geräten ermöglichen. Wer die Verwendung der Daten

nicht wünscht, muss ihr erst mühsam durch ein Schreiben an den Anbieter widersprechen. Verbraucher müssen bei smarten Geräten für ihren Schutz derzeit selbst sorgen, indem sie Datenschutzbestimmungen vor einem Vertragsabschluss aufmerksam prüfen und ungewollt erteilte Einwilligungen zurücknehmen.

Datenschutz bedeutet auch, dass Daten technisch vor fremdem Zugriff sicher sein müssen. In der letzten Zeit haben die vielen Einbrüche von Kriminellen und Hackern in IT-Systeme von Unternehmen weltweit gezeigt, dass Verbraucherdaten ein attraktives Angriffsziel sind. Derzeit konzentrieren sich die Angreifer noch auf Bank- und Kreditkartendaten. Smarte Systeme erfassen deutlich mehr Informationen, die auch für kriminelle Zwecke dienlich sein könnten.



Diskriminierung durch Profilbildung

Die Anhäufung von Nutzungs- und Verhaltensdaten erlaubt es Unternehmen, das Konsumverhalten von Verbrauchern in bestimmten Grenzen vorherzusagen. Grundlage für diese Vorhersagen ist eine systematische Auswertung aller gesammelten Daten. Wer im Internet ein Kinderbett bestellt, hat in Kürze sicherlich auch Bedarf an

Babynahrung. Wer am Smartphone gerne Reiseberichte über die Karibik liest, über ein geringes Einkommen verfügt und regelmäßig an der Ostsee unterwegs ist, kann vielleicht mit einer Werbung für eine Discount-Reise nach Mallorca zu begeistern sein.

Die gesammelten Daten können von Unternehmen zu Verhaltens- und Einkaufsprofilen zusammengestellt werden. Wie diese Profile im Detail erstellt werden, bleibt Verbrauchern verborgen. Die Aussagen, die aufgrund der Profile getroffen werden, können sie ebenfalls nicht beeinflussen.

Tatsächlich kann die Profilbildung nicht nur in passgenaue Werbung münden, sondern den Zugang zu bestimmten Angeboten oder Vergünstigungen erschweren. Durch niedrige Aktionspreise oder Sonderkonditionen für den Bezug von Waren und Dienstleistungen wollen Unternehmen den Absatz fördern. Durch Profilbildung können sie besser als je zuvor einschätzen, bei welchen Konsumenten eine Maßnahme zur Absatzförderung dauerhaft erfolgversprechend ist und bei welchen nicht. Nur wer das gewünschte Profil mitbringt, profitiert von günstigen Angeboten.

Informationen zur Lebensführung sind zum Beispiel auch für Versicherungen von Interesse. Allein der Kauf von Bergsteigerutensilien im Outdoor-Laden oder schlechte Fitnessdaten aus dem smarten Heimtrainer dürfen nicht die Chancen für den Abschluss beispielsweise einer günstigen Risikolebensversicherung verringern.



TIPP

Um Ihre Datenschutzrechte geltend zu machen, wenden Sie sich am besten schriftlich an den Betreiber des digitalen Dienstes.

Datenschutzrechte neu definieren

Verbraucher sollten deswegen immer wissen können, welche Daten ein Unternehmen aus smarten Geräten sammelt, wie diese verknüpft werden, wer darauf Zugriff hat und inwieweit sich dies nachteilig auswirken kann. Eine umfassende Transparenz ist derzeit noch nicht gesetzlich vorgeschrieben. Zumindest können Verbraucher ihre Datenschutzrechte auf Auskunft, Löschung und Berichtigung auch gegenüber den Sammlern von Nutzungs- und Verhaltensdaten geltend machen.

Problematisch ist aber die Tatsache, dass viele dieser Anbieter ihren Sitz im außereuropäischen Ausland haben. Für solche Dienste gelten die europäischen Regelungen nicht.

Wünschenswert wäre, dass Verbraucher immer die Möglichkeit haben, der Verwendung ihrer Daten zumindest zu widersprechen, wenn eine Nutzung für Zwecke außerhalb der reinen Vertragserfüllung erfolgen soll. Die Preisgabe sensibler Daten sollte keine notwendige Voraussetzung für den Abschluss von Verträgen sein dürfen.

3. Big Data

Hinter dem Begriff Big Data verbirgt sich, grob gefasst, die statistische Analyse extrem großer Datenmengen mittels computerbasierter Methoden. Leistungsfähige Großrechner und Datenspeicher erlauben der Wissenschaft, der Wirtschaft und der öffentlichen Verwaltung, aus einer Fülle von Einzelinformationen Aussagen über Zustände und Entwicklungen zu treffen. Die gewonnenen Erkenntnisse können als Grundlage für Entscheidungen dienen.

Die Datenquellen für Big Data sind sehr vielfältig. Das Internet dient dabei selbst als eine der Quellen, die ausgewertet werden können. Wer im Internet unterwegs ist, hinterlässt Spuren, nämlich Datenspuren. Beispiele dafür sind: Anfragen an eine Suchmaschine, Informationen zu den aufgerufenen Seiten, Nutzung von Apps, Informationen aus den Sensoren eines Smartphones. Der Trend, möglichst viele elektronische Geräte mit dem Internet zu verbinden, fördert Möglichkeiten zur massenhaften Erzeugung von verwertbaren Daten als Rohstoff für Big Data.



BIG DATA

So funktioniert Big Data



Wo spielt Big Data eine Rolle?

Die neuen Analysemethoden können überall dort zum Einsatz kommen, wo eine Vielzahl von unterschiedlichen, völlig ungeordneten Daten anfallen. In der Medizin können zum Beispiel komplexe Berechnungen zur Struktur von DNA vorgenommen werden. Die Klimaforschung kann Daten aus der weltweiten Wetterbeobachtung sammeln,

um damit Aussagen zu künftigen Entwicklungen zu treffen. Informationen aus der Beobachtung des Marktes helfen Unternehmen dabei, Entscheidungen zum Beispiel über neue Produkte, Produktionsmengen und Preise zu fällen. Die öffentliche Verwaltung profitiert für die Verkehrsplanung von der genauen Analyse der Verkehrsströme in den Städten oder auf den Autobahnen. Insbesondere die Einträge oder Nutzungsdaten von Suchmaschinen oder sozialen Netzwerken können Auskünfte zu Krankheitswellen oder zu bestimmten Bewegungen an den Finanzmärkten geben.

Noch steckt Big Data in den Kinderschuhen. Man darf jedoch davon ausgehen, dass diese Analysemethoden sehr schnell in immer mehr Bereichen zur Anwendung kommen werden.

Smarte, vernetzte Geräte und spezielle Sensoren sammeln viele Daten über ihre Umwelt. Nicht immer, aber sehr häufig sind darunter Daten, die einer bestimmten Person unmittelbar zugeordnet werden können. Die automatisierte Auswertung zum Beispiel von Suchmaschinenanfragen, Einträgen in sozialen Netzwerken oder im Adressbuch eines Smartphones sowie der Nutzungsdauer einer App stellen erhebliche Eingriffe in die Privatsphäre dar. Um aussagekräftig zu sein, benötigt Big Data aber möglichst viele Daten, die unkompliziert beschafft werden müssen.

Big Data und Datenschutz

Wer Big-Data-Methoden anwenden will, profitiert entweder von Gesetzen, die eine Auswertung bestimmter personenbezogener Daten per se erlauben, oder nutzt die Möglichkeit, Daten zu anonymisieren. Dabei werden Informationen so aufgezeichnet, dass sie keiner bestimmten Person mehr zugeordnet werden können. Sobald aber keine Anonymisierung vorgenommen wird, müssen Betroffene für die Nutzung ihrer Daten eine ausdrückliche Einwilligung geben.

Chancen und Risiken

Big-Data-Analyse erlaubt das Auffinden von Wirkzusammenhängen, die mit den herkömmlichen Mitteln bislang nicht oder nur mit Mühe erkannt werden konnten. Dazu kommt, dass Daten aufgrund moderner Technik in Echtzeit, also ohne große Verzögerung, ausgewertet werden können. Dies erleichtert die Anwendung.

Wo die Auswertung nicht anonymisiert erfolgt, ergeben sich jedoch Gefahren für die Privatsphäre, insbesondere wenn die Daten und die daraus abgeleiteten Erkenntnisse nicht vor unberechtigtem Zugriff geschützt sind. Ein uneingeschränktes Big Data würde zu einem „Big Brother“ der totalen Überwachung im Sinne George Orwells führen.

Ein blindes Vertrauen auf die Ergebnisse aus Big-Data-Anwendungen wäre sicherlich verfehlt. Genauso nachteilig wie die Profilbildung auf den Einzelnen wirken kann, so kann auch die Auswertung von Massendaten zu fehlerhaften Schlussfolgerungen führen.



GRIPPE-TRENDS

4. Web 3.0 – das Netz wird intelligent

Computer sind beeindruckende Rechenkünstler, und ihre Leistungsfähigkeit wird sich in den nächsten Jahren noch weiter erhöhen. Doch gleichgültig wie schnell oder zuverlässig ein System funktioniert, die Rechenmaschinen arbeiten derzeit noch weitgehend unselbstständig. Sie führen nur die Befehle aus, die ihr Benutzer eingegeben hat. Computer tun sich sehr schwer damit, Zusammenhänge selbstständig zu verstehen und dann aufgrund des eigenen Verständnisses zu handeln. Wissenschaft und Wirtschaft arbeiten daran, Computertechnologie intelligenter zu machen, sodass sie ähnlich wie Menschen in der Lage sind, auf der Grundlage eigener Bewertungen zu handeln. Das Internet führt in diesem Zusammenhang als Übertragungsweg zu vielfältigen Anwendungsmöglichkeiten, wenn Maschinen und Sensoren aller Art miteinander kommunizieren. Diese Entwicklungen werden unter den Begriff Web 3.0 gefasst. Das Web 2.0, das uns als Neuerung vor allem die Mitmachmöglichkeiten der sozialen Netzwerke wie Facebook und Google+ gebracht hat, soll erweitert werden um Vernetzungsmöglichkeiten unterschiedlichster Geräte.

Alles wird vernetzt

Im Web 3.0 sollen die smarten Geräte in der Lage sein, miteinander zu „sprechen“, also Informationen auszutauschen. Der heimische smarte Herd weiß dann zum Beispiel, welche Nahrungsmittel im Kühlschrank noch verfügbar sind, wodurch Verbraucher schnell erfahren, was sie kochen können. Der intelligente Stromzähler meldet dem

Stromversorger genau, zu welchen Zeiten und in welchem Umfang ein Haushalt Strom benötigt, was den Unternehmen eine bedarfsgerechte Planung bei der Energieerzeugung ermöglicht.

Je mehr Geräte vernetzt werden und je mehr Daten sie speichern und auswerten, desto vielfältiger werden die Möglichkeiten für automatische Abläufe. Grundlage für den Informationsaustausch zwischen Maschinen, das sogenannte „Internet der Dinge“, bilden einheitliche Maschinensprachen, an denen noch gearbeitet wird.

Das Netz versteht

Computer sind keine Menschen, deswegen muss ihnen ein menschenähnliches Denken zunächst beigebracht werden. Komplexe mathematische Verfahren helfen den Maschinen, bestimmte Umweltinformationen so zu verarbeiten, dass sie zu einer menschlichen Entscheidung gelangen. Je besser solche Verfahren die uns bekannten individuellen Entscheidungsprozesse nachahmen können, desto besser lassen sich die neuen Technologien im Alltag anwenden.

Unter den Begriff semantisches Web fallen all jene Methoden, die den Maschinen unter Anwendung von Internetdaten oder -technologien zur Erzeugung von Verständnis dienen.

Anwendungsbeispiele

Die Funktionen des Web 3.0 finden schon heute vereinzelt Anwendung. Die semantische Suchmaschine WolframAlpha (www.wolframalpha.com) sucht nicht nur nach reinem Text im Internet, sondern versteht Fragen und bereitet Informationen aus dem Netz entsprechend auf. Eine Anfrage wie „Bush vs. Obama“ führt zu einer Vergleichsübersicht von zwei Präsidenten der USA.

Das Produkt Google Now des gleichnamigen Internetunternehmens verknüpft gesammelte persönliche Daten wie Termine, Suchanfragen und getätigte Einkäufe. Die Software arbeitet damit als persönlicher Assistent, der darauf hinweist, was als Nächstes zu tun ist. Google Now versucht, menschliches Verhalten vorherzusagen. Ähnlich funktioniert das Programm Siri, das auf mobilen Geräten des Unternehmens Apple zu finden ist. Die semantische Suche von Siri beantwortet Fragen durch Auswertung der persönlichen Daten und von Daten im öffentlichen Internet.



SEMANTISCHE
SUCHE

Vor allem das Autofahren soll sich im Web 3.0 durch Vernetzung revolutionieren: Der Bordcomputer erhält über das Internet Wetterdaten und warnt automatisch vor Schnee und Hagel. Auf der Autobahn melden vorausfahrende PKW per Funk starkes Bremsen, das eigene Auto warnt auf dieser Grundlage sofort vor einer Gefahr. Sobald der PKW in einen bestimmten Umkreis um das eigene Heim fährt, springt dort die Heizung an und wärmt die Wohnung vor. Am nächsten Morgen werden die beim Verlassen des Hauses versehentlich offen gelassenen Fenster geschlossen, sobald die Zündung betätigt wird. Das smarte Auto kann das Fahrverhalten der Verbraucher genau überwachen. Dies machen sich schon jetzt Versicherungen zunutze. Kunden, die sich bereit erklären, Informationen zum Fahrstil mit dem Unternehmen zu teilen, erhalten eine Kfz-Versicherung, deren Beiträge an dem aus dem Fahrverhalten konkret errechneten Risikopotenzial ausgerichtet sind.

Verbraucher dürfen sehr gespannt sein, welche weiteren Möglichkeiten mit dem Web 3.0 einhergehen.



steuert die heimische Heizung



warnt vor schlechtem Wetter



schließt Fenster



warnt vor vorausliegenden Gefahren

Das allseits vernetzte Auto von morgen

Chancen und Risiken

Das Web 3.0 soll den Alltag seiner Anwender erleichtern. Tatsächlich bergen die neuen Technologien erhebliches Potenzial, um einfache oder komplexe Alltagsprobleme besser bewältigen zu können.

Doch je mehr Tätigkeiten automatisiert ablaufen, desto höher ist die Gefahr, Einblicke und Kontrolle zu verlieren. Sicherlich muss niemand Angst haben, dass sich die Schreckensvisionen eines HAL 2000 aus dem Film „2001: Odyssee im Weltraum“ oder von Skynet aus der Terminator-Reihe bewahrheiten, in denen Maschinen ein zerstörerisches und unkontrollierbares Eigenleben entwickeln. Ein blindes Vertrauen auf Technik wird aber in den seltensten Anwendungsfällen möglich sein. Vor allem die Probleme um den Datenschutz und die technische Datensicherheit erfordern eine dauerhafte Überwachung jener Geräte und Methoden, die uns und unser Handeln überwachen wollen. ||

Glossar



3G-Modul/4G-Modul: Unter diesem Begriff versteht man die eingebaute Funktionalität von mobilen Endgeräten wie Smartphones oder Tablets, die es erlaubt, über das Mobilfunknetz eine Internetverbindung herzustellen. Möchte man diese Funktion nutzen, sollte man vor dem Kauf darauf achten, ob das Gerät entsprechend ausgerüstet ist.



Modul 1:
„INTERNET ÜBER DAS
MOBILFUNKNETZ“

Bluetooth: Unter diesem Begriff versteht man einen Standard zur Datenübertragung per Funktechnik. Per Bluetooth lassen sich beispielsweise Daten wie Bilder von einem Smartphone oder Handy zu einem anderen übertragen.



Bluetooth

Datenpaket: Unter einem Datenpaket versteht man, vereinfacht gesagt, einen Teil eines Datenstroms, also eine konkrete Dateneinheit, die beispielsweise über das Internet versendet wird.

Drosselung: Unter einer Drosselung versteht man das Vorgehen meistens eines Internet- und Telefonanbieters, die Geschwindigkeit der Datenübertragung auf technischem Wege zu verringern, also die Bandbreite einzuschränken. Dies passiert meist, wenn man ein bestimmtes Datenvolumen ausgeschöpft hat.



Modul 1:
„FLATRATES UND
VOLUNTARIFE“

GPS: Die Abkürzung GPS steht für Global Positioning System und bezeichnet ein Navigationssystem, das mithilfe von Satelliten den Standort eines Teilnehmers auf einige Meter genau bestimmen kann. GPS findet man in vielen Auto-Navigationssystemen, aber zunehmend auch in Smartphones und anderen mobilen Endgeräten.



GPS (Android)

iTunes: iTunes ist ein Verwaltungsprogramm der Firma Apple, mit dem Mediendateien wie Musikstücke, Hörbücher, Filme etc. gekauft, organisiert und wiedergegeben werden können.



Ortungsdienste
(Apple iOS)



Silver Surfer – Lernbuch :
„QR-CODES“

QR-Code: Die Abkürzung QR steht für Quick Response, zu Deutsch schnelle Antwort. Bezeichnet werden damit Grafiken aus schwarzen und weißen Punkten, die es ermöglichen, Daten darzustellen. Mit einem entsprechenden Programm für mobile Endgeräte kann man über die eingebaute Kamera des Geräts diese Codes scannen und erhält die hinterlegten Informationen. Man kennt QR-Codes von Paketsendungen, Bahnreisen, aber auch von Plakaten in der Stadt.

Roaming: Vereinfacht versteht man unter Roaming – englisch für „herumwandern“ oder „streunen“ – die Fähigkeit von Mobilfunkteilnehmern, sich beispielsweise auch im Ausland in Netze einzuwählen und Dienste zu nutzen, also zum Beispiel Anrufe zu tätigen und zu empfangen. Roaming im Ausland kann mit hohen Kosten verbunden sein. Es lohnt sich daher, sich vorher zu informieren.

Router: Ein Router – zu Deutsch Verteiler – übernimmt im Netzwerk die Funktion, eine Internetverbindung auf mehrere Rechner zu verteilen und so für alle sich im Netzwerk befindlichen Computer und Geräte einen Zugang zum Internet zu ermöglichen.

Update: Bei einem Update wird ein Programm auf den aktuellen Stand gebracht. Hierfür muss in den meisten Fällen das Programm selbst mittels einer Internetverbindung auf einen Rechner der Herstellerfirma zugreifen können, um die Programmversionen abgleichen und gegebenenfalls aktualisieren zu können.



Wi-Fi: Dieser Kunstbegriff wird in Deutschland oft synonym zum Begriff WLAN, zu Deutsch: drahtloses lokales Netzwerk, genutzt, obwohl die beiden Wörter streng genommen nicht das gleiche bedeuten. Oft sieht man das Wi-Fi-Logo oder zumindest den Begriff an Türen von Cafés oder Hotels, die ihren Gästen die Internetnutzung über ein drahtloses Netzwerk ermöglichen.

Stichwortverzeichnis

A

Apps 16
- Datenschutztipps 24

B

Bandbreite 11 f.
Big Data 35

C

Cloud 17

D

Datenschutz 20 ff., 32 ff.
DSL 11

E

E-Wallet 27

F

Flatrate 9

H

Hotspot 14
Heimnetzwerk 6, 11

I

In-App-Kauf 16

K

Kabelanschluss 11

M

Mobile Payment 25
- Sicherheit 28
mobiles Bezahlen 25
Mobilfunknetz
- Internet über das
Mobilfunknetz 7
Mobilfunkstandard 8

N

NFC 26

P

Profilbildung 33

R

Router 12

S

Smart-Brille 30
Smarthome 31
Smart-Kamera 31
Smartphone 30
- App 16
- Betriebssysteme 15
- Datenschutztipps 24
- im Ausland 10
- Sicherheit 23
- Tarife 9
Smart-TV 30
Smartwatch 30

T

Tablet 30

V

Verbraucherschutz 31
Verschlüsseln von Daten 19
Volumentarif 9

W

Web 3.0 37
Wi-Fi 14
WLAN 13

Autoren



Helmut Eiermann leitet beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz den Bereich Technik. Zu seinen Aufgaben gehören die Kontrolle und Beratung in Fragen des technischen Datenschutzes und der Datensicherheit. Vor seiner Arbeit für den Datenschutzbeauftragten war er in der Bundesverwaltung in den Bereichen Systembetrieb, Systemadministration und Anwendungsentwicklung tätig.



Christian Gollner ist Jurist bei der Verbraucherzentrale Rheinland-Pfalz. Nach seinem Rechtsreferendariat war er unter anderem als Referent für Telekommunikation bei der Verbraucherzentrale Baden-Württemberg beschäftigt. Ein Schwerpunkt seiner Tätigkeit als Rechtsreferent liegt auf dem Datenschutzrecht.



Florian Preßmar arbeitet als Referent für Offene Kanäle und Medienkompetenz bei der Landeszentrale für Medien und Kommunikation und koordiniert das MedienKompetenzNetzwerk Mainz-Rheinhessen. Im Rahmen seiner Promotion an der Johannes Gutenberg-Universität Mainz entwickelte er gemeinsam mit der Verbraucherzentrale Rheinland-Pfalz die Silver-Surfer-Seminarreihe.



Barbara Steinhöfel arbeitet bei der Verbraucherzentrale Rheinland-Pfalz als Referentin für Telekommunikation und Medien. Zu ihren Aufgaben gehört die Aufklärung und Information zu Fragen im Bereich Telekommunikation und Medien. Vor der Übernahme des Referats arbeitete sie in der allgemeinen Rechtsberatung der Verbraucherzentrale Rheinland-Pfalz.



Jeanine Wein ist Geschäftsführerin von alles mit Medien, einer Agentur für Bildungsmedien. Als Germanistin und Linguistin unterrichtet sie an der Georg-August-Universität Göttingen. Seit mehreren Jahren gibt sie Silver-Surfer-Kurse in Rheinland-Pfalz, unter anderem am Zentrum für wissenschaftliche Weiterbildung der Johannes Gutenberg-Universität Mainz.

Titel:

Silver Surfer – SICHER ONLINE IM ALTER
Mobiles Internet & Smart-Technologien

Autoren:

Helmut Eiermann, Leiter des Bereichs Technik beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz; Christian Gollner, Verbraucherzentrale Rheinland-Pfalz e.V.; Florian Preßmar, MedienKompetenzNetzwerk Mainz-Rheinhessen/Landeszentrale für Medien und Kommunikation Rheinland-Pfalz; Barbara Steinhöfel, Verbraucherzentrale Rheinland-Pfalz e.V.; Jeanine Wein, alles mit Medien

Lektorat, Korrektorat, Gestaltung, Satz:

alles mit Medien

Anke Enders & Jeanine Wein GbR
Simrockstraße 16 b
65187 Wiesbaden
www.allesmitmedien.de

Druck:

NINO Druck GmbH, Neustadt/Wstr.

1. Auflage Mai 2014

Bildnachweis:

Renate Pepper: creative pictures – Lamberz
Titelbild: Florian Preßmar

Kooperationspartner:

Dieses Lernmaterial wurde gemeinsam von der Landeszentrale für Medien und Kommunikation Rheinland-Pfalz, dem MedienKompetenzNetzwerk Mainz-Rheinhessen und der Verbraucherzentrale Rheinland-Pfalz e.V. erstellt. Gefördert wurde das Projekt durch das Ministerium der Justiz und für Verbraucherschutz Rheinland-Pfalz. Wir danken dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz für die Mitwirkung. Für die landesweite Umsetzung der Seminarreihe danken wir dem Verband der Volkshochschulen von Rheinland-Pfalz e.V.

Herausgeber:

Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz
Turmstraße 10
67059 Ludwigshafen
www.lmk-online.de

Verbraucherzentrale Rheinland-Pfalz e.V.

Seppel-Glückert-Passage 10
55116 Mainz
www.vz-rlp.de

Bezugsadressen:

Verbraucherzentrale Rheinland-Pfalz e.V.
Seppel-Glückert-Passage 10
55116 Mainz
06131.28480
versand@vz-rlp.de

MedienKompetenzNetzwerk Mainz-Rheinhessen

Wallstraße 11
55122 Mainz
06131.279673
pressmar@mkn-online.de

Dieses Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung bedarf der vorherigen Zustimmung der Verbraucherzentrale Rheinland-Pfalz und der Landeszentrale für Medien und Kommunikation Rheinland-Pfalz. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmung und die Einspeicherung und Verarbeitung in elektronischen Systemen. Die Broschüre darf ohne Genehmigung der Verbraucherzentrale Rheinland-Pfalz und der Landeszentrale für Medien und Kommunikation Rheinland-Pfalz auch nicht mit (Werbe-)Aufklebern o. Ä. versehen werden. Die Verwendung dieses Werkes durch Dritte darf nicht zu absatzfördernden Zwecken geschehen oder den Eindruck einer Zusammenarbeit mit der Verbraucherzentrale Rheinland-Pfalz oder der Landeszentrale für Medien und Kommunikation Rheinland-Pfalz erwecken. Die auszugsweise Wiedergabe für wissenschaftliche und schulische Zwecke ist mit Quellenangabe gestattet. Es wird darauf hingewiesen, dass alle Angaben trotz sorgfältiger Bearbeitung ohne Gewähr erfolgen und eine Haftung der Autorinnen und Autoren ausgeschlossen wird. Trotz sorgfältiger inhaltlicher Kontrolle übernehmen wir keine Haftung für die Inhalte externer Links. Für den Inhalt der verlinkten Seiten sind ausschließlich deren Betreiber verantwortlich.

www.silversurfer-rlp.de

gefördert durch:

