

Bericht Datenschutz und Datensicherheit 2010.

Erleben, was verbindet.



Über diesen Bericht.

Erstmals betrachtet das Unternehmen sämtliche Bereiche, die mit dem Verarbeiten und dem Schutz von Daten zu tun haben. Deshalb heißt der Bericht für 2010 erstmals Bericht zu Datenschutz und Datensicherheit.

Mit diesem Bericht will die Deutsche Telekom „Transparenz schaffen“: Nicht nur Ereignisse des Jahres 2010 rund um das Thema Daten innerhalb des Unternehmens sollen dargestellt werden. Vielmehr sollen Kunden, Aufsichtsbehörden, Aufsichtsgremien, Politik, aber auch Aktionäre und Mitarbeiter erfahren, wie wichtige Prozesse und Strukturen aussehen, in denen Daten verarbeitet werden. Im zweiten Schritt wird erklärt, warum die Deutsche Telekom bestimmte Prozesse umsetzt und in bestimmten Strukturen arbeitet.

Der Bericht hält sich dabei an die aus dem vergangenen Jahr bekannte Struktur: Im Lagebericht gibt er einen Überblick über besondere Ereignisse des Jahres 2010 bei der Deutschen Telekom und betrachtet Zukunftsszenarien von Datenschutz und Datensicherheit. Im Kapitel Datenschutz im Detail finden Leser Informationen zu Datenschutz und Datensicherheit bei wichtigen Bezugsgruppen des Unternehmens wie Privat- und Geschäftskunden oder Arbeitnehmern. Die Deutsche Telekom versteht Datenschutz und -sicherheit als Service. Deshalb enthält der aktuelle Bericht erstmals einen Ratgeber zum sicheren Surfen im Netz, der auch in den Telekom Shops ausliegt.

Die Deutsche Telekom wird auch in Zukunft darauf setzen, beim Thema Datenschutz und Datensicherheit im Sinne des öffentlichen Interesses transparent zu kommunizieren. Mit dieser Praxis will sie eine Vorreiterrolle einnehmen. Wenn Sie Verbesserungsvorschläge haben: Lassen Sie es uns wissen. Wir wollen den eingeschlagenen Weg weiter gehen. Und wissen, dass wir noch nicht am Ziel sind.

Ihre Meinung an: datenschutzbericht@telekom.de.



Inhalt.

■ 2 Geleitwort des Vorstands

■ 5 Lagebericht

- 6 Datenschutz und Datensicherheit 2010 im Überblick
- 6 Besondere Ereignisse im Jahr 2010
- 9 Neue gesetzliche Regelungen
- 9 Prüfungen und Kontrollen durch externe und interne Stellen
- 10 Auskünfte an staatliche Stellen und Privatpersonen
- 12 Forschung und Entwicklung
- 13 Ausblick – Datenschutz und Datensicherheit 2011

■ 15 Entwicklung in einzelnen Bereichen

- 16 Privatkunden
- 24 Geschäftskunden
- 27 Arbeitnehmer
- 28 Internationale Entwicklungen
- 30 Systeme und Prozesse
- 38 Kommunikation nach innen und nach außen

■ 41 Datenschutzbeirat der Deutschen Telekom

■ 45 Ratgeber zum sicheren Umgang mit Daten

■ 55 Anhang

- 56 Besondere Maßnahmen in Datenschutz und Datensicherheit seit 2008
- 57 Organisation des Konzerndatenschutzes
- 58 Organisation der Datensicherheit im Konzern
- 60 Glossar
- 63 Abkürzungen
- 65 Impressum, Kontakt



Im Detail



Glossar

Geleitwort des Vorstands.



Dr. Manfred Balz

Liebe Leserinnen und Leser,

viele von uns haben sich daran gewöhnt, ihr Urlaubshotel via Satellitenbild im Internet zu auszusuchen oder ihre Fotos weltweit mit Freunden zu teilen. Das Jahr 2010 hat unserem Bild von grenzenloser Vernetzung einige Facetten hinzugefügt. Die Einstellung zur Privatsphäre bei Facebook, die aufgeheizte Debatte um Google Street View und die Aufregungen um Wikileaks zeigen: Das Thema Umgang mit Daten ist mitten in der Gesellschaft angekommen.

Erstmals seit das Bundesverfassungsgericht 1983 das Recht auf informationelle Selbstbestimmung im so genannten Volkszählungsurteil aus der Verfassung abgeleitet hat, wird über die Ausprägung und die Reichweite dieses Rechts intensiv öffentlich diskutiert. Der Bundesinnenminister hat Ende 2010 Eckwerte eines Gesetzentwurfs vorgelegt, der eine Grenze ziehen soll zwischen erlaubter und unerlaubter Sammlung und Verknüpfung von Daten.



„Daten sind der Rohstoff der vernetzten Welt.
Daten sind, wie Wasser, flüchtig.
Und Daten brauchen, ebenso wie Wasser,
besonderen Schutz.“

Aber: Verfügt der Nutzer über die nötigen Fertigkeiten, um mit seinen eigenen Daten verantwortungsvoll umzugehen? Hier besteht Lernbedarf. Unsere Kinder dürfen den Umgang mit dem Netz nicht nur durch unangeleitetes Experimentieren lernen. Eltern, Kindergärten und Schulen, wir alle, müssen dabei helfen. Aber nicht nur Medienkompetenz der Konsumenten tut not. Die Anbieter müssen verständlich darüber aufklären, was mit den Daten passiert.

Daten sind der Rohstoff der vernetzten Welt. Wir haben für unseren Bericht eine Bildwelt gefunden, die Wasser zeigt. Daten sind – wie Wasser – flüchtig. Und Daten brauchen ebenso wie Wasser besonderen Schutz.

Die Deutsche Telekom hat in jüngster Zeit den Preis für Datenverluste bezahlen müssen. Wir haben aus den Fehlern gelernt. Deshalb legen wir mit unserem Bericht seit 2008 offen, wie Daten in unserem Haus verarbeitet und geschützt werden. Wir stellen Pannen und Störfälle auf unserer Homepage dar, um Kunden, aber auch Aufsichtsbehörden, Politik, Aktionären und Mitarbeitern eine eigene Meinungsbildung zu ermöglichen. Wir stellen uns der Kritik – wenn Sie Anregungen haben, dann lassen Sie es uns wissen: datenschutzbericht@telekom.de.

Ich wünsche Ihnen eine kurzweilige und spannende Lektüre.

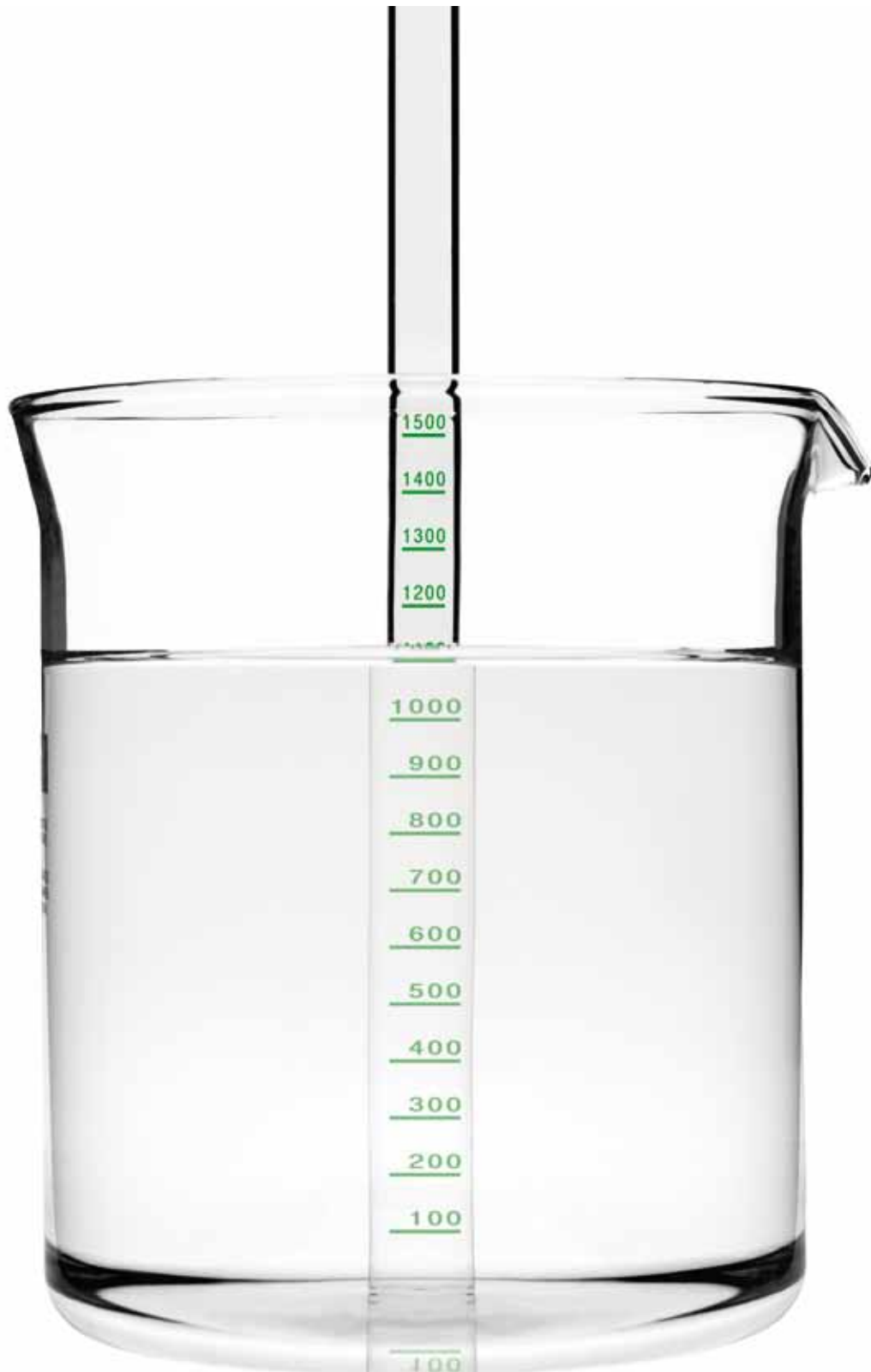
Ihr

Dr. Manfred Balz
Vorstand Datenschutz, Recht, Compliance




Lagebericht.

➡ Wer Datenschutz und Datensicherheit ernst nimmt, muss sich an seinen Ergebnissen messen lassen.



Datenschutz und Datensicherheit 2010 im Überblick.

In kaum einem Jahr der näheren Vergangenheit beherrschten Themen rund um Datenschutz und Datensicherheit die öffentliche Debatte wie im Jahr 2010. Aufmerksamkeit bekam die Berichterstattung über den Schutz personenbezogener Daten bislang hauptsächlich bei Datenpannen, ansonsten wurden Datenschutz und -sicherheit als selbstverständlich vorausgesetzt. Das Jahr 2010 brachte einen Paradigmenwechsel mit sich: Ausgelöst durch den Start des Panoramadienstes Google Street View in 20 deutschen Städten diskutierte eine breite Öffentlichkeit über Wochen hinweg über den Begriff des Privaten und Schutzwürdigen und die Grenzen dessen, was Bürger im Zeitalter des Internets von sich preisgeben sollen.

Die Politik reagierte schnell: Der damalige Bundesinnenminister Thomas de Maizière stellte im Dezember einen Gesetzentwurf zum Schutz der Persönlichkeitsrechte der Bürger im Internet vor („Rote-Linie-Gesetz“) . Ebenso hat die Industrie als Folge der öffentlichen Diskussion einen Datenschutzkodex für Geodatendienste (abzurufen unter: <http://www.bitkom.org>) erarbeitet, an dem sich die Deutsche Telekom maßgeblich beteiligt hat (siehe unten).

Getrieben wurde die Diskussion auch von wiederkehrenden Meldungen über den Umgang mit personenbezogenen Daten im sozialen Netzwerk Facebook. Die Politik bezog in dieser Auseinandersetzung Stellung: Verbraucherschutzministerin Ilse Aigner löschte ihr Konto bei Facebook und rief zum Boykott des Netzwerkes auf. Thomas de Maizière veröffentlichte im Juni im Rahmen seiner „14 Thesen zu den Grundlagen einer gemeinsamen Netzpolitik der Zukunft“ erste Forderungen nach Systemen, die ein Vergessen im Internet ermöglichen.

Im Herbst 2010 kam eine neue Dimension hinzu, als Wikileaks 250.000 geheime Dokumente aus dem amerikanischen Außenministerium veröffentlichte.

Die Deutsche Telekom hat diese Entwicklungen aufmerksam verfolgt und, wo sinnvoll, mit ausführlichen Informationen der Verbraucher durch Ratgeber reagiert.

Datenschutz.





bezeichnet den Schutz des Einzelnen vor Missbrauch personenbezogener Daten. Zweck des Datenschutzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt wird.

Datensicherheit.

umfasst die technischen und organisatorischen Maßnahmen zum Schutz von Daten gegen Veränderung und Verlust.

Besondere Ereignisse im Jahr 2010.

Beteiligung der Deutschen Telekom an Initiativen zum Datenschutz.

Die Deutsche Telekom versteht sich als treibende Kraft bei Datenschutz und Datensicherheit. Deshalb engagiert sie sich neben Stellungnahmen zu nationalen und internationalen Gesetzgebungsverfahren in Verbänden sowie unternehmensübergreifenden Initiativen zur Stärkung beider Themen in Wirtschaft und Gesellschaft. Beispiele hierfür sind die von der GSM Association (GSMA)  initiierte „Mobile Privacy Initiative“, die sich mit den industrieübergreifenden Standards für den Datenschutz bei Lokalisierungsdiensten befasst, oder der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) . Hier beteiligte sich das Unternehmen an einem Datenschutzkodex für Geodatendienste. Anlass waren die umfangreichen Diskussionen um Dienste wie Google Street View. Der Kodex hat das Ziel, die Akzeptanz von Geodatendiensten zu fördern, indem er im Wege der Selbstverpflichtung Grundsätze für einen angemessenen Ausgleich der Interessen von Widerspruchsberechtigten, Nutzern und Anbietern der Dienste festlegt. Der Branchenverband BITKOM legte dazu auf dem 5. Nationalen IT-Gipfel in Dresden Anfang Dezember 2010 einen Datenschutzkodex vor, der am 1. März 2011 im Rahmen der CeBIT in Hannover unter anderem von der Deutschen Telekom an den damaligen Bundesinnenminister Thomas de Maizière übergeben wurde. Der Bundesdatenschutzbeauftragte lobte diesen Kodex als ersten Schritt in Richtung einer gesetzlich verbrieften Kontrolle der Bürger über ihre eigenen Daten.

Darüber hinaus wurde ein unter Mitarbeit der Deutschen Telekom erstelltes Papier „Eckpunkte zur datenschutzkonformen Gestaltung von Home-Networks“ auf dem IT-Gipfel vorgestellt. Das Papier beschreibt Ansätze, wie eine vernetzte Gerätewelt im Eigenheim benutzerfreundlich, datenschutzkonform und sicher gestaltet werden kann.

Gerichtliche Aufarbeitung der Bespitzelungsaffäre.

In der so genannten Bespitzelungsaffäre fand zwischen Anfang September und Ende November 2010 die strafrechtliche Hauptverhandlung vor dem Landgericht Bonn statt. Mitarbeiter der damaligen Konzernsicherheit der Deutschen Telekom hatten in den Jahren 2005 und 2006 zur Aufklärung vermeintlicher Indiskretionen Telefonverbindungsdaten von 50 Personen erhoben und durch einen Berliner Unternehmer auswerten lassen. Zu den Betroffenen zählten insbesondere mehrere Vertreter des Aufsichtsrates der Deutschen Telekom, Betriebsratsmitglieder, Gewerkschaftsvertreter und Journalisten. Der Vorgang war im Mai 2008 von der Telekom selbst bei der Staatsanwaltschaft Bonn zur Anzeige gebracht worden. Nach Abschluss der Ermittlungen hatte die Staatsanwaltschaft Anklage gegen einen ehemaligen Abteilungsleiter bei der Konzernsicherheit, den Berliner Unternehmer sowie zwei weitere ehemalige Mitarbeiter der Konzernsicherheit erhoben. In Bezug auf den vormaligen Vorstandsvorsitzenden der Deutschen Telekom, Kai-Uwe Ricke, sowie den vormaligen Aufsichtsratsvorsitzenden der Deutschen Telekom, Dr. Klaus Zumwinkel, hat die Staatsanwaltschaft das Ermittlungsverfahren eingestellt.

Das Landgericht Bonn hat den ehemaligen Abteilungsleiter der Konzernsicherheit als Hauptangeklagten wegen Verstoßes gegen das Fernmeldegeheimnis und gegen das Bundesdatenschutzgesetz **G** sowie wegen Untreue Ende November 2010 zu einer Freiheitsstrafe von drei Jahren und sechs Monaten verurteilt. Das Urteil war zum Redaktionsschluss dieses Berichts am 1. März 2011 noch nicht rechtskräftig. Gegen die beiden mitangeklagten ehemaligen Mitarbeiter wurde das Verfahren gegen Zahlung einer Geldauflage eingestellt. Der mitangeklagte Berliner Unternehmer hatte Verhandlungsunfähigkeit geltend gemacht. Gegen ihn findet der Prozess zu einem späteren Zeitpunkt statt.

Die Deutsche Telekom spendet in Folge der Bespitzelungsaffäre rund 1,7 Millionen Euro an gemeinnützige Organisationen. Sie versteht dies als Zeichen ihrer unternehmerischen Verantwortung, die sie für die Vorgänge der Vergangenheit übernommen hat. Zusätzlich haben der Konzern und die Anwälte der betroffenen Aufsichtsräte, Betriebsräte und Gewerkschaftsvertreter eine Vereinbarung über individuelle Entschädigungsleistungen der Deutschen Telekom geschlossen. Auch mit den bespitzelten Journalisten und weiteren Betroffenen haben Gespräche über individuelle Entschädigungsleistungen begonnen oder werden im Jahr 2011 aufgenommen.

Missbrauchserkennungssysteme.



Nach Schätzungen internationaler Organisationen entstehen Telekommunikationsanbietern, so auch der Deutschen Telekom und ihren Kunden, insgesamt weltweit pro Jahr Schäden in Höhe von rund 50 Milliarden Euro durch Missbrauch. Ein solcher Missbrauch reicht von Anmeldebetrug und Nichtzahlung von Dienstleistungen über die Umgehung von Terminierungsentgelten (Weiterleitungsentgelte), Hacking von Telefonanlagen, Nutzung von Flat-Tarifen zu nicht vertraglich vereinbarten Konditionen bis hin zum Missbrauch von Mehrwertdiensten.

Um solche Szenarien aufzudecken, zu verfolgen und zu unterbinden, unterhält die Deutsche Telekom verschiedene Missbrauchserkennungssysteme auf Grundlage von § 100 Telekommunikationsgesetz. Diese Systeme sind aufgrund unterschiedlicher Konfigurationen in der Lage, einen jeweils unterschiedlichen Blickwinkel auf die verschiedenen Betrugsszenarien einzunehmen. Über alle Systeme wurden der Bundesdatenschutzbeauftragte und die Bundesnetzagentur schriftlich informiert.

Die Missbrauchserkennungssysteme werten Verkehrs- und Signalisierungsdaten aus (Verkehrsdaten entsprechen den Abrechnungsdaten, Signalisierungsdaten dienen dem technischen Auf- und Abbau eines Gesprächs). Gesprächsinhalte sind nie Gegenstand der Analyse. Es wird also nicht das gesprochene Wort aufgezeichnet, sondern welche Rufnummer mit welcher Rufnummer wie lange telefoniert hat. Die Systeme suchen dabei nicht nach bestimmten Verbindungen, sondern nach auffälligen Mustern aufgrund zuvor vom Bereich Datenschutz genehmigter Szenarien und Filter. Es wird sowohl nach vorgegebenen Suchroutinen nach Betrugsfällen als auch nach konkreten Verdachtsmomenten gesucht.

Begutachtung der Missbrauchserkennungssysteme.

Verschiedene Missbrauchserkennungssysteme der Deutschen Telekom waren in den Jahren 2005 und 2006 im Rahmen der Bespitzelung (siehe oben) missbräuchlich genutzt worden, um Verbindungsdaten zu verfolgen. Diese theoretisch mögliche Nutzung der Systeme wurde nach Bekanntwerden des Missbrauchs durch eine Reihe von Maßnahmen unterbunden.

So verschärfte und konkretisierte die Deutsche Telekom 2009 die Vorschriften zum Umgang mit den Missbrauchserkennungssystemen weiter: Der Bereich Datenschutz erstellte einen konkreten Katalog der bekannten Betrugsszenarien und gab die daraus resultierenden Filtereinstellungen der Erkennungssysteme frei, die diese Szenarien recherchieren können. Jedes mögliche neue Szenario und jeder neue Filter muss seither vom organisatorisch unabhängigen Bereich Datenschutz freigegeben werden.

Darüber hinaus hat die Deutsche Telekom eine Reihe weiterer Maßnahmen ergriffen:

- Personelle und organisatorische Trennung der Prozessschritte „Auftrag zur Recherche“, „Recherche eines konkreten Anfangsverdachts“, „Ermittlung“ und „Konsequenzenmanagement“
- Aufzeichnung der einzelnen Arbeitsschritte der jeweiligen Systembenutzer zur Verfolgung von möglichem Missbrauch der Systeme
- Vier-Augen-Prinzip in systemkritischen Arbeitsschritten, etwa Erstellung und Freischalten eines neuen Filters

Der Vorsitzende des Datenschutzbeirats und stellvertretende Aufsichtsratsvorsitzende der Deutschen Telekom, Lothar Schröder, und der Vorstand für Datenschutz, Recht und Compliance, Dr. Manfred Balz, begutachteten im April 2010 die Systeme zur Erkennung von Missbrauch, um sich von der Wirksamkeit der ergriffenen Maßnahmen einen Eindruck zu verschaffen. Dabei überzeugten sie sich von der Qualität des Datenschutzes sowie dem hohen Maß prozessualer und systematischer Standards, die die ausschließlich rechtskonforme Nutzung dieser Systeme gewährleisten. Über die Ergebnisse der Begutachtung informierte Lothar Schröder den Datenschutzbeirat der Deutschen Telekom im Mai 2010.

Sachverständigen-Gutachten zum Datenschutz.

Nach Bekanntwerden der Datenschutzvorfälle hatte die Deutsche Telekom noch im Frühjahr 2008 einen Sachverständigenbericht zum Datenschutz bei Dr. Gerhard Schäfer, weiland Vorsitzender Richter am Bundesgerichtshof, beauftragt. Dieser sollte einen weiteren Blick von außen auf die Systeme und Prozesse zu Datenschutz und Datensicherheit der Deutschen Telekom ermöglichen. Resultat des Berichts, der dem Konzernvorstand im Dezember 2009 und zu Beginn 2010 auch dem Datenschutzbeirat vorgelegt wurde, war eine Reihe von Empfehlungen zur Schärfung und Verbesserung einzelner Prozesse. So sehen die Empfehlungen unter anderem eine weitere Verfeinerung der Zugriffsrechte auf Kundendaten in Callcentern **[G]** vor. Darüber hinaus weisen sie zum Beispiel auf die Einhaltung von Löschrufen für die Daten aus gekündigten Verträgen hin.

Die Deutsche Telekom hat 2010 die Umsetzung der operativen Einzelmaßnahmen weitgehend abgeschlossen. Ein geringer Teil der Maßnahmen wird aktuell noch umgesetzt. Sämtliche Maßnahmen bewegen sich auf operativer Ebene. Missbrauchsfälle, wie etwa die im Rahmen der Daten-vorfälle bekannt gewordenen, wurden nicht gefunden.




Im März 2010 erklärte das Bundesverfassungsgericht die Vorratsdatenspeicherung für verfassungswidrig. Die Deutsche Telekom löschte die gespeicherten Daten unwiederbringlich.

Einstellung der Vorratsdatenspeicherung.



Am 2. März 2010 hat das Bundesverfassungsgericht die bestehenden Regelungen zur Vorratsdatenspeicherung **[G]** aus den Jahren 2008 und 2009 für verfassungswidrig erklärt. Die Regelungen verpflichteten Telekommunikationsanbieter unter anderem, die Telefonnummer des Anrufenden, Zeit und Länge des Anrufs, weitere Daten zu E-Mail- und Internetnutzung und im Mobilfunk die Funkzelle zu speichern. Die Deutsche Telekom hat nach dem Urteil die Speicherung und Beauskunftung sämtlicher Vorratsdaten unverzüglich gestoppt. Die gespeicherten Daten wurden unwiederbringlich gelöscht.

In den zuständigen politischen Gremien auf deutscher und europäischer Ebene wird derzeit diskutiert, wie mit dem Thema Vorratsdatenspeicherung zukünftig umgegangen werden soll. Die Deutsche Telekom plädiert für eine Lösung, die ein ausgewogenes Verhältnis von öffentlicher Sicherheit und Datenschutz, aber auch Nutzen und Kosten abbildet.

Umgang mit nicht autorisierten Vertriebsunternehmen.

Wie im Vorjahresbericht ausgeführt, wurden im Jahr 2009 von nicht autorisierten Callcentern  aus der Türkei Festnetzverträge mit Kunden für die ehemalige Konzerneinheit T-Home geschlossen. Diese Vorgänge sind inzwischen aufgeklärt. Die Deutsche Telekom hat Strafanzeigen erstattet und zivilrechtliche Ansprüche (Rückforderung der Prämien, Vertragsstrafe, Löschung von Daten etc.) geltend gemacht. Darüber hinaus wurde die Zusammenarbeit mit einigen Unternehmen beendet und Abmahnungen ausgesprochen. Die türkischen Callcenter wurden aufgefordert, den unrechtmäßigen Vertrieb von Produkten der Deutschen Telekom zu unterlassen. Während die strafrechtlichen Verfahren noch andauern, hat das Unternehmen die zivilrechtlichen Ansprüche erfolgreich abgeschlossen und den entstandenen materiellen Schaden in Höhe von rund 1,5 Millionen Euro kompensiert. Gleichzeitig hat die Deutsche Telekom neue Maßnahmen zur Prävention ähnlicher Vorgänge implementiert und führt sie weiter ein.

Neue gesetzliche Regelungen.

Im Jahr 2010 begann der Gesetzgeber, mit einem Gesetzentwurf zum Arbeitnehmerdatenschutz und zur Novelle des Telekommunikationsgesetzes (TKG)  wichtige Weichen für den Datenschutz zu stellen. Gleichzeitig gab es einige Änderungen im Bundesdatenschutzgesetz (BDSG)  hinsichtlich der Weitergabe von Daten an Dritte. Im Februar 2010 ist zunächst das Zugangserleichterungsgesetz in Kraft getreten, das den Zugang zu Internetseiten mit kinderpornographischen Inhalten erschweren soll. Auf der Grundlage des Koalitionsvertrags der Bundesregierung wurde die Umsetzung dieses Gesetzes ausgesetzt. Das Bundeskriminalamt hat für die Telekommunikationsunternehmen keine Sperrlisten zum Abruf zur Verfügung gestellt. Die Deutsche Telekom hat daraufhin die Anfang 2010 eingeleiteten Maßnahmen zur Erschwerung des Zugangs zu Webseiten mit kinderpornographischen Inhalten abgebrochen und die bis dahin errichtete Infrastruktur zurückgebaut.



Auf europäischer Ebene hat die Novellierung der europäischen Datenschutzrichtlinie von 1995 begonnen.

Die Details der Änderungen werden in den Kapiteln über Datenschutz und Datensicherheit für Privatkunden, Arbeitnehmer und internationale Entwicklungen dargestellt.




Prüfungen und Kontrollen durch externe und interne Stellen.


Auch im Jahr 2010 prüften interne und externe Stellen Systeme und Prozesse der Deutschen Telekom. Externe Prüfungen und Kontrollen wurden und werden weiterhin entweder von den staatlichen Aufsichtsbehörden oder – meist im Rahmen von Zertifizierungen – durch unabhängige externe Stellen durchgeführt. Intern überprüft die Deutsche Telekom zudem die Einhaltung der gesetzlichen Bestimmungen sowie der eigenen Sicherheits- und Datenschutzbestimmungen. Auf diese Weise sichert das Unternehmen kontinuierlich ein Schutzniveau, das zu den höchsten innerhalb der Telekommunikationsbranche gehört.

Staatliche Prüfungen und Kontrollen.

Der Konzerndatenschutz der Deutschen Telekom führt mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit  (Bundesdatenschutzbeauftragter) und der Bundesnetzagentur  kontinuierlich Gespräche zu aktuellen Fragen des Datenschutzes sowie den im Unternehmen hierzu ergriffenen Maßnahmen. Durch die frühzeitige Einbindung in kritische Datenschutzthemen wird die Transparenz gegenüber den Aufsichtsbehörden erhöht. Im Jahr 2010 wurden in intensiver Abstimmung mit dem Bundesdatenschutzbeauftragten weitere Maßnahmen zur Optimierung des Datenschutzniveaus umgesetzt, die sich aus seinen Beratungs- und Kontrollbesuchen in den Jahren 2008 und 2009 ergeben hatten. Weitere Beratungs- und Kontrollbesuche im Jahr 2010 hat es nicht gegeben.

Audits und Zertifizierungen.

Neben den durch staatliche Aufsichtsbehörden durchgeführten Kontrollen hat die Deutsche Telekom auch im Jahr 2010 ihre Aktivitäten rund um Zertifizierungen  und Audits  ausgeweitet. Insgesamt haben Zentralbereiche der Telekom über 450 interne und externe Audits zum Thema Datenschutz und Datensicherheit durchgeführt. Außerdem wurden im Vertrieb mehr als 100 Callcenter  zertifiziert oder es wurde mit der Zertifizierung begonnen. Auch die Zertifizierung von Exklusivpartnern der Deutschen Telekom, also Händlern, die ausschließlich Telekom-Produkte vertreiben, wurde 2010 gestartet.

Die Deutsche Telekom stützt sich bei der Sicherstellung eines hohen Datenschutz- und Datensicherheitsniveaus damit sowohl auf interne als auch externe Fachkompetenz. Darüber hinaus hat die Deutsche Telekom als Bestätigung des hohen Sicherheits- und Schutzniveaus im Jahr 2010 etwa eine Sicherheitszertifizierung nach ISO  27001 für ihr zentrales Sicherheitsmanagementsystem oder eine Datenschutzzertifizierung für ihren Rechnungsprozess im Privatkundensegment Festnetz erhalten. Die Details hierzu werden auf den Seiten 35 und 36 beschrieben.

Auskünfte an staatliche Stellen und Privatpersonen.

Anfragen an den Datenschutz.

Die Anzahl der über den Postweg, Fax oder über Online-Kanäle eingegangenen Anfragen zum Thema Datenschutz – entweder direkt beim Konzernschutz oder bei speziell eingerichteten Serviceadressen – ist von 7.460 im Jahr 2009 auf 10.808 Anfragen im Jahr 2010 gestiegen. Über die spezielle Service-E-Mail-Adresse datenschutz@telekom.de kamen im Jahr 2010 die meisten Anfragen. Bei Anfragen zur Konzerneinwilligungsklausel (KEK) geht es in der Regel um den Widerruf der bei Vertragsschluss erteilten Einwilligung zu Werbung oder Information. Anlass für eine solche Anfrage ist zum Beispiel der regelmäßige Erhalt von Werbematerial, Werbeanrufen oder -faxen. Die Kunden informieren sich, ob eine solche Einwilligung von Ihnen tatsächlich vorliegt bzw. welchen Umfang sie hat. Anfragen zu Verzeichniseinträgen zielen auf die Korrektur oder Löschung von Einträgen in öffentlichen Verzeichnissen (z. B. Telefonbuch, Auskunft). Die Deutsche Telekom gibt in diesen Fällen Auskunft im Rahmen ihrer gesetzlichen Verpflichtung. Direkt beim Datenschutz des Konzerns und seinen Datenschutzbeauftragten gingen rund 911 Anfragen ein, darunter auch die 190 Anfragen, die über den Bundesdatenschutzbeauftragten eingereicht wurden.

Der überwiegende Teil der Kundenanfragen betraf ein Auskunftersuchen nach § 34 Bundesdatenschutzgesetz [\[G\]](#). Danach kann ein Kunde unentgeltlich von einem Unternehmen Auskunft verlangen über die dort über ihn gespeicherten Daten, den Zweck der Speicherung, die Personen und Stellen, an die seine Daten regelmäßig übermittelt werden (Personen, Firmen, Stellen etc.), sowie insbesondere die Herkunft der Daten. Diese Anfragen beziehen sich auf alle über den Kunden gespeicherten Daten.

Bei Anfragen zur Konzerneinwilligungsklausel (KEK) geht es in der Regel um den Widerruf der bei Vertragsschluss erteilten Einwilligung zu Werbung oder Information. Anlass für eine solche Anfrage sind zum Beispiel der regelmäßige Erhalt von Werbematerial, Werbeanrufen oder -faxen. Die Kunden informieren sich, ob eine solche Einwilligung von Ihnen tatsächlich vorliegt bzw. welchen Umfang sie hat.

Anfragen zu Verzeichniseinträgen zielen auf die Korrektur oder Löschung von Einträgen in öffentlichen Verzeichnissen (z. B. Telefonbuch, Auskunft). Die Deutsche Telekom gibt in diesen Fällen Auskunft im Rahmen ihrer gesetzlichen Verpflichtung.

Im Gegensatz dazu geht es bei Anfragen zum Urheberrecht darum, welche Daten des Kunden an einen Dritten, den so genannten Rechteinhaber, in einem konkreten Fall herausgegeben wurden. Anfragen zum Urheberrecht werden entweder von Kunden gestellt, die eine anwaltliche Abmahnung wegen vermeintlicher Urheberrechtsverletzungen erhalten haben (wie zum Beispiel bei behaupteter rechtswidriger Nutzung von Tauschbörsen im Internet). Sie können auch von Anwälten der Rechteinhaber gestellt werden, die eine vermeintlich unzulässige Nutzung von urheberrechtlich geschützten Werken (z. B. Musik oder Video) behaupten. Häufig folgt auf eine Anfrage aufgrund urheberrechtlicher Verletzungen ein Auskunftersuchen nach § 34 Bundesdatenschutzgesetz durch den betroffenen Kunden.

Kontakt zur Deutschen Telekom.


Kunden, die von der Deutschen Telekom Auskunft über die über sie gespeicherten personenbezogenen Daten erhalten möchten, stehen verschiedene Informationskanäle zur Verfügung:

Post: Konzernbeauftragter für den Datenschutz,
Deutsche Telekom AG, Friedrich-Ebert-Allee 144, 53113 Bonn.
E-Mail: datenschutz@telekom.de

Verteilung und Art der Kundenanfragen an den Konzernschutz.



Anfragen zu Urheberrechtsverletzungen.


Im Jahr 2010 erhielt die Deutsche Telekom pro Monat einstweilige Anordnungen zur vorläufigen Speicherung von im Durchschnitt rund 200.000 IP-Adressen . Diese Adressen haben die Rechteinhaber oder deren Dienstleister bei ihren Recherchen nach unrechtmäßigem Anbieten urheberrechtlich geschützter Werke im Internet ermittelt. Die Zahl der angegebenen IP-Adressen entspricht dabei nicht der Zahl der tatsächlichen Nutzer, die geschützte Werke auf Plattformen angeboten haben: Experten gehen davon aus, dass hinter der Anzahl der angefragten IP-Adressen eine deutlich geringere Anzahl realer Personen steht. Dies hat technische Gründe: Während eine Person eine Tauschbörse nutzt, kann ihre IP-Adresse mehrfach recherchiert werden. Gleichzeitig kann eine Person über einen gewissen Zeitraum hinweg mehrere IP-Adressen genutzt haben.

IP-Adressen.



Voraussetzung für die Nutzung des Internets ist eine IP-Adresse (Internet-Protokoll-Adresse). IP-Adressen erlauben eine logische und eindeutige Adressierung von Geräten in IP-Netzwerken wie etwa dem Internet. Eine IP-Adresse wird in der Regel nicht dauerhaft vergeben, da die Anzahl der weltweit verfügbaren Adressen beim aktuellen IPv4-Protokoll geringer ist als die Anzahl der möglichen Geräte. Bei jeder neuen Interneteinwahl wird deshalb durch den Internetzugangsanbieter eine so genannte dynamische IP-Adresse vergeben. Die Deutsche Telekom speichert diese Kombination aus Benutzerkennung und IP-Adresse zur Bekämpfung technischer Angriffe auf die Netzinfrastruktur, der Spam-Versendung oder von Angriffen durch Schadsoftware wie Trojaner oder Bot-Netze sieben Tage lang. Dies geschieht auf Grundlage von § 100 Abs. 1 TKG und § 109 TKG.

Verlässliche Zahlen zur Entwicklung von Urheberrechtsverletzungen existieren nicht. Die Deutsche Telekom verzeichnet allerdings mit 2,28 Millionen beauskunfteten IP-Adressen im Jahr 2010 einen Zuwachs im Vergleich zum Vorjahr (1,4 Millionen). Grund für den Anstieg ist, dass zunehmend mehr Rechteinhaber diesen Weg zur Verfolgung ihrer Rechte nutzen.

Bei der Deutschen Telekom haben sich im Jahr 2010 Beschwerden von Nutzern gehäuft, die angeben, zum betreffenden Zeitpunkt nicht im Internet gewesen zu sein. In Einzelfällen könnten ungesicherte oder schlecht gesicherte WLAN-Verbindungen die Ursache sein. Die Deutsche Telekom hat daher unter anderem einen Ratgeber zum Datenschutz für Kunden entwickelt, der auf diese Problematik hinweist. Zudem ist in den Bedienungsanleitungen der Geräte ein Kapitel mit Hinweisen auf Verschlüsselung und Sicherheit Standard. Darüber hinaus sind die aktuellen WLAN-Router der Deutschen Telekom mit einem individuellen Netzwerkschlüssel versehen, und die WPA2-PSK-Verschlüsselung  ist bei Lieferung bereits aktiviert. Diese Voreinstellungen machen den Router besonders sicher.

IP-Beauskunftung.



Provider wie die Deutsche Telekom sind seit September 2008 gesetzlich verpflichtet, aus ihrem vorhandenen Datenbestand Inhabern von Urheber- und Leistungsschutzrechten auf Verlangen Auskunft über Kunden zu geben, die urheberrechtlich geschützte Werke in Internet-Tauschbörsen (Filesharing) angeboten haben sollen. Der Auskunftsanspruch der Rechteinhaber geht aus dem Urheberrechtsgesetz (§ 101 Abs. 2 UrhG) hervor. Aufgrund des damit verbundenen Eingriffs in das Fernmeldegeheimnis muss der Rechteinhaber zuvor eine gerichtliche Erlaubnis beantragen (§ 101 Abs. 9 UrhG). Innerhalb von sieben Tagen können Inhaber von Urheber- und Leistungsschutzrechten nach einer festgestellten Urheberrechtsverletzung bei Gericht eine einstweilige Anordnung erwirken, dass die im Zusammenhang mit einer Verletzung festgestellten IP-Adressen und deren Kundenzuweisung gesichert werden. Das Gericht prüft, ob alle gesetzlichen Voraussetzungen für eine Auskunft vorliegen. Untersucht wird dabei auch, ob der Antragsteller tatsächlich Inhaber der Urheber- bzw. Leistungsschutzrechte ist, ob es sich um eine offensichtliche Urheberrechtsverletzung in gewerblichem Ausmaß handelt und ob die Ermittlung der relevanten IP-Adresse, deren Zuordnung beim Provider abgefragt werden soll, durch die Rechteinhaber ordnungsgemäß erfolgt ist. Liegen alle Voraussetzungen vor, erfolgt ein abschließender Gerichtsbeschluss, auf den hin die Deutsche Telekom die gesicherten Daten an den jeweiligen Rechteinhaber oder dessen anwaltliche Vertretung herausgeben muss. Bevor sie dies tut, prüft sie, ob alle dafür notwendigen Beschlüsse und Angaben zur Beauskunftung korrekt vorliegen. Beauskunftet werden dann die vorliegenden Bestandsdaten. Darüber hinausgehende Verkehrsdaten, Kommunikationsinhalte oder sonstige darauf hinweisende Informationen sind nicht Gegenstand der Beauskunftung.

Nach Abschluss des Vorgangs löscht die Deutsche Telekom gemäß den gesetzlichen Vorgaben unverzüglich alle entsprechenden Daten.

Vergabe und Speicherung der IP-Adressen, der Nutzungszeiträume und die Zuordnung zur Kundenkennung durch die Deutsche Telekom folgen gängigen Methoden der digitalen und automatisierten Datenverarbeitung. Insbesondere die Benutzerkennung schließt Verwechslungen aus. Fehlerhafte Systemfunktionen der Datenverarbeitungs- und Datenbanksysteme auf Seiten der Deutschen Telekom sind praktisch ausgeschlossen. Die zur Auskunftserteilung notwendige Datensicherung erfolgt vollautomatisiert ohne händische Eingaben von IP-Adressen und Datumsangaben.

Telekommunikationsüberwachung nach § 109 TKG.

Verschiedene Gesetze des Bundes und der Länder verpflichten die Telekommunikationsunternehmen, den Sicherheitsbehörden die Überwachung von Telekommunikationsverkehren zu ermöglichen sowie Auskünfte über Verkehrs- und Bestandsdaten an diese zu erteilen.

Die rechtliche Grundlage für die Telekommunikationsüberwachung ergibt sich aus der Strafprozessordnung, dem Art. 10 Gesetz, dem Zollfahndungsdienstgesetz, dem Bundeskriminalamtgesetz sowie einzelnen Landespolizeigesetzen. Eine Telekommunikationsüberwachung muss je nach Rechtsgrundlage richterlich oder durch eine vergleichbare neutrale Institution (etwa den Leiter einer obersten Landesbehörde bzw. einen Bundesminister) angeordnet werden. Die betreffenden Gespräche werden dann über eine gesicherte Leitung an die Behörden geleitet. Die Deutsche Telekom hat dabei keinen Zugriff auf die Inhalte der Gespräche oder Datenverbindungen. Eine rechtlich korrekte Bearbeitung der Anfragen von Sicherheitsbehörden ist für ein Telekommunikationsunternehmen wie die Deutsche Telekom von besonderer Bedeutung, weil die Mitarbeiter andernfalls schnell in Gefahr geraten können, sich selbst wegen Strafvereitelung (bei angeblich unzureichender Auskunftserteilung) oder wegen Bruch des Fernmeldegeheimnisses (bei zu „großzügiger“ Auskunftserteilung) strafbar zu machen. Bei der Deutschen Telekom geben vier Stellen Auskünfte an staatliche Stellen: Für den Festnetz-/Internetbereich drei „Regionalstellen für staatliche Sonderauflagen“ in Frankfurt, Hannover und Berlin. Die in Münster angesiedelte Stelle „Behördenauskunft Mobilfunk“ erfüllt diese Aufgaben für den Mobilfunk bundesweit.

Weiterentwicklung der Beauskunftung.

Infolge der Gründung der Telekom Deutschland GmbH wurde es erforderlich, die bisherigen Prozesse der Auskunftserteilung bei der T-Mobile GmbH einerseits und bei der Deutschen Telekom AG (T-Home) andererseits auf Unterschiede hin zu untersuchen und im Einzelfall anzugleichen. Zudem bestehen in der Praxis für die Auskunft gebenden Unternehmen auch Handlungsfreiräume, da die bestehenden Rechtsvorschriften nicht alle Konstellationen des täglichen Lebens abdecken können. Um zudem möglichst nicht ad hoc Beurteilungen rechtlich komplexer Sachverhalte vornehmen zu müssen, überarbeitet die Deutsche Telekom ihre Beauskunftung gegenüber staatlichen Stellen. Ziel des Projekts ist es, im Jahr 2011 eine verlässliche Handlungsmaxime zur Beauskunftung an berechnigte staatliche Stellen zu erstellen. Sie soll für Mitarbeiter auch in Zweifelsfällen eine klare Richtschnur für ihr Handeln im Einzelfall geben, um dem Spannungsfeld zwischen Freiheit und Sicherheit unter Einbeziehung der Unternehmensinteressen möglichst angemessen gerecht zu werden. Gleichzeitig setzt sich die Deutsche Telekom für eine Präzisierung und bundesweite Vereinheitlichung der gesetzlichen Rahmenbedingungen der Beauskunftung ein.

Forschung und Entwicklung.

Anstatt mit Kreditkarte einfach mit dem Handy bezahlen. Eine SMS bekommen, wenn in der Wohnung ein Fenster aufgebrochen wird: Bereits bei der Entwicklung solcher Produkte Datenschutz und Datensicherheit eng einzubinden, ist Praxis bei der Deutschen Telekom (siehe Seite 33).

Die 2005 gemeinsam mit der Technischen Universität Berlin gegründeten Telekom Laboratories (T-Labs) entwickeln innovative Produkte für das Unternehmen und binden die Aspekte des Datenschutzes und der Datensicherheit bereits in diese Phase der Entwicklung ein.

Das innovative Forschungs- und Entwicklungsinstitut verbindet dabei praktische Produkt- und Dienstentwicklung mit wissenschaftlicher Forschung. Gut 300 Telekom-Experten und Wissenschaftler verschiedenster Fachrichtungen aus aller Welt arbeiten an Lösungen für die einfache, schnelle und sichere Kommunikation von morgen. Bei der Forschung und Entwicklung von zukunftsweisenden Produkten und Diensten werden in den T-Labs Aspekte des Datenschutzes und der Datensicherheit frühzeitig berücksichtigt.

Einige Beispiele aus der Forschungsarbeit der T-Labs zur Gewährleistung von Datenschutz und Datensicherheit sind:

- Entwicklung von Methoden zum frühzeitigen Erkennen von Missbräuchen und Hackerangriffen auf ein Kommunikationsnetz (z. B. durch Computerviren, -würmer)
- Minimierung des Anfalls und der Verwendung von kritischen Informationen über die Entwicklung von Verfahren, die eine Personalisierung erlauben, jedoch die Identität des Nutzers schützen
- Entwicklung eines optimierten Anonymisierungsverfahrens, das sich automatisch so anpasst, dass für Netzplanung oder Dienstoptimierung gesammelte Nutzungsdaten auch dann keinen Rückschluss auf den einzelnen Nutzer zulassen, wenn die Datenmengen gering sind oder verschiedene Auszüge aus Datenbanken miteinander verknüpft werden könnten
- Erforschung neuer Methoden zur Erleichterung des Identitätsmanagements: Zugangsdaten zu Nutzerkonten gehören zu den schützenswerten persönlichen Daten. Die zunehmende Anzahl von Passwörtern führt häufig zu laxerem Umgang mit den Sicherheitsmechanismen: schwache Passwörter, Notizzettel am PC-Monitor. Der Bereich „Identity-Management“ arbeitet hierbei an leichter handhabbaren Verfahren, bei denen einfache Bedienung mit höherer Sicherheit einhergeht. Beispielsweise können Identitäts-Provider die Menge der zu merkenden Passwörter verringern, während kontaktlose – oder virtuelle – Karten für eine sichere Übermittlung von Zugangsberechtigungen sorgen
- Entwicklung nutzerzentrischer Identitätsmanagement-Methoden: So können zum Beispiel Profilinformationen, das heißt Informationen über Interessen, Voreinstellungen, Nutzungsmuster etc., durch den Nutzer selbst und nicht durch den Diensteanbieter verwaltet werden. Der Nutzer hat es damit bei jeder Nutzung in der Hand, ob und welche Informationen er preisgeben will – ggf. sogar, unter welchem Pseudonym


Darüber hinaus haben Aspekte des Datenschutzes und der Datensicherheit Einfluss auf die Entwicklung von Produkten und Diensten genommen, die sich derzeit in der Produkteinführungsphase befinden. Sie wurden damit von der Idee bis zur Produkteinführung konsequent berücksichtigt:

Mobile Wallet („Mobile Brieftasche“): Bei dieser Neuentwicklung wird das Mobiltelefon mit so genannter Near-Field-Communications (NFC) – Technologie für den Zahlungsverkehr und die Bündelung von Kundenkarten genutzt, wird also quasi zur mobilen Brieftasche. Nutzer der neuen Technologie können ihre Bank- und Kundendaten auf der SIM-Karte speichern lassen, mit der der Netzbetreiber seine eigenen Dienste schützt. Da die Programme und Sicherheitsmechanismen von den Banken und Instituten, jedoch nicht vom Betreiber eingesehen werden können und die Auswahl etwa eines Bezahlendienstes dem Nutzer überlassen ist, wird Missbrauch erschwert, während ein anonymes Prepaid-Konto den Schutz der Privatsphäre gewährleistet.

Home Management-Anwendungen: Das Haus beziehungsweise die Wohnung der Zukunft ist vernetzt: Der Staubsauger, der ausgeht, wenn das Telefon klingelt. Die Alarmanlage, die eine Kurzmitteilung (SMS) schreibt, wenn sie eine Bewegung im Zimmer registriert. Keine Zukunftsszenarien mehr, sondern technisch realisierbar. Standardisierte Bedienkonzepte, Vertraulichkeit der Dateninhalte, Datenhoheit der Anwender, Transparenz und Kontrolle von Zugriffsberechtigungen sind dabei nur einige datenschutzrechtliche Herausforderungen, für die an Lösungen gearbeitet wird. Gleichzeitig geht es darum, für die potentiellen Nutzer zukünftiger Home Networks praktikable, sichere und vertrauenswürdige Lösungen anbieten zu können.


Ausblick – Datenschutz und Datensicherheit 2011.

Enthüllungen von Wikileaks, Industrieviren wie Stuxnet, aber auch Diskussionen darüber, was im Zeitalter des Internets die Begriffe „privat“ und „öffentlich“ bedeuten, waren Themen des vergangenen Jahres, die auch im Jahr 2011 auf der Agenda bleiben werden. Über die Verwendung persönlicher Daten durch soziale Netzwerke kam 2010 verstärkt auch eine Diskussion über das Löschen solcher Daten im Netz auf. Ideen wie die eines „digitalen Radiergummis“ oder eines Verfallsdatums für bestimmte Inhalte werden auch in den kommenden Monaten diskutiert werden. Im größeren Zusammenhang reicht die Debatte an Themen wie das Recht auf Vergessen und die Grenzen des Privaten im Zeitalter des Internets heran. Diese Diskussionen werden sicherlich über einen längeren Zeitraum immer wieder geführt werden.

Auf dem Gebiet der technischen Entwicklungen von Produkten und Anwendungen wird das Prinzip der digitalen Vernetzung auch im Jahr 2011 weiter ausgebaut und damit weitere oder auch neue Fragen nach Datenschutz und Datensicherheit aufwerfen. Cloud- oder Dynamic Computing  sorgt nicht nur bei Geschäftskunden für innovative Lösungen. Auch private Nutzer werden ihre Daten und ihre Software nicht

mehr auf dem Computer zu Hause oder auf dem Smartphone speichern. Von überall werden sie auf die Server zentraler Rechenzentren zugreifen, deren Schutzniveau zwar das eines durchschnittlichen Computers zu Hause bei weitem überschreitet – aber als Rechenzentrum natürlich auch Ziel von Angriffen werden könnte. Die ressourcensparende Stromnetz-Steuerung wird in den kommenden Jahren ausgebaut; Lösungen für intelligent kommunizierende Geräte zu Hause werden bald selbstverständlich sein. Bei all diesen Entwicklungen werden die Themen Datenschutz und Datensicherheit in Zukunft eine immer größere Rolle spielen. Die Deutsche Telekom trägt diesem gestiegenen Bedarf Rechnung: Im Jahr 2011 rollt das Unternehmen ein im Inland bereits praktiziertes Verfahren, das die Einbindung von Datenschutz und Datensicherheit schon in der Entwicklungsphase von Produkten und Dienstleistungen vorschreibt, weltweit aus (siehe Seite 33). Damit schafft der Konzern einen einheitlichen Schutz- und Sicherheitsstandard seiner Produkte und Leistungen. Technische Innovationen etwa im Bereich des Dynamic Computing oder der vernetzten Lebenswelt zu Hause wird die Deutsche Telekom mit Nachdruck unter dem Fokus Datenschutz und Datensicherheit begleiten und ein hohes Schutz- und Sicherheitsniveau als Wettbewerbsvorteil ausbauen.

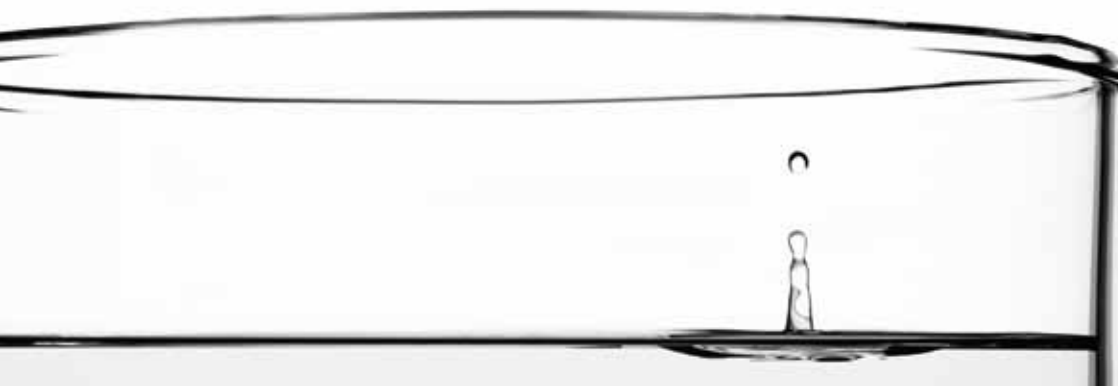
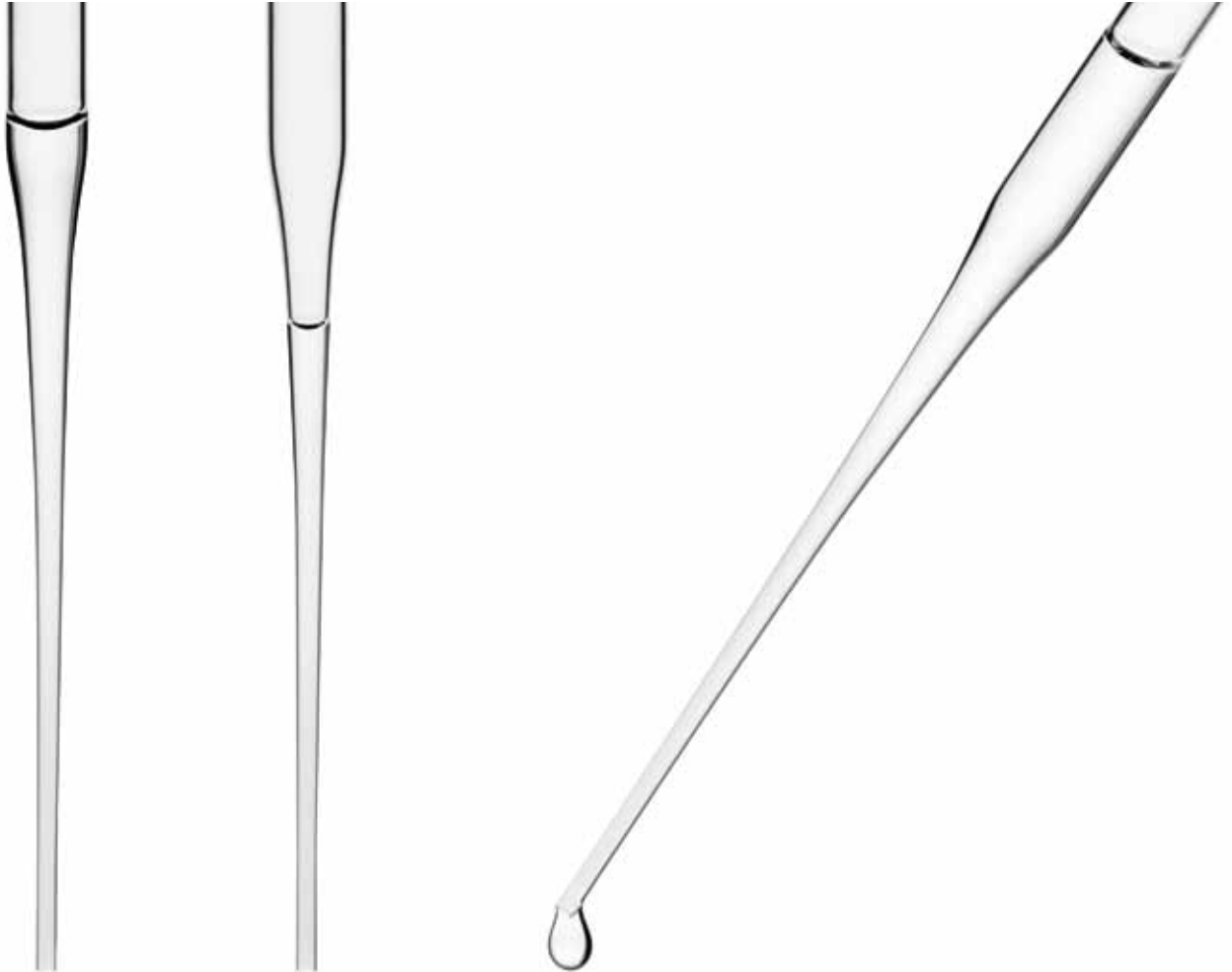
Der Angriff von Stuxnet auf iranische Atomanlagen im Jahr 2010 hat gezeigt: Unternehmen und Einrichtungen, die ihre Daten und Systeme sichern und schützen wollen, müssen künftig eine neue digitale Bedrohung mit ins Kalkül ziehen. Neben dem Umgang mit technischen Aspekten der Sicherheit wird für Unternehmen wichtiger, dass sie ihre Führungskräfte und Mitarbeiter für einen verantwortungsvollen Umgang mit Daten sensibilisieren und verdeutlichen, wie leicht Nachlässigkeiten zu Schäden für Unternehmen führen können. Gleichzeitig werden Unternehmen sich auch davor schützen müssen, dass Mitarbeiter vertrauliche Informationen preisgeben, um dem Unternehmen zu schaden. Hier hat die Deutsche Telekom nach den Datenskandalen der Vergangenheit wichtige Grundsteine für eine neue, moderne Unternehmenskultur gelegt, in der die Mitarbeiter mit ihren Anliegen ernst genommen werden, in der aber auch gleichzeitig transparente Regeln aufgestellt und im Zweifelsfall sanktioniert werden. Diese Kultur wird das Unternehmen ausbauen und stärken. Auf der technischen Seite wird die Deutsche Telekom 2011 Systeme und Prozesse kontinuierlich weiterentwickeln, um Angreifern immer einen Schritt voraus zu sein. Zudem wird sie ihre Schulungsmaßnahmen und Kampagnen für Datenschutz und Datensicherheit auf Aktualität prüfen und nachjustieren, wo Bedarf herrscht.

Auf gesetzlicher Ebene stehen im Jahr 2011 unter anderem die Unterzeichnung des „Rote-Linie-Gesetzes“ , eine Novellierung des Beschäftigtendatenschutzes sowie eine Novellierung der EU-Datenschutzrichtlinie an. Die Deutsche Telekom wird sich intensiv in die Diskussion rund um Gesetzesänderungen einbringen und beschlossene Gesetze und Novellen unverzüglich umsetzen und anwenden.




Entwicklung in einzelnen Bereichen.

➡ Datenschutz und Datensicherheit funktionieren, wenn jeder Bereich dazu beiträgt.



Privatkunden.

Gesetzliche Regelungen.

Zum 1. April 2010 traten neue Bestimmungen im Bundesdatenschutzgesetz  in Kraft, die die Datenübermittlung über Forderungen an Auskunftsteile, die Datennutzung zu Zwecken der Berechnung von Wahrscheinlichkeitswerten (Scorewerten) und erweiterte Auskunftsrechte des Betroffenen regeln.

Auskunftsteile sind Unternehmen, die geschäftsmäßig bonitätsrelevante Daten über Unternehmen oder Privatpersonen sammeln, um sie bei Bedarf für die Beurteilung der Kreditwürdigkeit eines Betroffenen gegen Entgelt zu übermitteln. Bisher war die Datenübermittlung an solche Auskunftsteile gesetzlich nicht klar geregelt. Nunmehr hat der Gesetzgeber mit der Neuregelung in § 28 a BDSG für eine Klarstellung gesorgt: Es werden fünf konkrete Fallkonstellationen beschrieben, unter denen zum Beispiel das Bestehen einer Forderung gegen Privatpersonen oder Unternehmen an eine solche Auskunftsteil übermitteln darf. Für die Deutsche Telekom waren diese Änderungen ebenfalls relevant. Auch die Telekom meldet unbestrittene offene Forderungen bei Auskunftsteilen wie der Schufa, dem Fraud Prevention Pool (Bürgel) oder der Accumio an. Es wurde prozessual sichergestellt, dass die nach Maßgabe des neuen § 28 a BDSG nunmehr notwendigen Hinweise an die Kunden erteilt und die erforderlichen Fristen zwischen Mahnung und Einmeldung eingehalten werden.

Darüber hinaus wurde die Datennutzung zur Berechnung von so genannten Wahrscheinlichkeitswerten (Scoring) in § 28 b BDSG neu geregelt. Häufig wird der Vertragsschluss an das Vorliegen der Zahlungsfähigkeit und -bereitschaft des Kunden geknüpft (z. B. die Gewährung eines Kredits oder der Abschluss eines Mobilfunkvertrages). Unternehmen bewerten die Liquidität einer Person häufig mittels bestimmter Scorewerte, die in einem als Scoring bezeichneten Verfahren ermittelt werden.

Die Datennutzung zur Berechnung von Scorewerten ist gemäß § 28 b BDSG nunmehr an bestimmte Voraussetzungen geknüpft: Die verwendeten Daten müssen nachweisbar erheblich für die Berechnung einer Zukunftsprognose sein, der Berechnung des Scorewerts muss ein wissenschaftlich anerkanntes Verfahren zugrunde liegen. Ein ausschließlich auf Anschriftendaten beruhender Scorewert ist nach § 28 b BDSG unzulässig.

Die Telekom berechnet einen Scorewert im Rahmen der Bonitätsprüfung eines Interessenten (Neukundenscore) sowie Scorewerte zu den Bestandskunden, d. h. zu Kunden, deren Vertragsverhältnis bereits länger als 5 Monate währt (Bestandskundenscore). Beide Scores geben einen Hinweis, wie wahrscheinlich es ist, dass der Kunde bzw. Interessent in den nächsten Monaten seinen Zahlungsverpflichtungen nicht nachkommen wird. Die Ausfallwahrscheinlichkeiten werden dabei jeweils mit Werten zwischen einem Prozent (sehr niedrige Ausfallwahrscheinlichkeit) und 99 Prozent (sehr hohe Ausfallwahrscheinlichkeit) angegeben.



Dr. Claus-Dieter Ulmer,
Datenschutzbeauftragter der
Deutschen Telekom.



Was unterscheidet den Datenschutz der Deutschen Telekom von dem anderer Unternehmen? Wohin entwickelt er sich in Zukunft?

Datenschutz hat bei der Deutschen Telekom durch die Datenvorfälle eine Dimension erhalten, die andere Unternehmen in dieser Form nicht kennen: Der Verlust von 18 Millionen Kundendaten und besonders die Bespitzelungsaffäre der Jahre 2005 und 2006 haben im Unternehmen eine wahre Schockwelle ausgelöst. Wir haben den Schwung dieser Welle für die bekannten grundlegenden Veränderungen im gesamten Konzern genutzt: Die Einrichtung eines Vorstandsressorts „Datenschutz, Recht und Compliance“ und die Neuausrichtung der Konzernsicherheit sind nur zwei Beispiele. Die Ereignisse der Vergangenheit haben uns dazu gebracht, unseren Datenschutz noch konsequenter weiterzuentwickeln, als wir es ohne entsprechende Vorfälle wahrscheinlich getan hätten. Heute haben wir einen Standard im Datenschutz erreicht, der in der deutschen Wirtschaft nicht selbstverständlich ist. Mittlerweile sind wir in vielen Bereichen Benchmark für andere Unternehmen. Wir teilen unsere Erfahrungen und was wir daraus abgeleitet haben, gerne. Denn wir sehen unsere besondere Verantwortung beim Thema Datenschutz. Dieser werden wir gerecht, indem wir Datenschutz als Service für unsere Kunden begreifen. Ihnen möchten wir mit Ratgebern oder persönlicher Beratung etwa in Chats zeigen, wie sie ihre persönlichen Daten im Alltag schützen können. Wir erfüllen unsere Verantwortung auch, indem wir uns noch stärker als Vorreiter in Sachen Datenschutz in der Deutschen Wirtschaft etablieren. Hier möchten wir Standards weit über die Grenzen unserer Branche hinaus setzen.

Scoring.





Bei Scoring handelt es sich um ein mathematisch-statistisches Verfahren, mit dem die Wahrscheinlichkeit, mit der eine bestimmte Person ein bestimmtes Verhalten zeigen wird, berechnet werden kann. Diese Wahrscheinlichkeit wird angegeben durch den so genannten Scorewert. So kann die Wahrscheinlichkeit des Zahlungsverhaltens des Kunden berechnet werden.

Als Spiegelbild der Regelungen zum Scorewert wurde das Auskunftsrecht des Betroffenen nach § 34 BDSG erweitert, um dem Transparenzgebot Rechnung zu tragen: Der Betroffene darf Auskunft verlangen über die innerhalb der vergangenen sechs Monate (bei Auskunfteien innerhalb der vergangenen 12 Monate) erhobenen bzw. genutzten Scorewerte und darüber, welche Datenarten für die Berechnung verwendet wurden. Des Weiteren hat der Betroffene einen Anspruch darauf, dass ihm nachvollziehbar in allgemein verständlicher Form erklärt wird, wie der Scorewert zustande kam und welche Bedeutung er hat. Aus Transparenzgründen wurde auch § 6 a BDSG erweitert, der nun vorschreibt, dass dem Betroffenen auf Nachfrage bei einer belastenden automatisierten Einzelentscheidung die der Entscheidung zugrunde liegenden wesentlichen Gründe erläutert werden.


Die Deutsche Telekom hat sich hinsichtlich dieser zusätzlichen Auskunftsrechte vorbereitet. Sofern ein Kunde beispielsweise fragt, warum sein Auftrag abgelehnt wurde, wird er vom allgemeinen Kundenservice zu eigens eingerichteten Teams verwiesen, die diese Nachfragen bearbeiten. Diese Mitarbeiter verfügen nun zusätzlich über die erforderlichen Informationen, um dem anfragenden Kunden den wesentlichen Ablehnungsgrund darlegen zu können. Auf diese Weise wird dem Auskunftsrecht Rechnung getragen, gleichzeitig kann aber nur eine eng begrenzte Anzahl speziell geschulter Service-Mitarbeiter auf die teilweise sensiblen Informationen zugreifen.


Weitere Gesetzgebungsverfahren laufen zur Umsetzung der Vorgaben der im Dezember 2009 auf europäischer Ebene in Kraft getretenen Richtlinien für den Kommunikationssektor. Diese europäischen Vorgaben müssen in deutsches Recht umgesetzt werden. Teil dieses Richtlinienpaketes ist die so genannte ePrivacy-Richtlinie (Datenschutzrichtlinie für elektronische Kommunikation). Sie erfordert einige Anpassungen des deutschen Datenschutzrechts. Kernelemente dieser erforderlichen Anpassung sind:

- Ausweitung der Pflicht zur Information über Datenpannen speziell für Anbieter von Kommunikationsdiensten. Die europäischen Vorgaben sehen eine Pflicht zur unverzüglichen Benachrichtigung der Aufsichtsbehörde und des Betroffenen im Fall einer Verletzung des Schutzes personenbezogener Daten vor, beispielsweise durch unberechtigte Verwendung seiner Daten. Darüber hinaus wird die Informationspflicht auch auf interne Vorgänge wie zum Beispiel Entwendung von Daten ausgedehnt
- Verschärfung der Anforderungen an die Einwilligung des Betroffenen in die Verarbeitung personenbezogener Daten. Dies betrifft die Ausdehnung der so genannten Opt-In-Lösung  etwa auf Cookies  in Browsern zum Surfen im Internet oder bei ähnlichen technischen Lösungen, mit denen ein Internetnutzer wiedererkannt werden kann. Dabei sind in erster Linie die Anbieter von Browsern adressiert: Der Internetnutzer soll besser über den Umgang mit seinen personenbezogenen Daten informiert werden und mehr Einfluss auf den Umgang mit seinen Daten beim Einsatz von Cookies haben, als es das deutsche Datenschutzrecht bisher vorsieht. Bei der Umsetzung dieser Vorgaben geht es beispiels-

weise um die Frage, ob der Nutzer jeden Cookie separat akzeptieren können muss oder ob es ausreicht, einmal in den Einstellungen seines Internetbrowsers wählen zu können, welchen Sicherheitsstandard er wünscht, verbunden mit der Möglichkeit, diese Einstellungen jederzeit ändern zu können.

Die Deutsche Telekom begrüßt die Verbesserungen des Schutzes personenbezogener Daten und bringt ihre Ideen hierzu im Gesetzgebungsverfahren zur Umsetzung der ePrivacy-Richtlinie ein. Sie hält es im Sinne eines umfassenden Schutzes allerdings für angebracht, die Anpassungen nicht nur auf Anbieter von Kommunikationsdiensten zu beschränken, sondern auf alle Branchen auszudehnen. Denn etwa auch in der Gesundheitsbranche wird mit sensiblen, personenbezogenen Daten umgegangen, die ein gleiches Maß an Schutz erhalten sollten. Ein solches Schutzniveau kann über die derzeit stattfindende Diskussion über eine Novellierung der europäischen Datenschutzrichtlinie von 1995 erreicht werden (siehe hierzu Seite 28).

Darüber hinaus sollen weitere Vorschriften im Telekommunikationsgesetz  angepasst werden. Kernelemente aus datenschutzrechtlicher Sicht sind:

- Anpassung von Vorschriften, um etwa eine Wartung von Systemen nach dem „Follow-the-Sun-Prinzip“ zu ermöglichen. Beispielsweise kann dann ein Wartungsvorgang morgens in Deutschland begonnen, nach Betriebschluss in den USA fortgesetzt und nach dortigem Arbeitsende in Indien beendet werden. Dabei gilt es, die Einhaltung datenschutzrechtlicher Regelungen sicherzustellen
- Überarbeitung der datenschutzrechtlichen Regelungen für die Nutzung von Standortdaten im Rahmen von so genannten Lokalisierungsdiensten (Location Based Services )

Opt-In, Opt-Out.

Opt-In bezeichnet einen Vorgang zur Nutzung von Kundendaten: Bei diesem Verfahren müssen Unternehmen für jede Nutzung von Daten die Zustimmung der Kunden erfragen. Sie dürfen die Daten nur dann nutzen, wenn der jeweilige Kunde explizit zugestimmt hat, etwa per E-Mail, Telefon oder SMS.



Bei der Opt-Out-Lösung nutzen Unternehmen die Kundendaten so lange, bis der jeweilige Kunde der Nutzung widerspricht. Über die Art und Weise der Nutzung müssen die Kunden in den Datenschutzhinweisen informiert werden.

Die Deutsche Telekom wird die Gesetzentwürfe bewerten und das Gesetzgebungsverfahren begleiten, um die Regelung nach deren Verabschiedung durch den Gesetzgeber zügig umsetzen zu können.

Speicherung und Sicherheit von Kundendaten.

Die Deutsche Telekom speichert und verarbeitet die Daten von fast 60 Millionen Privatkunden in Festnetz und Mobilfunk. Der Konzern ist sich seiner Verantwortung im Umgang mit diesen hoch sensiblen Daten bewusst. Ihr Schutz steht für die Deutsche Telekom an oberster Stelle. Auch im Jahr 2010 hat das Unternehmen Schritte unternommen, um den Schutz dieser Daten weiter zu verbessern.

Konzernweite Einwilligungsklausel zur Nutzung von Kundendaten.

Wie zahlreiche andere Unternehmen informiert die Deutsche Telekom Kunden über neue oder verbesserte Produkte und Dienste. Hierfür nutzt sie unter strengen Voraussetzungen die vorliegenden Kundendaten: Eine Ansprache darf nur erfolgen, wenn der Kunde seine Einwilligung zur Nutzung seiner Daten für Werbungs- und Marktforschungszwecke erteilt hat. Die Einwilligung wird in Form der so genannten konzernweiten Einwilligungsklausel (KEK)  eingeholt. Dabei kann der Kunde sich entscheiden, ob und in welcher Form er Werbung der Deutschen Telekom erhalten möchte. Das geschieht schriftlich im Rahmen eines Auftragsformulars, telefonisch oder online. Die Kunden der Deutschen Telekom können ihren Einwilligungsstatus im Kundenportal unter www.telekom.de jederzeit einsehen und ändern. Im Rahmen der Gründung der Telekom Deutschland GmbH  wurden alte Formen der Einwilligungsklausel in einem neuen System zusammengeführt und harmonisiert. Die Deutsche Telekom hat die Zusammenführung und Harmonisierung der Aufsichtsbehörde vorgestellt, beides wurde von dieser zustimmend zur Kenntnis genommen.


Gespeicherte Daten bei der Deutschen Telekom.

Die Deutsche Telekom speichert Kundendaten (Bestandsdaten) und Daten, die beim Telefonieren anfallen, die so genannten Verkehrsdaten. Die Verkehrsdaten sind technisch notwendig zur Herstellung und zum Aufrechterhalten der jeweiligen Verbindung. Danach werden sie zum Zweck der Abrechnung mit dem Kunden oder mit anderen Diensteanbietern verwendet. Folgende Verkehrsdaten werden hierfür bei Telefonanschlüssen (Festnetz, Mobilfunk und Internet) gespeichert und verwendet, soweit relevant:


- Rufnummer oder Kennnummer des anrufenden und des angerufenen Anschlusses
- in Anspruch genommene Dienstleistung
- Beginn und Ende der Verbindung
- bei Mobiltelefonie zusätzlich Standortkennung, Mobilfunk-Kartennummer und Mobilfunk-Gerätenummer
- bei Internetnutzung der lokale Einwahlknoten
- Abrechnungsdaten:
 - Beginn und Ende der einzelnen Verbindung
 - Verbindungsart
 - Volumen der übertragenen Daten
 - in Anspruch genommene kostenpflichtige Dienste
 - Informationen über etwaige Guthabenaufladung
- Daten über ankommende Verbindungsversuche und Benachrichtigungen werden nur im Rahmen eines entsprechenden Dienstangebotes (z. B. Mobilbox- und Kurzmitteilungsanwendungen) verwendet
- Nachrichteninhalte selbst werden nur dann gespeichert, wenn der Kunde dies beauftragt (z. B. Mobilbox- und Kurzmitteilungsanwendungen) oder entsprechende Dienste eine Zwischenspeicherung erfordern, z. B. bei Kurzmitteilungen (SMS) oder Multimedia-Messages (MMS)

Die Verkehrsdaten fallen bei jeder Verbindung an, da sie zur Herstellung bzw. Aufrechterhaltung der Verbindung erforderlich sind. Im Abrechnungsprozess werden die Verkehrsdaten aussortiert, die nicht abrechnungsrelevant sind. Diese werden gelöscht. Das betrifft insbesondere Verkehrsdaten, die im Rahmen einer Flatrate anfallen. Im Einzelverbindungs-nachweis werden diese Daten nicht ausgewiesen. Abrechnungsdaten werden bis zu 80 Tage nach Rechnungsversand gespeichert oder nach Kundenwunsch sofort nach Rechnungsversand gelöscht. IP-Adressen speichert die Deutsche Telekom zur Bekämpfung von Spam und schadhaftem Code (Viren, Würmer etc.) sieben Tage lang. Generell verfolgt die Deutsche Telekom den Grundsatz der Datensparsamkeit: Es werden nur so viele Daten gespeichert, wie nötig sind. Um diese Daten zu schützen, entwickelt das Unternehmen seine Systeme und Prozesse kontinuierlich weiter.

Sicherheit für Kundendaten durch „External Workforce Management“-Programm.

Die Deutsche Telekom arbeitet mit zahlreichen externen Partnern, etwa in den Bereichen IT, Callcenter , Entwicklung oder Vertrieb, zusammen. Diese Partner greifen auf interne (IT-)Systeme der Telekom zu, um ihre vertraglichen Aufgaben erfüllen zu können. Um diesen Systemzugriff unter jeglichem Aspekt sicher zu gestalten, hat der Vorstandsbereich Personal das Programm „External Workforce Management“ eingesetzt. Dieses stellt sicher, dass die rechtlichen Risiken aus dem Einsatz externer Kräfte erfasst, bewertet und reduziert werden. Darüber hinaus sorgt es dafür, dass die Identitäten externer Dienstleister eindeutig in den HR-Systemen erfasst werden. Neben den rechtlichen Risiken ergeben sich hieraus Risiken aus dem Umgang der externen Partner mit den Daten der Kunden der Deutschen Telekom und den dafür notwendigen IT-Systemzugängen. Durch das Programm wird im Wesentlichen sichergestellt, dass interne Mitarbeiter und (externe) Partner nur auf die für die Erfüllung ihrer Arbeit notwendigen Systeme zugreifen können und zum Beispiel keine sachfremden Daten sammeln können. Begleitende Prozesse stellen darüber hinaus sicher, dass alle Zugriffsberechtigungen nur im Rahmen der Aufgabenerfüllung aktiviert bleiben und diese im Falle der finalen Vertragserfüllung oder bei organisatorischem Wechsel umgehend gelöscht werden.

Sicherheit für Kundendaten durch cIAM – Identity Management.

Das IT-Programm Corporate Identity and Account Management (cIAM)  verwaltet digitale Identitäten für Benutzer und Arbeitsplätze innerhalb der Deutschen Telekom. Zweck ist es, über eine Standardisierung von Identitäts- und Account-Management-Prozessen sicherzustellen, dass nur die Mitarbeiter auf Systeme und Applikationen zugreifen können, die aktuell im oder für das Unternehmen arbeiten. Scheiden Mitarbeiter aus dem Unternehmen aus, ermöglicht das Identitätsmanagementsystem einen systemübergreifenden Entzug der Zugriffsberechtigungen auf angeschlossene Systeme und Applikationen. Verändern Mitarbeiter sich im Unternehmen, stellt das Identitätsmanagement sicher, dass ein automatischer Entzug von genutzten Rollen/Berechtigungen erfolgt.

Bisher erfolgten Account- und Berechtigungsvergaben sowie der Entzug der Berechtigungen dezentral, mit unterschiedlichen Prozessen und Akteuren. Das neue Verfahren gilt für alle Konzerneinheiten und hat die Freigabe der Sozialpartner erhalten. Die Implementierung hat begonnen und wird in den kommenden Jahren sukzessive auf weitere Systeme und Applikationen ausgeweitet.

Löschen von Vertragsdaten in internen Systemen.

Aufgrund gesetzlicher Verpflichtung müssen die Vertragsdaten von Kunden mit Ablauf des auf das Vertragsende folgenden Kalenderjahres gelöscht werden. Im Bereich von Kunden, die mehrere Verträge mit der Deutschen Telekom unterhalten, bedeutet das, dass die Vertragsdaten dann gelöscht werden müssen, wenn keinerlei Geschäftsbeziehungen mehr bestehen. Im Rahmen einer internen Kontrolle wurde festgestellt, dass das System für Festnetzkunden über keinen Regelprozess verfügte, nach dem die Vertragsdaten der Kunden innerhalb der gesetzlichen Vorgaben gelöscht werden. Die Bereinigung der zu löschenden Vertragsdaten wurde im Jahr 2010 abgeschlossen und ein automatisierter Prozess eingeführt, nach dem die automatische Löschung gemäß der gesetzlichen Vorgabe erfolgt. Im System für Mobilfunkkunden wurden die Vertragsdaten bis auf die Kundenkontaktdaten rechtskonform gelöscht. Seit Oktober 2010 erfolgt die Bereinigung des Systems um diese Daten kontinuierlich. Allerdings wird ihre vollständige Löschung aufgrund technischer Beschränkungen erst Ende 2011 beendet sein. Auch in diesem System wurde ein entsprechender Regelprozess für die Löschung implementiert.

Nachhaltige Kundenbeziehungen.

Eine Einhaltung der datenschutzrechtlichen Vorgaben im Umgang mit Kunden ist für die Deutsche Telekom selbstverständlich. Der Konzern legt Wert darauf, dass nicht nur seine eigenen Mitarbeiter die Vorschriften einhalten, sondern achtet besonders auch bei externen Vertriebspartnern auf Regelkonformität.


Compliance.



Compliance bezeichnet die Einhaltung von Regeln, Gesetzen und Richtlinien durch Unternehmen und deren Mitarbeiter. Die Deutsche Telekom legt Wert darauf, dass sich alle Mitarbeiter wertekonform verhalten und nach internen Regelungen und Gesetzen handeln. Der Bereich Compliance unterstützt die Mitarbeiter mit Serviceangeboten dabei, diesen Anspruch in ihrer täglichen Arbeit umzusetzen. Neben einer Richtlinienbank stehen den Mitarbeitern dafür Schulungen zur Verfügung. Über spezielle Portale können Mitarbeiter Verhaltensunsicherheiten klären und Hinweise zu regelwidrigem Verhalten geben.

Als Premiumdienstleister will die Deutsche Telekom ihren Kunden einen Service bieten, der über gesetzliche Mindeststandards hinausgeht. Dies gilt sowohl für den Bereich Datenschutz als auch für Service allgemein. Mit einem 2010 aufgesetzten Programm zur „Integrität im Kundenkontakt“ entwickelt die Deutsche Telekom ihren Vertrieb und Service weiter. Das Programm sieht vor, Vorgaben zu einem rechtlich und ethisch einwandfreien Verhalten und einer bedarfsgerechten Beratung im Kontakt zu Kunden zu etablieren. Ziel: langfristig zufriedene Kunden, die der Deutschen Telekom bezüglich eines rechtlich und menschlich korrekten Umgangs vertrauen.

Folgende Maßnahmen setzt die Deutsche Telekom seit Herbst 2010 um (Beispiele):

- Erweiterung des bestehenden Zertifizierungskonzepts für Vertriebspartner um den Themenschwerpunkt korrektes Verhalten und bedarfsgerechte Beratung
- Schulungen zur Qualifizierung der Außendienstmitarbeiter im Auftrag der Deutschen Telekom, Schulungen für Mitarbeiter in Callcentern 
- Ergänzungen im verbindlichen Verhaltenshandbuch (Code of Contact) für Außendienstmitarbeiter im Auftrag der Deutschen Telekom
- Verhaltensanforderungen zur Integrität im Kontakt mit Kunden als fester Bestandteil des Verhaltenskodex für alle Mitarbeiter (Code of Conduct)



Manuela Mackert,
Chief Compliance Officer
der Deutschen Telekom.



Compliance bedeutet die Einhaltung von Gesetzen, Richtlinien und Verhaltensregeln durch Unternehmen und deren Mitarbeiter. Gibt es dabei Schnittstellen zum Thema Datenschutz?

Natürlich! Compliance und Datenschutz haben viele Berührungspunkte. Zum einen: Jeder Datenschutzverstoß stellt auch einen Compliance-Fall dar. Zum anderen: Die Mitarbeiter in unserem Bereich sind natürlich in vertrauliche Sachverhalte und Ermittlungen eingebunden. Dabei ist es unerlässlich, dass sie selbst die Vorgaben des Datenschutzes einhalten. Wir bekommen unterschiedlichste Hinweise auf Gesetzes- oder Richtlinienverletzungen. Nur wenn sich die Hinweisgeber darauf verlassen können, dass sie auf Wunsch anonym bleiben und ihre Angaben in jedem Fall vertraulich behandelt werden, werden sie überhaupt eine Meldung abgeben. Und nur, wenn auch die Persönlichkeitsrechte direkt oder indirekt Betroffener beachtet werden, verhält sich die Deutsche Telekom umfassend gesetzeskonform – eben compliant.

Datenschutz ist also aus zweierlei Gründen für Compliance grundlegend: Er sichert uns das Vertrauen unserer Hinweisgeber. Und er stellt sicher, dass die Rechte der Betroffenen gewahrt bleiben.





Ich will noch einen Schritt weiter gehen: Compliance wird durch einen funktionierenden Datenschutz überhaupt erst möglich. Deshalb ist Datenschutz gerade in unserem Bereich auch kein „Kann-Thema“, sondern zwingende Voraussetzung für unsere erfolgreiche Arbeit zum Wohle des Konzerns und seiner Mitarbeiter.

Sonderthemen im Bereich Privatkunden.

Die Deutsche Telekom hat auch im Jahr 2010 ihre Serviceleistungen weiter ausgebaut. Dabei hat das Unternehmen die Anforderungen an den Datenschutz und die Datensicherheit von vornherein berücksichtigt. In Fällen, in denen Mängel im Bereich Datenschutz und Datensicherheit festgestellt wurden, hat die Deutsche Telekom umgehend reagiert und Maßnahmen zur Behebung ergriffen.


Im Jahr 2010 haben darüber hinaus strukturelle Veränderungen innerhalb des Unternehmens zu Änderungen auch für Datenschutz und Datensicherheit geführt.

Änderungen infolge Gründung der T-Deutschland GmbH.

Als zum 1. April 2010 die damaligen Konzernbereiche T-Home und T-Mobile in der Telekom Deutschland GmbH  zusammengefasst wurden, bedeutete dies für den Kundendatenschutz zahlreiche organisatorische Vereinfachungen und gleichzeitig Weiterentwicklungen. So wurde 2010 unter anderem eine neue Organisationsstruktur zum Risikomanagement im Vertrieb aufgebaut, die die Sicherheit von Daten im Vertrieb und die Umsetzung von Vorgaben zur Compliance  gewährleistet. Darüber hinaus führt der neue Organisationsbereich Audits  und Zertifizierungen  von Vertriebspartnern durch. Ihm obliegt ebenfalls die Vertriebs- und Servicekontrolle.

Auch wenn der Weg zu einem integrierten Angebot von Festnetz und Mobilfunk viele datenschutzrechtliche Herausforderungen mit sich brachte, ergeben sich mit der Integration beider Geschäftsfelder aus Daten schutzsicht viele Erleichterungen. Ein kurzer Rückblick auf die Situation vor dem Zusammenschluss verdeutlicht dies: Ein Kunde, der sowohl einen Festnetzanschluss, als auch einen Mobilfunkanschluss der Deutschen Telekom besaß, hatte zwei Vertragspartner: die Deutsche Telekom AG (T-Home) und die T-Mobile Deutschland GmbH. Aus Datenschutzsicht bedeutete dies eine getrennte Kundendatenhaltung. Ein Austausch der Kundendaten zwischen T-Home und T-Mobile war nur mit Einwilligung des Betroffenen rechtlich zulässig. So war es nicht möglich, den Kunden auf beide Anschlüsse anzusprechen, was oft genug auch für den Kunden unverständlich war.

Heute stellt sich die Ausgangslage einfacher dar: Die Telekom Deutschland GmbH ist der einzige Vertragspartner des Kunden, unabhängig davon, ob der Kunde einen Festnetz- und/oder einen Mobilfunkanschluss hat. Damit geht einher, dass zukünftig nur noch eine einheitliche Datenbank existieren soll, in der alle Kundendaten gespeichert und verarbeitet werden. Die Kundenberatung hat dann Zugriff auf alle Verträge, die ein Kunde mit der Telekom eingegangen ist. Die Integrationsmaßnahmen rund um die Gründung der Telekom Deutschland GmbH fanden

bei datenschutzrechtlichen Fragen in enger Abstimmung mit den Aufsichtsbehörden (insbesondere mit dem Bundesdatenschutzbeauftragten ) statt. Ein wichtiges mittelfristiges Projekt für das Jahr 2011 ist die Vereinheitlichung der verschiedenen IT-Landschaften im Festnetz- und im Mobilfunkbereich, d. h. die Migration und die Zusammenführung der Daten aus den alten Systemen in einen gemeinsamen Datenspeicher, der allen Anforderungen an eine datenschutzgerechte und sichere Datenverarbeitung gerecht wird.

Die Deutsche Telekom unterliegt der Verpflichtung, bei technologischen und/oder organisatorischen Änderungen das geforderte Sicherheitskonzept nach TKG § 109 anzupassen. Schwerpunkte des Konzepts sind der Schutz des Fernmeldegeheimnisses und der Schutz personenbezogener Daten, der Schutz von Telekommunikationsanlagen vor unerlaubten Zugriffen und die Abschirmung von Telekommunikationssystemen gegen äußere Angriffe und Katastrophen. Aufgrund der Verschmelzung von T-Mobile und T-Home zur Telekom Deutschland GmbH wurde daher ein modifiziertes Sicherheitskonzept für die Telekom Deutschland GmbH aus den bereits bestehenden Einzelkonzepten von T-Mobile und T-Home entwickelt. Die Deutsche Telekom hat das Sicherheitskonzept im Oktober 2010 der Bundesnetzagentur als ihrer Aufsichtsbehörde im deutschen Markt vorgelegt. Eine Stellungnahme der Bundesnetzagentur stand zum Zeitpunkt des Redaktionsschlusses noch aus.

Twitter – ein neues Element der Kundenberatung.

Die Telekom hilft, jetzt auch online: Immer mehr Kunden wünschen sich bei Fragen schnellen, unbürokratischen Kontakt zur Deutschen Telekom. Diesen stellt das Unternehmen seit Mai 2010 über den Online-Dienst Twitter als Element in der Kundenberatung her. Da sämtliche Dialoge über Twitter weltweit öffentlich zugänglich sind, wurden interne Rahmenbedingungen zur Nutzung des Kommunikationsdienstes für die Kundenberatung festgelegt, um den Datenschutz im Sinne der Kunden sicherzustellen. Die Mitarbeiter sind angewiesen, soziale Dienste nur zur Kontaktaufnahme und für allgemeine, nicht vertragsbezogene Fragen zu nutzen. Auf diese Weise wird die Privatsphäre der Kunden geschützt. Sobald der Kunde eine individuelle Beratung wünscht, greifen die Mitarbeiter zu anderen Kommunikationsmöglichkeiten wie E-Mail oder Brief. Diese Regeln werden den Mitarbeitern vor Ort durch den Kundenservice in Schulungen vermittelt.

Regeln zur Nutzung von Twitter & Co für die Kundenberatung.



1. Soziale Netzwerke und öffentliche Foren, z. B. Twitter, Facebook etc. dürfen lediglich zur initialen Kontaktaufnahme verwendet werden, mit dem Ziel, unverzüglich auf einen anderen geschützten bzw. nicht-öffentlichen Kommunikationskanal (E-Mail, SMS, Post, Telefon) umzuschwenken.
2. Über soziale Netzwerke und Foren selbst darf keine individuelle teilnehmeranschluss oder -anschriftbezogene Kundenberatung durchgeführt werden. Eine allgemeine Produktberatung ist jedoch zulässig.
3. Die Anzahl der Mitarbeiter, die Aufgaben der Kundenberatung in sozialen Netzwerken oder Foren wahrnehmen, ist zu begrenzen. Diese Personen sind hinsichtlich der Nutzung des Mediums besonders zu schulen und es ist zu empfehlen, diese Personen auch besonders auf die datenschutzrechtlichen Regelungen zur Nutzung sozialer Netzwerke und Foren zu verpflichten.
4. Unabhängig davon sind die Personen mit einer Verpflichtungserklärung auf das Daten- und Fernmeldegeheimnis zu verpflichten und entsprechend zu sensibilisieren. Dies muss vor der Aufnahme der Nutzung erfolgen.
5. Soweit beabsichtigt ist, dass die Mitarbeiter mit realem Namen an der Kundenberatung teilnehmen, muss hierüber zuvor der Betriebsrat informiert werden. Dies kann nicht gegen den Willen des Mitarbeiters erfolgen.
6. Die über die sozialen Netzwerke geführten Dialoge sind nach näherer Beteiligung des Betriebsrats regelmäßig auf die Erhaltung des Kommunikationsverhaltens gem. Punkten 1 und 2 zu auditieren.
7. Beim Beginn eines jeden Kommunikationsvorgangs ist der Kunde/ Interessent darauf hinzuweisen, dass er keinesfalls persönliche Daten über die öffentlichen Kanäle des Netzwerks preisgeben sollte. Es wird empfohlen, den Hinweis mit Group Privacy abzustimmen.
8. Kein zur Kundenberatung in sozialen Netzwerken und Foren berechtigter Mitarbeiter darf einen Kunden oder Interessenten über soziale Netzwerke auffordern, seine persönlichen Daten öffentlich preiszugeben oder sich dort zu legitimieren.
9. Soweit ein Kunde/Interessent seine persönlichen Daten über die öffentlichen Kanäle eines sozialen Netzwerks preisgibt, darf die Kommunikation hier nicht weiter fortgesetzt werden. Auf gar keinen Fall darf eine Bestätigung dieser Informationen über diesen öffentlichen Kanal erfolgen.
10. Mitarbeitern, die sich hierbei nicht an die vorgenannten Grundsätze halten, muss die Berechtigung zur Teilnahme an einer Kundenberatung im Rahmen der sozialen Netzwerke unverzüglich wieder entzogen werden.





„Telekom hilft“ heißt der neue Internet-Service der Telekom Kundenberatung. Über den Onlinedienst Twitter und über Facebook geben Mitarbeiter Rat und Hilfestellung.

Fehlerbeseitigung im Mobilfunk mittels „Customer-Experience-Management“.

Ihren Kunden den bestangesehenen Service zu bieten, ist erklärtes Ziel der Deutschen Telekom. Vor diesem Hintergrund hat die Telekom Deutschland GmbH mit dem so genannten Customer-Experience-Management Tool (CEM-Tool) eine Anwendung entwickelt, um im Mobilfunk zukünftig Fehler bzw. Probleme aus Kundensicht zu analysieren und geeignete Maßnahmen zur Störungs- bzw. Problembeseitigung zu initiieren. Derzeit befindet sich das Instrument in der Abstimmung mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Es ist geplant, das CEM-Tool nach erfolgter Freigabe für den Einsatz in anderen Technologiebereichen weiterzuentwickeln.

Nutzung von Geodaten durch die Deutsche Telekom.

Dienstleistungen, die auf Geodaten  zugreifen, werden mehr und mehr Bestandteil des Alltagslebens. Gleichzeitig bieten Geodienste  viele Impulse für weitere innovative Entwicklungen. Auch die Deutsche Telekom nutzt für Dienstleistungen Kartenmaterial von entsprechenden Anbietern: So integriert beispielsweise die Telekom-Tochter Immoscout24 Bilder von Google Street View in ihr Angebot. Auch DeTeMedien bietet auf www.telefonbuch.de gemeinsam mit den Telefonbuchverlagen eine Verknüpfung von öffentlichen Telefonbucheinträgen mit Häuseraufnahmen aus der

Vogelperspektive und Schrägansicht an. Das hierfür genutzte Kartenmaterial ist im Internet frei zugänglich. Der Kunde hat die Möglichkeit, der Verknüpfung seiner Adresse mit dem Kartenmaterial jederzeit zu widersprechen. Im Jahr 2010 hat die Deutsche Telekom die Hinweise auf diese Widerspruchsmöglichkeiten im Sinne von Transparenz und Verbraucherefreundlichkeit noch deutlicher hervorgehoben: Sie hat insbesondere die Datenschutzhinweise auf „telefonbuch.de“, „gelbseiten.de“ und „dasoertliche.de“ um eine gesonderte Information ergänzt.

Löschung von Daten auf Leihgeräten aus den T-Shops.

Kunden können sich in den T-Shops Geräte leihen, wenn etwa ihr eigenes Mobiltelefon in Reparatur ist. Laut einer Kundenbeschwerde waren auf einem dieser Leihgeräte die Daten eines vorherigen Nutzers vorhanden. Daraufhin wurde der Prozess zur Löschung mobiler Endgeräte der Telekom Shop Vertriebsgesellschaft (TSG) geprüft und mittels einer Stichprobe auditiert. Ergebnis: Der Prozess der Löschung war gut bekannt und dokumentiert. Kleinere Dokumentationslücken gab es nur in einem Shop, in allen anderen Shops wurde der Prozess eingehalten. Im auffälligen Shop wurden die Mitarbeiter noch einmal gesondert geschult. Weitere Stichprobenaudits in den Shops erfolgen regelmäßig.

Löschung auf zur Reparatur gegebenen Geräten.

Wird ein Mobiltelefon in einem T-Shop zur Reparatur gegeben, schickt dieser das Gerät zum Hersteller. Der betroffene Kunde erhält im Regelfall ein anderes repariertes Gerät aus einem so genannten Austauschpool zurück. Die Löschung der Daten auf den jeweiligen Geräten ist in diesem Prozess verbindlich geregelt: Der Kunde verpflichtet sich, persönliche Daten von seinem Mobiltelefon zu löschen, bevor er es abgibt. Da ein Löschen aufgrund des technischen Defekts des Geräts durch den Kunden unter Umständen nicht möglich ist, wird auch der Hersteller vertraglich zum Löschen von Daten verpflichtet, die gegebenenfalls noch auf dem Gerät gespeichert sind. Einzelne Kundenbeschwerden besagten, dass nicht alle Hersteller die Daten konsequent löschen, obwohl die datenschutzrechtlichen Anforderungen durch die Deutsche Telekom klar definiert sind. Unabhängig von diesen Vorfällen hat die Deutsche Telekom damit begonnen, den gesamten Löschprozess auf Schwachstellen zu überprüfen.

Missbrauch von T-Online-Kennungen.

Mehrere Staatsanwaltschaften ermitteln, weil 2009 Kennungen von T-Online-Kunden mutmaßlich durch Tricks (z. B. Phishing) in die Hände von Betrügern gelangten. Die Kennungen wurden von den Tätern genutzt, um so genannte Load-Keys über die Portale Softwareload und Gamesload zu kaufen. Hierbei handelt es sich um Aktivierungsschlüssel, die einen Download von Software über das Internet ermöglichen. Die betroffenen Kunden erhielten für das Herunterladen von Software Beträge in Rechnung gestellt, die sie nicht zuordnen konnten. Die Telekom hatte die Kun-

den gebeten, Strafanzeige wegen Betruges zu stellen. Die daraufhin geführten Ermittlungen wurden von Anfang an von der Telekom begleitet und unterstützt. Die internen Ermittlungen des Konzerns haben keinen Anhaltspunkt dafür gegeben, dass Mitarbeiter in die Fälle verwickelt sind. In den vergangenen Jahren gab es immer wieder Betrugsfälle, die auf Identitätsdiebstahl oder so genanntes Social Engineering zurückzuführen sind. Dabei versuchen Täter beispielsweise, über soziale Netzwerke Informationen wie Zugangsdaten ihrer Opfer zu bekommen. Den Betrug über Telefonrechnungen hat die Telekom durch technische Maßnahmen seit Oktober 2009 unterbunden: Kunden können nur noch von ihrem eigenen Anschluss aus die Bezahlart „Telefonrechnung“ wählen. Betrügerische Käufe, etwa über Kreditkarten, lassen sich allerdings nicht völlig ausschließen.

Weitergabe von Zugangsdaten an ein soziales Netzwerk.

Im November 2010 hat die Deutsche Telekom einen Online-Hinweis geschaltet, der beim Einloggen auf T-Online-Konten sichtbar ist. Er informiert Kunden über ein erhebliches Missbrauchsrisiko, wenn sie in einem sozialen Netzwerk ihre persönlichen Zugangsdaten weitergeben. Anlass für diesen Hinweis war eine neue Funktion in einem sozialen Netzwerk. Dieses hat seinen Nutzern die Möglichkeit eröffnet, ihr Adressbuch, wie etwa das T-Online-Adressbuch, in das Netzwerk zu laden. Der Anbieter gleicht die so gewonnenen Daten mit seiner internen Datenbank ab. Er kann so herausfinden, wer bereits Mitglied ist und wer (noch) nicht.

Die Deutsche Telekom hält eine solch umfassende Weitergabe persönlicher Daten für unzulässig: Sie ermöglicht, dass Dritte auf das jeweilige persönliche Konto des Kunden im Telekom-Kundencenter zugreifen können. Damit haben sie auch Zugriff auf Funktionen wie E-Mail, Onlinebanking und sämtliche Vertragsdaten. Darüber hinaus handelt es sich um ein vertragswidriges Verhalten, da die Weitergabe der persönlichen Zugangsdaten gemäß den allgemeinen Geschäftsbedingungen untersagt ist. Außerdem ist eine solche Verknüpfung auch insofern bedenklich, als dadurch sensible personenbezogene Daten Dritter übermittelt werden, ohne dass der Kunde darüber informiert ist oder eingewilligt hat. Hierin sieht die Deutsche Telekom einen Verstoß gegen bundesdatenschutzrechtliche Bestimmungen. Diese Bewertung ändert sich nicht durch Beteuerungen von Betreibern einiger sozialer Dienste, diese Daten nicht zu internen Zwecken zu nutzen.

Erhebung von Bewegungsdaten zur Erfassung von Geschwindigkeiten.

Die Hersteller von Navigationsgeräten haben ein Interesse an möglichst präzisen Stauprognosen, die als Zusatzdienste angeboten werden. Auf diese Weise kann ein optimierter Verkehrsfluss zur Stauvermeidung oder -verringering erreicht werden. Um Prognosen zu erstellen, möchten die Dienstleister die Bewegungsdaten von Mobiltelefonen nutzen. Hierzu bieten Mobilfunkanbieter den Herstellern von Navigationssystemen Daten als Vorleistungsprodukt an. Da diese Daten grundsätzlich auf einen bestimmten Mobilfunkanschluss und damit auf eine bestimmte Person zurückgeführt werden können, muss eine Anonymisierungslösung gefunden werden, die die persönlichen Daten der Mobilfunkeinsteiger schützt. Missbrauch von Daten muss generell ausgeschlossen werden, etwa das Ahnden von Geschwindigkeitsübertretungen. Zwei Wettbewerber bieten diesen Dienst bereits an, die Deutsche Telekom möchte ihn ebenfalls aufnehmen.

Mit dem Bundesdatenschutzbeauftragten wurden die Möglichkeiten diskutiert, wie Daten anonymisiert werden müssen. Darüber hinaus wurde geklärt, wie lange und in welcher Form Informationen (so genannte Lokalisierungsdaten), mit denen sich Rückschlüsse auf die Bewegung des Mobiltelefons ziehen lassen, gespeichert oder den Betreibern von Navigationssystemen zur Verfügung gestellt werden dürfen. Die gefundene Lösung fand die Zustimmung des Bundesdatenschutzbeauftragten. Das Produkt soll im Laufe des Jahres 2011 eingeführt werden.

Mahnverfahren durch Kanzlei Seiler.

Wenn ein Kunde bei ausstehenden Rechnungen auf Mahnungen der Deutschen Telekom nicht reagiert, übernehmen die Rechtsanwälte Seiler und Kollegen die weitere Geltendmachung der offenen Kundenforderungen.

Der zuständige Landesdatenschutzbeauftragte Baden-Württemberg wies die Deutsche Telekom auf verschiedene Punkte hin, die aus Sicht der Behörde bei der Kanzlei Seiler datenschutzrechtlich zu beanstanden sind. Dazu zählten beispielsweise die Form der Benachrichtigung der Betroffenen oder die Löschrufen für die Schuldnerdaten. In einer Diskussion mit dem Landesdatenschutzbeauftragten wurde Übereinstimmung darin erzielt, dass das Bundesdatenschutzgesetz **[G]** auch auf Anwaltskanzleien anwendbar ist, soweit die anwaltliche Schweigepflicht nicht beeinträchtigt ist. In weiteren Gesprächen konnten die vom Landesdatenschutzbeauftragten kritisierten Aspekte geklärt werden: Um den Kunden die Ausübung ihres Auskunftsrechts nach § 34 Bundesdatenschutzgesetz zu erleichtern, hat die Telekom Deutschland auf Anregung der Aufsichtsbehörde hin Rechtsanwalt Seiler diesbezüglich von seiner Schweigepflicht entbunden. Auskünfte zu den Inkassodaten kann nun auch der Rechtsanwalt im Auftrag der Telekom Deutschland erteilen. Außerdem wurde die Benachrichtigung der Schuldner durch Rechtsanwalt Seiler erweitert.

Geschäftskunden.

Cloud Computing – Dynamic Computing.

Der Cloud Computing-Markt ist ein Markt mit hohem Wachstumspotenzial. Betrug sein Volumen im Jahr 2009 weltweit rund 13 Milliarden Euro, sagen verschiedene Analysten einen Anstieg auf 45 Milliarden Euro und zum Teil bis zu 150 Milliarden Euro bis 2013 voraus. Die Deutsche Telekom hat die Erschließung dieses Wachstumsmarkts in ihrer im März 2010 vorgestellten Strategie „Verbessern – Verändern – Erneuern“ als Kernelement identifiziert. Hier will das Unternehmen mit neuen Produkten Kundenbedürfnissen entsprechen und am Wachstum partizipieren.

Cloud Computing bietet dem Kunden zahlreiche Vorteile, insbesondere enorme Kosteneinsparungen. Für Anbieter solcher Lösungskonzepte bringt es Herausforderungen im Bereich der technischen Bereitstellung und der Gewährleistung einer hohen Sicherheit mit sich.

Die Deutsche Telekom bietet verschiedene Cloud Computing-Lösungen unter dem Begriff Dynamic Computing an. Sie konzentriert sich in ihrem Angebot aktuell auf den Geschäftskundenbereich. Informationen unter <http://geschaefstkunden.telekom.de>

T-Systems liefert solche Dienstleistungen dabei sowohl für den internen Bedarf als auch für Geschäftskunden der Deutschen Telekom. Die Sicherheit der Cloud Computing-Dienste ist dabei ein kritischer Erfolgsfaktor. Sie wird durch eine konzernweite übergreifende Zusammenarbeit verschiedener Bereiche der Deutschen Telekom gewährleistet. So entwickelt der Bereich IT-Sicherheit die technischen Sicherheitsanforderungen. Der Bereich Datenschutz stellt sicher, dass der Schutz der verarbeiteten Daten Priorität hat. Bereits bei der Entwicklung der Dynamic Computing-Services durch T-Systems floss konzernweites Fachwissen ein. Das Unternehmen hat die aktuellen Risiken und Bedrohungsszenarien für die Dynamic Computing-Plattform im Detail untersucht und eine umfangreiche technische Lösung etabliert: Dabei hat die Deutsche Telekom eine sichere Gesamtarchitektur der Cloud konzipiert und umgesetzt, in der die einzelnen Anwendungen der Kunden komplett und sicher voneinander getrennt werden können. Die Umsetzung und der weitere Entwicklungsprozess werden von den Bereichen Datenschutz und IT-Sicherheit kontinuierlich im Rahmen des Privacy and Security Assessment (PSA) -Verfahrens (siehe Seite 33) begleitet. Dies gilt nicht nur für die Plattform selbst, sondern auch für alle Anwendungen, die darauf betrieben werden. Alle Migrationen aus der klassischen Betriebsumgebung in die Cloud werden über den PSA-Prozess durch Spezialisten begleitet. Damit wird sichergestellt, dass die Sicherheitsdokumentation (standardisiertes Datenschutz- und Sicherheitskonzept) für die betroffene Anwendung auf dem neusten Stand ist.

Cloud Computing – Dynamic Computing.



Beim Cloud Computing (von Cloud, englisch für Wolke) werden Infrastrukturen der Informationstechnologie, die bisher im Gebäude eines Kunden aufgestellt wurden, zentral in Rechenzentren zusammengeführt. So werden zum Beispiel Rechenkapazität, Datenspeicher-, Software- und Programmierumgebungen als Service angeboten und dynamisch über ein Netzwerk an den Bedarf des Kunden angepasst zur Verfügung gestellt. Der Kunde benötigt, gerade im Geschäftskundenbereich, wesentlich weniger eigene IT-Infrastrukturen und kann dadurch unter anderem hohe Kosteneinsparungen erreichen. Er beauftragt eine Dienstleistung eines Providers wie Netzbandbreiten, Rechen- und Speicherressourcen und passt sie jederzeit nach Bedarf an. Der Mietpreis richtet sich nach der tatsächlich verbrauchten Kapazität.

Cloud Computing bietet für Geschäftskunden zusätzliche Sicherheit:

- Eine zentrale Bereitstellung von Daten in einer Wolke kann die Anzahl existierender Kopien von Datensätzen reduzieren, da diese nicht mehr auf jedem Rechner einzeln, sondern in der Wolke gespeichert werden
- Wenn Daten an nur einer Stelle gespeichert werden, kann ein effizienteres Zugriffsmanagement betrieben werden

Auch für den Privatkunden bietet Cloud Computing mehr Sicherheit und birgt gleichzeitig Einsparpotenziale:

- Die Server der Wolke, in der die Daten gespeichert sind, sind erheblich besser geschützt als die meisten privaten PCs und Laptops. Die meisten Provider (auch die Deutsche Telekom) machen Backup-Sicherungen, um Daten nach einem möglichen Ausfall eines Servers wieder herstellen zu können
- Der Kunde spart Geld für zusätzlichen Speicherplatz auf dem heimischen PC und seinem Smartphone
- Jeder kann von überall bequem auf seine eigenen Dateien zugreifen

Die Deutsche Telekom hat sich als einer der großen Anbieter der Branche auch bei Diskussionen und Entwicklungen rund um das Thema Sicherheit von Cloud Computing  engagiert, etwa im Rahmen der Aktivitäten des BITKOM . Hier wurde zuletzt der Entwurf der „BSI-Mindestsicherheitsanforderungen an Cloud Computing-Anbieter“ gemeinsam mit den Branchenvertretern kommentiert. Darüber hinaus sieht die Deutsche Telekom die Einrichtung eines übergreifenden Security-Lagezentrums der Industrie als erforderlich an. Außerdem befürwortet das Unternehmen eine Sicherheitszertifizierung seitens des Bundesamtes für Sicherheit in der Informationstechnik (BSI) für Sicherheitsleistungen in der Wolke.

De-Mail.



Die E-Mail ist Medium Nummer eins bei der schriftlichen Kommunikation. Täglich versenden und empfangen Anwender weltweit rund 247 Milliarden elektronische Nachrichten. Doch die E-Mail stößt dort an ihre Grenzen, wo der Inhalt vertraulich ist oder der fristgerechte Eingang nachweisbar sein muss. Und nicht immer ist gewährleistet, dass der angezeigte Absender der tatsächliche ist oder ob die Nachricht auf ihrem Weg durchs Internet abgefangen und manipuliert wurde. Daher ist E-Mail für verbindliche geschäftliche Abläufe – also für den Behörden- und Geschäftsverkehr – nur eingeschränkt geeignet.

Die Bundesregierung hat im Rahmen ihrer Hightech-Strategie ein Gesetz auf den Weg gebracht, das neben rechtlichen Grundlagen den technischen Rahmen für die elektronische Kommunikation per De-Mail bindend vorgibt. Das Gesetz wird in diesem Jahr verabschiedet. Im Anschluss können sich Unternehmen als De-Mail-Provider beim Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizieren lassen. Das Amt wacht darüber, dass die strengen Datenschutzbestimmungen eingehalten werden.

Als Weiterentwicklung der E-Mail ermöglicht die De-Mail künftig einen einfachen, sicheren und nachweisbaren Austausch elektronischer Nachrichten zwischen privaten Nutzern, Unternehmen und Behörden. Sie verbindet die Vorteile der E-Mail mit der Zuverlässigkeit eines Einschreibens. Jeder Absender ist dem De-Mail-Provider aufgrund einer persönlichen Erstidentifizierung bekannt. Nutzer erhalten auf Wunsch eine qualifiziert signierte Bestätigung, dass und an wen sie eine Nachricht versendet haben und wann sie beim Empfänger eingetroffen ist. So lässt sich die gesamte Geschäfts- und Verwaltungskommunikation wie Angebote, Verträge, Rechnungen und Mahnungen schnell, bequem und ohne Medienbruch elektronisch erledigen. Druck-, Kuvertier-, Frankier- und Zustellkosten entfallen in erheblichem Ausmaß.

T-Systems hat in mehreren Projekten umfassende Erfahrungen mit der De-Mail-Anbindung von Unternehmen und Verwaltungen und mit der Integration von Geschäftsprozessen gesammelt. Zum Beispiel hat das Unternehmen in der T-City Friedrichshafen bereits mehr als 40 Unternehmen, Kammern und Behörden über De-Mail verbunden. Das Bundesministerium des Innern hatte die De-Mail bis März 2010 dort sechs Monate lang getestet. Ziel war ein lebensechtes Szenario mit möglichst vielen Anwendungsbereichen der De-Mail.

Im Gegensatz zu einer regulären E-Mail bietet De-Mail erhöhte Sicherheit:

- gesicherter Versand: Die De-Mail bietet einen deutlich höheren Sicherheitsgrad und die Nachweisbarkeit von Versand und Empfang einer Nachricht. Wenn Nutzer ein De-Mail-Konto eröffnen wollen, müssen sie sich einmalig persönlich identifizieren
- sichere Datenübertragung: Ein Muss ist die Sicherheit bei der Datenübertragung. Verwendet wird daher unter anderem das bewährte und aus dem Internet bekannte SSL-Verschlüsselungsverfahren  (Internet-Seiten mit der URL https://). Die beteiligten Server bauen eine direkte Verbindung auf und müssen sich gegenseitig authentisieren
- gesicherte Zustellung: Der wichtigste De-Mail-Bereich ist der sichere Empfang und Versand von Nachrichten oder Dokumenten auf allen Ebenen – analog zum klassischen Brief heute. Um sicherzugehen, dass die De-Mail  nicht verloren geht, erhält der Absender einen qualifiziert signierten Nachweis darüber, dass seine Nachricht versendet wurde und wann sie im Postfach des Empfängers eingegangen ist. Um Manipulationsversuche sichtbar zu machen, werden die Nachrichten außerdem mit einer Prüfsumme versehen. Diese Prüfsumme wird vom De-Mail-Anbieter aus allen Inhalten der Nachricht berechnet, ähnlich wie man aus einer langen Zahl durch Addieren der einzelnen Ziffern eine viel kürzere Quersumme bilden kann. Ändert man später eine Ziffer, verändert sich auch die Quersumme und weist so auf die Modifizierung hin. Diese Überprüfung wird grundsätzlich bei jeder Übertragung vom empfangenden Provider durchgeführt.

Smart Energy – Über Smart Meters zu Smart Grids.

Intelligente Stromnetze (Smart Grids **G**) sind in der Lage, auf Basis von gemessenem Lastverhalten die Erzeugung von Energie zu regeln. So können bei Bedarf zusätzliche dezentrale Energieproduzenten wie etwa Kraft-Wärme-Kopplungsanlagen, Solar- oder Windkraftanlagen beziehungsweise abgeschaltet werden. Die konventionellen Grundlast-Versorger (z. B. Kohlekraftwerke) können so sparsamer eingesetzt und somit CO₂ eingespart werden. Diese intelligenten Stromnetze erfordern eine Vernetzung elektrischer Geräte einzelner Haushalte mit dem jeweiligen Stromversorger und den Austausch zwischen beiden Systemen. Dadurch werden Nutzungsspitzen ermittelt und Regeln entwickelt, wann Energie für Geräte effizient bereitgestellt wird. Insgesamt wird hierbei deutlich, dass eine gesicherte und datenschutzkonforme Datenverarbeitung und -übertragung von besonderer Bedeutung ist. Eine Manipulation der Regelkreisläufe zwischen Erfassung des Energieverbrauchs und Steuerung der Energieproduktion hätte weitreichende Auswirkungen. Ebenso muss dem Kunden weitgehend die Steuerungsmöglichkeit über die ihn betreffenden Informationen erhalten bleiben. Beide Ansätze waren bei den althergebrachten Modellen der Stromversorgung nicht zentraler Bestandteil der Lösung. Die Deutsche Telekom bringt deshalb ihr gesamtes Know-how in der Absicherung und Gestaltung derartiger Infrastrukturen mit ein und gestaltet damit wesentliche Elemente für eine zukunftssichere Energieversorgung.

Smart Metering.



Smart Metering bietet die Möglichkeit, den Verbrauch von Strom, Wasser, Wärme und Gas in einem vorgegebenen Zeitintervall zu erfassen und zu verarbeiten. Der Verbraucher erhält eine Übersicht über den Verbrauch und kann damit sein Energieverhalten anpassen, schnell, zeitnah und energiebewusst handeln und somit wertvolle Ressourcen einsparen. In Zukunft wird es darüber hinaus entsprechende Tarifmodelle geben.

Technologien wie Smart Metering **G** (intelligente, da vernetzte Zählereinheiten für Strom, Gas, Wasser oder Wärme) bilden die Basis der Vernetzung. Auf dem Weg dorthin sind Energielieferanten bereits seit Jahresbeginn 2010 verpflichtet, den Endverbrauchern auf Wunsch eine monatliche, viertel- oder halbjährliche Abrechnung zukommen zu lassen. Dazu schreibt der Gesetzgeber seit 2010 die Installation von so genannten Smart Metern in Neubauten und bei Sanierungen vor.

Die Deutsche Telekom bietet mit Smart Metering & Home Management (siehe auch <http://www.telekom.de/smartmetering>) eine modular aufgebaute Datenkommunikationslösung an. Diese richtet sich an Wohnungswirtschaft, Messstellenbetreiber, Energieversorger, Vertriebsgesellschaften und Verteilnetzbetreiber.



Den Energieverbrauch messen und das Nutzungsverhalten energiebewusst anpassen – Smart Metering macht's möglich.


Da bei diesen neuen Anwendungen ein erhebliches Maß an persönlichen Daten ausgetauscht wird, ist die Gewährleistung eines hohen Datenschutzes und Datensicherheitsniveaus von besonderer Bedeutung. Die Bereiche Datenschutz und IT-Sicherheit haben das Sicherheits- und Datenschutzniveau der beteiligten Unternehmen überprüft. Im Rahmen der Überprüfung wurde festgestellt, dass in bestimmten Vertragskonstellationen Verantwortlichkeiten nicht eindeutig genug beschrieben waren. Dies wurde bereinigt, indem ein Mustervertragsentwurf für die Auftragsdatenverarbeitung interner und externer Partner erstellt wurde. Zudem wurden technisch alle notwendigen Maßnahmen ergriffen, um hier einen größtmöglichen Schutz zu gewährleisten. Für die Übermittlung der Daten von den Zählereinheiten (Smart Meters) zu den Energieversorgungsunternehmen wurde in einem Datenschutzkonzept dokumentiert, wer welche Daten auslesen kann und wie diese verarbeitet werden. Der Schutz von Kundendaten und die datenschutzkonforme Verarbeitung wurden im Rahmen der Freigabe des Datenschutzkonzeptes durch die Bereiche Datenschutz und IT-Sicherheit bestätigt.



Sonderthema im Bereich Geschäftskunden.

Empfehlungen in Das Örtliche.

DeTeMedien und Partnerverlage der Herausgeber- und Verlegergemeinschaften für Das Örtliche, Das Telefonbuch und Gelbe Seiten möchten, dass den Kontaktangaben eines Dienstleisters Bewertungen von Kunden beigefügt werden können. Die bereits implementierte Funktion wurde nach der Intervention der zuständigen Aufsichtsbehörde deaktiviert.

Die Aufsichtsbehörde hat die fehlende Information derjenigen, die bewertet werden sollen, über ihre Reaktionsmöglichkeiten (z. B. Opt-Out-Möglichkeit , redaktionelle Bearbeitung von Einträgen) beanstandet. Nach der Abschaltung der Funktion hat die Deutsche Telekom die DeTeMedien bei der datenschutzkonformen Ausgestaltung beraten. In mehreren Gesprächen wurden mit der zuständigen Aufsichtsbehörde die Umsetzungsmöglichkeiten und zu erfüllenden Anforderungen erörtert. Aktuell werden die Details der Umsetzung vorbereitet. Bei der Umsetzung geht es etwa um Ausgestaltung der Vorabinformation an denjenigen, der eine Empfehlung bekommt. Dieser muss Gelegenheit haben, zu widersprechen. Dieses Vorgehen ist als so genannte Opt-Out-Lösung allgemein anerkannt.

Arbeitnehmer.

Der Schutz von Arbeitnehmerdaten umfasst zwei Aspekte: Es geht zum einen um den Schutz der Mitarbeiterdaten vor unberechtigter externer und interner Nutzung und Verarbeitung von Daten. Zum anderen umfasst Arbeitnehmerdatenschutz aber auch die Voraussetzungen und Bedingungen für berechtigte interne Verwendungen, etwa zur Ermittlung von Straftaten: Ein Unternehmen ist verpflichtet, eventuelles Fehlverhalten zu untersuchen, um mögliche Verletzungen von Rechten Dritter (z. B. Kunden, andere Mitarbeiter) zu verhindern oder zur Aufklärung eines Sachverhaltes beizutragen.

Gesetzliche Regelungen.

Die Bundesregierung hat im August 2010 einen Gesetzentwurf beschlossen, der Änderungen im Beschäftigtendatenschutz vorsieht. Die erste Lesung im Parlament fand im Februar 2011 statt. Kernpunkt der Gesetzänderung ist die Schaffung klarer Regeln, wie ein Unternehmen das Fehlverhalten seiner Beschäftigten untersuchen darf und was dabei verboten ist. Personalisierte systematische Testverfahren, so genannte Screenings, sind nach dem Entwurf nur noch in sehr eingeschränkter Form möglich. Präventive Datenabgleiche können nur noch in anonymisierter oder pseudonymisierter Form durchgeführt werden, also dann, wenn ein Rückschluss auf die individuelle Person entweder gar nicht oder sehr eingeschränkt möglich ist. Die Deutsche Telekom hat nach den Bespitzelungsvorfällen der Vergangenheit bereits vor dem Gesetzentwurf darauf verzichtet, Datenabgleiche mit personenbezogenen Daten zur Aufdeckung von erwartetem oder möglichem persönlichem Fehlverhalten durchzuführen. Das Unternehmen begrüßt es, dass diese strenge Vorgehensweise

jetzt festgeschrieben werden soll und für solche Maßnahmen eine Anonymisierung oder Pseudonymisierung gefordert wird. Zur Implementierung der neuen Regelungen im Konzern Deutsche Telekom wurde bereits eine Projektgruppe eingerichtet. Diese identifiziert die Bereiche, Prozesse und Richtlinien des Konzerns, die aufgrund der neuen Bestimmungen angepasst werden müssen, und stößt deren Umsetzung an.

Vereinbarungen und Leitfäden.

Die Deutsche Telekom hat im Berichtszeitraum im Bereich des Beschäftigtendatenschutzes verschiedene Maßnahmen durchgeführt, die Missbräuche verhindern, personenbezogene Daten ihrer Beschäftigten schützen und einen Ausgleich verschiedener Interessen sicherstellen.

- Mit der „**Konzernbetriebsvereinbarung zur Verhinderung von Missbräuchen in IT-Systemen**“ hat die Deutsche Telekom gemeinsam mit dem Betriebsrat präventive Maßnahmen abgestimmt, die von vornherein verhindern sollen, dass Mitarbeiter IT-Systeme missbräuchlich nutzen. Diese Maßnahmen sind in erster Linie technische Systembegrenzungen, die die Handlungsmöglichkeiten eines Nutzers von vornherein auf die notwendigen Schritte limitieren
- Ein „**Leitfaden Personaldatenschutz**“ leitet Mitarbeiter und Führungskräfte durch das komplexe Thema des Beschäftigtendatenschutzes und informiert alle Beschäftigten über ihre Rechte und deren Durchsetzung. Der Leitfaden wurde auf der Intranetseite der Telekom veröffentlicht

Sonderthemen im Arbeitnehmerdatenschutz.

Fehlerhafte Arbeitsabläufe im Bereich Personal.

Die Mitarbeiter der Deutschen Telekom können über ein Computersystem ihre Personalangelegenheiten wie Arbeitszeiterfassung, Einsehen der Zielvereinbarungen oder Reiseplanung abwickeln. Die Änderung eines Services innerhalb dieses Systems führte zu fehlerhaften Arbeitsabläufen. Dadurch waren Zielvereinbarungsvorschläge leitender Angestellter für andere Mitarbeiter kurzzeitig abrufbar. Der Fehler wurde unmittelbar nach Entdeckung behoben. Die Betroffenen haben ein Entschuldigungsschreiben erhalten.

Ungerechtfertigte Zugriffsberechtigungen im Personalbereich.

Mitarbeiter der Deutschen Telekom, die auf Kundendaten oder die Daten von Mitarbeitern zugreifen können, erhalten hierfür Berechtigungen. Diese Berechtigungen werden nach einem Mehr-Augen-Prinzip vergeben. Das bedeutet: Mitarbeiter können sich Berechtigungen nicht selbst ausstellen, sondern müssen die Freigabe zumindest einer weiteren Person erhalten. Im Bereich Personal genügte ein System den organisatorischen Anforderungen nicht: In Einzelfällen erhielten Mitarbeiter trotz Vier-Augen-Prinzip Berechtigungen zum Zugriff auf Daten, die zur Ausübung ihrer Tätigkeit nicht notwendig waren. Im Rahmen einer datenschutzrechtlichen Prüfung des Bereichs wurde dieser Sachverhalt bekannt. Die Deutsche Telekom entzog den betroffenen Mitarbeitern die nicht zulässigen Berechtigungen unmittelbar. Gleichzeitig wurde das Mehr-Augen-Prinzip zur Vergabe von Berechtigungen in diesem Bereich neu gestaltet und ausgebaut. Damit wurde die gefundene Lücke geschlossen.

Übermittlung von Log-Informationen im Rahmen der Auftragsdatenverarbeitung.


Die Geschäftskunden der T-Systems benötigen zur eigenen Qualitätssicherung und zur Erfüllung der gesetzlichen Vorschriften zur Auftragsdatenverarbeitung (§ 11 Bundesdatenschutzgesetz) Übersichten über die Zugriffe des Dienstleisters auf ihre Datenbestände. Diese Übersichten wurden und werden den Kunden auf Anforderung in unterschiedlicher Form (online oder in Dokumentenform) zur Verfügung gestellt.

Im Zusammenhang mit einer Überprüfung wurde festgestellt, dass die Übersichten großteils in nicht pseudonymisierter Form übergeben wurden, obwohl es zur Erfüllung der Kontrollpflichten der Kunden nicht zwingend erforderlich war, die Information mit den Klarnamen der Mitarbeiter zu übergeben. Zusammen mit den fachverantwortlichen Stellen wird an einem neuen, standardisierten Reportingverfahren gearbeitet, das T-Systems übergreifend zentral zur Verfügung gestellt wird. Bis zur Einführung dieses Verfahrens wird durch individuelle Lösungen eine möglichst umfassende Pseudonymisierung der Informationen veranlasst.

Internationale Entwicklungen.

Gesetzliche Regelungen.

Bis zum 15. Januar 2011 konnten Unternehmen zu der geplanten Novellierung der europäischen Datenschutzrichtlinie von 1995 Stellung nehmen.

Die Novelle verfolgt unter anderem das Ziel, Auswirkungen neuer Technologien für den Datenschutz zu behandeln, die Rechte von Bürgern zu stärken, die Datenschutzsituation in der Europäischen Union zu verbessern sowie eine wirksamere Durchsetzung der Vorschriften zu erreichen. Die Deutsche Telekom hat sich an der Diskussion beteiligt und begrüßt insbesondere die geplante Harmonisierung der Datenschutzvorschriften und das Vorhaben, ein hohes Schutzniveau für Daten, die in Länder außerhalb der Europäischen Union übermittelt werden, zu erreichen. Ebenso begrüßt sie die Überlegung, eine Datenschutz-Zertifizierung auf EU-Ebene einzuführen. Außerdem setzt sich die Telekom unter anderem dafür ein, dass Unternehmen Kundendaten für nicht vertragsnotwendige Zwecke nur dann verwenden dürfen, wenn der betroffene Kunde zuvor eingewilligt hat (so genannte Opt-In-Lösung ). Die Telekom vertritt hier bewusst eine Position, die Kundenrechte stärkt, während viele Unternehmen der Branche einen weniger eingeschränkten Umgang mit Kundendaten wünschen.

Maßnahmen länderübergreifender Zusammenarbeit.

Internationale Zusammenarbeit innerhalb des Konzerns.

Die Deutsche Telekom erzielt mittlerweile über 50 Prozent ihres Umsatzes außerhalb Deutschlands. Sie ist als international operierendes Unternehmen in unterschiedlichen Ländern in und außerhalb der Europäischen Union aktiv. Vor diesem Hintergrund ist Datenschutz für das Unternehmen ein wichtiges internationales Thema und muss übergreifend und grenzüberschreitend umgesetzt werden.

In den jeweiligen Ländern gelten verschiedene datenschutzrechtliche Bestimmungen und Gesetze, die sich in der Europäischen Union weitestgehend aus der europäischen Datenschutzrichtlinie ableiten, sich länderspezifisch jedoch unterscheiden. Bei Ländern, die nicht Mitglied der Europäischen Union sind, sind die Unterschiede noch größer. Vor diesem Hintergrund ist eine enge internationale Abstimmung innerhalb des Konzerns wichtig, um bei nicht einheitlichen Datenschutzvorschriften dennoch ein weltweit einheitliches hohes Datenschutzniveau im Unternehmen sicherzustellen.

Hierzu verbessert die Deutsche Telekom ihre internationale Zusammenarbeit innerhalb des Konzerns stetig. So werden Instrumente wie etwa Standards für Datenschutzprüfungen von IT-Systemen oder Onlineschulungen für den länderübergreifenden Einsatz entwickelt.

Bereits im Datenschutzbericht 2009 hat die Telekom angekündigt, dass eine engere Zusammenarbeit im internationalen Bereich für 2010 angestrebt wird. 2010 hat das Unternehmen Initiativen ausgebaut und eingeleitet, um länderübergreifenden Datenschutz im Interesse der Kunden sicherzustellen.



Die Deutsche Telekom verbessert ihre internationale Zusammenarbeit ständig.

Die **International Privacy Circles (IPCs)** bilden hierfür die Basis. Diese finden bereits seit mehreren Jahren einmal pro Jahr in jeder der zu drei Regionen zusammengefassten globalen Einheiten der Deutschen Telekom statt. Die Datenschutzverantwortlichen der Landesgesellschaften in den drei Regionen Europa/Afrika, Amerika und Asien/Pazifik treffen sich zum Fach- und Meinungsaustausch. Ziel der Privacy Circles ist darüber hinaus die Vermittlung eines einheitlichen Wissensstands zum Beispiel bei grenzüberschreitenden Datentransfers, aber auch internationalen Entwicklungen sowohl auf regulatorischer als auch auf technischer Ebene.

Ende November 2010 wurde zusätzlich die **International Privacy Taskforce** ins Leben gerufen. Im Unterschied zu den International Privacy Circles werden hier Datenschutzthemen in kleinen Arbeitsgruppen aus operativer Sicht der teilnehmenden Länder betrachtet. Zu den Erfahrungen und Bedarfen werden gemeinsame Lösungen entwickelt, die in das internationale Datenschutzrahmenwerk des Konzerns einfließen. Dabei werden unter anderem gesetzliche Anforderungen zum internationalen Datentransfer innerhalb und außerhalb der Europäischen Union, Entwicklungen zum Mitarbeiterdatenschutz, Verfahren zur Datenschutzbewertung von Fachbereichsprojekten und der Ausbau des Datenschutz-Intranets zu einer Informations- und Schulungsplattform thematisiert.

Zusammenarbeit außerhalb des Konzerns: Beteiligung an der „Mobile Privacy Initiative“.


Die Deutsche Telekom beteiligt sich nicht nur im Rahmen europäischer und internationaler öffentlicher Gremien und Einrichtungen an der Weiterentwicklung international verbindlicher Datenschutzstandards, sondern arbeitet auch an von der Industrie geförderten Initiativen mit. So begleitet das Unternehmen die von der GSM Association (GSMA) **[G]** initiierte „Mobile Privacy Initiative“, die im Januar 2011 begründet worden ist. Die GSMA **[G]** ist ein 1987 gegründeter weltweiter Mobilfunkverband, in dem über 800 Mobilfunkanbieter und Unternehmen zusammengeschlossen sind. Ziel der „Mobile Privacy Initiative“ ist es, führende Mobilfunkanbieter, Endgerätehersteller und Entwickler mobiler Softwareapplikationen auf einen gemeinsamen Datenschutzstandard zu verpflichten und den Kunden klar und transparent darüber zu informieren, welche Daten zu welchen Zwecken gesammelt werden. So soll der Benutzer etwa bei Location-Based Services – also Diensten, die auf den aktuellen Standort des Benutzers zugreifen – von einer Software informiert und um Freigabe dieser Informationen gebeten werden, wenn dies zur Erbringung der Leistung notwendig ist. Außerdem sollen der Umfang und die Nutzung dieser Daten klar und übersichtlich dargestellt werden. Insbesondere in Bezug auf Teilnehmer außerhalb der Europäischen Union, wo zum Teil keine oder sehr unterschiedliche Datenschutzgesetze existieren, ist das ein erster Schritt in Richtung eines gemeinsamen Rahmens. Die im Januar 2011 veröffentlichten „Privacy Principles“ (Datenschutzgrundsätze) enthalten die gemeinsamen Datenschutzstandards. Sie bilden die Grundlage für detaillierte, produktorientierte Richtlinien mit dem Ziel, kundenfreundliche Standards auf allen Ebenen der Produktentwicklung zu etablieren. Für 2011 wird angestrebt, diese spezifischen Richtlinien zum Datenschutz zu erarbeiten. Ein erster Entwurf für eine Richtlinie für Entwickler von mobilen Softwareapplikationen liegt bereits vor und soll noch im Jahr 2011 verabschiedet werden. Das wäre ein großer Erfolg, da sich so auch Unternehmen in Ländern außerhalb der Europäischen Union zu strengeren Datenschutzanforderungen verpflichten würden.


Sonderthema im Bereich internationale Entwicklungen.

Everything Everywhere – United Kingdom.

Zum 1. Juli 2010 haben die Deutsche Telekom und France Telecom ihre jeweiligen Tochtergesellschaften in Großbritannien in einem gemeinsamen Unternehmen unter dem Namen „Everything Everywhere“ fusioniert. Dabei stand aus Datenschutzsicht die Migration der Systeme mit personenbezogenen Daten im Mittelpunkt. Im Detail ging es um die Einhaltung der Vorgaben der Datenschutzgesetze und der unternehmensinternen Vorgaben. Dabei wurden auch Schritte zum Betriebsübergang aus Datenschutzsicht aufgezeigt. Die konkrete Umsetzung der Anforderungen hat begonnen und wird im Jahr 2011 abgeschlossen.

Systeme und Prozesse.

Das Jahr 2010 hat mit seinen viel diskutierten Vorfällen um Daten gezeigt: Daten sind einer permanenten Gefahr ausgesetzt. Eine absolute Sicherheit von Daten ist dabei unmöglich. Es kann immer nur darum gehen, Prozesse und Systeme so sicher wie möglich zu gestalten und Angreifern immer einen Schritt voraus zu sein. Hier fordert sich die Deutsche Telekom jeden Tag aufs Neue heraus: Sie testet ihre Systeme und Prozesse zum Schutz der Kundendaten und zum Schutz der eigenen Vermögenswerte kontinuierlich und entwickelt sie permanent weiter. Mit Zertifizierungen  durch unabhängige Institute erbringt die Deutsche Telekom den Nachweis, dass sie die relevanten Normen und Standards erfüllt. Experten bescheinigen dem Unternehmen ein vorbildliches Sicherheitsniveau.

Im Jahr 2010 hat die Deutsche Telekom ihre Konzepte und Regelungen für Sicherheit und Datenschutz konsolidiert, vereinheitlicht und noch stärker aufeinander abgestimmt und damit das Schutzniveau des Konzerns weiter gestärkt. Ein Resultat dieser Bestrebungen ist das so genannte Privacy and Security Assessment (PSA) . Es gewährleistet, dass Anforderungen bezüglich Sicherheit und Datenschutz bei den neu entwickelten Systemen und Anwendungen bereits in der frühen Phase der Produktentwicklung berücksichtigt werden.

Ein integraler Bestandteil des unternehmensinternen Kontrollsystems sind zahlreiche Datenschutz- und Datensicherheitsaudits. Diese vervollständigen die Gesamtheit der präventiven und reaktiven Maßnahmen, die zum Schutz vertraulicher Informationen und personenbezogener Daten bei der Deutschen Telekom eingesetzt werden.



Thomas Tschersich,
Leiter IT-Sicherheit der
Deutschen Telekom.



Wo steht die Deutsche Telekom heute, wenn es um Datensicherheit geht? Und wo steht sie in Zukunft?

Lange Jahre wurde bei der Entwicklung neuer Produkte in der Telekommunikations- und IT-Branche ein klassischer Zweischnitt gemacht: Erst wurde ein Produkt entwickelt, dann das fertige Produkt sicher gemacht im Sinne eines Schutzes vor unerwünschtem Datenabzug – das ist ineffizient und führt häufig zu Kompromissen, bei denen die Funktionalität Vorrang vor der Sicherheit hat. Die Deutsche Telekom geht einen anderen Weg: Vor Jahren haben wir damit begonnen, das Thema Sicherheit bereits in die Vorplanungen von Produkten einzubinden und die Entwicklung zu begleiten. Mittlerweile sind wir im gesamten Prozess bis zum fertigen Produkt vertreten und damit einer der Vorreiter unserer Branche. Sicherheit ist bei uns ein Design-Kriterium und längst keine Zusatzfunktion mehr.

Unser Anspruch ist es zudem, Sicherheit in bestehenden Produkten und ganzen Systemen auf einem hohen Niveau zu erhalten, dabei mit der technischen Entwicklung Schritt zu halten und neuen kriminellen Ideen immer ein Stück voraus zu sein. Viele externe Experten bescheinigen uns, hier eine vorbildliche Stellung eingenommen zu haben. Wir wollen das konsequent ausbauen. Damit aber nicht genug. Wir arbeiten auch daran, einen neuen Standard für sichere Produkte zu etablieren und damit unsere Philosophie „Sicherheit als Design-Kriterium“ weiterzuverbreiten. Allein schaffen wir das natürlich nicht. Einen solchen Standard in der gesamten Telekommunikationsindustrie zu etablieren geht nur, wenn andere mitziehen. Daran arbeiten wir.

Sicherheitsmanagement der Deutschen Telekom.

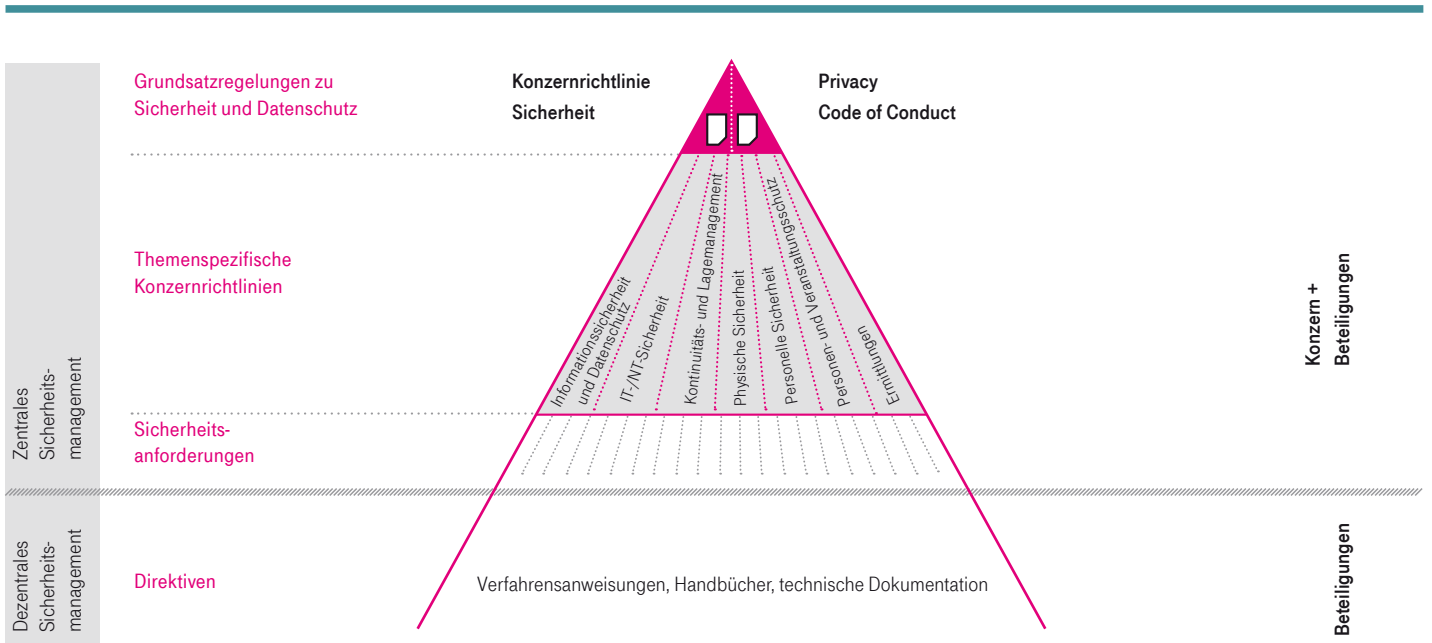
Der Vorstand der Deutschen Telekom ist gemäß Paragraph 91 des Aktiengesetzes verpflichtet, geeignete Maßnahmen zu treffen, um Entwicklungen frühzeitig zu erkennen, die den Fortbestand der Gesellschaft gefährden können. Diese Verpflichtung schließt insbesondere ein internes Kontrollsystem ein. Verstöße gegen Datenschutz- und Sicherheitsbestimmungen sind so weit wie möglich auszuschließen. Zu diesem Zweck entwickelt die Deutsche Telekom unter anderem das konzernweite Sicherheitsmanagementsystem ständig fort. So hat sie es auch im Jahr 2010 an aktuelle Entwicklungen angepasst und auf weitere Konzernteile ausgedehnt.


Wesentlicher Teil des Sicherheitsmanagementsystems ist neben dem Datenschutz der Bereich Zentrales Sicherheitsmanagement der Deutschen Telekom. Das Zentrale Sicherheitsmanagement [G] setzt sich aus den drei Organisationseinheiten Group Security Policy (GSP), Group

Business Security (GBS) und Group IT Security (GIS) zusammen. Es regelt das Zusammenspiel aller Funktionen im Konzern, die Sicherheit gewährleisten. Das Zentrale Sicherheitsmanagement hat im Dezember 2010 die Zertifizierung [G] nach ISO [G] 27001 (zu ISO 27001 siehe Seite 37) erhalten und erfüllt damit den wichtigsten internationalen Standard.

Das Sicherheits- und Datenschutzmanagement wurde im Jahr 2010 kontinuierlich weiterentwickelt. Unter anderem wurde als seine operative Grundlage ein konzernweit einheitliches, verpflichtendes Regelwerk geschaffen, das die Regelungen für Sicherheit und Datenschutz harmonisiert. Diese Regelungsgrundlagen von Sicherheit und Datenschutz werden in folgender Grafik verdeutlicht:

Regelungsrahmen zu Sicherheit und Datenschutz.



An der Spitze des Regelungsrahmens stehen die beiden grundlegenden Dokumente zur Sicherheit und zum Datenschutz der Deutschen Telekom: Der Privacy Code of Conduct  enthält die internen Anforderungen des Umgangs mit personenbezogenen Daten (allgemeine Datenschutzbestimmungen), die Konzernrichtlinie Sicherheit die sicherheitsrelevanten Grundsätze des Konzerns. Der Privacy Code of Conduct und Konzernrichtlinie Sicherheit bilden gleichsam eine Art „Grundgesetz“ für den konzernweiten Datenschutz und die Sicherheit.

Diese Bestimmungen werden durch sieben weitere themenspezifische Konzernrichtlinien konkretisiert:

- Informationssicherheit und Datenschutz
- IT-/NT-Sicherheit
- Kontinuitäts- und Lagemanagement
- physische Sicherheit
- personelle Sicherheit
- Personen- und Veranstaltungsschutz
- Ermittlungen

Mit diesen Konzernrichtlinien werden in transparenter Weise verbindliche, an der internationalen Norm ISO 27001 orientierte Standards gesetzt, um ein adäquat hohes und konsistentes Sicherheits- und Datenschutzniveau innerhalb des Konzerns Deutsche Telekom zu gewährleisten (zu ISO 27001 siehe Seite 37).


Die 2010 überarbeiteten Regelwerke des zentralen Sicherheitsmanagements werden in Deutschland und in den internationalen Beteiligungen sukzessive implementiert. In den einzelnen Einheiten werden sie durch lokale Regelungen ergänzt und ausgestaltet. Die Richtlinien sind in der Deutschen Telekom AG und der T-Deutschland GmbH bereits in Kraft getreten. Es ist geplant, die Umsetzung in allen relevanten Konzerngesellschaften bis Ende 2011 abzuschließen.

Frühwarnsysteme.

Die Deutsche Telekom als größter Anbieter von Kommunikationsdienstleistungen in Deutschland ist ein beliebtes Ziel von Hackerattacken, die immer wieder neue Herausforderungen mit sich bringen. Das Unternehmen reagiert auf diese Herausforderungen mit Hilfe eines Frühwarnsystems, das darauf abzielt, Informationen über Angreifer zu ermitteln, neue Angriffe zu erkennen und bessere Abwehrstrategien zu entwickeln.

Grundsätzlich gilt, dass ein Frühwarnsystem umso besser ist, je mehr Datenquellen und Datenmaterial für die Analysen zur Verfügung stehen. Schon bei der Konzeption wurden die strengen rechtlichen Maßstäbe von Fernmeldegeheimnis und Datenschutz berücksichtigt. Mit dem Aufbau des Frühwarnsystems wird ein speziell an den Risiken und Bedürfnissen des Unternehmens orientiertes Bild der Sicherheitslage im Internet generiert. Ziel ist es, mit Hilfe der selbst gewonnenen Informationen und deren Zusammenführen mit den allgemein verfügbaren Herstellerinformationen die Kunden sowie vertrauliche Daten der Deutschen Telekom bestmöglich vor Gefahren im Internet zu schützen. Weiterhin wird es damit möglich, frühzeitig Anpassungsbedarfe der Sicherheitsmechanismen zu erkennen und diese zu implementieren.


Lockvogelsysteme – Honeypots.

Zentraler Bestandteil des Telekom-Frühwarnsystems sind so genannte Honeypots  (Englisch für Honigtöpfe). Honeypots sind aus dem Internet erreichbare isolierte Serversysteme, die keine Verbindung zu den realen Systemen der Deutschen Telekom haben. Die Honeypots sind damit unabhängig von der Infrastruktur der Deutschen Telekom und können selbst im Falle einer Kompromittierung nicht zu einer Gefährdung werden. Die Honeypot-Systeme sind selbstlernend, das bedeutet, dass unbekannte Angriffe aufgezeichnet, analysiert und danach in der Erkennung berücksichtigt werden. Die Deutsche Telekom hat im April 2010 mit dem Aufbau solcher Honeypot-Systeme begonnen. Andere Provider arbeiten mit vergleichbaren Systemen. Die Deutsche Telekom pflegt hierzu einen engen Austausch unter anderem innerhalb der durch die Bundesregierung geförderten „Anti-Botnet-Initiative“, die zum Ziel hat, die Anzahl verseuchter Endkunden-Computer zu reduzieren.

Seit ihrer Einrichtung haben die Honeypots mehr als 500.000 Angriffe von Hackern erkannt. Die so gewonnenen Einblicke über Angriffsarten und -methoden hat die Deutsche Telekom genutzt, um erfolgreiche Angriffe auf ihre realen Systeme abzuwenden und Kunden zu informieren, deren Rechner Teil eines Botnetzes und damit fremd gesteuert sind.


Diese und andere Frühwarnsysteme verbessert die Deutsche Telekom ständig, um den bestmöglichen Schutz der Kunden- und der eigenen Daten zu gewährleisten. Und das mit Erfolg: Bis heute wurden durch die Honeypot-Systeme keine Verwundbarkeiten an Systemen der Deutschen Telekom aus dem Internet entdeckt. Gleichzeitig wird eine Ausweitung der Honeypots speziell zur Analyse von Angriffen im Mobilfunk geprüft.

Telekom-CERT.

Das Computer Emergency Response Team (CERT)  der Deutschen Telekom betreibt ein international ausgerichtetes Management bei Sicherheitsvorfällen für alle Informations- und Netzwerktechnologien des Konzerns Deutsche Telekom. Es bildet eine zentrale Anlaufstelle für die Meldung von Vorfällen und etabliert Mechanismen zur Früherkennung von Angriffen auf intern und extern erreichbare Systeme. Die Hauptaufgaben des CERTs sind:

- Schwachstellenmanagement (Vulnerability and Advisory Management – VAM)
- Koordination von Maßnahmen bei Vorfällen mit Sicherheitsrelevanz (Incident Management) oder mit Kundendatenbezug
- interne Herausgabe und Bewertung von Warnhinweisen zu neu erkannten Schwachstellen
- konzernweite Frühwarnung und -erkennung von technischen Angriffen gegen die Netzinfrastruktur
- Vertretung der Deutschen Telekom AG gegenüber nationalen und internationalen Gremien (z. B. dem weltweiten CERT-Dachverband FIRST, Forum of Incident Response Teams).

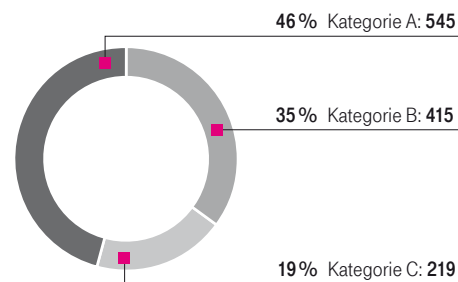
Im Jahr 2010 hat das Team Hinweise zu 1 135 Schwachstellen in Softwarekomponenten, die in der Deutschen Telekom verwendet werden, erstellt und intern darüber informiert. Die Schwachstellen reichen von Sicherheitslücken in Webservertechnologien bis zu Schwachstellen in Betriebssystemen. Soweit zum Zeitpunkt des Bekanntwerdens schon eine Lösungsmöglichkeit gefunden wurde, kommuniziert das Telekom-CERT diese ebenfalls.

Das Telekom-CERT sieht weiterhin eine starke Gefährdung durch so genannte Driveby Exploits , bei denen der Computer des Benutzers durch das alleinige Betrachten einer Webseite infiziert wird. Hierbei werden Verwundbarkeiten in Webbrowsern (speziell ältere Versionen des Microsoft-Internet-Explorers) und Browsererweiterungen ausgenutzt.

Privacy and Security Assessment (PSA).

Das Privacy und Security Assessment (PSA) Verfahren wurde 2010 bei der Deutschen Telekom in Deutschland eingeführt. Damit wurden die bisherigen Freigabe-Verfahren für Datenschutz und technische Sicherheit ersetzt und in ein gemeinsames Verfahren integriert. Für diesen Schritt hatte das Unternehmen auf Erfahrungen aus einzelnen Bereichen zurückgegriffen, die die Methode schon zuvor angewandt hatten. Die Deutsche Telekom praktiziert die Verzahnung von Datenschutz und technischer Sicherheit als eines von wenigen Unternehmen weltweit.

PSA-Projektkategorien.



Das PSA-Verfahren schafft einen transparenten und dokumentierten Prozess, der in effizienter Weise ein hohes Maß an Sicherheit und Datenschutz für komplexe und kritische Produkte und Dienstleistungen ermöglicht. Dies findet bereits in der Entwicklungsphase und nicht erst kurz vor oder nach der Einführung neuer Produkte und Dienstleistungen statt. Anhand eines Fragebogens wird zu Prozessbeginn die Datenschutz- und Sicherheitsrelevanz eines Projekts nach der Kategorisierung A, B und C festgelegt. Danach richtet sich die Betreuungstiefe. Je kritischer ein Projekt, desto umfassender ist der Beratungs- und Betreuungsansatz seitens der Bereiche Datenschutz und Datensicherheit (A-Projekte). Je unkritischer ein Projekt ist, desto mehr werden Standardanforderungen genutzt (B-Projekte). Sicherheits- und Datenschutzerfordernisse lassen sich durch das PSA-Verfahren schnell und effizient umsetzen. Letztendlich kann mit diesen Standards auch abgeklärt werden, dass für ein Projekt keine Datenschutz-/Sicherheitsrelevanz besteht (C-Projekte). Auf diese Weise wird ein optimaler Ressourceneinsatz bei allen Beteiligten sichergestellt.

Ein solches Vorgehen ist in der Telekommunikationsbranche bislang einmalig. Bei Regulierungsbehörden oder Standardisierungsgremien genießt es Vorbildcharakter.

Im Jahr 2010 wurden mit diesem Verfahren rund 1.200 Projekte nach den drei Kategorien A, B und C betrachtet. Fast 960 Projekte entfielen dabei auf die Kategorien A und B und wurden damit im PSA-Verfahren

betreut. So begleitete der Konzern etwa die Entwicklung der Dynamic Computing-Dienstleistungen. Auch die Vorbereitungen zum Umbau des Telefonnetzes auf IP-basierte Telefonie werden kontinuierlich von den Bereichen Datenschutz und Datensicherheit mit gestaltet.

Eine solche frühzeitige und permanente Einbindung von Datenschutz und Datensicherheit bietet den Kunden der Deutschen Telekom in allen Produkten und Dienstleistungen ein einheitlich hohes Datenschutzniveau. Neben einer inhaltlichen Weiterentwicklung und Optimierung soll das Verfahren im Jahr 2011 auch in ausländischen Konzerneinheiten eingeführt werden.

Privacy by Design.



Privacy by Design (Datenschutz als Designkriterium) beschreibt, dass der Aspekt des Schutzes und des sorgsamem Umgangs mit personenbezogenen Daten bereits bei der Entwicklung neuer Produkte oder Dienste zu berücksichtigen ist. Unternehmen beachten dadurch zum einen die rechtlichen Anforderungen an den Datenschutz im frühestmöglichen Stadium. Zum anderen können sie damit Datenschutz zu einem Differenzierungskriterium machen, indem sie bereits bei der Entwicklung von Produkten unterschiedliche Bedürfnisse von Nutzern bei der Freigabe persönlicher Daten berücksichtigen. In der Praxis können so etwa bei der Gestaltung einer Smartphone-Anwendung Funktionen für den Austausch sensibler Daten entwickelt werden. Es muss hier etwa möglich sein, zu entscheiden, welche konkreten Daten ausgetauscht werden sollen.

Security by Design.

Security by Design (Sicherheit als Designkriterium) ist ein Begriff, der zunehmend auf Konferenzen und in Diskussionsforen verwendet wird, auch wenn er sich noch nicht als stehender Begriff etabliert hat. Er meint, dass neben dem Schutz der personenbezogenen Daten auch gewährleistet sein muss, dass diese Daten sicher verarbeitet werden und sicher vor unberechtigten Zugriffen sein müssen. Das bedeutet, dass die Maxime bei der Produktentwicklung sein muss, Sicherheitsanforderungen bereits sehr früh zu berücksichtigen. Aufwändige Nachbesserungen werden somit vermieden und ein maximales Sicherheitsniveau erreicht. Die Produkte sind dann so sicher wie technisch möglich und nicht nur so sicher wie nötig gestaltet.


Privacy and Security by Design.

Privacy and Security by Design (Datenschutz und Sicherheit als Designkriterium). Für die Zukunft kann erwartet werden, dass ein Verfahren, das beide Aspekte berücksichtigt, zum Standardverfahren wird.

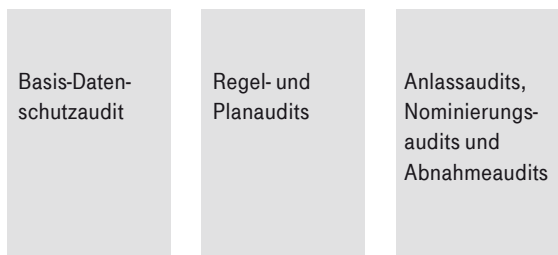
Auditierungen und Zertifizierungen.

Innerhalb des Konzerns Deutsche Telekom finden regelmäßig Auditierungen und Zertifizierungen im Bereich des Datenschutzes und der Datensicherheit statt. Die Deutsche Telekom greift dabei auf ein System von Audits und Zertifizierungen durch externe und interne Stellen zurück. Das Unternehmen nimmt damit in der Telekommunikationsbranche eine Vorbildfunktion ein: Zertifizierungen für Unternehmensbereiche sind in der Telekommunikationsbranche noch die Ausnahme.

Kategorien für Auditierungen.

Die Audits  der Deutschen Telekom zur internen Kontrolle und Überwachung der Umsetzung von Vorgaben zum Datenschutz und zur Datensicherheit lassen sich in drei Kategorien unterteilen:

Kategorien Audits Deutsche Telekom AG.



Das Basis-Datenschutzaudit wird sowohl national als auch international durchgeführt. Dabei wird überprüft, ob die Vorgaben des Konzerndatenschutzes eingehalten wurden. Die zweite Kategorie umfasst Audits von Systemen wie etwa der IT und Produkten. Darüber hinaus wird überprüft, ob die Organisationsstruktur und die internen Prozesse der Deutschen Telekom den aktuellen Datenschutz- und Sicherheitsanforderungen entsprechen. Die dritte Kategorie sind anlassbezogene Audits bei Vorfällen oder Verdachtsmomenten und Abnahmeaudits zur Freigabe von priorisierten Projekten. Das bedeutet: Bevor ein Projekt wie etwa die Markteinführung eines neuen Produkts im Echtlauf gestartet wird, wird geprüft, ob es alle geforderten und notwendigen Datenschutz- und Sicherheitsvorschriften erfüllt. Im Rahmen von Nominierungsaudits werden neue Vertriebspartner vor der Aufnahme von Geschäftsbeziehungen auditiert. Bestehende Vertriebspartner werden durch ein wiederkehrendes Regelaudit geprüft.

Durchgeführte Audits.

Im Jahr 2010 haben allein die Zentralbereiche interne Revision, Konzerndatenschutz und Zentrales Sicherheitsmanagement rund 450 Audits zu Datenschutz und Sicherheit durchgeführt: Ein großer Teil der Audits zu Datenschutz und Sicherheit betraf die IT und die Netztechnik. Diese Audits dienen dem Ziel, die im Konzern eingesetzten Informations- und Netzwerktechnologien zu sichern. So wird zum Beispiel die Umsetzung der Berechtigungs-, Datenschutz-, und Sicherheitskonzepte konzernweit überprüft, um etwaige Lücken zu identifizieren. Solche Lücken können etwa durch Sicherheitsmängel in Softwarelösungen entstehen, die erkannt und zusammen mit Industriepartnern beseitigt werden.

Audit.



Bei einem Audit handelt es sich um ein allgemeines Untersuchungsverfahren, das dazu dient, zum Beispiel Systeme, Prozesse, Organisationen und Standorte hinsichtlich der Erfüllung von Anforderungen und Richtlinien zu bewerten.

Um ein Zertifikat zu erhalten, wird bei dem Unternehmen in einem von externen Auditoren durchgeführten Audit überprüft, ob die internen Systeme und Prozesse die Anforderungen für den Erhalt des Zertifikats erfüllen. Nach Erhalt des Zertifikats müssen diese Audits regelmäßig (alle ein bis drei Jahre) wiederholt werden.


Neben diesen von externen Stellen durchgeführten Audits führen Unternehmen oft auch verschiedene interne Audits durch. Mit diesen überprüfen sie die Einhaltung ihrer eigenen internen Anforderungen und Richtlinien.

Ein weiterer Schwerpunkt der durchgeführten Audits dient der Überprüfung, ob technische und organisatorische Maßnahmen sowie Prozesse zur Datensicherheit und zum Datenschutz eingehalten wurden. Die übrigen Audits verteilen sich auf die Gewährleistung der übergreifenden Sicherheit, etwa auf personelle oder physische Sicherheitsmaßnahmen. Hierunter fallen etwa Überprüfungen zur Einhaltung der Brandschutzvorschriften oder der Zutrittsregelungen.

Die Ergebnisse dieser Audits dienen der Sicherstellung eines hohen Datenschutz- und Sicherheitsniveaus, indem sie entweder die Effektivität der internen Systeme und Prozesse nachweisen oder etwaige Schwachstellen frühzeitig erkennen und abstellen helfen.

Audits im Bereich Vertrieb.


Im Jahr 2010 hat die Deutsche Telekom im Bereich Vertrieb darüber hinaus die systematische Zertifizierung der Vertriebspartner des Telekom Deutschlandgeschäfts durch unabhängige externe Auditoren fortgesetzt. Diese Zertifizierung umfasst unter anderem die Themenbereiche Datenschutz, IT-Sicherheit und Qualitätsmanagement. Die externen Überprüfungen der Vertriebspartner zahlen auf die konzernweite strategische Zielsetzung „Integrität und Wertschätzung im Kundenkontakt“ ein (siehe Seite 19).

Im Jahr 2010 wurden im Vertrieb 37 Callcenter , die nach den Vorgaben der Deutschen Telekom Kundenanrufe tätigen, erfolgreich durch den TÜV-Rheinland zertifiziert. Im Oktober 2010 wurde damit begonnen, rund 70 Callcenter, die im Auftrag der Deutschen Telekom Kundenservice betreiben, zertifizieren zu lassen. Gleichzeitig wurde damit angefangen, rund 350 Exklusivpartner im Handel prüfen zu lassen. Diese Zertifizierungen sollen im Jahr 2011 abgeschlossen sein.

Darüber hinaus verfolgte die Deutsche Telekom durch Kunden und Mitarbeiter gemeldetes nicht regelkonformes Verhalten von Vertriebspartnern und Mitarbeitern stringent und sanktionierte es.

Standard-Datenschutzaudits.

Die Deutsche Telekom auditiert regelmäßig wichtige Prozesse, Systeme und Bereiche in den so genannten TOP-Audits. Diese waren 2010:

1. **Audit  Vorratsdatenspeicherung T-Home/T-Mobile:** Nach Aufhebung der Regelungen zur Vorratsdatenspeicherung  durch das Bundesverfassungsgericht im März 2010 wurde mittels eines Audits überprüft, ob entsprechend den Vorgaben des Verfassungsgerichts alle Daten ordnungsgemäß gelöscht wurden. Das Audit hat die unwiederbringliche Datenlöschung bestätigt. Mit erfolgter Löschung und dem Ende der Vorratsdatenspeicherung  ist dieses Audit zukünftig nicht mehr erforderlich
2. **Audit Ermittlungsprozess:** Es wurde untersucht, ob die internen Ermittlungen innerhalb der Deutschen Telekom datenschutzkonform durchgeführt werden. Das Audit bestätigte die datenschutzkonforme Durchführung
3. Mit einem weiteren **Audit** wurde das System für das **Kundenmanagement im Mobilfunk** überprüft. Das entsprechende System zum Kundenmanagement im Festnetz wird darüber hinaus im Jahr 2011 auditiert. Mittelfristig werden beide Systeme sukzessive als Folge der Gründung der T-Deutschland GmbH zusammenwachsen und dementsprechend zukünftig einheitlich auditiert
4. Das **SAP-HR-Audit** überprüfte die Datenerhebungen und die Verarbeitung von Mitarbeiterdaten, also etwa die Einhaltung der vereinbarten Zugriffsberechtigungen

5. **Audit Data Warehouse:** 2010 erfolgte eine Überprüfung der Einhaltung datenschutzrechtlicher Vorgaben beim Data Warehouse für den Mobilfunk. Das entsprechende System für das Festnetz wird im Jahr 2011 auditiert. Wie bei weiteren Systemen, die bisher noch getrennt für Festnetz und Mobilfunk existieren, werden mittelfristig beide Systeme sukzessive als Folge der Gründung der T-Deutschland GmbH zusammenwachsen und dementsprechend künftig einheitlich auditiert.

Gefundene Schwachstellen wurden und werden von den Fachseiten geschlossen und die Umsetzung der Maßnahmen vom Konzerndatenschutz überprüft.

Folgende zentrale interne und externe Überprüfungen fanden im Jahr 2010 statt:

Ergebnisse des nationalen und internationalen Basis-Datenschutzaudits 2010.

Mit dem jährlichen Basis-Datenschutzaudit misst die Deutsche Telekom das allgemeine Datenschutzniveau im Konzern und identifiziert mögliche strukturelle Schwachstellen. Das Basis-Datenschutzaudit befragt Mitarbeiter und wird seit 1997 in der Deutschen Telekom durchgeführt, seit 2006 auch auf internationaler Ebene. Im Jahr 2010 wurden Form und Inhalte gegenüber den Vorjahren grundsätzlich überarbeitet. Wurden früher Geschäfts- und Teamleiter befragt, steht nunmehr die direkte Befragung einer repräsentativen Stichprobe von 65.000 Mitarbeitern in Deutschland und 20.000 Mitarbeitern im Ausland (insgesamt rund 40 Prozent der Mitarbeiter) im Fokus. Dies ermöglicht eine bessere zielgruppenspezifische Auswertung der Ergebnisse sowie darauf basierend eine bessere Maßnahmenentwicklung.

Im internationalen Bereich werden neben den Mitarbeitern zusätzlich auch die lokalen Datenschutzbeauftragten in Form einer Selbstauskunft über das Datenschutzniveau in der jeweiligen Organisation befragt. Die Angaben der Selbstauskunft werden durch stichprobenartige Audits vor Ort überprüft. So wurde im Jahr 2010 die Selbstauskunft mehrerer Landesgesellschaften (T-Mobile USA, T-Mobile Niederlande und T-Systems USA) gesondert auditiert und durchweg ein angemessenes Datenschutzniveau festgestellt. Im ersten Halbjahr 2011 werden weitere Vor-Ort-Audits bei Landesgesellschaften umgesetzt.

Gegenstand der Befragung waren Themen wie Datenschutzbewusstsein, Schulungsintensität und -nutzen, Kenntnisse der Nutzung von Tools wie E-Mail-Verschlüsselung und Aktenvernichtungsmöglichkeiten sowie der Datenschutzprozesse. Ein Ergebnis dieser Befragung war, dass 75 Prozent der Befragten in Deutschland und 63 Prozent der Befragten in den Auslandsgesellschaften das Datenschutzniveau in der Telekom als „sehr hoch“ oder „hoch“ einschätzen. Auch persönlich halten 87 Prozent der Mitarbeiter in Deutschland und 80 Prozent der Mitarbeiter in den Auslandsgesellschaften das Thema Datenschutz für „sehr wichtig“ oder „wichtig“.


Auch wenn die Ergebnisse überwiegend positiv waren, unternimmt die Deutsche Telekom zur nachhaltigen Entwicklung und Festigung des Datenschutzniveaus kontinuierlich Anstrengungen. So wird der Konzerndatenschutz im Jahr 2011 insbesondere das Schulungskonzept und -portfolio im Inland weiter ausbauen.

Audits an ausländischen Standorten.

Die Geschäftskundensparte der Deutschen Telekom, die T-Systems, bietet internationale IT-Dienstleistungen für die Deutsche Telekom selbst aber auch für Geschäftskunden an. Im Jahr 2010 wurden mehrere dieser ausländischen Standorte (zum Beispiel in Brasilien, Spanien und Ungarn) hinsichtlich der Gewährleistung eines angemessenen Datenschutzniveaus überprüft. Diese Audits werden als Point of Production-Audits (PoP-Audits) bezeichnet.

Mit den Privacy Code of Conduct-Audits (PCoC-Audits) wurde die Einhaltung der in den allgemeinen Datenschutzbestimmungen (so genannter Privacy Code of Conduct, siehe www.telekom.com/datenschutz) festgeschriebenen Regeln zur Sicherstellung eines angemessenen Datenschutzniveaus innerhalb des gesamten Konzerns Deutsche Telekom überprüft. Dies geschah etwa bei T-Mobile USA, T-Systems North America, T-Mobile Niederlande und der Telekom Kroatien.

Erhaltene Zertifizierungen.

Auditierungen sind ein wichtiger Baustein zum Erreichen eines adäquaten Datenschutzniveaus. Viele weitere Kontrollmechanismen stellen bei der Deutschen Telekom sicher, dass Datenschutz- und Datensicherheitsmaßnahmen implementiert sind. Dies sind neben Organisationskontrollen nach dem Bilanzrechtsmodernisierungsgesetz (BilMoG)  die Prozesse zur Beratung, Prüfung und Freigabe von Datenschutz- und Sicherheitskonzepten, externe Prüfungen durch Aufsichtsbehörden und die Bearbeitung von Hinweisen und Beschwerden von Kunden und Mitarbeitern zu Datenschutzproblemen. Hinzu kommen Zertifizierungen nach anerkannten Standards.


Zertifizierung.



Eine Zertifizierung ist ein Verfahren, das durch externe, unabhängige Stellen wie etwa TÜV und DEKRA durchgeführt wird und mit dessen Hilfe die Einhaltung bestimmter Anforderungen an Produkte und Dienstleistungen und ihre jeweiligen Herstellungsverfahren einschließlich der Handelsbeziehungen, Personen und Systeme nachgewiesen wird. Zertifizierungsverfahren zeichnen sich durch besondere Objektivität aus, sind dafür aber besonders zeitintensiv und aufgrund des erforderlichen Aufwandes mit hohen Kosten verbunden. Zertifizierungen werden nach nationalen und internationalen Normen durchgeführt.

Verschiedene Konzernteile und Bereiche der Deutschen Telekom haben diverse Zertifizierungsverfahren durchlaufen und erfüllen damit einen anerkannt hohen Standard:

Zertifizierung des Rechnungsprozesses für Privatkunden durch den TÜViT.


Nachdem bereits im Juni 2009 der erste Teil des Rechnungsprozesses für Privatkunden im Festnetz, die Verkehrsdatenverarbeitung, auditiert und zertifiziert wurde, hat der TÜViT im September 2010 die beiden noch ausstehenden Teile ebenfalls bestätigt. Im zweiten Teil wurden die Rechnerdarstellung auf Papier und Online-Auskunftssysteme zertifiziert, und in Teil drei die Bereitstellung von Rechnungsinformationen für die Bilanzierung und andere Nachweise. Damit ist der gesamte Abrechnungsprozess der Deutschen Telekom für Privatkunden im Festnetz zertifiziert. Der TÜViT hat dem Unternehmen das Datenschutzzertifikat „Trusted Site Privacy“ erteilt. Eine Prüfung nach den Trusted Site Privacy-Kriterien umfasst sowohl die Bewertung des Datenschutzes als auch eine Bewertung der IT-Sicherheit. Hierfür wurden über einen Zeitraum von zwei Jahren verschiedene IT-Systeme und -Schnittstellen auditiert und sicherheitstechnische Untersuchungen durchgeführt. Die empfohlenen Auflagen wurden umgesetzt. Damit sind alle Anforderungen des Kundendatenschutzes erfüllt. Die Deutsche Telekom ist das erste und bisher einzige Telekommunikationsunternehmen, das den kompletten Rechnungsprozess von unabhängigen Gutachtern des TÜViT hat überprüfen und zertifizieren lassen. Der Prozess umfasst das Erheben und Verarbeiten sämtlicher Daten, die über 27 Millionen Kunden täglich beim Telefonieren übers Festnetz erzeugen. Eine entsprechende Zertifizierung  soll auch im Bereich Mobilfunk erfolgen.

ISO 27001-Zertifizierung.



Der internationale Standard für Informationssicherheit ist in der ISO/IEC 27001 beschrieben. Er spezifiziert die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung der Risiken innerhalb der gesamten Organisation. Die Vergabe von ISO 27001-Zertifikaten erfolgt durch akkreditierte Zertifizierungsinstitute. Sie umfasst die Themen Dokumentenlenkung, ständige Verbesserung des Managementsystems, Management von organisations-eigenen Werten, personelle Sicherheit, physische Sicherheit, Betriebs-/ Kommunikationsmanagement, Zugangskontrolle, Beschaffung, Entwicklung und Wartung von IT-Systemen, Umgang mit Informationssicherheitsvorfällen, Sicherstellung des Geschäftsbetriebs (Kontinuität), Einhaltung von Vorgaben. Die Zertifizierung ist unabhängig von der Art der Organisation und damit beispielsweise auch auf Handelsunternehmen, gemeinnützige oder staatliche Organisationen anwendbar.


Zertifizierung der Telekom Shops.

Die Telekom Shops haben die Zertifizierung  ihrer datenschutz- und sicherheitsrelevanten Prozesse auch im Jahr 2010 erfolgreich abgeschlossen und dürfen im zweiten Jahr in Folge das DEKRA-Siegel „Datenschutz und Datensicherheit gemäß dem Bundesdatenschutzgesetz“ tragen. Die DEKRA attestierte den Telekom Shops eine Steigerung des Datenschutzniveaus sowie eine erhöhte Sensibilität und Kompetenz der Mitarbeiter und bestätigte in ihrem Abschlussbericht, dass das Thema Kundendatenschutz im Verkaufsraum für die Mitarbeiter sehr wichtig und präsent ist.



Die Deutsche Telekom lässt ihre Shops durch unabhängige Gutachter prüfen und zertifizieren.

Zertifizierungen nach internationalem Standard.

Im Jahr 2010 haben unter anderem die Deutsche Telekom für ihr zentrales Sicherheitsmanagementsystem und Teile der T-Deutschland GmbH eine Zertifizierung nach der internationalen Norm ISO  27001 erhalten. Bei T-Systems wurde auch im Jahr 2010 der Prozess der Zertifizierung der deutschen Organisation und von 17 Landesgesellschaften fortgesetzt. Dies dient dem Erhalt des Dachzertifikats über die Einführung eines Informationssicherheits-Managementsystems durch T-Systems. Darüber hinaus wurden allein in diesem Jahr 160 ISO27001-Audits weltweit durchgeführt.

Kommunikation nach innen und nach außen.

Der Umgang mit personenbezogenen Daten ist Vertrauenssache: Vertrauen der Kunden in das Unternehmen, dem sie ihre persönlichen Daten anvertrauen. Vertrauen aber auch der Deutschen Telekom gegenüber den Mitarbeitern, die mit den sensiblen Daten umgehen. Vertrauen in beide Richtungen braucht Kommunikation in beide Richtungen. Daher steht die Deutsche Telekom für eine transparente Information ihrer Kunden und bietet ihren Mitarbeitern Sicherheit im Umgang mit personenbezogenen Daten. Hierzu nutzt die Deutsche Telekom eine Vielzahl von Kommunikationsmitteln und -wegen nach außen wie nach innen.

Kommunikation zum Kunden.

Die Deutsche Telekom begreift Datenschutz und Datensicherheit als Kundenservice: Zum einen sieht sie es als ihren Auftrag an, Kunden und Interessierte über Gefahren, aber auch Schutzmöglichkeiten im Umgang mit dem Internet zu informieren. Zum anderen gibt sie Auskunft über den Umgang mit gespeicherten Kundendaten. Die Deutsche Telekom nutzt verschiedene Medien zur Information und baut ihre Kommunikation stetig aus.

Im Jahr 2010 hat das Unternehmen erstmals mittels Pressemitteilung und Online-Informationen auf den europäischen Datenschutztag aufmerksam gemacht, der seit 2005 stattfindet. Zum Datenschutztag 2011, der am 28. Januar stattgefunden hat, hat die Deutsche Telekom ihre Aktivitäten ausgebaut: So veröffentlichte sie im Vorfeld des Tages eine Umfrage zum Umgang der Deutschen mit dem Internet (www.telekom.com/datenschutz oder www.studie-life.de) und verteilte in den Fußgängerzonen deutscher Großstädte Ratgeber mit Tipps zum sicheren Surfen im Internet. Am Datenschutztag selbst veranstaltete das Unternehmen einen Online-Chat zu allen Fragen rund um den Datenschutz bei Produkten und Dienstleistungen mit internen und externen Experten. Rund 180 Interessierte haben dieses Angebot wahrgenommen. In Zukunft möchte die Deutsche Telekom ihre Aktivitäten zum europäischen Datenschutztag weiter ausbauen und hierzu noch stärker mit Organisationen und weiteren Unternehmen zusammenarbeiten. Gleichzeitig will sich das Unternehmen in der öffentlichen Debatte um Datenschutz und Datensicherheit noch stärker an Diskussionen beteiligen.

Mit folgenden weiteren Maßnahmen richtete sich die Deutsche Telekom 2010 an die Öffentlichkeit:

- Eine neue Auflage des Ratgebers „Datenschutz zu Hause – gewusst wie!“ gibt Interessierten Tipps, um sich vor Internetkriminalität zu schützen und Missbrauch vorzubeugen. Die Broschüre liegt in den T-Shops aus und steht unter www.telekom.com/datenschutz zum Download
- In Radiobeiträgen etwa zur sicheren WLAN-Verschlüsselung oder zum sicheren Online-Shopping klärt die Deutsche Telekom Nutzer auf

- Unter www.telekom.com/datenschutz informiert die Deutsche Telekom kontinuierlich über den aktuellen Stand des Datenschutzes. Außerdem bietet sie Tipps für den sicheren Umgang mit dem Internet und erläutert Gesetzesänderungen, die den Datenschutz betreffen
- Neben den Präsentationen auf der Messe CeBIT und der Internationalen Funkausstellung in Berlin hat der Konzerndatenschutzbeauftragte persönlich Beratungen für Kunden in ausgewählten T-Shops in Deutschland angeboten
- Im Rahmen von Vorträgen an Schulen klärte der Datenschutzbeauftragte Kinder und Jugendliche zum bewussten und verantwortungsvollen Umgang mit dem Internet auf. Das Angebot ist über die Internetseite www.telekom.com/datenschutz abrufbar

Kommunikation zum Mitarbeiter.

Mitarbeiter handeln dann im Sinne von Datenschutz und Datensicherheit, wenn sie sich der Themenkomplexe bewusst sind und auch in schwierigen Situationen sicher reagieren können. Beides zu vermitteln ist Aufgabe der Kommunikation zu den Mitarbeitern der Deutschen Telekom.

Was für jeden Mitarbeiter gilt, ist selbstverständlich auch für das Top-Management des Konzerns verpflichtend: Datenschutz und Datensicherheit sind umso wirksamer, je stärker Führungskräfte von Anfang an in diese Bereiche eingebunden werden. In einem in Zusammenarbeit mit dem Personalbereich neu gestalteten Prozess werden alle neu eingestellten Top-Manager für den Datenschutz innerhalb der Deutschen Telekom sensibilisiert. Der Konzerndatenschutzbeauftragte informiert und klärt die Führungskräfte und Manager zu Beginn ihrer Tätigkeit persönlich über den besonderen Stellenwert des Datenschutzes auf. Regelmäßige Führungskräftebildungen zum Thema stellen sicher, dass die Führungskräfte über den aktuellen Stand informiert sind.

2010 lagen die Schwerpunkte dabei in der Einführung einer dezentralen Datenschutzorganisation sowie in der Zusammenarbeit mit den Datenschutzkoordinatoren der Deutschen Telekom. Die Datenschutzkoordinatoren helfen bei der Einführung und Umsetzung der konzernweiten Datenschutzanforderungen. Unterstützt werden sie dabei vor Ort von den sogenannten Datenschutzbrückenköpfen, die vom Vorstand benannt werden und die datenschutzspezifischen Vorgaben des Unternehmens operativ umsetzen. In regelmäßigen Treffen tauschen sich die Datenschutzkoordinatoren über aktuelle Themen und ihre Erfahrungen aus. Ziel dieser Treffen ist die Unterstützung der Brückenköpfe bei der Umsetzung und Abstimmung der Vorgaben des Konzerndatenschutzes.

Die Datenschutzbrückenköpfe, die wie die Datenschutzkoordinatoren bereits seit 2009 im Unternehmen implementiert sind, hielten 2010 monatliche Treffen zum Erfahrungs- und Informationsaustausch ab.

Um den Mitarbeitern die Gelegenheit zu geben, sich vor Ort persönlich über Datenschutz zu informieren, besuchte der Datenschutzbeauftragte zehn Standorte in Deutschland und stand im Rahmen einer Telefon-Hotline für Fragen Rede und Antwort.

Das bereits umfangreiche Datenschutz-Schulungsangebot wurde um ein weiteres webbasiertes Lerntool erweitert. Zusätzlich wurden aufbauende Schulungsmaßnahmen wie etwa ein Workshop zum neu eingeführten PSA-Verfahren **G** angeboten. Darüber hinaus wird das Bewusstsein der Mitarbeiter für sicherheitskonformes Verhalten in regelmäßigen Schulungen gestärkt.

Die Deutsche Telekom prüft Schulungsangebot und -inhalte in regelmäßigen Abständen in internen Audits. So wurden 2010 die Datenschulungen für Mitarbeiter analysiert. Dabei hat sich herausgestellt, dass Umfang und Inhalte der Maßnahmen als positiv bewertet werden können.

Der sowohl national als auch international neu gestaltete Datenschutz-Intranetauftritt ging im September 2010 online.



Passwörter und Zugangsdaten sollten geheim bleiben. Zum europäischen Datenschutztag hat die Deutsche Telekom rund um das Thema sichere Daten informiert.

Datenschutzbeirat der Deutschen Telekom.

➡ Erfolgreich ist, wer ein Thema aus unterschiedlichsten Blickwinkeln betrachtet.



Aufgabe und Funktion.

Der Datenschutzbeirat der Deutschen Telekom berät den Vorstand als unabhängiges Beratungsgremium und ermöglicht einen konstruktiven Austausch mit führenden Datenschutzexperten und Persönlichkeiten aus Politik, Lehre, Wirtschaft und unabhängigen Organisationen zu datenschutzrelevanten Themen. Der Datenschutzbeirat wurde im Februar 2009 gegründet und ergänzt die interne Datenschutz- und Sicherheitsorganisation der Deutschen Telekom um einen unabhängigen und gesellschaftlich vielfältigen Blick von außen.

Der Datenschutzbeirat deckt ein breites Themenfeld ab: Er befasst sich mit Geschäftsmodellen und -prozessen zum Umgang mit Kunden- und Mitarbeiterdaten ebenso wie mit der IT-Sicherheit und der Angemessenheit von entsprechenden Maßnahmen, mit internationalen Datenschutzfragen sowie mit den Implikationen neuer gesetzlicher Regelungen. Zu seinen Aufgaben gehören die Beurteilung von Datenschutz- und Datensicherheitsmaßnahmen sowie die Erarbeitung von Vorschlägen und Empfehlungen an Vorstand und Aufsichtsrat auch im Kontext der „digitalen“ Gesellschaft.

Zusammensetzung.

Die Mitglieder des Datenschutzbeirats werden von der Deutschen Telekom jeweils für zwei Jahre berufen. Berufen werden bewusst führende Datenschutzexperten sowie Persönlichkeiten aus unterschiedlichen Berufsgruppen, um eine qualifizierte externe kritische Reflexion von Datenschutz und Datensicherheit zu gewährleisten. Im Jahr 2010 zählten zu seinen Mitgliedern:


- Wolfgang Bosbach, MdB, Rechtsanwalt und Vorsitzender des Bundestags-Innenausschusses
- Dr. Michael Bürsch, MdB a. D., Mitglied des „Centrum for Corporate Citizenship Deutschland“ (CCCD)
- Peter Franck, Mitglied des Vorstands Chaos Computer Club (CCC)
- Prof. Dr. Hansjörg Geiger, Honorarprofessor für Verfassungsrecht an der Johann-Wolfgang-Goethe-Universität in Frankfurt/Main und von 1998 bis 2005 Staatssekretär im Bundesministerium der Justiz, Präsident des Bundesamtes für Verfassungsschutz und des Bundesnachrichtendienstes a. D.

- Prof. Peter Gola, Vorsitzender des Vorstands der Gesellschaft für Datenschutz und Datensicherheit (GDD)
- Bernd H. Harder, Rechtsanwalt, Mitglied des Hauptvorstands des BITKOM e.V., Lehrbeauftragter an der Hochschule der Medien Stuttgart und an der Technischen Universität München (TMU)
- Gisela Piltz, MdB, stellvertretende Fraktionsvorsitzende der FDP-Bundestagsfraktion
- Dr. Gerhard Schäfer, Vorsitzender Richter am Bundesgerichtshof (BGH) i. R.
- Lothar Schröder, Vorsitzender des Datenschutzbeirates, Mitglied des ver.di-Bundesvorstands und stellvertretender Aufsichtsratsvorsitzender der Deutschen Telekom AG, Mitglied der Enquetekommission „Internet und digitale Gesellschaft“
- Silke Stokar, MdB a. D., ehemalige innenpolitische Sprecherin der Fraktion Bündnis 90/Die Grünen
- Prof. Dr. Peter Wedde, Professor für Arbeitsrecht und Recht in der Informationsgesellschaft an der Fachhochschule Frankfurt/Main

Beispiele seiner Arbeit im Jahr 2010.

Der Datenschutzbeirat hat sich seit 2009 nicht nur als wichtiges Beratungsgremium etabliert, sondern unterstützt die Deutsche Telekom dabei, eine Vorreiterrolle in Sachen Datenschutz und -sicherheit einzunehmen. So hat das Gremium im Jahr 2010 eine Selbstevaluation seiner Arbeit durchgeführt, um seine unabhängige Rolle als Beratungsgremium zu überprüfen. In diesem Zusammenhang bewerteten die Mitglieder beispielsweise den Informationsaustausch mit der Deutschen Telekom in den Sitzungen des Datenschutzbeirats und die Ernsthaftigkeit des Umgangs der Deutschen Telekom mit den Empfehlungen des Gremiums als positiv.

Der Datenschutzbeirat kann Datenschutz- und Datensicherheitsthemen auf eigene Initiative hin aufgreifen. Er ist aufgerufen, selbständig Themen einzubringen und entsprechende Vorschläge und Empfehlungen für den Vorstand der Telekom zu erarbeiten.

Dieser hohe Freiheitsgrad ermöglichte dem Datenschutzbeirat, den Fokus seiner Arbeit von der Befassung mit „Aufarbeitungsthemen“ in Richtung zukunftsweisender Aspekte des Datenschutzes und der Datensicherheit zu erweitern. Standen im Jahr 2009 insbesondere die Neuorganisation der Konzernsicherheit und die Neuausrichtung des Datenschutzes im Vordergrund, waren es 2010 zunehmend Themenfelder wie etwa Cloud Computing  und Netzneutralität, die die Rolle der Deutschen Telekom als Schrittmacher eines datenschutzkonformen Unternehmens in der Telekommunikationsbranche und in der digitalen Gesellschaft unterstreichen.



Lothar Schröder,
Vorsitzender des Datenschutzbeirats,
Mitglied des ver.di-Bundesvorstands und
stellvertretender Aufsichtsratsvorsitzender
der Deutschen Telekom AG.




Warum braucht die Deutsche Telekom einen Datenschutzbeirat – und andere Unternehmen nicht?

Ganz klar: Nicht nur die Deutsche Telekom braucht einen Datenschutzbeirat – andere Unternehmen auch! Die Vorteile eines solchen Gremiums liegen auf der Hand: Ein Unternehmen kann sich externen Sachverstand aus unterschiedlichsten Bereichen ins Haus holen, die es mit internen Kräften nicht abdecken könnte. Die breit gefächerte Besetzung des Gremiums bietet der Deutschen Telekom gleichzeitig die Möglichkeit, ihren Einsatz für Schutz und Sicherheit von Daten über die Multiplikatoren aus dem Beirat in unterschiedliche Bereiche der Gesellschaft zu tragen.

Ein Datenschutzbeirat lebt von einem doppelten Vertrauensverhältnis. Das wird bei der Deutschen Telekom besonders deutlich: Wir haben uns seit 2009 davon überzeugen können, dass das Unternehmen den Datenschutz konsequent verbessert hat und das Thema Schutz und Sicherheit von Daten sehr ernst nimmt. Unser Vertrauen in die Deutsche Telekom ist während der Arbeit des Beirats stetig gewachsen. Gleichzeitig sind wir uns bewusst, dass uns das Unternehmen selbst ein hohes Maß an Vertrauen entgegenbringt, indem es uns Einblick in seine Strukturen und Maßnahmen in einem solch sensiblen Bereich gewährt. Ich denke, sowohl der Beirat als auch das Unternehmen selbst entwickelt sich in der Zusammenarbeit weiter und schärft dabei auch das Aufgabenspektrum eines Datenschutzbeirats. Wertvolle Erfahrungen, auf die andere Unternehmen unbedingt zurückgreifen sollten.

In insgesamt fünf Sitzungen behandelte der Datenschutzbeirat 2010 eine breite Palette von Themen. So hat er sich etwa mit den Missbrauchserkennungssystemen der Deutschen Telekom, dem Sachverständigenbericht von Dr. Schäfer und Maßnahmen zum Risikomanagement in Vertrieb und Service befasst. Er diskutierte über eine Stiftung Datenschutz, den Entwurf des Beschäftigtendatenschutzgesetzes und beriet über die Wirksamkeit der Zugriffskontrollen in Kundenbestandssystemen sowie das Sicherheitsniveau von Vertriebspartnerportalen. Ein weiteres Beratungsfeld in 2010 war das auch derzeit in der Öffentlichkeit intensiv diskutierte Thema Netzneutralität. Hierbei ging es dem Datenschutzbeirat vor allem um die entsprechenden datenschutzrelevanten Implikationen möglicher „Vorfahrtsrechte“ für definierte Daten.

Ferner diskutierte der Datenschutzbeirat datenschutz- und datensicherheitsrelevante Aspekte des Cloud Computing  und des Telekom-IP-TV „Entertain“. Er hat zu diesen Themenkomplexen entsprechende Stellungnahmen und Empfehlungen an den Vorstand der Deutschen Telekom kommuniziert.

Der kritische Blick externer Experten auf die Anforderungen an Datenschutz und IT-Sicherheit sowie deren Umsetzung in der Deutschen Telekom hat sich bewährt. Der Vorstand der Deutschen Telekom wird den konstruktiven Dialog mit dem Datenschutzbeirat weiterhin fortführen.



Ratgeber zum sicheren Umgang mit Daten.

➡ Wer das richtige Wissen hat, kann seine Daten besser schützen.



Wir leben im Zeitalter der Digitalisierung – wir erledigen unsere privaten Bankgeschäfte online, kaufen über das Internet ein und pflegen immer häufiger unsere sozialen Kontakte im Netz. Mit dem Verhalten der Nutzer hat sich auch die Kriminalität verändert. Das Ausspionieren von Zugangsdaten oder das Knacken von privaten WLAN-Verbindungen sind die modernen Varianten des Handtaschendiebstahls und des Einbruchs. Jeder weiß, wie mit einigen Handgriffen Haus und Handtaschen gesichert werden. Wir sollten für die Nutzung des Internets die gleiche Routine entwickeln.

Indem Sie die folgenden Tipps beachten, können Sie sich vor Internetkriminalität schützen und Missbrauch vorbeugen. Wenn Sie Fragen zum Thema Datenschutz allgemein oder bei der Deutschen Telekom haben, können Sie sich im Internet unter www.telekom.com/datenschutz informieren oder eine E-Mail an datenschutz@telekom.de schicken.

PC-Sicherheit und Basisschutz.

Damit Ihre privaten Daten auf dem PC auch privat und sicher bleiben, beachten Sie die folgenden Tipps.

Machen Sie sich immer bewusst, wie sensibel die Daten sind.

Bei vertraulichen Informationen sollten Sie keinen öffentlichen PC verwenden, da Sie nicht wissen, ob dieser ausreichend gegen Viren, Würmer, Trojaner und äußere Angriffe geschützt ist.

Schützen Sie Ihren PC vor Einblicken. Achten Sie darauf, wer auf Ihren Bildschirm schauen kann, wenn Sie sensible Daten wie Benutzernamen und Kennwörter eingeben.

Halten Sie Ihr System immer auf dem aktuellen Stand.

Softwareanbieter entwickeln ihre Produkte ständig weiter und schließen damit aufkommende Sicherheitslücken. Halten Sie daher Ihre Software und besonders die Virenschutzsoftware auf dem aktuellsten Stand, um sich vor Angriffen zu schützen. Die Telekom bietet ein Sicherheitspaket an, das vor diesen Angriffen schützt und monatlich gebucht werden kann. www.t-online.de/sicherheitspaket

Gewährleisten Sie hohe Sicherheitseinstellungen.

Um Ihre Daten zu schützen, installieren Sie ein Virenschutzprogramm und ein Anti-Spyware-Programm. Wichtig ist auch, dass Sie Ihre persönliche Firewall einrichten. Durch die Konfiguration schützen Sie sich vor Angriffen aus dem Internet. Nutzen Sie auch den Viren-Scanner Ihres E-Mail-Anbieters, um einen möglichst hohen Sicherheitsstandard zu erhalten.

Prüfen Sie Downloads und E-Mail-Anhänge.

Viren werden gerne über Dateianhänge verbreitet. Öffnen Sie daher nur vertrauenswürdige Anhänge von Personen, die Sie tatsächlich kennen. Bei Software-Downloads verhält es sich ähnlich: Wenn Ihnen der Anbieter oder die Seite nicht Vertrauen erweckend erscheint, sollten Sie den Download nicht ausführen.

Sichern Sie Ihren PC mit Kennwort.

Um Ihren PC und damit Ihre Daten vor dem Zugriff Dritter zu schützen, sollten Sie ihn immer durch ein Passwort sperren. Achten Sie darauf, dass das Passwort ein sehr sicheres ist. Nach Eingabe des korrekten Passworts wird der Bildschirm wieder freigegeben und Sie können Ihre Arbeit fortsetzen. Empfohlen wird, dass die Bildschirm- und Tastatursperre fünf Minuten nach der letzten Benutzereingabe mit dem Bildschirmschoner einsetzt. Im privaten Bereich ist die Aktivierungszeit natürlich frei wählbar. Nach Bedarf kann man die Sperre auch sofort aktivieren. Das geht bei einem Windows-Betriebssystem, indem man die Tastenkombination Strg + Alt + Entf drückt und dann die Option „Arbeitsstation sperren“ auswählt.

Schalten Sie Funkschnittstellen aus.

Um Ihren privaten PC vor Angriffen von außen zu schützen, schalten Sie alle aktuell nicht benötigten Funkschnittstellen ab – wenn Sie aus dem Raum gehen, machen Sie ja auch das Licht aus! Also warum nicht den WLAN-Sender am Router ausschalten, wenn Sie nicht im Internet sind? Die meisten Modelle haben heute einen Knopf auf der Rückseite. Das Gleiche gilt auch für Ihr Handy, beispielsweise bei der Bluetooth-Schnittstelle, um es zum einen vor Viren, Würmern und Trojanern zu schützen und um zum anderen Unbefugten nicht den Zugang zu Ihren persönlichen Daten wie dem Adressbuch, dem Kalender oder Ihren Bildern zu ermöglichen. Konfigurieren Sie Ihre drahtlosen Zugänge auf die von Ihnen genutzten Geräte. Damit erschweren Sie Dritten zusätzlich den Zugang (siehe Seite 48).

Datensicherung.

Damit Sie ganz sichergehen, sollten Sie besonders von wichtigen Daten regelmäßig eine Sicherheitskopie, zum Beispiel auf CD-ROM/DVD oder einer externen Festplatte, anfertigen.

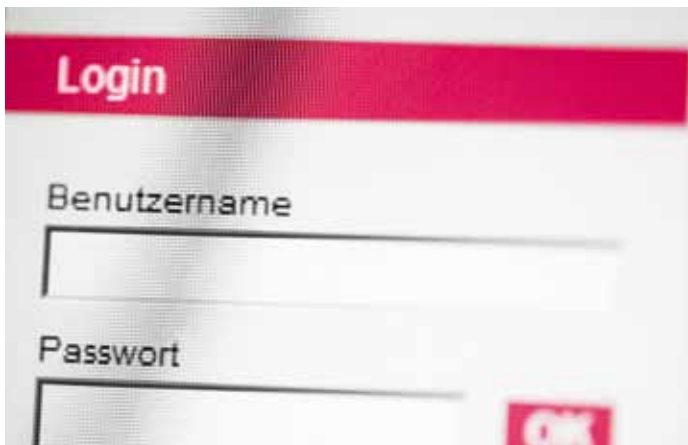
Gestaltung eines sicheren Passworts.

Ohne Passwort geht im Internet nicht viel. Und je besser ein Passwort ist, umso sicherer sind die Daten, die sich dahinter verbergen, geschützt.

Online-Banking, E-Mails lesen oder einen Beitrag im Anglerforum schreiben – wer sich im Web 2.0 bewegt, kommt früher oder später immer an einen Punkt, an dem Anmeldenamen und Passwörter gefragt sind. Der Anmeldenamenname bereitet dabei meist keine Probleme. Doch spätestens beim fünften Passwort wird es schwierig, noch den Überblick zu behalten. Dazu kommt, dass ein sicheres Passwort leider das Gegenteil von einprägsam ist. Wie erstelle ich also ein sicheres Passwort, das sich merken lässt? Hier erfahren Sie, wie Sie Hacker zur Verzweiflung bringen und Ihre Daten schützen.

Wie erstelle ich ein sicheres Passwort?

Die goldene Regel für ein sicheres Passwort lautet: Es sollte von Außenstehenden nicht als sinnvolles Wort erkannt werden. Um ein solches Passwort zu erhalten, gibt es einen einfachen Trick: Denken Sie sich einen Satz aus, den Sie sich gut merken können. Von diesem Satz verwenden Sie nur die Anfangsbuchstaben und ersetzen einzelne Buchstaben durch Zahlen und Sonderzeichen. Ein Beispiel für einen solchen Satz wäre: „Wir zwei essen gerne Pizza mit Salami.“ Die Anfangsbuchstaben ergeben die Kombination „WzegPmS“. Nun kommen die Zahlen und Sonderzeichen ins Spiel. Hier können Sie Ihrer Fantasie freien Lauf lassen. Bei unserem Beispielsatz ersetzen wir das „z“ durch eine „2“ und fügen am Ende noch ein „!“ an. Unser sicheres Passwort lautet dann „W2egPmS!“. Dieses Passwort besteht aus 8 Zeichen. Dies ist die Untergrenze, die Experten für ein sicheres Passwort empfehlen. Grundsätzlich gilt: Je länger und komplexer ein Passwort ist, desto besser.



Ein komplexes Passwort schützt persönliche Daten und macht es Online-Betrügern schwer.

Der Grund: Hacker probieren mit Programmen systematisch alle Möglichkeiten aus, wie ein Passwort aufgebaut sein kann. Mit jedem zusätzlichen Zeichen steigt also die Zahl der möglichen Passwörter und damit auch die der nötigen Durchläufe, die ein solches Computerprogramm zum Knacken Ihres Passworts benötigt.

Erstellen Sie für jeden Zugang ein Passwort.

Eine weitere wichtige Vorsichtsmaßnahme: Verwenden Sie nach Möglichkeit für unterschiedliche Zugänge unterschiedliche Passwörter. Denn ab und an gelingt es Datendieben, ganze Kundendateien inklusive aller Zugangsdaten auszuspionieren. Ein Passwort, das den Dieben so in die Hände fällt, ist nicht mehr sicher. Denn die Hacker werden auch dieses Passwort ausprobieren, wenn sie sich einen Zugang erschleichen wollen. Ein sicheres Passwort ist also immer eines, das Sie nur für einen Zugang verwenden. Das sollte auf jeden Fall für Ihren Zugang zum Online-Banking gelten.

Bewahren Sie Passwörter sicher auf.

Zusätzlich sollten Sie Ihre Passwörter nur an sicheren Plätzen aufbewahren, zu denen nur Sie Zugang haben. Der beste Platz dafür ist natürlich Ihr Kopf. Der schlechteste Platz ist wohl Ihr Browser. Sie sollten daher vor allem bei wichtigen Passwörtern auf die „Autovervollständigen-Funktion“ verzichten und sie nie auf der Festplatte speichern oder auf einem Zettel in der Nähe des PCs notieren. Ändern Sie Passwörter regelmäßig. In regelmäßigen Abständen sollten Sie Ihr Passwort ändern, um den Schutz vor Datendiebstahl zu erhöhen. Wir empfehlen Ihnen, das mindestens alle drei Monate zu tun.

Wann benötige ich ein sicheres Passwort?

Das Problem bei sicheren Passwörtern ist: Sie sind unheimlich schwer zu merken. Egal ob der Name der Ehefrau oder der Geburtstag der Oma – jede Gedächtnisstütze macht ein Passwort unsicherer. Doch möglicherweise benötigen Sie nicht immer ein Passwort, das absolut sicher ist. Etwa beim oben genannten Anglerforum müssen Sie vermutlich nicht so vorsichtig sein wie beim Online-Banking.

Überlegen Sie daher gut, bevor Sie ein Passwort wählen:

- Schützt es persönliche oder geschäftliche Informationen (z. B. E-Mails, Kontakte etc.)?
- Können mit dem Zugang finanzielle Transaktionen getätigt werden (wie beispielsweise beim Online-Banking oder bei Internet-Auktionshäusern)?
- Haben Sie bei dem entsprechenden Zugang wichtige Daten, etwa Ihre Kreditkartennummer oder Bankverbindung, hinterlegt? Wenn Sie eine dieser Fragen mit Ja beantworten, dann sollten Sie unbedingt ein möglichst sicheres Passwort wählen. Falls nicht, genügt möglicherweise auch ein weniger sicheres Passwort. Natürlich sollten Sie auch hier darauf achten, es eventuellen Hackern nicht zu leicht zu machen.

WLAN-Sicherheit.

Immer mehr Menschen benutzen zu Hause oder im öffentlichen Raum drahtlose Funknetzwerke (Wireless Local Area Networks, kurz WLAN), um ins Internet zu kommen.

Sie sind praktisch, da von jedem beliebigen Ort der Zugang ins Internet möglich ist. Sie bergen aber auch Sicherheitsrisiken. Generell kann man sagen, dass jede drahtlose Verbindung weniger Sicherheit bietet als eine Netzwerkverbindung per Kabel. Bei der drahtlosen Verbindung werden die Daten per Funk an den Empfänger übermittelt und können abgefangen werden.

Laut einem Urteil des Bundesgerichtshofs (BGH) vom 12. Mai 2010 (I ZR 121/08) ist jeder private WLAN-Betreiber dazu verpflichtet, sein Netz mit einem Passwort zu schützen. Verschafft sich ein Dritter unerlaubt Zugang zu Ihrem ungesicherten WLAN und führt illegale Handlungen durch, können Sie als Inhaber von einem dadurch Geschädigten zur Unterlassung und zur Erstattung der damit verbundenen Rechtsverfolgungskosten gezwungen werden.

Daher ist es wichtig, dass Sie Ihren WLAN-Router verschlüsseln, damit Ihre privaten E-Mails, Benutzernamen und Kennwörter nicht in die falschen Hände gelangen. Übrigens: Die aktuellen WLAN-Router der Deutschen Telekom sind alle mit einem individuellen Netzwerkschlüssel versehen, und die WPA2-PSK-Verschlüsselung ist bei Lieferung bereits aktiviert. Die wichtigen Informationen zur Konfiguration finden Sie in der Betriebsanleitung des Routers.

In Ihrem Haushalt können Sie sich vor Datendieben schützen, indem Sie folgende Punkte beachten:

Sichern Sie Ihren WLAN-Router.

Dies ist die wichtigste Vorsichtsmaßnahme, da der WLAN-Router die Verbindung zwischen Ihrem Computer und Ihrem Internetanschluss herstellt. Bevor Sie Ihr WLAN in Betrieb nehmen, sollten Sie einige Grundeinstellungen ändern: Zunächst sollten Sie die SSID, die den Netzwerknamen bezeichnet, manuell ändern und ihr einen persönlichen Namen geben. Wählen Sie dabei lieber einen Fantasienamen, der keine Rückschlüsse auf Sie persönlich oder Ihren Internetanbieter zulässt. Um die Sicherheit zu erhöhen, sollte die Ausstrahlung der SSID verhindert werden, damit der Name Ihres Routers im Netzwerk nicht gefunden werden kann. Da Sie den Namen Ihres Routers kennen, werden Sie ihn selbstverständlich finden.



**Surfen im Netz, immer und überall.
Ein verschlüsselter WLAN-Router
ist ein erster Schritt, dabei auch
sicher zu sein.**

Richten Sie eine Verschlüsselung ein.

Eine weitere Schutzmaßnahme ist die Verschlüsselung Ihres WLAN. Diese geschieht bei den meisten WLAN-Systemen über WPA2-PSK – PSK (Pre-Shared Key) übersetzt: vorher vereinbarter Schlüssel. Dabei wird beim Verbindungsaufbau ein „Schlüssel“ (Passwort) gebraucht, um ins Netz zu kommen. Wichtig ist, dass Sie hier einen sicheren Kennwortschutz wählen. Mehr Informationen zur Erstellung von Passwörtern finden Sie unter dem Punkt „Gestaltung eines sicheren Passworts“.

Richten Sie einen Filter gegen Datendiebe ein.

Um die Sicherheit der eigenen Daten zu erhöhen, können Sie einen MAC-Adressen-Filter einrichten. Die MAC-Adresse ist eine Nummer, mit der sich jede Netzwerkkarte und damit jeder internetfähige Computer identifizieren lässt. Wenn Sie nur die von Ihnen benötigten MAC-Adressen zulassen, haben fremde Computer keine Chance. Wie finde ich die MAC-Adresse? Beispiel Windows: Gehen Sie im Startmenü in den Bereich „Systemsteuerung“. Dort klicken Sie auf das Symbol „System“ und wählen im Bereich „Hardware“ den Geräte-Manager. Dort finden Sie den Punkt „Netzwerkadapter“. Normalerweise finden sich dort zwei Einträge – einer trägt im Namen meist den Zusatz „Wireless“. Nach einem Doppelklick auf diesen Eintrag finden Sie verschiedene Menüs vor: Dort steht im Bereich „Erweitert“ die MAC-Adresse.

Schalten Sie Ihr WLAN ab.

Wenn Sie Ihr WLAN nicht nutzen, sollten Sie es abschalten. Auf diese Art und Weise schützen Sie sich nicht nur vor Datendieben, sondern sparen auch Strom.

Sicherheitsinformation des BSI.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt zudem, sämtliche Einstellungen an einem WLAN-Router bei der Einrichtung Ihres WLAN über ein Kabel und nicht drahtlos durchzuführen.

Besonders wenn Sie die öffentlich zugänglichen HotSpots nutzen, sollten Sie die hier folgenden Tipps berücksichtigen, um Ihre Daten bestmöglich zu schützen:

Deaktivieren Sie Ihre Netzwerkfreigabe.

Wenn Sie HotSpots nutzen, sollte die Datei- und Verzeichnisfreigabe auf Ihrem Laptop oder dem mobilen Endgerät deaktiviert sein. In der Regel können Sie diese Freigabe in den Netzwerkeinstellungen Ihres Betriebssystemes deaktivieren. Sie sollten nie mit einem Benutzerkonto angemeldet sein, das Administratorenrechte besitzt.

Aktivieren Sie Ihre Firewall.

Bevor Sie sich in ein fremdes WLAN einwählen, aktivieren Sie Ihre Firewall. Die Firewall überwacht den Datenverkehr von und zu Ihrem Rechner und hilft so dabei, Angriffe von Schadsoftware zu unterbinden.

Stellen Sie keine automatische Verbindung her.

Stellen Sie keine Verbindung mit dem HotSpot her, wenn Sie nicht wissen, wer für das Betreiben des Zugangs verantwortlich ist. Sie sollten auch keine automatische Verbindung mit Drahtlosnetzwerken zulassen, sondern immer manuell auswählen, mit welchem Netz Sie sich verbinden möchten.

Achtung bei falschen HotSpots.

Um an vertrauliche Daten zu gelangen, richten Kriminelle eigene drahtlose Netzwerke ein, die der Startseite des tatsächlichen HotSpots, beispielsweise von T-Mobile, sehr ähnlich sind. Bei der Verbindung mit dem falschen HotSpot werden Sie aufgefordert, Informationen, wie zum Beispiel Ihre Kreditkartennummer, anzugeben, angeblich um ein neues HotSpot-Konto zu eröffnen. Diese Manipulationstechnik ist angelehnt an die Phishing- und Pharming-Technik, die in dem Kapitel „Sicheres Online-Banking und Schutz vor Phishing-Angriffen“ erläutert wird. Über die richtige Installation und Einrichtung eines sicheren WLAN-Zugangs können Sie sich auf <http://hilfe.telekom.de> informieren.

Sicheres Online-Banking und Schutz vor Phishing-Angriffen.

Immer mehr Menschen wickeln ihre Bankgeschäfte über das Internet ab. Diese Bankfiliale ist zu jeder Tages- und Nachtzeit erreichbar und kann bequem von zu Hause aus bedient werden.

So bequem das Online-Banking von zu Hause auch ist, es birgt Risiken, da mit sensiblen Daten gearbeitet wird. Daten wie PINs und TANs, die den Zugriff auf das Konto ermöglichen, fallen bei Unachtsamkeit immer wieder Betrügern in die Hände. Dies passiert sehr häufig durch Phishing-Angriffe, die auch nach Einschätzung des Bundeskriminalamts ein hohes Gefährdungs- und Schadenspotenzial besitzen. Phishing ist eine Wortzusammensetzung aus den Begriffen „Password“ und „Fishing“ und bezeichnet das Abgreifen von Passwörtern sowie PINs und TANs. Durch gefälschte E-Mails und Internetseiten, mit denen der Kunde aufgefordert wird, seine Kontodaten inklusive Passwörtern anzugeben, gelangen Kriminelle an die sensiblen Daten. Meist leitet ein Link die Benutzer auf die gefälschten Webseiten von Banken und anderen Unternehmen, die dem Original sehr ähnlich sehen.

Damit Sie sich vor diesen Angriffen schützen können, achten Sie auf die folgenden Punkte:

Achtung bei Phishing-E-Mails!

- In den meisten Fällen hat das Anschreiben der gefälschten E-Mail eine allgemeine, unpersönliche Anrede, zum Beispiel „Lieber Kunde der XY Bank“
- Bei einer Phishing-E-Mail wird zu einer zügigen und notwendigen Handlung aufgefordert, wobei auch Drohungen verwendet werden („Wenn Sie nicht sofort Ihre Daten aktualisieren, gehen diese verloren ...“)
- Achten Sie immer auf die komplette Absenderadresse der E-Mail. Wenn die Adresse nicht eindeutig Ihrer Bank zuzuordnen ist, fragen Sie lieber noch einmal direkt nach und sichern sich ab
- Ihre Bank wird Sie nie auffordern, vertrauliche Daten wie etwa PIN und TAN in einem Formular innerhalb einer E-Mail anzugeben. Auch telefonisch wird Ihre Bank Sie nie nach sensiblen Daten fragen. Wenn Sie sich unsicher sind, rufen Sie direkt unter der Ihnen bekannten Nummer Ihre Bank an und rückversichern Sie sich
- Phishing-E-Mails sind in manchen Fällen in schlechtem Deutsch verfasst. Umlaute wie ä, ö, ü fehlen mitunter. Das liegt daran, dass diese Nachrichten von Computerprogrammen aus anderen Sprachen schnell und einfach übersetzt werden
- Am sichersten ist es, nie über einen E-Mail-Link auf eine Webseite zu gehen. Rufen Sie die Seite immer direkt aus Ihrem Browser heraus auf. Achten Sie darauf, dass die Adresse der Seite korrekt geschrieben ist.

Aufpassen bei Phishing-Webseiten.

- Achten Sie immer auf das Sicherheitszertifikat, das durch das Sicherheitsschloss-Symbol in der unteren rechten Ecke Ihres Browsers angezeigt wird. Ist dieses nicht vorhanden, handelt es sich um eine nicht sichere Seite
- Wenn es sich um eine sichere Verbindung handelt, wird das Kürzel „https://“ in der Adresszeile des Browsers angezeigt. Dieses Verschlüsselungsverfahren verhindert, dass die Daten in der Zeit, in der Sie daran arbeiten, gelesen oder manipuliert werden können. In den seltensten Fällen kann auch das gefälscht sein. Um sicherzugehen, geben Sie die Adresse Ihrer Bank immer selbständig in die Adresszeile Ihres Browsers ein und folgen Sie keinem Link
- Auf der Login-Seite werden von Ihrer Bank nie die TAN-Codes abgefragt. Sollte das dennoch der Fall sein, setzen Sie sich bitte unverzüglich mit Ihrer Bank in Verbindung

Generelle Vorsichtsmaßnahmen beim Online-Banking.

- Bewahren Sie Ihre persönlichen Daten wie Passwörter, PINs und TANs immer an einem sicheren Ort auf und speichern Sie diese nie auf Ihrem PC ab, auch nicht in einem so genannten Passwort-Manager. Sind diese Daten auf dem PC gespeichert, könnten sie ausgelesen werden
- Gestalten und verwahren Sie Ihr Passwort sicher (siehe „Gestaltung eines sicheren Passwortes“). Für das Online-Banking sollten Sie auf jeden Fall ein spezielles Passwort verwenden, das Sie nicht für andere Zwecke nutzen. Das Kennwort sollte regelmäßig geändert werden, um die Sicherheit zu erhöhen
- Bankgeschäfte sollten nur vom eigenen privaten PC oder Mobilfunkgerät im privaten Umfeld durchgeführt werden. Achten Sie darauf, sich nach Beendigung der Sitzung abzumelden und den Zwischenspeicher (Cache) Ihres PCs zu leeren
- Wichtig ist auch hier, dass Sie immer eine aktuelle Virenschutzsoftware benutzen und Sicherheits-Updates durchführen, um Sicherheitslücken zu schließen
- Überprüfen Sie regelmäßig Ihre Kontobewegungen. Setzen Sie sich unverzüglich mit Ihrer Bank in Verbindung, wenn Ihnen etwas verdächtig vorkommt oder Unstimmigkeiten auftreten. Das rät auch der Bundesverband Deutscher Banken

Wenn Ihnen etwas verdächtig oder ungewöhnlich erscheint, sperren Sie Ihren Zugang zum Online-Banking. Dies können Sie telefonisch bei Ihrer Bank in Auftrag geben oder direkt über eine entsprechende Funktion im Online-Banking-Fenster veranlassen.

Das Sicherheitsbarometer.

Ein hilfreiches Werkzeug für den sicheren Umgang mit dem Internet ist das Sicherheitsbarometer, das vor neuartigen und wiederkehrenden Risiken warnt.

Das Sicherheitsbarometer sowie aktuelle Informationen rund um das Thema Online-Sicherheit finden Sie auch unter www.t-online.de/sicherheit auf den Serviceseiten der Deutschen Telekom.

Die aktuelle Gefahrenlage zeigt das Barometer in vier Stufen an:

Die Stufe Grün wird als „Normales Risiko“ bezeichnet und informiert darüber, wie sich Nutzer schützen sollten, damit der Grundschutz möglichst hoch ist.

Die Stufe Gelb wird als „Erhöhtes Risiko“ bezeichnet und hat die Aufgabe, die Nutzer vor akuten Bedrohungen zu warnen, deren Verbreitung oder Schadensausmaß allerdings begrenzt sind. Beispiele sind Phishing- oder Pharming-Angriffe mit begrenztem Ausmaß.

Die Stufe Orange wird als „Hohes Risiko“ bezeichnet und soll die Nutzer vor akuten Bedrohungen warnen, deren Verbreitung oder Schadensausmaß signifikant sind.

Die Stufe Rot wird als „Internet-Alarm“ bezeichnet und soll die Nutzer vor aktuellen Bedrohungen warnen, die die Verfügbarkeit oder Integrität von PCs und Netzwerken in großem Ausmaß gefährden.

In Zeiten normaler Risikolage, das heißt, wenn keine akuten Warnungen vorliegen, informiert das Barometer über die Basis-Sicherheitsmaßnahmen und sensibilisiert für aktuelle sicherheitsrelevante Themen oder Bedrohungen. Die Zielgruppe des Barometers sind Privatanwender und kleine Unternehmen, die eine gängige Anbindung an das Internet über DSL, ISDN oder Modem nutzen.

Verhalten im sozialen Netzwerk.

Durch das Web 2.0 haben die sozialen Netzwerke Einzug in unseren Alltag gehalten.

Jeder ist heutzutage in der Lage, Informationen in die Welt zu senden und zu empfangen, und so geben Mitglieder von sozialen Netzwerken wie Xing, Facebook, MySpace, StudiVZ etc. wie selbstverständlich private Daten preis. Das Internet ist kein rechtsfreier Raum. Dennoch halten sich nicht alle an die geltenden Datenschutzbestimmungen, an die Regelung zum Recht am eigenen Bild oder an die Urheberrechte. Dies schafft Risiken für die Privatsphäre, derer sich viele Nutzer nicht bewusst sind. Aus diesem Grund ist es wichtig, sich in sozialen Netzwerken an bestimmte Umgangsformen zu halten.



Soziale Netzwerke sind fester Bestandteil unseres Alltags. Aber auch hier ist nicht jede Information für alle bestimmt.

Vorab: Lesen Sie die allgemeinen Geschäftsbedingungen und Datenschutzhinweise der Plattform-Betreiber genau. Aus ihnen ergibt sich in aller Regel, wie die Betreiber mit Ihren persönlichen Daten umgehen.

Gestaltung des eigenen Profils.

- In erster Linie gilt es, möglichst keine persönlichen Daten wie E-Mail-Adressen, Telefonnummern, Messenger-Daten, Fotos etc. preisgeben. Denn wer viel über sich verrät, macht es anderen leicht, ihm beispielsweise Phishing-Nachrichten oder unerwünschte Werbung zukommen zu lassen
- In Chats und Diskussionsforen können Sie anstelle des eigenen Namens auch einen Spitznamen angeben, auch wenn die Betreiber dieser Sites dazu aufrufen, den richtigen Namen zu nennen. Wenn Sie dennoch nicht auf Ihren eigenen Namen verzichten möchten, sollten Sie zumindest den Nachnamen zum Initial abkürzen
- Den Zugriff auf das eigene Profil können Sie bei den Einstellungen einschränken. Am sichersten ist es, nur Freunden den Zugang zu erlauben

Profilbilder.

- Auch wenn es bei den jungen Netzwerknutzern normal scheint, sich anhand von Fotos im Internet darzustellen, missachten zu freizügige Bilder die Regeln zum Schutz der Privatsphäre. Aus diesem Grund sollten Sie sich gut überlegen, welche Fotos Sie von sich im Internet zeigen. Fotos in Strandkleidung oder Unterwäsche sind grundsätzlich tabu. Die meisten Menschen würden im Alltag kaum Unbekannten ihr Privatleben offenbaren, oder? Bedenken Sie also stets, was Sie wirklich von sich preisgeben wollen

Fotoalben.

- Die Funktion, Fotos in Online-Fotoalben hochzuladen, wird oft und gerne genutzt. Um auch hierbei kein Risiko einzugehen, sollte man darauf achten, nur direkten Freunden Zugang zu diesen Alben zu gewähren
- Grundsätzlich sollte man nur die Fotos hochladen, an denen man auch die Rechte besitzt
- Fotos, die Sie einmal ins Internet hochgeladen haben, bleiben oft lange im Cache gespeichert, auch wenn Sie die Bilder oder auch das ganze Fotoalbum wieder löschen

Privatsphäre.

- Alle Einstellungen, die ein soziales Netzwerk zum Schutz der Privatsphäre anbietet, sollten Sie kennen und gegebenenfalls auch nutzen. Wie Sie in den verschiedenen sozialen Netzwerken Ihre Privatsphäre richtig schützen, können Sie im Internet auf der Seite www.klicksafe.de nachlesen

Freunde hinzufügen.

- Oft erhalten Sie eine Freundschaftseinladung von jemandem, den Sie nicht kennen. Bevor Sie eine Einladung annehmen oder an andere verschicken, sollten Sie gründlich prüfen, um wen es sich dabei handelt
- Persönliche Daten sollten nur echten Freunden zugänglich gemacht werden
- Da Sie selbst nicht auf unvorteilhaften Bildern gezeigt werden oder private Kommentare über sich auf den Pinnwänden dieser Sites lesen möchten, sollten Sie auch die Privatsphäre von Freunden und Bekannten respektieren und erst nach Absprache Bilder von ihnen ins Netz stellen. Da jeder „Freund“ die für Freunde freigegebenen Daten sehen kann, sollten Sie sich immer gut überlegen, wen Sie als solchen aufnehmen

Verabredungen im Internet.

- Soziale Netzwerke werden häufig dafür genutzt, sich mit Freunden zu verabreden oder andere Termine zu besprechen. Private Informationen wie Verabredungen oder „Ich bin heute Abend allein zu Hause“ sollten jedoch auf keinen Fall auf den Pinnwänden angegeben werden. Solche Informationen sollte man nur privat, zum Beispiel per E-Mail oder Messenger wie ICQ, Skype etc. austauschen

Melde- und Ignorierfunktion.

- Personen, Inhalte oder Gruppen, die gegen den Verhaltenskodex der Netzwerke verstoßen, sollten Sie unbedingt melden. Sie können entweder den Melde-Button auf Ihrer Profiseite dafür nutzen oder sich an Ihre örtliche Polizeidienststelle wenden
- Nutzern, die Sie belästigen, können Sie mit Hilfe der Ignorierfunktion den Zugang zu Ihrer Seite versperren. Diese können Ihnen dann auch keine Nachrichten mehr schicken. Zusätzlich sollten Sie diese Personen auch bei Ihrem Anbieter melden



Die Deutsche Telekom steht ihren Kunden mit Rat und Tat auch beim Thema Datenschutz zur Seite. Den Ratgeber gibt's im Telekom-Shop oder online.

Sicherheit für Kinder im Internet.

In der heutigen Zeit ist der Umgang mit dem Internet bereits im Kindesalter fast selbstverständlich. Kein Wunder, dass sich Eltern um die Sicherheit ihrer Kinder sorgen, wenn diese das Internet nutzen.

Es gibt jedoch Möglichkeiten, dieser Sorge vorzubeugen. So sensibilisieren Sie Ihr Kind für den richtigen Umgang mit dem Internet:

- Entdecken Sie das Internet gemeinsam, damit Ihr Kind von Anfang an den richtigen Umgang damit lernt! Sie sollten außerdem regelmäßig nach neuen Erfahrungen im Internet fragen und/oder einen Blick auf den Bildschirm werfen, wenn Ihr Kind am PC sitzt

Auf der Internetseite www.klick-tipps.net können Sie sich zusammen mit Ihrem Kind informieren, auf welchen Seiten Kinder surfen können, ohne befürchten zu müssen, mit ungeeigneten Inhalten konfrontiert zu werden. In der Initiative www.ein-netz-fuer-kinder.de fördert die Deutsche Telekom kindgerechte Angebote im Internet und schafft einen sicheren Surfraum – etwa mit der Suchmaschine www.fragfinn.de.

- Vereinbaren Sie Regeln für die Internetnutzung und informieren Sie sich in diesem Zusammenhang über Schutzvorrichtungen. Es gibt spezielle Filter, die auf dem Computer installiert werden und pornografische, gewaltverherrlichende oder rechtsradikale Seiten automatisch sperren. www.millionen-fangen-an.de/#/Kinderschutzsoftware
- Persönliche Daten sollte Ihr Kind keinesfalls weitergeben – keine Angaben zum Alter, zum Wohnort oder zu Treffpunkten. Sogar bei der Erstellung einer E-Mail-Adresse oder eines Namens für Chaträume sollte Ihr Kind ausschließlich auf Spitznamen zurückgreifen
- Sprechen Sie über Risiken von Treffen! Im Internet kennengelernte Personen sollte Ihr Kind nur nach Rücksprache mit Ihnen treffen. Kinder können nicht erkennen, ob diese Person gut gemeinte Absichten hat
- Diskutieren Sie den Wahrheitsgehalt von Inhalten mit Ihren Kindern
- Ermutigen Sie Ihr Kind zu guter Netiquette, also zu angemessenem Verhalten. Dies ist besonders dann wichtig, wenn Ihr Kind im Internet mit Fremden in Kontakt tritt
- Nutzen Sie Filterprogramme, damit Ihr Kind nur einen eingeschränkten Zugang zum Internet hat und nur altersgerechte Seiten besucht
- Weitere umfassende Informationen zum Thema Sicherheit im Netz finden Sie auf der Seite www.klicksafe.de, die im Auftrag der Europäischen Kommission die Medienkompetenz im Umgang mit dem Internet fördern soll



Wie schützt man sich vor unerlaubten Werbeanrufen?

Werbeanrufe ohne die Einwilligung der Verbraucher waren schon vor der Gesetzesänderung im August 2009 verboten.

Solche unerwünschten Werbeanrufe stellen nach dem Gesetz gegen den unlauteren Wettbewerb eine unzumutbare Belästigung dar. Seit der Änderung werden Verstöße gegen dieses Gesetz mit hohen Bußgeldern (bis zu 50.000 Euro) bestraft.

Unter welchen Bedingungen dürfen Sie zu Werbezwecken angerufen werden?

- Damit Sie zu Werbezwecken angerufen werden dürfen, müssen Sie eine Einwilligung erteilen. Hierzu müssen Sie darüber informiert sein, welche Daten von wem für welchen Zweck verwendet werden sollen. Der Text, mit dem Sie Ihre Einwilligung abgeben, muss Ihnen beispielsweise deutlich machen, wer Sie für Werbezwecke anrufen möchte
- Ihre Einwilligung muss freiwillig sein, das heißt auf Ihrer freien Entscheidung beruhen. Wenn Sie vermuten, dass Ihnen die Einwilligung untergeschoben wird, oder Sie das Gefühl haben, zur Abgabe der Einwilligung gezwungen zu werden, sollten Sie Ihre Zustimmung verweigern
- Für die Deutsche Telekom ist das Vorliegen einer Einwilligung des Verbrauchers in die telefonische Werbung Voraussetzung für einen Werbeanruf
- Werbeanrufe ohne Anzeige der Rufnummer sind laut neuem Gesetz nicht mehr erlaubt
- Wenn Sie von Unternehmen angerufen werden, deren Kunde Sie niemals waren, können Sie von Ihrem Auskunftsrecht Gebrauch machen. Das Bundesdatenschutzgesetz (BDSG) beinhaltet weitgehende Auskunftsrechte für die Verbraucher

Nach § 34 Bundesdatenschutzgesetz (BDSG) können Sie über die folgenden Sachverhalte im Unternehmen Auskunft verlangen:

- die zu Ihrer Person gespeicherten Daten, dazu gehört auch die Herkunft dieser Daten
- Empfänger, an die diese Daten weitergegeben werden/wurden
- den Zweck der Speicherung

Beschweren Sie sich in jedem Fall bei dem Unternehmen, das die Werbeanrufe veranlasst hat, und untersagen Sie ihm gegebenenfalls die weitere Nutzung Ihrer Daten für Werbezwecke.

Wie Sie vorgehen können, wenn Sie trotz allem ohne Zustimmung angerufen werden:

Zur Aufdeckung dieser unerwünschten Werbeanrufe bittet die Bundesnetzagentur um die Mithilfe der Verbraucher. Im Falle von Werbeanrufen, die Sie ohne Ihr Einverständnis erhalten, sollten Sie sich unbedingt die folgenden Daten notieren:

- Datum und Uhrzeit des Anrufs
- den Namen des Anrufers und des Unternehmens, für das er tätig ist
- falls möglich die Telefonnummer (die Unterdrückung der Rufnummer bei Werbeanrufen stellt einen Verstoß gegen das Telekommunikationsgesetz dar und wird mit bis zu 10.000 Euro Bußgeld bestraft)
- den Grund des Anrufs

Diese Informationen können Sie auf der Internetseite der Bundesnetzagentur eingeben (www.bundesnetzagentur.de). Die Regulierungsbehörde kann dann nach eigener Prüfung ein Ordnungswidrigkeitenverfahren einleiten.



Anhang.

||| → Bei Datenschutz und Datensicherheit darf nichts Zufall sein. Gute Organisation und die richtigen Maßnahmen sind der Weg zum Erfolg.



Besondere Maßnahmen in Datenschutz und Datensicherheit seit 2008.

Die Deutsche Telekom hat besonders nach der Bespitzelungsaffäre und den Datenvorfällen der Vergangenheit Maßnahmen entwickelt, die dazu beitragen sollen, dass sich solche Vorfälle nicht wiederholen können. Die Maßnahmen sind sowohl organisatorischer als auch technischer Art und greifen auf allen Konzernebenen. Transparent und offen über Sicherheit und Schutz von Daten in all seinen Facetten zu informieren, ist ein Leitgedanke der DTAG. Darüber hinaus nutzt das Unternehmen seine Expertise, um Kunden und Interessierten Hilfestellung im Umgang mit persönlichen Daten im Internet zu geben.

Das hat die Deutsche Telekom getan.

- Oktober 2008: Schaffung des Vorstandsressorts Datenschutz, Recht, Compliance als erster DAX 30-Konzern. Mittlerweile sind andere DAX 30-Konzerne nachgezogen
- 10-Punkte-Sofortmaßnahmenprogramm (März 2009)
- Neuausrichtung der Konzernsicherheit und der Steuerungsstrukturen „Vier-Augen-Prinzip“
- Frühjahr 2009: Veröffentlichung des ersten Datenschutzberichts als erster DAX 30-Konzern. Ziel: offene, transparente Kommunikation der Datenvorfälle und Maßnahmen zum Datenschutz
- Veröffentlichung eines Datenschutzreports unter www.telekom.com/datenschutz, der über sämtliche aktuellen Vorkommnisse informiert
- Februar 2009: Einrichtung eines Datenschutzbeirats mit führenden Datenschutzexperten aus Politik, Lehre, Wirtschaft und unabhängigen Organisationen
- Mitte 2010: Einführung eines einheitlichen Sicherheits- und Datenschutzverfahrens mit standardisierten Dokumente für die deutschen Konzerngesellschaften

Verbesserter Datenschutz.

- Abschalten unsicherer Systeme
- Einführung von Systembeschränkungen bei abgehenden Kundenanrufen durch Callcenter, um Massendatenabrufe zu verhindern: Mitarbeiter können jeweils nur auf den aktuellen Datensatz eines Kunden zugreifen
- Engere Definition der Aufgabenbereiche in der Kundenbetreuung, Verringerung der Zugriffsmöglichkeiten auf Kundendaten. Grundsätzlich: Zugriff nur auf Daten, die für die Arbeit benötigt werden (Need-to-know-Prinzip), Erhöhung der allgemeinen Kontrollen und der Kontrollen der Administratoren durch den konzerneigenen Datenschutz
- Systematische Protokollierung von Datenzugriffen
- Nachverfolgung von Zugriffen auf besonders sensible Datenbanken mittels so genannter Logfiles
- Verschärfung der Vorgaben für Benutzerkennungen und Passwörter
- Umsetzung einer Vielzahl von Sicherheitsmaßnahmen in einzelnen IT-Systeme, um unberechtigte Nutzung zu verhindern
- Schulung sämtlicher Mitarbeiter zum Thema Datenschutz und regelmäßige Verpflichtung auf das Daten- und Fernmeldegeheimnis

Transparenz/Zertifikate.

- Prüfung und Zertifizierung von Systemen, Prozessen und Vertriebspartnern durch unabhängige Gutachter als erstes Telekommunikationsunternehmen

Sensibilisierung der Öffentlichkeit.

- Kostenlose Datenschutzbroschüre unter www.telekom.com/datenschutz
- Regelmäßige Radiobeiträge mit Tipps zum sicheren Surfen im Netz etc.
- Regelmäßige Chats zu Datenschutz und Datensicherheit
- Beratung zum Datenschutz unter datenschutz@telekom.de
- Unterstützung von Initiativen wie fragFINN e.V., Deutschland sicher im Netz, Teachtoday
- Umfangreiche Information von Kunden, deren Computersysteme mit Schadssoftware verseucht sind



Organisation des Konzerndatenschutzes.

Der Konzerndatenschutz betreut unter Leitung des Konzerndatenschutzbeauftragten die nationalen Gesellschaften unmittelbar in Fragen des Datenschutzes und wirkt konzernweit auf ein angemessenes Datenschutzniveau in der Deutsche Telekom Gruppe hin. Der Konzerndatenschutzbeauftragte nimmt die gesetzliche Funktion des Datenschutzbeauftragten wahr, bestimmt die strategische Ausrichtung des Konzerns in Fragen des Datenschutzes und vertritt den Konzern in allen Angelegenheiten des Datenschutzes nach innen wie nach außen.

Der Konzerndatenschutz untergliederte sich 2008 in vier Abteilungen. Aufgrund der Datenschutzvorfälle wurde 2009 eine weitere Abteilung (Auditierung und technischer Sachverständiger) eingerichtet.

Als Datenschutzansprechpartner vor Ort sind auf Ebene der Legaleinheiten, Betriebe und sonstigen Organisationseinheiten Datenschutzstellen und Datenschutzkoordinatoren installiert. Bei den internationalen Beteiligungen wird diese Funktion von den hierzu benannten „Data Protection Officers“ wahrgenommen. Sowohl die Datenschutzkoordinatoren als auch die Data Protection Officers stehen in ständigem Kontakt mit dem Konzerndatenschutz.

Die Abteilungen im Einzelnen:

1. Richtlinien und Vorgaben.

Die Abteilung Richtlinien und Vorgaben ist verantwortlich für Grundsatzfragen im Datenschutz. Zur Sicherstellung eines rechtskonformen, einheitlichen Handelns werden konzernweit gültige Leitlinien und Policies zum Datenschutz erarbeitet und die Prozesse innerhalb des Konzerndatenschutzes entwickelt. Neben interner und externer Kommunikation im Datenschutz und der Koordinierung der internationalen Datenschutzorganisation im Konzern zählen die Steuerung fachübergreifender Projekte sowie datenschutzrelevante Entwicklungen zum Aufgabenspektrum des Teams.

2. Kundendatenschutz.

Die Abteilung Kundendatenschutz berät und unterstützt den Konzern und die strategischen Geschäftsfelder des Konzerns in Fragen des Kundendatenschutzes; insbesondere bei der Einführung von Geschäftsmodellen und -prozessen bezüglich der rechtlichen Möglichkeiten und der organisatorischen Anforderungen zur Nutzung von Kundendaten sowie der Sicherstellung der technischen Anforderungen bei der IT-gestützten Verarbeitung von Kundendaten.

3. Mitarbeiter- und Aktionärsdatenschutz.

Die Abteilung Mitarbeiter- und Aktionärsdatenschutz berät und unterstützt den Konzern und die strategischen Geschäftsfelder des Konzerns in Fragen des Personaldatenschutzes und, soweit es um personenbezogene Daten Dritter geht, die nicht Telekommunikationskunden sind (z. B. Aktionäre, Lieferanten). Zu den Aufgaben gehören darüber hinaus die Beratung der Betriebsräte des Konzerns, insbesondere des Konzernbetriebsrats, in Fragen des Datenschutzes sowie die Vertretung der Konzerngesellschaften gegenüber den Aufsichtsbehörden in Personaldatenschutzfragen auf der operativen Ebene.

4. Produkte und Dienstleistungen.

Die Abteilung Produkte und Dienstleistungen erbringt Datenschutzdienstleistungen für ausgewählte Beteiligungsgesellschaften des Konzerns, unterstützt interne Projekte sowie Vertriebsaktivitäten bei Geschäftskundenprojekten und begleitet die datenschutzkonforme Entwicklung von Produkten des Konzerns.

5. Auditierung und technischer Sachverständiger.

Diese Abteilung entwickelt datenschutzspezifische Auditierungsgrundsätze und -prozesse und steuert deren Implementierung im Konzern. Sie führt Audits eigenständig durch bzw. steuert datenschutzrelevante Auditierungen im Konzern. Sie konzipiert Maßnahmenpläne auf Basis der Auditierung und überwacht deren Umsetzung. Zudem ist sie interne Sachverständigen-Instanz für den Datenschutz bei komplexen technischen Fragestellungen. Die Abteilung wird derzeit ausgebaut.

Organisation der Datensicherheit im Konzern.

Der Bereich Group IT Security ist verantwortlich für die Entwicklung und Umsetzung konkreter Konzern-Sicherheitsanforderungen in der Informations- und Telekommunikationstechnik und stellt damit einen integralen Bestandteil der Organisation zur Sicherstellung der Datensicherheit dar. Um dieser Verantwortung gerecht werden zu können, hat die Group IT Security folgende vier Tätigkeitsfelder etabliert:

Sicherheitsanforderungen.

Festlegung, Erstellung und Veröffentlichung konzernweiter Sicherheitsstrategien, -standards, -anforderungen und -prozesse.

Prozesseinbindung.

Einbringen der Sicherheitsaspekte in relevante Projekte.

Maßnahmenumsetzung.

Beratung und Koordination von Sicherheitsabnahmen und Audits zur Überprüfung der Einhaltung sowie Überwachung aktueller Verletzbarkeiten. Außerdem Mitarbeit an und Beratung in Projekten.

Technologie.

Marktbeobachtung und Evaluierung relevanter Technologien mit Verantwortung für neue Sicherheitskomponenten und Realisierung von Einsparpotenzialen.

Organisation.

Die Group IT Security gliedert sich in zwei Abteilungen, die für die Themen Sicherheit der Produktionsinfrastruktur und Sicherheit in IT-Diensten und Applikationen verantwortlich sind. Darüber hinaus wurde ein Bereich für die Auftragssteuerung, das Schnittstellenmanagement und das Reporting eingerichtet.

Durch diese Struktur sind Schnittstellen zu anderen Konzernbereichen klar definiert, was eine effiziente Unterstützung der Chief Information Officer- und Chief Technical Officer-Bereiche ermöglicht. Die Abteilung Sicherheit der Produktionsinfrastruktur und der Technologie-Bereich (Chief Technical Officer-Organisation) arbeiten eng zusammen. Themen der Informationssicherheit aus dem Chief Information Officer-Bereich werden dabei primär mit der Abteilung Sicherheit in IT-Diensten und Applikationen geklärt.

Die spezifischen Aufgaben der Abteilungen Sicherheit der Produktionsinfrastruktur und Sicherheit in IT-Diensten und Applikationen werden von spezialisierten Gruppen wahrgenommen. Ein Großteil der Aufgaben weist dabei einen strategischen und konzeptionellen Charakter auf – die operative Umsetzung erfolgt in den jeweiligen Fachbereichen.

Sicherheit in IT-Diensten und Applikationen.

Auftrag der Abteilung Sicherheit in IT-Diensten und Applikationen ist es, die Sicherheit von IT-Diensten und Applikationen, von kundenseitigen Portalen bis hin zu Buchungssystemen, sicherzustellen.

Die Gruppe Sicherheit in IT-Anwendungen (SIA) gewährleistet grundsätzlich die Sicherheit der internen Anwendungen der Deutschen Telekom, wobei insbesondere geschäftskritische Anwendungen im Fokus stehen.

Die Gruppe Sicherheit in Portalsystemen (SIP) verantwortet die Sicherheit von Portalen der Deutschen Telekom, wobei primär Kundenportale und durch externe Partner erreichbare Portale im Fokus stehen. Beispiele für solche massenwirksamen Breitenportale sind t-online.de und Portale der Load-Familie.

Vervollständigt wird die Abteilung durch die Gruppe Sicherheit in Office- und Kommunikationsdiensten (SOK) mit dem Fokus auf Entwicklung und Umsetzung von Strategien und Konzepten zur Sicherheit von Bürokommunikationsnetzen, -diensten und -infrastrukturen.

Sicherheit der Produktionsinfrastruktur.

Die Abteilung Sicherheit der Produktionsinfrastruktur (SPI) gestaltet die Sicherheit für die Technik der Deutschen Telekom, die für die Abwicklung der Wertschöpfungsprozesse erforderlich ist. SPI ist dabei in Anlehnung an die Architektur des „Next Generation Network Security Framework“ in drei Gruppen unterteilt:

Die Sicherheit in Zugangs- und Transportnetzen wird durch die Etablierung von technischen Sicherheitsmaßnahmen gewährleistet. Betrachtet werden hier Zugangsplattformen des Festnetzes und Mobilfunks, Aggregationsysteme und Weitverkehrsnetze sowie entsprechende netznahe Produkte und Dienste für Privat- und Geschäftskunden.

Eine weitere Gruppe gewährleistet die Sicherheit für alle seitens des Konzerns betriebenen Netzdienste, Rechenzentrums-, Management- und Kontrollinfrastrukturen. Neben der Abwicklung von Projektanfragen werden vom Team Sicherheit in Netzdiensten und Rechenzentren insbesondere durch aktuelle Sicherheitsthemen getriebene Projekte direkt initiiert. So etwa das Thema Cloud- oder Dynamic Computing.



Für die Sicherheit von Endgeräten sowie von Systemen und Applikationen, die Services für externe Kunden der Deutschen Telekom bereitstellen, ist die Gruppe Sicherheit in Endgeräten und Services verantwortlich. Eine wesentliche Herausforderung ist zum Beispiel zurzeit der Bereich der „Social Communities“, in dem viele externe Partner noch nicht die hohen Sicherheitsanforderungen der Deutschen Telekom anlegen und Individualsysteme einsetzen.

Vierter Bestandteil der Abteilung Sicherheit der Produktionsinfrastruktur ist das Computer Emergency Response Team. Das Team betreibt ein international ausgerichtetes Sicherheitsvorfallmanagement in der technischen Sicherheit des Konzerns und etabliert Mechanismen zur Früherkennung von Angriffen auf extern erreichbare IT-Systeme. Zu seinen weiteren Aufgaben zählen das Schwachstellenmanagement und der Austausch über neu erkannte Schwachstellen mit weltweit verteilten Notfallteams anderer Unternehmen.

Glossar.

Audits.

Untersuchungsverfahren, die bewerten, ob und wie weit Anforderungen und Richtlinien erfüllt werden. Eine Spezialform von Audits sind sogenannte Penetrationstests, hierbei handelt es sich um hochspezialisierte technische Überprüfungen.

Auskunftsersuchen.

Kunden können unentgeltlich von einer nicht-öffentlichen Stelle Auskunft verlangen über die gespeicherten Daten, den Zweck der Speicherung, die Personen und Stellen, an die ihre Daten regelmäßig übermittelt werden, sowie die Herkunft der Daten.

Bundesdatenschutzgesetz (BDSG).

Das deutsche Bundesdatenschutzgesetz regelt zusammen mit den Datenschutzgesetzen der Länder und anderen bereichsspezifischen Regelungen den Umgang mit personenbezogenen Daten, die in IT-Systemen oder manuell verarbeitet werden.

Bundesnetzagentur (BNetzA).

Die BNetzA ist eine selbständige Bundesoberbehörde für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen im Geschäftsbereich des Bundesministeriums für Wirtschaft und Technologie mit Sitz in Bonn. Seit dem 13. Juli 2005 ist die Regulierungsbehörde für Telekommunikation und Post, die aus dem Bundesministerium für Post und Telekommunikation und dem Bundesamt für Post und Telekommunikation hervorging, umbenannt in Bundesnetzagentur. Sie reguliert unter anderem den Telekommunikationsmarkt.

Callcenter.

Unternehmen oder Abteilungen eines Unternehmens für Dienstleistungen, das operatorgestützte Sprachdienste anbietet. Dabei wickelt eine größere Anzahl von Operatoren eingehende Anrufe über eine Hotline oder abgehende Anrufe als Direktmarketing ab.

Cloud Computing/DynamicComputing.

Cloud Computing bzw. Rechnerwolke ist primär der Ansatz, abstrahierte IT-Infrastrukturen (z. B. von Rechenkapazität, Datenspeicher, Netzwerkkapazitäten oder auch Software) dynamisch an den Bedarf des Nutzers angepasst über ein Netzwerk zur Verfügung zu stellen. Die Verarbeitung der Daten durch die Anwendungen verblasst somit für den Nutzer in einer so genannten Wolke.

Compliance.

Bedeutet die Einhaltung von Verhaltenskodizes und die Erfüllung von Gesetzen, Standards und internen Richtlinien. Dadurch sollen materielle und immaterielle Schäden von den Unternehmen und ihren Mitarbeitern abgewendet werden.

Cookies.

Kleine Dateien, die ein Webserver im Webbrowser abspeichert, um die Informationen später wieder abrufen zu können. Beispiele für die Verwendung von Cookies sind Einkaufskörbe auf Onlineshop-Seiten und die Personalisierung von Internetseiten.

Data Warehouse.

Ein Data Warehouse („Datenlager“) ist eine zentrale Datenbank eines Unternehmens, in der sich Daten aus unterschiedlichen Quellen befinden. So werden zum Beispiel Kundendaten aus mehreren Systemen zusammengefasst.

De-Mail.

Dienste, die auf einer elektronischen Kommunikationsplattform einen sicheren, vertraulichen und nachweisbaren Geschäftsverkehr für jedermann im Internet sicherstellen sollen. Unter <https://www.de-mail.t-online.de> können sich Interessierte für den Dienst registrieren.

Driveby Exploits.

Hierbei werden Verwundbarkeiten in Webbrowsern (speziell ältere Versionen des Microsoft-Internet-Explorers) und Browsererweiterungen ausgenutzt, so dass schon eine Betrachtung einer verseuchten Webseite zu einer Infektion des Computersystems führen kann.

Geodaten.

Geodaten bezeichnen digitale Informationen, denen eine räumliche Lage zugewiesen ist. Beispielsweise können Fotos eine geografische Zuordnung erhalten und so eindeutig dem Ort zugeordnet werden, an dem das Bild entstanden ist.

**Geodatendienste.**

Geodatendienste sind Webservices, die Geodaten in strukturierter Form zugänglich machen. Geodatendienste können Geodaten in unterschiedlichste netzwerkbasierende Geoanwendungen einbinden, um so die Daten in interaktiven Karten darzustellen oder weiterzuverarbeiten. Beispiele für Geodatendienste sind Google Street View oder Microsoft Bing.

Honeypots.

Honeypots sind aus dem Internet erreichbare isolierte Serversysteme, die Schwachstellen simulieren.

Internationale Organisation für Normung (ISO).

Die Internationale Organisation für Normung erarbeitet internationale Normen in vielen Bereichen. Ausnahmen sind hier Elektrik und Elektronik, für die die Internationale elektronische Kommission (IEC) zuständig ist, sowie Telekommunikation, für die die Internationale Fernmeldeunion (ITU) zuständig ist. Gemeinsam bilden die drei Organisationen die WSC (World Standards Cooperation).

IP-Adresse.

Adresse in Computernetzen, die auf dem Internet-Protokoll (IP) basiert. Sie wird Geräten zugewiesen, die an das Netz angebunden sind, und macht die Geräte so adressierbar und damit erreichbar.

Konzerneinwilligungsklausel (KEK).

Nach § 95 Telekommunikationsgesetz dürfen die Bestandsdaten des Kunden für Werbezwecke nur verwendet werden, wenn der Kunden dem zuvor zugestimmt hat. Die Deutsche Telekom erfragt eine solche Einwilligung über die so genannte Konzerneinwilligungsklausel. Mit dieser Klausel kann der Kunde auch im Sinne des § 7 des Gesetzes gegen den unlauteren Wettbewerb bestimmen, ob ihn die Deutsche Telekom für Werbezwecke anrufen bzw. ihm eine E-Mail oder SMS / MMS schreiben darf.

Location Based Services (LBS).

Location Based Services (deutsch: standortbezogene Dienste) stellen einem Nutzer ortsbezogene Informationen über ein mobiles Gerät zur Verfügung. Hierzu müssen die Dienste auf die Standortdaten des jeweiligen Nutzers zugreifen.

Near Field Communication (NFC).

Ein Übertragungsstandard zum kontaktlosen Austausch von Daten über kurze Strecken. NFC kann an Terminals als Zugriffsschlüssel auf Inhalte und für Services verwendet werden, beispielsweise für bargeldlose Zahlungen, papierloses Ticketing, Online-Streaming oder Downloads.

Opt-In Lösung.

Unternehmen dürfen Kundendaten nur dann verwenden, wenn der betroffene Kunde zuvor eingewilligt hat.

Opt-Out-Lösungen.

Unternehmen verwenden Kundendaten so lange, bis der jeweilige Kunde der Nutzung widerspricht. Über die Art und Weise der Nutzung müssen die Kunden in den Datenschutzhinweisen informiert werden.

Rote-Linie-Gesetz.

Das geplante Gesetz dient dem Schutz vor besonders schweren Eingriffen in das Persönlichkeitsrecht durch unzulässige Veröffentlichungen in Telemedien. Es soll verhindern, dass durch im Netz gezielt zusammengetragene personenbezogene Daten Persönlichkeitsprofile erstellt werden können. Beispiele sind Standortdaten, die ein Mobiltelefon per GPS-Signal versendet, oder Webdienste mit Gesichtserkennungsfunktion. Auch sollen Suchanfragen nicht einsehbar sein, da darüber Rückschlüsse auf die suchende Person gezogen werden können.

Privacy Code of Conduct.

Der Privacy Code of Conduct (PCoC) ist eine konzernweite Leitlinie der Deutschen Telekom zum Datenschutz, den das Unternehmen auf Grundlage europarechtlicher Vorgaben im Jahr 2004 eingeführt hat. Er regelt einheitlich die internen Anforderungen bezüglich des Umgangs mit personenbezogenen Daten in der Deutschen Telekom Gruppe.

Smart Grids.

Intelligente Stromnetze (Smart Grids) sind in der Lage, auf Basis von gemessenem Lastverhalten die Erzeugung von Energie zu regeln. So können bei Bedarf zusätzliche dezentrale Energieproduzenten wie etwa Kraft-Wärme-Kopplungsanlagen, Solar- oder Windkraftanlagen beziehungsweise abgeschaltet werden.

Smart Metering.

Der Service umfasst das Auslesen, Verarbeiten, Darstellen sowie Fakturieren des Verbrauchs von Strom, Wasser über intelligente Zähler in Industrie und Haushalt. Smart Metering senkt Kosten erheblich und erlaubt den Zugriff auf einen massenmarktfähigen Service. Es eröffnet vor allem Energieversorgern, Messstellenbetreibern und der Wohnungswirtschaft die Möglichkeit, innovative Produkte und Dienstleistungen anzubieten, da es Verbrauchsdaten nahezu in Echtzeit liefert.

Social Media.

Social Media bezeichnet eine Vielfalt digitaler Medien und Technologien, die es Nutzern ermöglicht, sich untereinander auszutauschen und mediale Inhalte einzeln oder in Gemeinschaft zu gestalten. Beispielsweise: Twitter, Facebook, Xing, LinkedIn.

Telekom Deutschland GmbH.

Zum 1. April 2010 wurden die bislang eigenständigen Geschäftseinheiten für Festnetz „T-Home“ und Mobilfunk „T-Mobile“ in Deutschland zur Telekom Deutschland GmbH zusammengelegt.

Verkehrsdaten.

Verkehrsdaten im Sinne des Telekommunikationsgesetzes sind Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden.

Volkszählungsurteil.

Das Volkszählungsurteil ist eine Grundsatzentscheidung des Bundesverfassungsgerichts vom 15. Dezember 1983, mit der das Grundrecht auf informationelle Selbstbestimmung als Bestandteil des allgemeinen Persönlichkeitsrechts und der Menschenwürde etabliert wurde. Das Urteil gilt als Meilenstein des Datenschutzes. Anlass war eine für April bis Mai 1983 geplante, aufgrund des Urteils erst 1987 modifiziert durchgeführte Volkszählung in der Bundesrepublik Deutschland.

Vorratsdatenspeicherung.

Vorratsdatenspeicherung bezeichnet die Verpflichtung der Anbieter von Telekommunikationsdiensten zur Registrierung von elektronischen Kommunikationsvorgängen, ohne dass ein Anfangsverdacht oder eine konkrete Gefahr besteht. Damit soll eine verbesserte Verhütung und Verfolgung von schweren Straftaten ermöglicht werden.

WPA2-PSK.

Dies bezeichnet eine Verschlüsselungsmethode für Drahtlosnetzwerke.

Zentrales Sicherheitsmanagement.

Das Zentrale Sicherheitsmanagement koordiniert das Zusammenspiel aller Funktionen im Konzern, die die Sicherheit gewährleisten.

Zertifizierungen.

Zertifizierungen sind Verfahren, mit deren Hilfe die Einhaltung bestimmter Standards für Produkte oder Dienstleistungen und ihre jeweiligen Herstellungsverfahren nachgewiesen werden kann.



Abkürzungen.

BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Bundesdatenschutzbeauftragter
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
ciAM	Corporate Identity Account Management – verwaltet digitale Identitäten für Benutzer und Arbeitsplätze innerhalb der Deutschen Telekom
CEM-Tool	Customer Experience Management Tool
DRC	Vorstandsbereich Datenschutz, Recht und Compliance
GBS	Group Business Security
GIS	Group IT Security
GPR	Group Privacy
GSMA	Global System for Mobile Communications Association (ehemals Groupe Speciale Mobile Association)
GSP	Group Security Policy
IPC	International Privacy Circles
KEK	Konzerneinwilligungsklausel
PSA	Privacy and Security Assessment
T-Labs	Telekom Laboratories
TKG	Telekommunikationsgesetz
TSG	Telekom Shop Gesellschaft



Impressum.

Deutsche Telekom AG
Corporate Communications
Postfach 2000, D-53105 Bonn
Telefon 0228 181 4949
Telefax 0228 181 94004

www.telekom.com

Konzept:
Deutsche Telekom AG und
HGB Hamburger Geschäftsberichte GmbH & Co. KG, Hamburg

Gestaltung und Produktion:
HGB Hamburger Geschäftsberichte GmbH & Co. KG, Hamburg

Fotos:
Deutsche Telekom AG, Getty Images, Wolfram Scheible

Reproduktion:
PX2@Medien GmbH & Co. KG, Hamburg

Druck:
Broermann Druck + Medien GmbH, Troisdorf

KNr. 642 100 151 (deutsch)
KNr. 642 100 152 (englisch)

Kontakt.

Datenschutz Deutsche Telekom AG
datenschutz@telekom.de
www.telekom.com/datenschutz



Deutsche Telekom AG
Friedrich-Ebert-Allee 140
D-53113 Bonn

www.telekom.com