DATENSCHUTZ IM INTERNET

HÄUFIG GESTELLTE FRAGEN

Der Schutz der persönlichen Daten gilt als ein hohes Gut der informationellen Selbstbestimmung. Das Bundesverfassungsgericht spricht sogar von einem Datenschutz-Grundrecht. Wem wir welche unserer Daten anvertrauen, was damit geschieht und welche Kontrolle wir über sie behalten, ist entscheidend für unser Vertrauen gegenüber privaten und staatlichen Diensten und Anbietern auch im Internet.

Beim Einkaufen oder bei Bankgeschäften im Internet aber auch bei der Nutzung von Chats, Sozialen Netzwerken oder beim Versenden von E-Mails geben wir persönliche Daten an private Anbieter weiter und wollen diese vor einem unberechtigten Zugriff geschützt wissen.

Zugleich hinterlassen wir, wenn wir mit dem Smartphone, dem Tablet oder dem Notebook online unterwegs sind, unbewusst Daten, die eine personenbezogene Aussage über unseren Standort, unsere Interessen oder unser Kauf- und Nutzungsverhalten gestatten.

Um persönliche Daten vor Missbrauch zu schützen, bedarf es durchsetzungsfähige rechtliche Rahmenbedingungen, modernste technische Sicherheitsvorkehrungen und natürlich auch eine hohe Eigenverantwortung der Nutzer. Die Politik, die Anbieter und Dienste aber auch der Nutzer selbst sind gefordert, wenn dies gelingen soll. Eine vollständige Sicherheit ist natürlich auch hier wie in keinem Lebensbereich garantiert.

Welche rechtlichen Vorgaben setzt die Politik im Datenschutz und was muss ich selber beachten? Welche Institutionen sind wann gefordert: Der Datenschutzbeauftragte oder das Europäische Parlament? Welche technischen Schutzmöglichkeiten stehen überhaupt zur Verfügung und wie funktionieren sie? Das sind einfache Fragen, die sich jeder, der das Internet nutzt, stellen muss. Die Fakten sind aber nicht immer so einfach, sondern oft kompliziert und komplex: Phishing, Tracking, save harbor, wpa und https?

Unsere Broschüre greift die häufig gestellten Fragen zum Datenschutz im Internet auf und bietet kurze und verständliche Antworten. Sie richtet sich weniger an die Fachleute als viel mehr an die, denen die politischen, rechtlichen und technischen Zusammenhänge noch nicht so vertraut sind.

Im Auftrag der Konrad-Adenauer-Stiftung herausgegeben von Tobias Wangermann

Erarbeitet von Stefan Gehrke (buero fuer neues denken) sowie Frank Bergmann, Matthias Bunk, Michael Sieben und Daphne Wolter.

Konrad-Adenauer-Stiftung, Berlin 2014

ISBN 978-3-95721-048-7

www.kas.de

Konrad Adenauer Stiftung

Die Verordnung bringt vor allem neue Rechte für die Nutzer und erlegt den Unternehmen neue Pflichten auf. Wobei EU-Unternehmen die neuen Datenschutzstandards auch als Geschäftsvorteil nutzen können.

Erklärtes Ziel der Europäischen Kommission ist es, die Datenschutzregelungen in Europa zu harmonisieren. Die gesetzlichen Regeln für den Datenmarkt in Europa stammen aus dem Jahr 1995. Google, Facebook etc. gab es da noch nicht, das Online-Shopping steckte noch in den Kinderschuhen. So verstand man damals unter Datenschutz lediglich den Schutz der Angestellten vor den Vorgesetzten und den der Bürger vor dem Staat. Heute kommt der kommerzielle Aspekt (Unternehmen – Kunde) als entscheidender Faktor hinzu. Ein gemeinsames europäisches Datenschutzrecht ist ein Standortvorteil im Wettbewerb um die digitalen Märkte. Für die Wirtschaft ist ein gemeinsamer Standard, wenn schon nicht weltweit, dann wenigstens auf europäischer Ebene, sehr wichtig.

Mehr Kontrolle über Datenrechte

Ein in ganz Europa einheitlicher und hoher Datenschutzstandard stärkt das Vertrauen der Konsumenten in europäische Dienstleistungen besonders im Informationsbereich. Die EU hat es sich in der Datenschutzreform insbesondere zum Ziel gesetzt, gleiche Wettbewerbsbedingungen zwischen den vor allem in den USA beheimateten Internetunternehmen, deren Geschäftsmodell maßgeblich von der Verarbeitung personenbezogener Daten abhängig ist, und den EU-Unternehmen zu schaffen. Der Anwendungsbereich der EU-Datenschutzverordnung (DSVO) sieht vor, dass Internet-Nutzer in Zukunft mehr Kontrolle über ihre privaten Daten im Netz bekommen. Auch internationale Unternehmen wie Facebook und Google sollen sich zukünftig zwingend an das europäisches Datenschutzrecht halten müssen, sobald sie ihre Angebote auch EU-Bürgern anbieten. Die Absicherung der Daten aller europäischen Bürger wäre damit gewährleistet.

Während das EU-Parlament inzwischen einen Verordnungsentwurf beschlossen hat, ist bei den Verhandlungen der Mitgliedsstaaten noch kein Kompromiss in Sicht. Die Bundesregierung befürchtet unter anderem, dass der aktuelle hohe deutsche Standard im Datenschutz nicht in allen Bereichen gehalten werden könne.

…des Bundes und der Länder?

Die Kontrolle und Überwachung der Einhaltung der Datenschutzgesetze gehören zu den zentralen Aufgabe der Datenschutzbehörden, die es sowohl auf Bundes- als auch auf Länderebene gibt. Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) ist zuständig für

- die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch öffentliche Stellen des Bundes
- die Einhaltung des Datenschutzes auf Bundesebene von öffentlichen (z. B. Behörden) und
- nicht-öffentlichen (z. B. Unternehmen, Vereine, Restaurants, Kanzleien, …) Stellen.

Zudem hat jedes Bundesland einen eigenen Datenschutzbeauftragten. Dieser ist jeweils für die Einhaltung des Datenschutzes für öffentliche und nicht-öffentliche Stellen auf Landesebene zuständig.

Recht auf Anrufung

Jedermann kann sich an die BfDI wenden, wenn man der Auffassung ist, dass öffentlichen und nicht-öffentlichen Stellen sein Persönlichkeitsrecht beziehungsweise sein Recht auf Informationszugang nicht hinreichend beachtet haben. Wer meint, durch

den Umgang mit seinen Daten seitens einer nicht-öffentlichen Stelle in seinen Rechten verletzt worden zu sein, kann sich an die

Aufsichtsbehörde des jeweiligen Landes wenden.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Dieses Gremium beschäftigt sich mit aktuellen Fragen des Datenschutzes in Deutschland und nimmt zu ihnen Stellung. Die Beschlüsse und Entschließungen der Konferenz sind rechtlich zwar nicht bindend, haben jedoch auf Grund der fachlichen Kompetenz der Konferenzteilnehmer auch faktische Auswirkungen auf die Entwicklung des Datenschutzes in Deutschland.

Der Düsseldorfer Kreis dient seit 2013 als Gremium in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder der Kommunikation, Kooperation und Koordinierung der Aufsichtsbehörden im nicht-öffentlichen Bereich und setzt sich u.a. mit dem Themen Datenschutz in sozialen Netzwerken und Online-Werbung auseinander.

TIPP:

Beschluss des Düsseldorfer Kreises zum Datenschutz in sozialen Netzwerken:
http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/08122011DSInSozialenNetzwerken.html?nn=409242

Welche Vorteile bringt die Europ. Datenschutzverordnung?

Welche Kompetenzen haben die Datenschutzbeauftragten…

… zwischen der EU und den USA und wie datensicher ist die Anwendung in der Praxis?

Als „Safe Harbor" (englisch für „sicherer Hafen") wird eine Vereinbarung zwischen der Europäischen Union und den USA aus dem Jahr 2000 bezeichnet. Darin geht es um die Übermittlung von personenbezogenen Daten – also zum Beispiel Namen, Telefonnummern und Kundendaten – durch europäische Unternehmen an US-amerikanische Unternehmen und Organisationen.

Eigentlich verbietet die Europäische Datenschutzrichtlinie, Daten an Nicht-EU-Länder zu übermitteln, die über keine dem EU-Recht vergleichbare Datenschutzstandards verfügen. Im Fall der USA hat man jedoch eine Sonderregelung getroffen – nicht zuletzt deshalb, weil Amerika für die Europäische Union einer der wichtigsten Handelspartner ist. Gemäß der Safe Harbor-Vereinbarung müssen sich US-amerikanische Abnehmer von Daten allerdings verpflichten, *bestimmte Prinzipien* einzuhalten, etwa die Daten vor Missbrauch zu schützen und die Betroffenen über die Erhebung und Weitergabe von Informationen zu benachrichtigen. Tun sie dies nicht, können sie von US-Gerichten zu Geldbußen verurteilt werden.

Europäisches Parlament fordert Aussetzung des Abkommens

In der Vergangenheit ist die Zahl von Unternehmen, die sich zu den Safe Harbor-Prinzipien bekennen, kontinuierlich gestiegen. Gleichzeitig wurde aber auch zunehmend Kritik an der Vereinbarung laut: So hat eine Studie aus dem Jahre 2008 ergeben, dass viele amerikanische Unternehmen die Prinzipien nicht oder nur unzureichend erfüllen. Bisher ist es jedoch nicht möglich, diese Unternehmen vor einem europäischen Gericht zu belangen. Im Zuge der NSA-Affäre wurde außerdem deutlich, dass amerikanische Behörden europäische Datenschutzregelungen sogar bewusst verletzt haben.

Das Europäische Parlament hat daher im März 2014 mit deutlicher Mehrheit gefordert, die Safe-Harbor-Vereinbarung einstweilen auszusetzen. Die Europäische Kommission hat bereits reagiert und den USA ein Ultimatum gestellt: Bis zum Sommer 2014 soll Safe Harbor nachgebessert werden – sonst droht dem vermeintlich „sicheren Hafen" die Blockade.

TIPP:

Ausführliche Informationen des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit:
http://www.bfdi.bund.de/DE/EuropaUndInternationales/Art29Gruppe/Artikel/SafeHarbor.html?nn=409532

Liste des US-Handelsministeriums zu US-Unternehmen, die sich zu den Safe-Harbor-Prinzipien bekennen:
http://safeharbor.export.gov/list.aspx

… ohne die Durchleitung durch Amerika („Schengen-Netz") sinnvoll und sicherer?

Die Enthüllungen der britischen Tageszeitung „The Guardian" und der amerikanischen „Washington Post" über die anlasslose Überwachung der weltweiten digitalen Kommunikation durch die sogenannten „Five Eyes" haben eine Debatte über ein „Schengen-Netz" angeregt.

Internetdaten sollen dabei den „Schengen-Raum" nicht verlassen, wenn Start- und Zielrechner sich auf dem Gebiet befinden, in dem Personen in Europa ohne Grenzkontrollen reisen können. Auch wenn der konkrete Umfang der Überwachung durch die Geheimdienste der fünf Länder („Five Eyes") USA, Kanada, Großbritannien, Australien und Neuseeland noch im Dunkeln liegt, verspricht man sich von einem innereuropäischen Datenverkehr einen größeren Schutz vor Spionage.

Internetdaten orientieren sich nicht an nationalen Grenzen

Das Internet ist ein globaler Verbund aus verschiedenen Teilnetzen, die sich nicht an nationalen Grenzen orientieren. Nach einer Untersuchung des Instituts für Internet-Sicherheit nehmen derzeit unter 20 Prozent der Verbindungen im Schengen-Raum ihren Weg außerhalb dieser Grenzen, weil die Verbindung kürzer oder wirtschaftlicher ist. Tatsächlich kann man das jedoch kaum feststellen: Telekommunikationsunternehmen agieren global, so dass es schwerfällt zu definieren, wann ein Kommunikationsvorgang „deutsch" oder „europäisch" ist. Ein Webserver mit der Endung „.de" kann beispielsweise in den USA oder Großbritannien stehen. Für sie ist es nahezu unmöglich, rein europäischen Netzverkehr zu erzeugen. Sichtbar und unsichtbar enthalten deutsche Websites häufig Verbindungen zu Servern außerhalb des Schengen-Raums.

Experten der Internet-Branchenverbände sehen daher kaum einen Nutzen in einem Datenverkehr, der auf 26 Staaten in Europa beschränkt würde. Einige halten dies sogar für schädlich, da eine trügerische Sicherheit vermittelt werde. Die Außengrenzen dieses Schengen-Netzes könnten im Gegensatz zu echten Grenzen nicht kontrolliert werden. Andernfalls würde die Freiheit im Netz zerstört, die man mit einem Schengen-Netz doch sichern wollte. Einen besseren Schutz bietet der Einsatz von Verschlüsselungstechniken.

…an Behörden weitergeben?

Wenn es um den Schutz der öffentlichen Sicherheit geht, müssen Unternehmen Informationen über ihre Kunden an den Staat weitergeben. Die gesetzliche Grundlage hierfür bildet das Telekommunikationsgesetz. Es legt unter anderem fest, unter welchen Bedingungen Telefonanbieter in Deutschland *Bestandsdaten* an Polizei, Ermittlungsbehörden und Geheimdienste weitergeben müssen. Bestandsdaten sind Daten, die ein Telefonanbieter über einen Kunden erhebt. Dazu gehören der Name, das Geburtsdatum und die Adresse, aber auch PINs und Passwörter.

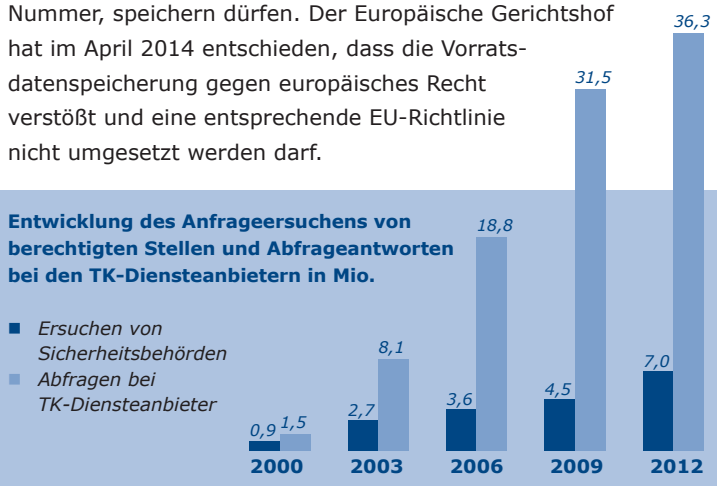
Gesetzesänderung erlaubt Identifizierung per IP-Adresse

Um diese Bestandsdaten geht es in der Änderung des *Telekommunikationsgesetzes* vom 1. Juli 2013. Das neue Gesetz legt fest, dass nun auch dynamische IP-Adressen, also individuelle IP-Adressen, die bei jeder Verbindung mit dem Netz neu zugewiesen werden, weitergegeben werden können. Damit ist es möglich, die Identität von Internetnutzern festzustellen. Hierzu brauchen die Ermittler in der Regel die Genehmigung eines Richters (Richtervorbehalt). Unternehmen mit mehr als 100.000 Kunden müssen Daten auch automatisiert mit Hilfe einer elektronischen Schnittstelle übermitteln können. Die Abfrage von Bestandsdaten ist außerdem nicht nur bei Straftaten möglich, sondern auch bei Ordnungswidrigkeiten. Gerade der letzte Punkt ist unter Datenschützern umstritten. Kritiker des Gesetzes befürchten, dass dadurch die Rechte der Sicherheitsorgane gegenüber dem Bürger unverhältnismäßig gestärkt und private Daten unschuldiger Personen an staatliche Behörden weitergegeben werden.

Vorratsdatenspeicherung ist verboten

Heftig diskutiert wird auch über die Vorratsspeicherung. Hierbei geht es um die Frage, ob staatliche Stellen *Verkehrsdaten*, also Informationen zur Dauer eines Telefonats oder der angerufenen Nummer, speichern dürfen. Der Europäische Gerichtshof hat im April 2014 entschieden, dass die Vorratsdatenspeicherung gegen europäisches Recht verstößt und eine entsprechende EU-Richtlinie nicht umgesetzt werden darf.

Entwicklung des Anfrageersuchens von berechtigten Stellen und Abfrageantworten bei den TK-Diensteanbietern in Mio.



Quelle: Bundesnetzagentur, Tätigkeitsbericht Telekommunikation 2012/13, S. 266.

…von wem weitergegeben werden?

Im Zeitalter der digitalen Vernetzung sind persönliche Daten zu einer neuen Währung geworden. Mit ihrer Hilfe können Unternehmen individuelle Nutzerprofile erstellen und ihre Produkte zielgerichtet an den Verbraucher bringen. Die Weitergabe von Daten ist daher ein viel diskutiertes Thema. Grundsätzlich gilt: Unternehmen dürfen Kundendaten erheben und weitergeben, wenn diese zur Erfüllung des Vertrags dienen. So darf beispielsweise ein Reisebüro Informationen über einen Kunden an eine Fluggesellschaft übermitteln, solange die Daten nur zur Buchung eines bestimmten Fluges verwendet werden.

Darüber hinaus finden sich meist in den Allgemeinen Geschäftsbedingungen (AGB) Bestimmungen zur Weitergabe von Daten. Viele Unternehmen lassen sich zusichern, dass sie dem Nutzer Werbung für ihre Angebote schicken dürfen. Das sogenannte Listenprivileg erlaubt es einem Anbieter außerdem, ganze Kataloge personenbezogener Daten an Dritte zu verkaufen. Diese Daten können Angaben wie den Namen, die Adresse oder das Geburtsdatum einer Person, aber auch die Zuordnung zu einer bestimmten Gruppe (zum Beispiel: „kauft gerne Bücher zum Thema Datenschutz") beinhalten.

Auch Meldeämter dürfen Daten weitergeben

Es gibt auch noch einen anderen Weg für Unternehmen, an Daten zu gelangen. In Deutschland ist jeder Bürger verpflichtet, sich bei den zuständigen Bezirksämtern in das sogenannte Melderegister einzutragen. Die Meldeämter dürfen die gespeicherten Daten auch ohne ausdrückliche Erlaubnis des Betroffenen weitergeben, zum Beispiel an einen Adresshändler. Der Bürger kann jedoch gegen die Weitergabe seiner Daten Einspruch einlegen *(Opt-out-Lösung)*. Hierzu bietet der Bundesverband der Verbraucherzentralen einen Musterbrief an. Mit dem 1. Mai 2015 wird sich diese Praxis ändern. Dann tritt das neue *Bundesmeldegesetz* in Kraft. Es soll die verschiedenen Landesmeldegesetze ablösen und das deutsche Melderecht harmonisieren. Registerauskünfte, die der Werbung und dem Handel mit Adressen dienen, sind dann nur noch mit Einwilligung der betroffenen Person möglich *(Opt-in-Lösung)*.

TIPP:

- *Informationsseite des Verbraucherzentrale Bundesverband zur Datenweitergabe:* **https://www.surfer-haben-rechte.de/cps/rde/xchg/digitalrechte/hs.xsl/datenschutz.htm#tba1995**
- *Hilfe zur Anforderung einer Selbstauskunft:* **https://selbstauskunft.net/**
- *Informationen rund um das neue Bundesmeldegesetz:* **http://www.bmi.bund.de/DE/Themen/Moderne-Verwaltung/Verwaltungsrecht/Meldewesen/Bundesmeldegesetz/bundesmeldegesetz_node.html**

… von Daten haben?

Identitätsdiebstal ist Betrug. Sollte ein Fremder Ihre Daten benutzen, um auf Ihre Rechnung im Internet einzukaufen oder Dienstleistungen in Anspruch zu nehmen, sollten Sie umgehend die entsprechenden Konten sperren lassen und bei der Polizei Anzeige wegen Identitätsdiebstahl erstatten. Wiederholen Sie diese Anzeige in jedem einzelnen Fall. Dokumentieren Sie jeden Fall möglichst genau und nehmen Sie Kontakt mit einem spezialisierten Anwalt auf. Er kann Ihnen auch helfen, die Forderungen, die Ihnen gegenüber erhoben werden, abzuwenden. Das gilt auch mit Blick auf die weiteren Konsequenzen (Schufa etc.). Drängen Sie außerdem darauf, dass bei den Dienstleistern und Händlern die falschen Daten über Sie gemäß § 35 des Bundesdatenschutzgesetzes (BDSG) umgehend gelöscht werden. Die Unternehmen sind außerdem verpflichtet, Ihnen darüber einen Beleg innerhalb einer 14-tägigen Frist zukommen zu lassen.

Schadenshaftung beim Online-Banking

Auch beim Online-Banking gibt es gesetzliche Regelungen, durch die Sie als Verbraucher zumindest teilweise geschützt sind. Entsteht Ihnen hier durch den Missbrauch Ihrer Daten ein Schaden und Ihnen ist nicht grobe Fahrlässigkeit nachzuweisen, haften Sie nur in einer Höhe von 150 Euro Selbstbeteiligung. Im Rahmen der Anpassung an die SEPA-Richtlinien regeln seit 2009 §675c bis §676c des Bürgerlichen Gesetzbuches (BGB) die Normen der Zahlungsdienste. Diese sehen in dieser Situation die Banken für den verbleibenden Schadensbetrag in der Haftung. Grobe Fahrlässigkeit kann vorliegen, wenn Sie die Sicherheitshinweise, die Ihnen Ihre Bank gibt, nicht beachten. Geben Sie beispielsweise, durch eine E-Mail aufgefordert, gleich mehrere TAN-Nummern auf einer gefälschten Bankwebseite an, kann die Bank sich auf Ihre Sicherheitshinweise berufen und Sie für den Schaden haftbar machen.

Sorgfaltspflicht beachten

Die Rechtsprechung zeigt, dass die Grenze zwischen Fahrlässigkeit und grober Fahrlässigkeit bedeutsam für die Haftungszuweisung ist. Informieren Sie sich daher regelmäßig über die aktuellen Sicherheitshinweise, die Ihre Bank oder andere Dienstleister im Internet (z.B. auch Auktionsplattformen) Ihnen zur Verfügung stellen. Ähnlich wie beim Verlust der Kreditkarte ist eine schnelle Meldung und damit Sperrung Ihres Kontos wichtig, um auch hier Ihrer Sorgfaltspflicht nachzukommen.

TIPP:

Wertvolle Hinweise für den sicheren Umgang mit den eigenen Daten im Internet können die Seiten des Bundesamtes für Sicherheit in der Informationstechnik **(http://www.bsi.de)** *und der Aktion „klicksafe" (***http://www.klicksafe.de***) geben.*

Welche rechtlichen Konsequenzen kann der Missbrauch …

… zum Datenschutz?

Bislang elf Bundesländer und der Bund gewähren Bürgern allgemein und ohne Voraussetzung Akteneinsicht bei öffentlichen Verwaltungen. Dieses Recht wird üblicherweise als Informationsfreiheit bezeichnet. Es ist kein Grundrecht, da Artikel 5 des Grundgesetzes (GG) nur Zugang zu allgemein zugänglichen Informationen garantiert. Auf Bundesebene trat das Informationsfreiheitsgesetz am 01.01.2006 in Kraft.

Datenschutz ist Grundrecht

Das Recht auf informationelle Selbstbestimmung leitet sich aus Artikel 2 GG ab. Das Bundesverfassungsgericht sieht die freie Entfaltung der Persönlichkeit unter den Bedingungen der Informationsgesellschaft bedroht, wenn kein Schutz gegen unbegrenzte Speicherung und Verwendung persönlichen Daten besteht.

Freiheitlich-demokratisches Gemeinwesen braucht Informationen

Staat, Wirtschaft und Gesellschaft sind in der Informationsgesellschaft stärker aufeinander angewiesen. Öffentliche Kontrolle

findet nicht nur durch Parlamente, Rechnungshöfe und Medien, sondern auch durch den Bürger selbst statt: Die Bürgergesellschaft braucht Verwaltungsinformationen. Sie sind für das Funktionieren des demokratischen Gemeinwesens notwendig.

Zwei Säulen der Informationsgesellschaft

Datenschutz und Informationsfreiheit werden oft als zwei Säulen der Informationsgesellschaft bezeichnet. Zum Ausdruck kommt dies dadurch, dass der Bundesbeauftragte für den Datenschutz auch für die Informationsfreiheit zuständig ist. Obwohl beide Bereiche von einer Person wahrgenommen werden, bestehen naturgemäß Konflikte zwischen Datenschutz und Informationsfreiheit. Das Grundrecht auf informationelle Selbstbestimmung schützt gerade den, der intensiv kommuniziert und agiert. Er braucht diesen Schutz in der Informationsgesellschaft ganz besonders. Diesem sind dort Grenzen gesetzt, wo das Interesse der Allgemeinheit die Preisgabe und Nutzung auch personenbezogener Daten erforderlich macht.

Wird das Gebot der Datensparsamkeit beachtet, d.h. nur die notwendigen Daten zu erheben und zu speichern, können Widersprüche zwischen den beiden Säulen von Beginn an reduziert werden.

Steht das Informationsfreiheitsgesetz im Widerspruch …

Wie funktioniert Verschlüsselung?

Bei der Verschlüsselung wird ein lesbarer Text (Klartext) durch ein Verschlüsselungsverfahren in einen unlesbaren Text (Geheimtext) umgewandelt. Das Verfahren zur Verschlüsselung besteht aus einem Schlüssel und einer Regel (Chiffre). Durch Anwendung des Schlüssels auf den Klartext gemäß der Regel entsteht die verschlüsselte Botschaft, der Geheimtext. Hinzu kommt eine weitere Regel, um die verschlüsselte Botschaft mit dem Schlüssel wieder zu entschlüsseln. Wichtig ist dabei, dass die Verschlüsselung und Entschlüsselung von Informationen einfach ist, wenn der Schlüssel bekannt ist. Anders herum soll ohne Kenntnis des Schlüssels eine Entschlüsselung auch dann praktisch unmöglich sein, wenn der Angreifer über beträchtliche Mittel verfügt und das Verfahren kennt.

Man unterscheidet zwischen symmetrischer und asymmetrischer Verschlüsselung. Beim symmetrischen Verfahren werden Ver- und Entschlüsselung mit dem gleichen Schlüssel vorgenommen. Es muss also zuvor ein geheimer Schlüssel vereinbart und geheim gehalten werden. Dagegen gibt es bei der asymmetrischen Verschlüsselung zwei Schlüssel: einen öffentlichen, für jeden zugänglich, sowie einen privaten Schlüssel, der verborgen bleiben muss. Die Information wird mit dem öffentlichen Schlüssel verschlüsselt und kann nur mit dem privaten wieder entschlüsselt werden.

Bei der Wahl eines Verfahrens oder einer Software zur Verschlüsselung spielt Vertrauen eine große Rolle. Ein Verschlüsselungsverfahren darf keine sogenannte Hintertür haben, die zum Beispiel dem Entwickler des Verfahrens eine Art Generalschlüssel lässt, mit dem sich alle verschlüsselten Informationen entschlüsseln lassen.

TIPP:

Großes Vertrauen genießen Techniken und Programme, deren Funktionsweise offen liegt. Das gilt zum Beispiel für die Verschlüsselung mit AES, für E-Mail-Verschlüsselung mit OpenPGP und für Software wie TrueCrypt.

Wie muss ein sicheres Passwort aussehen?

Das Wichtigste ist zunächst, überhaupt ein eigenes Passwort zu verwenden. Bei neuen Geräten oder neuer Software ist von Herstellerseite häufig ein Standardpasswort oder PIN voreingestellt (z. B. „0000" oder „passwort"). Ein solches muss sofort nach Inbetriebnahme durch ein individuelles Passwort ersetzt werden.

Nach einer Empfehlung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sollte ein gutes Passwort, ...

- mindestens zwölf Zeichen lang sein.
  (Ausnahme: Bei Verschlüsselungsverfahren wie z. B. WPA und WPA2 für WLAN sollte das Passwort mindestens 20 Zeichen lang sein.)
- aus Groß- und Kleinbuchstaben sowie Ziffern und Sonderzeichen (?!%+…) bestehen.
- keine Namen von Familienmitgliedern, des Haustieres, des besten Freundes, des Lieblingsstars oder deren Geburtsdaten usw. enthalten.
- wenn möglich nicht in Wörterbüchern vorkommen.
- nicht aus gängigen Varianten und Wiederholungs- oder Tastaturmustern bestehen, also nicht „asdfgh" oder „1234abcd" usw.

Um sich Passwörter zu merken, sollte man sie niemals unverschlüsselt auf dem PC liegen lassen oder gar einen Notizzettel an den Bildschirm kleben. Auch ist es nicht ratsam, für viele Anwendungen das gleiche Passwort zu verwenden, da ein Angreifer im schlimmsten Fall mehrere Benutzerkonten (z. B. E-Mail, Online-Banking, Online-Shops, Soziale Netzwerke usw.) missbrauchen kann.

TIPP:

Denken Sie sich einen Satz aus und verwenden Sie von jedem Wort nur den 1. Buchstaben (oder nur den 2. oder letzten, etc.). Anschließend verwandeln Sie bestimmte Buchstaben in Zahlen oder Sonderzeichen: „Morgens stehe ich auf und putze mir meine Zähne drei Minuten lang." Nur die 1. Buchstaben: „MsiaupmmZdMl". „i und l" sieht aus wie „1", „&" ersetzt das „und": Ms1a&pmmZ3M1". (Beispiel von www.bsi-fuer-buerger.de).

Weiterhin sollten Sie die Passwörter regelmäßig ändern.

Wer viele Passwörter zu verwalten hat, kann ein Passwort-Verwaltungsprogramm wie z. B. das kostenlose KeePass verwenden. Dann muss man sich nur noch ein (allerdings sehr gutes) Masterpasswort merken, um Zugriff auf die anderen Passwörter zu bekommen.

Wie funktioniert Verschlüsselung?

Wie muss ein sicheres Passwort aussehen?

Die Begriffe „privacy by default" (deutsch: datenschutzfreundliche Voreinstellungen) und „privacy by design" (deutsch: Datenschutz durch Technik) sind Grundsätze, die in den Planungen der Europäischen Union zur Reform des Datenschutzrechts eine maßgebliche Rolle spielen.

Das Prinzip **„privacy by default"** besagt, dass die Standardeinstellungen, zum Beispiel eines Profils in einem Sozialen Netzwerk, immer die datenschutzfreundlichsten sein müssen. Einige Anbieter von Sozialen Netzwerken sind gegen dieses Prinzip, da es nach ihrer Ansicht die spezifischen Funktionen dieser Netzwerke verkenne, Dinge zu teilen und sich zu vernetzen. Die Befürworter von „privacy by default" setzen dem entgegen, dass der Nutzer, der mehr von sich in der Öffentlichkeit zeigen wolle, weiterhin die Möglichkeit habe, sein Profil selbst Schritt für Schritt nach außen zu öffnen. Das Benutzerprofil sei lediglich nach der Registrierung in einem Sozialen Netzwerk nicht standardmäßig öffentlich und von Suchmaschinen auffindbar.

„Privacy by design" beschreibt, datenschutzrechtliche Erfordernisse bereits bei der Entwicklung neuer Technologien zu berücksichtigen und von Anfang an in die Konzeption mit einfließen zu lassen, anstatt sie hinterher mit viel Aufwand durch zusätzliche Eingriffe oder Programme zu realisieren. Dabei gilt es auch zu beachten, dass der Nutzer solcher Geräte in die Lage versetzt wird, Optionen, um seine Daten schützen zu können, leicht und verständlich auffindet. Dies kann durch die Bereitstellung von geeigneten Datenschutz-Werkzeugen oder Vorkehrungen für eine anonyme Nutzung geschehen.

Kritiker dieser Begriffe merken an, dass diese Grundsätze bereits seit langem in § 3a Bundesdatenschutzgesetz verankert sind. Dort heißt es, dass Systeme an dem Ziel auszurichten sind „so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen". Man müsse sich nur daran halten.

Was bedeuten „privacy by default" und „privacy by design"?

Kryptographie ist die Wissenschaft von der Verschlüsselung einer Botschaft. Das Wort setzt sich zusammen aus den altgriechischen Worten kryptós = verborgen und gráphein = schreiben. Mit der Entwicklung der modernen Datenverarbeitung bezieht sich der Begriff weiter gefasst auf die Definition, Konstruktion und Konzeption von Informationssystemen, die gegen unbefugtes Lesen und Verändern zu schützen sind. Das Gegenstück zur Kryptographie ist die Kryptoanalyse, die sich mit dem Entschlüsseln von verschlüsselten Botschaften, ohne den Schlüssel zu kennen, beschäftigt.

Die Kryptographie hat drei Hauptziele, um Informationen zu schützen:

- Vertraulichkeit: Schutz vor fremden Augen
- Integrität: Schutz vor Manipulation
- Authentizität: Schutz vor falschen Absendern

Um diese Ziele zu erreichen, werden mehrere Verfahren angewendet, die mehr oder weniger komplexe mathematische Funktionen zur Grundlage haben.

Die ersten Erwähnungen von kryptographischen Verfahren gehen auf Herodot (gest. um 424 v. Chr.) zurück, der eine die Klarschrift durch Wachs verbergende Tafel beschrieb. Gelegentlich wurde dem Boten die Botschaft auf den kahlrasierten Kopf geschrieben und er nach einiger Zeit, dann wieder mit vollem Schopf, auf den Weg geschickt. Im Mittelalter entstanden dann komplexe mathematische Verfahren, wie die Vigienère-Verschlüsselung, die lange Zeit als unknackbar galt.

Das Vigienère-Quadrat

Klar	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Im 20. Jahrhundert wurden überwiegend Maschinen zur Verschlüsselung verwendet, wovon die von Deutschland im zweiten Weltkrieg verwendete ENIGMA eine der bekanntesten ist. Aber auch diese hatte ihre Schwachstellen und wurde schließlich durch das britische Militär entschlüsselt.

Heute wird die Kryptographie durch Computer bestimmt, die eine fast unbegrenzte Anzahl an Verschlüsselungsmöglichkeiten bieten. Auf der anderen Seite ermöglichen diese Hochleistungsrechner auch das Ausprobieren von fast unendlichen Möglichkeiten.

Was bedeuten „privacy by default" und „privacy by design"?

Was ist Kryptographie?

Worauf muss man bei der Installation von Apps achten?

Apps (Abk. für Applikationen) sind kleine Programme, die u. a. auf Smartphones oder Tablet-Computern installiert werden können und verschiedene Anwendungen bereitstellen. Die bekanntesten und größten digitalen Marktplätze für Apps sind der Play Store von Google und der iTunes Store von Apple. Unter den dort angebotenen vielen hunderttausend Apps gibt es kostenpflichtige und kostenlose. Die Apps benötigen für eine reibungslose Funktion Zugriff auf unterschiedliche Bereiche des Smartphones oder Tablets. Bei einigen App-Stores können Sie vor dem Herunterladen sehen, auf welche Funktionen Ihres Geräts die App zugreifen kann. Nicht immer ist diese Berechtigung für das Funktionieren der App nötig. Das Smartphone-Betriebssystem Android kennt z. B. rund 160 verschiedene Berechtigungen, die nicht nur Hardware-Elemente wie z. B. Kamera oder Mikrofon ansteuern können, sondern auch sämtliche Inhalte des Gerätes auslesen und übermitteln. Das muss nicht immer mit bösen Absichten geschehen, so ist z. B. für kostenlose Apps ein Einblick in die Nutzergewohnheiten der eigentliche Preis für die Nutzung der App.

Bösartige Apps dagegen können unbemerkt Schadsoftware auf Ihrem Gerät installieren und vertrauliche Daten ebenfalls unbemerkt an den Angreifer senden. Manche dieser sogenannten Malware-Apps stellen unbemerkt teure Telefonverbindungen her oder versenden kostenintensive SMS, andere lesen Passwörter aus oder geben regelmäßig Positionsdaten weiter.

TIPP:

- *Installieren Sie Apps nur aus vertrauenswürdigen Quellen.*
- *Lesen Sie die Bewertungen von anderen Nutzern in den App-Stores.*
- *Überprüfen Sie die Berechtigungen, auch wenn Ihnen nicht immer sofort klar sein wird, warum eine App einen bestimmten Zugriff benötigt. Im Zweifel verzichten Sie auf eine Installation.*
- *Aktualisieren Sie die Apps regelmäßig („Update"), überprüfen Sie aber weiterhin die Berechtigungen, es könnten neue hinzugekommen sein.*
- *Seien Sie vorsichtig bei populären Spielen; diese werden gelegentlich von Nachahmern kostenlos angeboten, enthalten aber mitunter schädliche Funktionen.*
- *Löschen Sie Apps, die Sie nicht benutzen oder nur zu Testzwecken installiert haben.*

Warum sind normale E-Mails unsicher?

Auf E-Mails möchte heute niemand mehr verzichten. Zu schnell, einfach und günstig ist der Versand von Nachrichten über das Internet. Eine E-Mail wird über ein bestimmtes Protokoll (z. B. POP3, SMTP oder IMAP) über das Internet verschickt. Dabei wird die Nachricht auf dem Weg vom Sender zum Empfänger über eine Vielzahl von Servern geleitet. Ist eine E-Mail nicht verschlüsselt, kann jeder, der Zugriff auf diese Server hat, den Inhalt der Nachricht lesen oder speichern. Der viel gehörte Satz „Eine E-Mail ist so sicher wie eine Postkarte" – also für jeden, der sie sieht, ohne Mühe lesbar – trifft auf unverschlüsselte Mails voll und ganz zu. Da die Server, über die die elektronischen Nachrichten transportiert werden, nicht unbedingt in Deutschland stehen müssen, ist ein eventuell Mitlesender auch nicht an das hier geltende Briefgeheimnis gebunden.

Verschlüsselte E-Mails in Deutschland

Eine Gruppe von deutschen E-Mail-Anbietern (T-Online, web.de, gmx.de, Freenet) versendet seit dem 1. April 2014 E-Mails nur noch verschlüsselt. Im Zuge der Enthüllungen über das Lesen von E-Mails u. a. durch den US-amerikanischen Geheimdienst NSA wollen sie damit eine E-Mail „Made in Germany" einführen und garantieren die SSL-Verschlüsselung von Mails beim Versand innerhalb

dieser Anbietergruppe. Zudem sichern sie zu, dass der Mailverkehr nur über deutsche Server läuft und damit dem strengen deutschen

Datenschutzrecht unterliegt.

Wenn Sie Ihre E-Mails über einen anderen Anbieter versenden oder zusätzliche Sicherheit wünschen, stehen Ihnen u. a. die Verschlüsselungsprogramme OpenPGP oder GnuPG zur Verfügung, deren Anwendung jedoch eine gewisse Einarbeitung voraussetzt.

TIPP:

- *Verschlüsseln Sie E-Mails, wenn Sie wichtige, schützenswerte Inhalte versenden.*
- *Erkundigen Sie sich bei Ihrem E-Mail-Anbieter, ob er zur „E-Mail made in Germany"-Gruppe gehört und passen Sie ggf. die Einstellungen an.*
- *Wenn Sie auf Ihrem Smartphone E-Mails versenden und empfangen, überprüfen Sie auch dort die Einstellungen.*
- *Anleitungen zur Verschlüsselung von E-Mails finden Sie z. B. unter www.verbraucher-sicher-online.de oder www.sicher-im-netz.de*

Worauf muss man bei der Installation von Apps achten?

Warum sind normale E-Mails unsicher?

…beim Online-Einkauf sicher?

Shopping per Mausklick ist heute eine der beliebtesten Möglichkeiten, schnell und günstig einzukaufen. Ob Kleidung, Schuhe, Elektrogeräte, Möbel, Reisen oder Lebensmittel – es gibt kaum noch etwas, was sich nicht über das Internet bestellen lässt. Insbesondere bei der ersten Bestellung bei einem Online-Shop sind Kreditkarten häufig das einzig akzeptierte Zahlungsmittel, da sie für den Verkäufer eine Zahlung garantieren. Aber auch sonst sind die Geldkarten eine beliebte und komfortable Zahlungsmethode im Netz.

Bei der Bezahlung mit der Kreditkarte über das Internet müssen alle relevanten Daten der Karte eingegeben werden. Das ist neben dem Namen des Karteninhabers, der Kartennummer und der Gültigkeit vor allem der sogenannte CSC-Code (Card Validation Code = Kartenprüfnummer). Mit dieser dreistelligen Zahl, die auf der Rückseite der Kreditkarte steht, lässt sich feststellen, ob die Karte tatsächlich physisch vorliegt. Jeder, der alle genannten Daten inkl. des CSC-Codes vorliegen hat, kann mit den Daten bezahlen, ganz gleich ob er Inhaber der Karte ist oder nicht.

Achten Sie also darauf, dass die Kreditkartendaten bei der Übermittlung nicht mitgelesen werden. Dazu sollten Sie aktuelle Anti-Virenprogramme installiert haben, damit Ihr Rechner frei von Schadsoftware ist.

TIPP:

- *Kaufen Sie nur bei vertrauenswürdigen Online-Händlern ein. Achten Sie beispielsweise auf solche Gütesiegel wie „Trusted Shops", die einen Käuferschutz garantieren.*
- *Achten Sie darauf, dass der Verkäufer die Daten nur über eine verschlüsselte Verbindung übermittelt. Sie erkennen das am „https" im Adressfeld des Browsers.*
- *Verzichten Sie auf eine Bezahlung mit Kreditkarte, wenn Sie an einem öffentlichen Rechner surfen, z. B. in einem Internet-Café.*
- *Geben Sie keinesfalls Ihre Kreditkartendaten ein, wenn Sie durch eine E-Mail darum gebeten wurden (sogenanntes Phishing). Ihre Bank wird sie niemals per E-Mail zur Eingabe dieser Daten auffordern.*
- *Überprüfen Sie zeitnah und regelmäßig Ihre Kreditkartenabrechnung und kontaktieren Sie bei Unregelmäßigkeiten Ihre Bank.*
- *Wenn möglich, bezahlen Sie mit Rechnung.*

Ist die Angabe der Kreditkartennummer…

Unter dem Begriff Big Data werden zwei Aspekte zusammengefasst: Zum einen die immer größer werdenden Datenmengen, die mit herkömmlichen Methoden der Datenverarbeitung nicht mehr ausgewertet werden können, zum anderen IT-Lösungen, die dabei helfen sollen, die Informationsflut in den Griff zu bekommen. Die Quellen für Big Data sind vielfältig:

- Informationen aus Web- und Social-Media-Quellen
- Informationen von Sensoren, Messgeräten oder anderen Instrumenten, sogenannte Machine-to-Machine-Data
- Daten aus Transaktionen, wie Quittungen, Abrechnungen, Belegen, Rechnungen, etc.
- Biometrische Daten, wie z. B. Fingerabdrücke
- un- oder halbstrukturierte Aufzeichnungen wie handschriftliche Notizen, E-Mails, etc.

Unternehmen erhoffen sich von der Auswertung dieser Datenmengen die Schaffung neuer Geschäftsmodelle, Wettbewerbsvorteile oder Einsparungen. Die Wissenschaft setzt auf die Potenziale durch statistische Auswertungen, die Vorhersagen ermöglichen und neue Erkenntnisse hervorbringen können. Staatliche Stellen rechnen beispielsweise mit besseren Ergebnissen bei der Kriminalitätsbekämpfung, dem Umweltschutz oder der Gesundheitsvorsorge.

Kritiker warnen vor der Gefahr des Machtmissbrauchs, Manipulation oder Diskriminierung durch die maschinelle Auswertung der Datenmengen und sehen dadurch die Gefahr einer Grundrechtsverletzung. Zudem könnte Big Data zu einem falschen Vertrauen in die Prognosefähigkeit führen und menschliche Intuition und Analysefähigkeit in den Hintergrund drängen.

Ein wichtiger Aspekt beim Thema Big Data ist daher Datenschutz und Anonymisierung, damit keine Rückschlüsse auf einzelne Personen gezogen werden können. Zudem sollte man sich bei der Auswertung von Daten nicht ausschließlich auf die Deutung durch Maschinen verlassen.

Was bedeutet Big Data und wo liegen die Chancen?

Wie kann ich mein W-LAN wirklich schützen?

Ein Funknetzwerk (W-LAN) erleichtert die Verbindung von Endgeräten (Laptops, Smartphones, Tablet-Computern u. a.) mit dem Router, der den Zugang zum Internet ermöglicht. W-LAN ist die Abkürzung für Wireless Local Area Network (deutsch: drahtloses lokales Netzwerk) und erspart das Verlegen von Kabeln. Dieser große Vorteil des W-LANs bedeutet aber auch gleichzeitig eine Gefahr, denn die Funknetze machen nicht an Gebäudegrenzen Halt und sind daher auch für Außenstehende sicht- und ggf. abhörbar. Fast alle Router, die heute von Internetanbietern zur Verfügung gestellt werden, haben einen W-LAN-Zugang, der in den Standardeinstellungen unverschlüsselt ist. Die Verschlüsselung muss also beim Einrichten des lokalen Netzwerks vom Kunden selbst aktiviert werden.

Es gibt verschiedene Möglichkeiten, das W-LAN zu verschlüsseln. Dabei sollten Nutzer nicht mehr auf die veralteten Standards WEP und WPA setzen, da deren Codierungen sich mit wenig Aufwand knacken lassen. Die derzeit sicherste Methode, sein Netzwerk gegen Angriffe von außen abzusichern, ist die WPA2-Verschlüsselung. Allerdings müssen nicht nur der Router und das WLAN-Modul im Computer diesen Modus unterstützen, sondern auch alle an das Netz angeschlossenen Geräte, wie Smartphones oder internetfähige Fernseher. Falls dies nicht der Fall ist, sollten Sie erwägen, das Gerät mit einem Kabel an das LAN anzuschließen.

TIPP:

- *Schützen Sie den Zugang zu Ihrem Router mit einem komplizierten Zugangspasswort. Die sogenannte SSID (Service Set Identifier) sollte mindestens 18 Zeichen lang sein und – wie immer bei Zugangscodes – keine bekannten Worte oder einfache Zahlenkombinationen enthalten. Siehe auch „Wie muss ein sicheres Passwort aussehen?"*
- *Wenn Sie nicht laufend neue Geräte an das Netzwerk anschließen, machen Sie ihr W-LAN für Außenstehende unsichtbar. Die Einstellungen dazu finden Sie auf der Benutzeroberfläche des Routers.*
- *Nutzen Sie die Nachtschaltung des Routers, der sich dann zu von Ihnen festgelegten Zeiten aus- und wieder einschaltet.*
- *Tragen Sie die IP- und MAC-Adressen der angeschlossenen Geräte fest in den Router ein, dann können sich fremde Computer trotz ggf. bekanntem Passwort nicht einwählen.*

Wie kann ich mein W-LAN wirklich schützen?

Wie kann ich mein Smartphone sicherer machen?

Für viele Nutzer ist das Smartphone bereits heute der neue Personal Computer. Fast alles, was man mit dem PC online machen kann, kann das Smartphone häufig einfacher und schneller: E-Mails lesen, Online-Shopping und -Banking, navigieren und soziale Netzwerke nutzen. Auf dem Smartphone sind daher auch viele Zugangsdaten gespeichert, die für Kriminelle von großem Interesse sein können. Ein Smartphone sollte daher genauso gut gegen Angriffe geschützt werden wie ein herkömmlicher Computer. Hinzu kommt, dass ein Mobiltelefon leicht verloren oder gestohlen werden kann, so dass auch die Verschlüsselung oder das Fernlöschen der Daten eine wichtige Rolle für die Sicherheit spielen.

Was Sie bei der Auswahl und Installation der Apps auf dem Smartphone beachten sollten, haben wir bereits bei der Frage „Worauf muss man bei der Installation von Apps achten?" beantwortet.

Um einen Basisschutz für sein Smartphone zu erreichen, gibt es zunächst einige hilfreiche Funktionen und Handlungsempfehlungen:

- Führen Sie Gespräche mit vertraulichem Inhalt nicht über das Mobiltelefon. Diese Geräte sind nur mit hohem Aufwand abhörsicher zu machen.
- Nutzen Sie die Tastatur- und Displaysperren des Geräts sowie die PIN zur Sperrung der SIM-Karte. Gesichtserkennung und einfache Wischgesten sind nicht sicher!
- Lassen Sie bei Verlust des Geräts umgehend die SIM-Karte sperren. Bei einigen Anbietern können Sie dies selbst online machen.
- Schalten Sie drahtlose Schnittstellen (z. B. Bluetooth, W-LAN) des Geräts ab, wenn Sie sie nicht benötigen.
- Installieren Sie eine App, die es Ihnen ermöglicht, das Gerät nach Verlust zu orten oder im Notfall alle Daten darauf zu löschen (Remote-Wipe-Funktion).

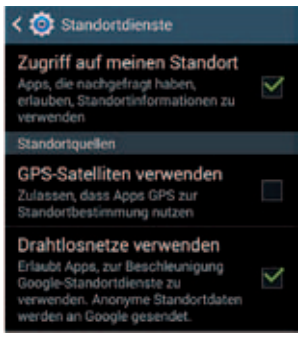
Wie alle anderen Geräte, die mit dem Internet verbunden sind, kann auch ihr Smartphone von Viren und Trojanern befallen werden. Mittlerweile gibt es auch für die mobilen Computer eine große Anzahl von Anti-Viren-Apps. Einige davon sind als Basisversionen kostenlos und können in Ruhe ausprobiert werden.

Wie kann ich mein Smartphone sicherer machen?

…nicht weitergeleitet werden?

Viele Apps erbeten vom Smartphone-Nutzer das Recht, den genauen oder ungefähren Standort ermitteln zu dürfen. Ob eine App dieses Recht erfordert, sehen Sie bei der Installation in der Liste der Berechtigungen. Bei vielen Smartphone-Programmen ist diese Funktion zur Nutzung der gewünschten App-Eigenschaften zwingend notwendig, wie z. B. bei Navigationsanwendungen. Andere funktionieren – z. T. im begrenzten Umfang – auch ohne die Weitergabe des Standorts.

Es gibt zwei verschiedene Möglichkeiten der Standortermittlung: Zum einen erlaubt die GPS-Funktion über eine Verbindung zu mehreren Satelliten einen sehr genaue Bestimmung des eigenen Standorts. Zudem nutzen einige Apps zur zusätzlichen Ortung (oder wenn kein GPS-Satellit erreichbar ist, z.B. in geschlossenen Gebäuden) das W-LAN oder das Mobilfunknetz. Hier werden bekannte W-LAN-Router oder die Sendemasten der Mobilfunkanbieter zur Ortsbestimmung genutzt. Diese Vorgehensweise ist nicht so genau wie die GPS-Ortung, liefert aber zumindest einen ungefähren Standort.



Bei Geräten mit dem Google-Betriebssystem Android lassen sich über den Systemmenüpunkt „Standortdienste" die GPS-Ortung sowie die Ortsbestimmung über W-LAN-Zugangspunkte einzeln abschalten. Beim Apple-Betriebssystem iOS heißt dieser Punkt „Ortungsdienste". Wer nicht über die Sendemasten der Mobilfunkanbieter geortet werden möchte, muss die Telefonfunktion abschalten, z. B. das Gerät in den Flugmodus versetzen. Allerdings kann man dann auch nicht mehr telefonieren.

Auch die Sozialen Netzwerke wie z. B. Facebook greifen auf die Standortdaten zu und übermitteln sie auf die eigenen Server. Wer eine Weitergabe dieser Daten verhindern möchte, sollte Facebook oder Twitter in einem Browser aufrufen anstatt eine App zu verwenden. Browser dürfen den Standort nur dann abrufen, wenn das der Nutzer ausdrücklich erlaubt hat.

Wirklich anonym bewegt sich mit einem Smartphone nur, wer das komplette Betriebssystem und die Standard-Apps austauscht. Das wiederum ist jedoch mit neuen Risiken verbunden, so dass als letzter Tipp für Anonymität bleibt, das Gerät auszuschalten und zuhause zu lassen.

Was muss ich tun, damit meine Standortdaten…

…und wie ich deren Löschung beantragen kann?

Wenn wir im Internet unterwegs sind, hinterlassen wir an vielen Stellen unsere Daten: Anmeldeinformationen, Passwörter, Einkaufslisten, Rechnungen, Kreditinformationen, unseren Standort und vieles mehr. Wenn man dagegen in einem „normalen" Geschäft etwas einkauft und bar bezahlt, bleibt man anonym.

TIPP:

Schreiben Sie Unternehmen an und fragen Sie, was über Sie gespeichert ist und an wen es eventuell weiter gegeben wurde. Bei Amazon, eBay und Facebook erhalten Sie oft komplette Dossiers über Ihr Kaufverhalten und die daraus hergeleiteten Interessen. Das soziale Netzwerk Facebook stellt sogar einen Link zur Verfügung unter dem Sie die über Sie gespeicherten Daten herunterladen können:
http://www.facebook.com/help/405183566203254/

Um die Kreditwürdigkeit von Kunden überprüfen und das sogenannte Scoring erstellen zu können, legen Auskunfteien wie Schufa, Bürgel und Creditreform umfangreiche Datensammlungen an. Einmal im Jahr müssen die Auskunfteien auf Anfrage kostenlos darüber aufklären, welche Daten sie zu einer Person gespeichert haben und wer die Daten zu welchem Zweck erhalten hat.

Allein der Verkäufer könnte sich vielleicht an das Gesicht erinnern. Einzeln betrachtet scheint die Speicherung vieler dieser persönlichen Daten harmlos zu sein. Zusammengesetzt kommen sie jedoch Personen- und Persönlichkeitsprofilen sehr nahe und sind daher nicht nur für Werbetreibende (siehe Beitrag über „Big Data") interessant.

Mit der Neufassung des gesetzlichen Datenschutzes im Jahr 2009 wurden den Bürgern umfassende Auskunftsrechte über die Weitergabe ihrer Daten erteilt. Auch Banken müssen seitdem die Grundlagen einer Kreditentscheidung offenlegen.

TIPP:

Nutzen Sie die Möglichkeit der Eigenauskunft und erfahren Sie, was die Auskunfteien über Sie gespeichert haben. Überprüfen Sie die Einträge genau und korrigieren Sie sie gegebenenfalls, denn nicht immer sind die Daten vollständig und häufig sogar falsch.

Einen guten Überblick über Organisationen und was diese über Sie gespeichert haben, gibt das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein unter den Link:
https://www.datenschutzzentrum.de/selbstdatenschutz/checkheft/

Wie kann ich erfahren, wer welche Daten von mir besitzt…

Ja – unter bestimmten Voraussetzungen. Grundsätzlich sind die Rechte auf Berichtigung, Löschung und Sperrung von Daten für öffentliche Stellen des Bundes in § 20 des Bundesdatenschutzgesetzes (BDSG) und für nicht-öffentliche Stellen in § 35 BDSG geregelt. Personenbezogene Daten müssen von öffentlichen und nicht-öffentlichen Stellen gelöscht werden.

Recht auf Löschung

In Fällen, in denen zum Beispiel eindeutig rechtswidrige Inhalte vorliegen und nicht gegen den Anbieter vorgegangen werden kann, helfen auf dem offiziellen Weg die Datenschutzaufsichtsbehörden weiter.

Man hat aber auch selbst die Möglichkeit, die Löschung die Profildaten in sozialen Netzwerken voranzutreiben. Dies ist jedoch meist nicht mit einem Klick getan, sondern oft mit zahlreichen Zwischenschritten verbunden. Der Grund: Soziale Netzwerke wie Google+ und Facebook leben von ihren Mitgliedern und deren Daten. Zwar beteuern alle Anbieter, dass bei Löschung die Daten auch von ihren Servern verschwinden, doch das lässt sich nicht prüfen. Auf Antrag müssen die Betreiber jedoch alles entfernen.

Sind persönliche Einträge aber erst im Umlauf, ist es schwer, sie komplett aus dem Gedächtnis des Internets zu löschen. Denn es reicht oft nicht aus, das Profil oder den Account zu entfernen, da z. B. Suchmaschinen längst Kopien von den Webseiten erstellt haben. Hier hat jedoch das im Frühjahr 2014 ergangene „Google-Urteil" des Europäischen Gerichtshofs die Rechte der Nutzer gestärkt. Dieser kann nun verlangen, dass der Internetkonzern die Verweise (Links) auf seine Daten löscht. Das bedeutet unter anderem auch, dass der Konzern jetzt grundsätzlich für die Links verantwortlich ist. (Der Link zum Urteil: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070de.pdf). Dennoch: Wer seine Meinung gern öffentlich in Internetforen kundtut, sollte sich vergewissern, ob ihm auch ein Recht auf Löschung der Beiträge zusteht, wenn er seinen Account aufgibt. Es ist rechtlich nämlich äußerst strittig, ob sich ein solches Recht nur ausnahmsweise ergibt, insbesondere wenn die Forenbeiträge urheber- oder datenschutzrechtlichen Schutz genießen.

TIPP:

Schützen Sie aktiv Ihre Privatsphäre und überlegen Sie genau, welche Daten Sie wirklich im Netz preisgeben wollen. Denn die Daten können jederzeit kopiert und an anderer Stelle im Netz veröffentlicht werden. Praktische Hinweise im Netz, wie man seinen Account auf Facebook, Google und Foren löschen kann, finden Sie hier:

- **http://www.e-recht24.de/artikel/datenschutz/7460-daten-loeschen-facebook-twitter-google.html**
- **http://www.deinguterruf.de/Themen/daten-loeschen-lassen-recht-negative-daten-loeschen.aspx**

Daten sind im Online-Geschäft eine virtuelle Handelsware. Datenkonzerne wie Google und Facebook überholen derzeit mit Ihrem Börsenwert bereits Energiekonzerne. Alter, Beziehungsstatus, Ausbildung, Lieblingsmusik, Fotos und Informationen über Hobbys sind ein begehrter Rohstoff – all diese Informationen nutzen die Anbieter, um maßgeschneiderte Zielgruppen für ihre Werbekunden zusammenzustellen. Beim Handel mit Daten gelten inzwischen die üblichen Regeln von Angebot und Nachfrage. Die Daten werden entweder selbst gehandelt oder es wird eine Dienstleistung angeboten, welche die Werbung an die Nutzer verschickt, die sich für die beworbenen Produkte interessieren könnten.

Über eine Milliarde Menschen sind derzeit bei Facebook als Mitglieder registriert. Sie sind spätestens seit dem Börsengang das Kapital für das Unternehmen. Je mehr Mitglieder auf der Plattform ihre persönlichen Daten preisgeben, umso zielgerichteter kann personalisierte Werbung eingeblendet werden. Das heißt aber auch im Umkehrschluss, dass die Nutzung eines sozialen Netzwerkes deshalb kein Geld kostet, da mit der Währung „Daten" gezahlt wird.

Für mehr Transparenz und Medienkompetenz im Umgang mit den persönlichen Daten hat sich die Online-Werbebranche Selbstregulierungsmaßnahmen auferlegt. Unter dem Dach des Zentralverbands der deutschen Werbewirtschaft hat der Deutsche Datenschutzrat Onlinewerbung (DDOW) offiziell die Arbeit aufgenommen. Per Klick auf ein bestimmtes Piktogramm können Nutzer seitdem feststellen, welche Dienstleister hinter der Datenerhebung und -nutzung stehen. Zudem können Privatnutzer auf einer zentralen Website anbieterübergreifend entsprechend ihrer persönlichen Vorlieben den Einsatz von nutzungsbasierter Online-Werbung durch Drittanbieter steuern. Der Link zur DDOW:
http://meine-cookies.org/DDOW/index.html

TIPP:

Wenn Sie im Netz unterwegs sind, hinterlassen Sie bewusst jeweils nur dort persönliche Informationen, wo für Sie auch ein Interesse an einem weiteren Kontakt besteht.

Achten Sie beispielsweise darauf, bei einem Angebot oder einem Update automatisch angekreuzte Zusatzangebote zu löschen oder unnötige persönliche Angaben nicht auszufüllen.

… wenn jemand ohne meine Erlaubnis persönliche Dinge von mir ins Netz stellt?

Wenn man feststellt, dass private Daten ohne vorherige Einwilligung online sind, sollte man mit dem Betreiber der entsprechenden Webseite Kontakt aufnehmen und diesen zur Löschung der betreffenden Daten nach §35 des Bundesdatenschutzgesetzes auffordern. Um den Betreiber einer deutschen Webseite zu erreichen, ist ein Blick in das Impressum hilfreich. In Deutschland ist jeder Betreiber einer Webseite verpflichtet, eine Adresse im Impressum anzugeben.

Handelt es sich um private Bilder, sollte man auf das Recht am eigenen Bild (§22 Kunsturhebergesetz, kurz: KunstUrhG) verweisen. Die Einschränkungen hierzu sind in §23 KunstUrhG zu finden. Bei sonstigen Daten ist ein Verweis auf das allgemeine Persönlichkeitsrecht ratsam.

Bei im Ausland betriebenen Webseiten sind meist das Kontaktformular oder ebenfalls das Impressum der erste Weg, um mit dem Betreiber Kontakt aufzunehmen. Fehlt diese Möglichkeit, dann sollte man versuchen, über den sogenannten Domain-Registrar der Webseite den Eigentümer der Domain zu ermitteln. Diesen kann man dann ebenfalls zum Löschen der betreffenden Daten auffordern. Bleiben Sie in jedem Fall hartnäckig und bestehen Sie darauf, dass Ihre Daten aus dem Internet gelöscht werden. Sollten diese einfachen Möglichkeiten scheitern, dann ist auf jeden Fall der Rat eines Anwalts einzuholen.

Versuchen Sie zu klären, wie Fremde in den Besitz Ihrer Daten gekommen sein könnten. Überprüfen Sie Ihren Rechner auf Schadsoftware. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt Empfehlungen zur sicheren Konfiguration von Windows-PCs. Dort ist eine Auswahl an geeigneten Virenschutzprogrammen aufgeführt. Ändern Sie alle Passwörter, die Sie zur Anmeldung bei Sozialen Netzwerken, Online-Shops, E-Mail-Accounts und anderen Online-Diensten nutzen.
Siehe auch unter dem Stichwort „Wie muss ein sicheres Passwort aussehen?”

TIPP:

Empfehlungen des BSI für die sichere Konfiguration von Windows-Rechnern:
https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/BasisschutzComputer/basisschutzComputer_node.html

Wer mehr wissen will:

Den Text des Bundesdatenschutzgesetzes finden Sie in der gemeinsam vom Bundesministerium für Justiz und Verbraucherschutz und der juris AG betriebenen Datenbank frei verfügbar:
http://www.gesetze-im-internet.de/bdsg_1990/index.html

Die aktuell amtierende Bundesbeauftragte für Datenschutz und Informationsfreiheit, Andrea Voßhoff, sowie viele Informationen zum Thema finden Sie hier:
http://www.bfdi.bund.de

Das Bundesamt für Sicherheit in der Informationstechnik bietet vor allem praktische Hinweise für private Nutzer, wie Sie Ihren Computer sichern, welche Gefahren drohen und wie Sie sich im Netz bewegen sollten:
https://www.bsi-fuer-buerger.de

Die EU-Initiative „klicksafe” folgt dem 1999 gestarteten Safer Internet Programm der EU. „klicksafe” ist in Deutschland ein gemeinsames Projekt der Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz (Projektkoordination) und der Landesanstalt für Medien Nordrhein-Westfalen (LfM).

Sie finden dort nicht nur Informationen zum Datenschutz, sondern erhalten auch Hinweise zu anderen Sicherheitsfragen wie Jugendschutz, Cybermobbing oder Urheberrecht:
http://www.klicksafe.de

Das Virtuelle Datenschutzbüro bündelt als Plattform Informationen und Materialien verschiedenster Partner, unter denen die Datenschutzbeauftragten der Länder, der Kirchen und mehrerer öffentlich-rechtlicher Sendeanstalten sind:
https://www.datenschutz.de/

Sachbücher, die einen allgemeinen und verständlichen Überblick vermitteln, sind u. a.:

- Peter Schaar: Überwachung total. Wie wir in Zukunft unsere Daten schützen. Aufbau Verlag 2014.
- Bernhard C. Witt: Datenschutz kompakt und verständlich: Eine praxisorientierte Einführung. Vieweg + Teubner Verlag 2007, 2. Auflage 2010.

Wie kann ich mich wehren, …

Literatur und Hinweise