

Bericht Datenschutz und Datensicherheit 2011



Erleben, was verbindet.



Bericht Datenschutz und
Datensicherheit 2011

Über diesen Bericht.

Der Bericht Datenschutz und Datensicherheit der Deutschen Telekom blickt nunmehr auf eine vierjährige Geschichte und eine breite Weiterentwicklung zurück. Mit dem aktuellen Bericht bleibt die Deutsche Telekom ihrer Linie treu, Kunden, Aufsichtsbehörden und -gremien, Politik, Aktionären und Mitarbeitern offen zu legen, wie Datenschutz und Datensicherheit im Unternehmen umgesetzt werden. Gleichzeitig informiert der Konzern über wesentliche Strukturen und Prozesse im Umgang mit ihm anvertrauten Daten. Nicht zuletzt bezieht das Unternehmen Stellung in der politischen und juristischen Diskussion zu aktuellen Datenschutzthemen und äußert sich zur politischen und Expertendebatte beim Thema Datensicherheit.

Die bewährte Struktur des Berichts bleibt erhalten: Im Lagebericht finden Leser einen Überblick über besondere Ereignisse des Jahres 2011 in Datenschutz und Datensicherheit, sowohl außerhalb als auch innerhalb der Deutschen Telekom. Ebenso richtet das Unternehmen in diesem Kapitel den Blick in Richtung Zukunft der beiden Themen. Datenschutz im Detail beleuchtet Entwicklungen und Ereignisse in Datenschutz und Datensicherheit zielgruppenspezifisch. Ihre breite Expertise zum sicheren Surfen im Netz stellt die Deutsche Telekom in den unterschiedlichsten Formaten Kunden und Interessierten zur Verfügung. Dieser Servicegedanke spiegelt sich auch im aktuellen Bericht wider: Interessierte finden hier die Neuauflage des entsprechenden Ratgebers.

Die Deutsche Telekom wird ihren Weg weiterhin beschreiten, mit ihrer offenen Informationspraxis und aktiven Beteiligung an der Diskussion um Datenschutz und Datensicherheit diese zentralen Themen im öffentlichen, aber auch politischen Bewusstsein und in den Fachgemeinden weiter zu verankern und stärker voranzutreiben.

1. Geleitwort des Vorstands.	6	5. Ratgeber zum sicheren Umgang mit Daten.	57
2. Lagebericht.	9	5.1. PC-Sicherheit und Basisschutz.	58
2.1. Datenschutz und Datensicherheit 2011 im Überblick.	10	5.2. Gestaltung eines sicheren Passworts.	59
2.2. Besondere Ereignisse im Jahr 2011.	10	5.3. WLAN-Sicherheit für Zuhause.	60
2.3. Neue gesetzliche Regelungen.	11	5.4. Online-Shopping.	62
2.4. Prüfungen und Kontrollen durch externe und interne Stellen.	12	5.5. Smartphones – so surfen Sie sicher.	63
2.5. Auskünfte an staatliche Stellen und Privatpersonen	13	5.6. So nutzen Sie Apps sicher.	64
2.6. Forschung und Entwicklung.	16	5.7. Spurenlos im Netz.	64
2.7. Ausblick Datenschutz und Datensicherheit 2012.	18	5.7. Phishing.	66
3. Entwicklung in einzelnen Bereichen.	21	5.8. Social Engineering.	67
3.1. Privatkunden.	22	5.9. Das Sicherheitsbarometer.	68
3.2. Geschäftskunden.	29	5.10. Verhalten im Sozialen Netzwerk.	68
3.3. Beschäftigte.	32	5.11. Sicherheit für Kinder im Internet.	70
3.4. Internationale Entwicklungen.	34	6. Anhang.	73
3.5. Systeme und Prozesse.	38	6.1. Besondere Maßnahmen in Datenschutz und Datensicherheit seit 2008.	74
3.6. Kommunikation nach innen und nach außen.	46	6.2. Organisation des Konzerndatenschutzes.	75
4. Datenschutzbeirat der Deutschen Telekom.	51	6.3. Organisation der Datensicherheit im Konzern.	76
4.1. Aufgabe und Funktion.	52	6.4. Glossar.	78
4.2. Zusammensetzung.	52	6.5. Abkürzungen.	81
4.3. Beispiele seiner Arbeit im Jahr 2011.	54	7. Impressum.	84

Geleitwort des Vorstands.



Dr. Manfred Balz

Liebe Leserinnen und Leser,

was uns wichtig ist, möchten wir in guten Händen wissen: Unsere Kinder geben wir nur in eine zuverlässige Betreuung. Unsere Geldgeschäfte wickeln wir mit Finanzinstituten ab, denen wir glauben trauen zu können. Und unsere Daten? Sie vertrauen wir am liebsten Unternehmen an, bei denen wir sicher sind, dass sie gut geschützt werden.

Mehr als 170 Millionen Kunden setzen dieses Vertrauen in die Deutsche Telekom. Wir sind uns der großen Verantwortung bewusst, die sich daraus ergibt: Täglich arbeiten wir daran, dass Ihre Daten bei uns vor Zugriffen geschützt sind, und wir kommunizieren offen, wie wir mit Ihren Daten umgehen. Die Natur hat ausgeklügelte Schutzmechanismen entwickelt, damit die Arten überleben. Wir müssen die besten Prozesse und Systeme einsetzen, um zu schützen, was Sie uns anvertrauen. Viel haben wir auf diesem Weg erreicht. Dennoch müssen wir weiter mit wachen Augen nach vorne blicken.

„Die Natur hat ausgeklügelte Schutzmechanismen entwickelt, damit die Arten überleben. Wir müssen die besten Prozesse und Systeme einsetzen, um zu schützen, was Sie uns anvertrauen: Ihre Daten.“

Datenschutz wird zunehmend auf dem internationalen Parkett verhandelt und soll länderübergreifende Standards setzen. Als international tätiges Unternehmen begrüßen wir diese Entwicklung. Eine weitere Form der Internationalisierung lässt uns aber aufhorchen: Cyber-Angriffe nehmen weltweit zu, die Angreifer leiten ihre Schadcodes in Sekundenschnelle über Server in aller Welt und sind nicht mehr feststellbar. Wir müssen auf der Hut sein und die Angriffsmuster kennen, um uns zu wappnen. Wir müssen Sicherheitslösungen entwickeln und uns mit Unternehmen und Politik dazu austauschen. Zum Datenschutz müssen wir uns auch in die politische Diskussion einmischen und unsere Erfahrungen teilen. Und: Wir müssen weiterhin transparent informieren, was mit den uns anvertrauten Daten geschieht – und was nicht! Unser Datenschutzbeirat aus unabhängigen Experten wirkt mit uns in die Gesellschaft und die Politik hinein – auch in Ihrem Interesse.

Die Deutsche Telekom beschreitet seit einigen Jahren den Weg von Analyse und Austausch und transparenter Kommunikation zu den Ergebnissen. Bisher mit guten Erfolgen. Was dieser Weg langfristig bringt, wird die Zukunft zeigen. Sicher ist: Wir wollen ihn weiter beschreiten und freuen uns, dass Sie uns begleiten.

Ich wünsche Ihnen eine aufschlussreiche Lektüre!

Ihr Dr. Manfred Balz
Vorstand Datenschutz, Recht, Compliance

Einigeln funktioniert nur in der Natur. Moderne Unternehmen setzen auf offene Kommunikation und schaffen so Vertrauen.



2.1. Datenschutz und Datensicherheit 2011 im Überblick.


Das Jahr 2010 hatte in Datenschutz und Datensicherheit neue Impulse bewirkt: Über Wochen diskutierte eine breite Öffentlichkeit über die Definition dessen, wie weit im Zeitalter des Internets der Begriff der persönlichen Daten definiert werden muss und wie personenbezogene Daten angemessen geschützt werden können. Diese Diskussion setzte sich im Jahr 2011 fort und erhielt gleichzeitig neuen Schwung: Die Frage nach staatlicher Überwachung und der Notwendigkeit von Massendatenauswertungen rückte gleich mehrfach in den Fokus. In Deutschland beherrschte diese Thematik nach Bekanntwerden von Funkzellenabfragen bei einer Demonstration in Dresden über Wochen die Medien. Angefacht durch die Aufdeckung der „Zwickauer Terrorzelle“ und geschürt durch Aktionen verschiedener Gruppen wurde auch das Thema Vorratsdatenspeicherung zu einem viel und vor allem kontrovers diskutierten Gegenstand der öffentlichen Debatte. Gleichzeitig erfuhren US-amerikanische Internetdienste eine kritische Würdigung durch neue Funktionen auf Facebook oder die neuen Geschäftsbedingungen für die Nutzung von Google-Produkten.

Datensicherheit – und besonders „Cybersecurity“ – errangen 2011 bislang nicht gekannte allgemeine Aufmerksamkeit: Millionen von gehackten Kundenkonten bei Sony oder von der Hackergruppe „Anonymous“ lahmgelegte Webseiten des FBI zeigten einer breiten Bevölkerung, welche vollkommen unterschiedliche Tragweite und Qualitäten Angriffe aus dem Netz annehmen können. Die ständige Bedrohungslage aus dem Internet verdeutlichte auch der unter dem Namen „Operation Ghost Click“ bekannt gewordene Fahndungserfolg der US-Behörde FBI: Nach fünf Jahren Ermittlungsarbeit gelang es dem FBI, in Estland Cyberkriminelle festzunehmen, die weltweit Millionen von Rechnern mit dem Trojaner „DNS-Changer“ infiziert hatten. Diese kriminelle Energie machte auch vor den Kunden der Deutschen Telekom nicht halt: Unter den weltweit vier Millionen infizierten Rechnern befanden sich Anfang 2012 rund 16.500 von Kunden der Deutschen Telekom. Die Kunden wurden identifiziert und informiert. Gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnologie und dem Bundeskriminalamt stellte die Deutsche Telekom der Öffentlichkeit online einen Schnelltest zur Verfügung, der anzeigte, ob ein Computer infiziert war. Zum Redaktionsschluss des Berichtes am 2. April 2012 wurde dieser über 20 Millionen Mal aufgerufen. Rund 80.000 Klicks davon

erhielten die Rückmeldung, dass eine Infizierung des Computers vorliegt. Nachdem jedoch Medien einen Direktlink zur Warnmeldung mit Hinweis auf einen infizierten Computer publiziert hatten, ist hier mit einer statistischen Ungenauigkeit zu rechnen.

2.2. Besondere Ereignisse im Jahr 2011.


Beteiligungen der Deutschen Telekom an Initiativen zu Datenschutz und Datensicherheit.

Im Jahr 2011 hat die Deutsche Telekom ihre Aktivitäten im gesellschaftlichen und politischen Umfeld weiter vorangetrieben. Neben Stellungnahmen zu nationalen und internationalen Gesetzgebungsverfahren hat sie sich in Verbänden sowie unternehmensübergreifenden Initiativen zur Stärkung der Themen Datenschutz und Datensicherheit in Wirtschaft und Gesellschaft engagiert. 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. Auf nationaler Ebene hat die Deutsche Telekom gemeinsam mit Unternehmen der Branchen Telekommunikation und Informationstechnologie sowie dem Branchenverband Bitkom den Verein „Selbstregulierung in der Informationswirtschaft e.V.“ gegründet. Im Rahmen dieses Vereins werden künftig Selbstverpflichtungsansätze umgesetzt, wie etwa der Datenschutzkodex für Geodatendienste . Im ersten Schritt wird der Verein eine zentrale Informations- und Widerspruchsweltweite für Geodatendienste sowie eine telefonische Beratungsstelle im Laufe des Jahres 2012 bereitstellen. Anlass waren die öffentlichen Diskussionen und der Informationsbedarf um Dienste wie Google Street View.

Ein weiteres Aktionsfeld der Deutschen Telekom war die Mitarbeit bei der Ausarbeitung einer Selbstverpflichtung der Online-Werbewirtschaft unter dem Dach des Zentralverbands der deutschen Werbewirtschaft (ZAW) und Bundesverband Digitale Wirtschaft (BVDW). Die Selbstverpflichtung verfolgt das Ziel, die Transparenz bei nutzungsbasierter Online-Werbung (so genanntes Online Behavioral Advertising) gegenüber dem Endverbraucher zu erhöhen und dafür einen institutionellen Rahmen durch Gründung des Online-Werberats zu schaffen.

Gleichzeitig beteiligte sich die Deutsche Telekom intensiv an politischen Prozessen, die helfen sollen, den Datenschutz und

Datensicherheit zu verbessern. Die Deutsche Telekom hat sich deshalb insbesondere beim IT-Gipfel eingebracht. Ebenso beteiligte sie sich an der Diskussion um Einrichtung und Ausgestaltung der geplanten Stiftung Datenschutz und sicherte ihre Unterstützung für die Einrichtung zu.

Ein weiteres Engagement der Deutschen Telekom war die Mitarbeit in der „Promotorengruppe Sicherheit“ der Forschungsunion  der Bundesregierung. Dieses Beratungsgremium unterstützt die Arbeit der Bundesregierung mit Vorschlägen, wie sich Kommunikationsnetze effektiver schützen lassen. Dabei spielen insbesondere Forschungsfragen eine Rolle, die helfen können, das Sicherheits- und Datenschutzniveau mit neuen technologischen Ansätzen zu stärken.

Bewertung der Konzernorganisation Datenschutz.

Auf Eigeninitiative der Deutschen Telekom fand eine Untersuchung zur Beurteilung der konzerninternen Datenschutzorganisation statt. Diese wurde durch einen externen Prüfer vorgenommen. Gegenstand dieser Untersuchung waren Kontrollprozesse und -strukturen, die nicht nur die relevanten gesetzlichen Anforderungen, sondern auch weiterführende interne Vorgaben abdecken. Im Ergebnis bestätigten die Prüfer der Deutschen Telekom, dass sie die vorgeschriebenen und freiwilligen Kontrollen nachweislich umsetzt, wodurch das innerhalb der Deutschen Telekom beabsichtigte hohe Datenschutzniveau erreicht wird.

Datenschutzlösung für anonymes Internetsurfen mit IPv6-Adressen.

Die Deutsche Telekom stellte im November 2011 als erstes Telekommunikationsunternehmen eine Lösung für anonymes Surfen mit dem neuen Internetstandard IPv6 vor. Über ein dreistufiges Verfahren können die zwei unterschiedlichen Bestandteile der 2012 wirksam werdenden IP-Adressen zuverlässig verschleiert werden. IP-Adressen werden bei der Nutzung des Internets vergeben und sind Voraussetzung fürs Surfen im Netz mit dem jeweiligen Endgerät (zum Beispiel PC, Laptop, Smartphone). Mit der entwickelten Datenschutzlösung kann der Nutzer selbst entscheiden, wie anonym er durchs Internet surfen und seine Identität verschleiern will. Damit leistet die Deutsche Telekom mehr als das aktuelle bundesdeutsche Recht auf informationelle Selbstbestimmung fordert. Die Produkteinführung ist für 2012 geplant. Während der Umstellungszeit werden der

bisherige Standard IPv4 sowie der neue IPv6 unterstützt (siehe Seite 24).

Individuelle Entschädigungszahlungen für Betroffene der Bespitzelungsaffäre.

Die so genannte Bespitzelungsaffäre der Deutschen Telekom wurde im Jahr 2010 gerichtlich aufgearbeitet. Die strafrechtliche Hauptverhandlung endete vor dem Landgericht Bonn mit einer Verurteilung des ehemaligen Abteilungsleiters der Konzernsicherheit: Als Hauptangeklagter wurde er wegen Verstoßes gegen das Fernmeldegeheimnis und gegen das Bundesdatenschutzgesetz sowie wegen Untreue Ende November 2010 zu einer Freiheitsstrafe von drei Jahren und sechs Monaten verurteilt. Das Urteil war zum Redaktionsschluss Anfang April 2012 noch nicht rechtskräftig.

Die Deutsche Telekom hatte in Folge der Bespitzelungsaffäre rund 1,7 Millionen Euro an gemeinnützige Organisationen gespendet. Sie versteht dies als Zeichen ihrer unternehmerischen Verantwortung, die sie für die Vorgänge der Vergangenheit übernommen hat. Zusätzlich hatten der Konzern und die Anwälte der betroffenen Aufsichtsräte, Betriebsräte und Gewerkschaftsvertreter eine Vereinbarung über individuelle Entschädigungsleistungen der Deutschen Telekom geschlossen (siehe Bericht Datenschutz und Datensicherheit 2010). Im Laufe des Jahres 2011 hat die Deutsche Telekom auch mit den bespitzelten Journalisten sowie sonstigen Betroffenen (etwa mitbetroffenen Angehörigen) abschließende Vereinbarungen über individuelle Entschädigungszahlungen getroffen.

2.3. Neue gesetzliche Regelungen.

Der Gesetzgeber hat im Jahr 2011 weitere wichtige Weichenstellungen für den verbesserten Schutz von Daten vorgenommen. Auf deutscher und europäischer Ebene gab es Änderungen und Novellen von Gesetzen, die Telekommunikationsdienstleister wie die Deutsche Telekom berücksichtigen müssen. Dazu gehört das Telekommunikationsgesetz, das verbesserte Bestimmungen zum Verbraucher- und Datenschutz erhalten und somit seitens des Gesetzgebers das Vertrauen in den Telekommunikationsmarkt stärken soll. Hierzu zählt vor allem die Verbesserung der Rechtsposition des Verbrauchers beim Umgang mit sensiblen Kundendaten. Das Beschäftigtendatenschutzgesetz soll vor allem

präventive Screenings bei Fehlverhalten eines Mitarbeiters begrenzen und in das Bundesdatenschutzgesetz integriert werden. Auf europäischer Ebene strebt die geplante EU-Datenschutzverordnung eine Harmonisierung der Datenschutzbestimmungen an, um Verbrauchern innerhalb der EU ein einheitliches Verbraucherschutzniveau zu gewährleisten. Alle drei Novellierungen wurden im Jahr 2011 weiter vom Gesetzgeber vorangetrieben und sollen im Laufe der Jahre 2012 und 2013/2014 in Kraft treten.

Als führender Anbieter von Telekommunikationsprodukten und -services hat sich die Deutsche Telekom in die drei Gesetzgebungsverfahren frühzeitig eingebracht. Ziel ist es, Kunden ein Höchstmaß an Rechtssicherheit und Schutz im Umgang mit personenbezogenen Daten sowie Informationen zu bieten. Mit der schnellen Umsetzung aktueller und künftiger Gesetzesänderungen leistet die Deutsche Telekom ihren Beitrag zum rechtskonformen Datenschutz in einer vernetzten Lebens- und Arbeitswelt. Die Kapitel unter „Entwicklung in einzelnen Bereichen“ berücksichtigen die gesetzlichen Änderungen bei Datenschutz und -sicherheit im Detail.

2.4. Prüfungen und Kontrollen durch externe und interne Stellen.



Interne und externe Stellen prüften auch im Jahr 2011 Systeme und Prozesse der Deutschen Telekom. Externe Prüfungen und Kontrollen erfolgen entweder durch die staatlichen Aufsichtsbehörden oder im Rahmen von Zertifizierungen zumeist durch unabhängige externe Stellen. Im Rahmen der Sorgfaltspflicht übernimmt die Deutsche Telekom mit dem Vorstandsressort Datenschutz, Recht und Compliance eine weitere interne Kontrollfunktion: Das Unternehmen überprüft zusätzlich selbst die Einhaltung der gesetzlichen Regelungen sowie der eigenen Sicherheits- und Datenschutzbestimmungen. Auf diese Weise sichert das Unternehmen kontinuierlich ein Schutzniveau, das zu den höchsten innerhalb der Telekommunikationsbranche gehört. Gleichzeitig fließen die gewonnenen Erkenntnisse in den stetigen Ausbau von Datenschutz und -sicherheit ein. Das Ziel der Deutschen Telekom ist es, damit die Spitzenposition der Branche einzunehmen.

Staatliche Prüfungen und Kontrollen.


Der Konzerndatenschutz der Deutschen Telekom führt insbesondere mit dem Bundesbeauftragten für den Datenschutz und die




Ein hohes Niveau in Datenschutz und Datensicherheit bedarf Prüfungen und Kontrollen von externer und interner Seite.

Informationsfreiheit (Bundesdatenschutzbeauftragter), aber auch mit der Bundesnetzagentur  kontinuierlich Gespräche zu aktuellen Fragen des Datenschutzes sowie den im Unternehmen hierzu ergriffenen Maßnahmen. Über die gesetzlichen Informations- und Berichtspflichten hinaus bindet die Deutsche Telekom die Aufsichtsbehörden frühzeitig in kritische Datenschutzthemen ein, um die Transparenz und die Zusammenarbeit zu fördern. Im Februar 2011 hat der Bundesbeauftragte für Datenschutz und Informationsfreiheit einen Beratungs- und Kontrollbesuch bei der Congstar GmbH, einem Tochterunternehmen der Telekom Deutschland GmbH , durchgeführt. Ziel war es, die Erhebung und Verarbeitung von Kundendaten zu prüfen.

Audits und Zertifizierungen.

Die Deutsche Telekom hat auch im Jahr 2011 ihre Zertifizierungen und Audits  weiterentwickelt und ausgeweitet. Neben den Kontrollen von staatlichen Aufsichtsbehörden haben die Zentralbereiche 220 Audits zu Datenschutz und -sicherheit durchgeführt. Um ein gleichbleibend hohes Datenschutzniveau am Verkaufsort zu gewährleisten, absolvierte das Unternehmen in seinen Telekom Shops wiederholt Kontrollen mit dem Ziel der Einhaltung der Vorgaben zum Datenschutz. Auch im Jahr 2011


wurden die datenschutz- und sicherheitsrelevanten Prozesse in Telekom Shops von der DEKRA Certification GmbH erfolgreich auditiert. Wie im Vorjahr erhielt die Deutsche Telekom Zertifizierungen nach der internationalen Norm ISO/IEC 27001  für ihr Sicherheitsmanagementsystem und Teile der 2010 neu gegründeten Telekom Deutschland GmbH bestätigt. Bei der Konzerntochter T-Systems wurde im Jahr 2011 der Prozess der Zertifizierung der deutschen Organisation und von 19 Landesgesellschaften fortgesetzt. Dies dient dem Erhalt des Dachzertifikats über die Einführung eines konzernweiten Informationssicherheits-Managementsystems. Darüber hinaus wurden im Jahr 2011 bei der Deutschen Telekom allein 188 ISO/IEC 27001-Audits weltweit durchgeführt.

2.5. Auskünfte an staatliche Stellen und Privatpersonen.

Anfragen an den Datenschutz.

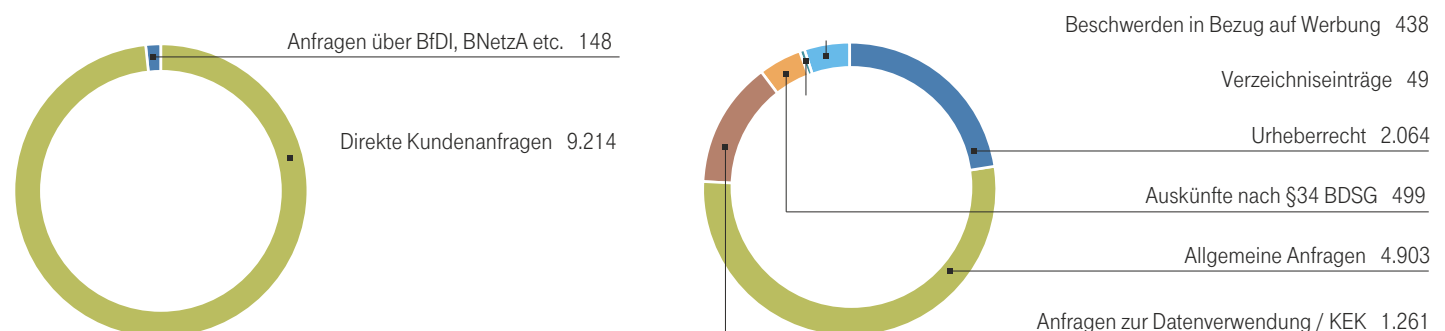
Im Jahr 2011 sind die Anfragen zum Thema Datenschutz zurückgegangen. Erreichten die Deutsche Telekom im Jahr 2010 über den Postweg, Fax oder über Online-Kanäle – entweder direkt beim Konzerndatenschutz oder bei speziell eingerichteten Serviceadressen – 10.808 Anfragen, waren es im Jahr 2011 nur noch 9.362. Über die spezielle Service-E-Mail-Adresse datenschutz@telekom.de gingen im Jahr 2011 die meisten Anfragen ein. Ungefähr ein Achtel aller Anfragen wurden direkt an den

Konzerndatenschutzbeauftragten gerichtet. Davon kamen 148 vom Bundesbeauftragten für Datenschutz und Informationsfreiheit sowie weitere über die Bundesnetzagentur.

Die meisten Anfragen, 2003 im vergangenen Jahr, erfolgten zum Thema Abmahnung wegen vermeintlicher Urheberrechtsverletzung. Hierbei geht es darum, welche Daten des Kunden an einen Dritten, den so genannten Rechteinhaber, in einem konkreten Fall herausgegeben wurden. Anfragen zum Urheberrecht werden vorwiegend von Kunden, die eine anwaltliche Abmahnung wegen vermeintlicher Urheberrechtsverletzungen erhalten haben (wie zum Beispiel bei behaupteter rechtswidriger Nutzung von Tauschbörsen im Internet), oder deren Rechtsbeistand gestellt. Häufig folgt auf eine Anfrage aufgrund urheberrechtlicher Verletzungen ein Auskunftersuchen  nach § 34 Bundesdatenschutzgesetz, da betroffenen Kunden die Weitergabe ihrer Daten und die entsprechende Rechtsgrundlage erklärt haben möchten (Näheres siehe Seite 15).


Ein anderer Teil der Anfragen betraf Auskunftersuchen nach §34 BDSG, die ohne konkreten Anlass an die Deutsche Telekom gerichtet wurden. Nach § 34 BDSG kann ein Kunde unentgeltlich von einem Unternehmen Auskunft über die dort über ihn gespeicherten Daten, den Zweck der Speicherung, die Personen und Stellen, an die seine Daten regelmäßig übermittelt werden, sowie insbesondere die Herkunft der Daten verlangen. Diese Anfragen beziehen sich auf alle über den Kunden gespeicherten Daten.

Verteilung und Art der Kundenabfragen an den Konzerndatenschutz



Anfragen insgesamt* 9.362

* Nicht enthalten sind die internen 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 sind zum Beispiel der regelmäßige Erhalt von Werbematerial, Werbeanrufen oder -faxen. Die Kunden informieren sich, ob eine solche Einwilligung von ihnen tatsächlich vorliegt oder welchen Umfang sie hat. Anfragen zu Verzeichniseinträgen zielen auf die Korrektur oder Löschung von Einträgen in öffentlichen Verzeichnissen (zum Beispiel Telefonbuch, Auskunft). Die Deutsche Telekom gibt in diesen Fällen Auskunft im Rahmen ihrer gesetzlichen Verpflichtung.

Ein weiteres Thema, weswegen sich Kunden an die Deutsche Telekom wenden, ist die Beratung zu Sicherheitsfragen (PC-Schutz, Viren, Würmer, Spam, Phishing etc.) und der Umgang mit den persönlichen Daten im Bereich Social Media. Die Deutsche Telekom bietet durch praktische Tipps und gezielte Hilfestellung einen Beitrag zur Sicherheit im Netz und steigert die Kundensensibilisierung für Datenschutz und -sicherheit (siehe Seite 57).

Kontakt zur Deutschen Telekom.

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

Post: Konzernbeauftragter für den Datenschutz,
Deutsche Telekom AG,
Friedrich-Ebert-Allee 140,
53113 Bonn.

E-Mail: datenschutz@telekom.de

Anfragen an den Personaldatenschutz.

Mitarbeiter können sich zu fachlichen Fragen bezogen auf ihre Projekte, aber auch zu persönlichen Fragen, die ihr Arbeitsverhältnis mit der Deutschen Telekom betreffen, an die Deutsche Telekom wenden. Im Berichtszeitraum 2011 bearbeitete das Unternehmen 2179 Anfragen und Eingaben. Diese gingen über den Postweg, Telefax, Telefon oder Online-Kommunikation ein. Während knapp zwei Drittel der Anfragen auf fachliche Fragen entfielen, betrafen 682 Vorgänge die Datenverarbeitung im konkreten Beschäftigungsverhältnis. Gefragt wurde häufig, wie personenbezogene Daten in Leistungsnachweisen an externe Dienstleister weitergegeben werden dürfen, welche Datenschutzrechte bei Vertretungsregelungen

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 Internetwahl wird deshalb durch den Internetzugangsanbieter eine so genannte dynamische IP-Adresse vergeben. Mit der Einführung des neuen Standards IPv6 wird dieses Prinzip beibehalten (siehe Seite 24). Die Deutsche Telekom speichert diese Kombination aus Benutzererkennung 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 Telekommunikationsgesetz und § 109 Telekommunikationsgesetz.

für Zugriffe auf E-Mail- und Kalender-Anwendungen zu beachten sind oder wie die Handhabung von Dokumenten für die elektronische Personalakte erfolgt. Auch die datenschutzkonforme Vorgehensweise bei Mitarbeiterumfragen und den Umgang mit Urlaubslisten behandelten die Fragen im Jahr 2011.


Anfragen an das Deutsche Telekom CERT.

Das Cyber Emergency Response Team (CERT) der Deutschen Telekom ist in der Deutschen Telekom Group international verantwortlich für das Krisen- und Incident Management von Cyber-Vorfällen. Darüber hinaus ist das CERT zentraler Ansprechpartner für Anfragen oder Sicherheitsmeldungen von externen Personen oder Organisationen. Internet Service Provider, die Strafverfolgungsbehörden sowie Behörden und die Security Community kontaktieren das CERT, um auf Sicherheitsvorfälle oder Bedrohungen aufmerksam zu machen, die die Deutsche Telekom AG oder deren Kunden betreffen könnten. Beispiele hierfür sind die Information über die Verteilung illegaler Inhalte im Internet oder das Anlegen von Phishing-Webseiten. Im Jahr 2011 sind über das Eingangstor des CERT – CERT@telekom.de – 681 Meldungen eingegangen. 109 von diesen Meldungen waren so schwerwiegend, dass diese als Cyber-Vorfälle klassifiziert und durch das CERT bearbeitet und betreut wurden.

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 zugeben, 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.

Kontakt zum Deutsche Telekom CERT.

Personen außerhalb der Deutschen Telekom können über das CERT Sicherheitsvorfälle melden, die die Deutsche Telekom bedrohen oder bei denen aus Diensten der Deutschen Telekom heraus Dritte bedroht werden. Hierfür steht die folgende E-Mail Adresse zur Verfügung: cert@telekom.de

Anfragen zu Urheberrechtsverletzungen.

Im Jahr 2011 erhielt die Deutsche Telekom einstweilige Anordnungen zur vorläufigen Speicherung von durchschnittlich 100.000 IP-Adressen pro Monat. Diese Adressen haben die Rechteinhaber oder deren Dienstleister bei Recherchen nach Angeboten urheberrechtlich geschützter Werke im Internet ermittelt.

Verlässliche Zahlen zur Entwicklung von Urheberrechtsverletzungen existieren nicht. Die Deutsche Telekom verzeichnet allerdings mit 1,23 Millionen vorläufig gespeicherten IP-Adressen im Jahr

2011 einen Rückgang um ca. 50 Prozent im Vergleich zum Vorjahr. Belastbare empirische Untersuchungen für diesen Rückgang gibt es nicht. Der Rückgang dürfte aber unter anderem darauf zurückzuführen sein, dass Kunden bei Vertragsabschluss eine allgemeine Aufklärung über das Thema erhalten und in den Bedienungsanleitungen etwa der WLAN-Router ein Kapitel mit Hinweisen auf Verschlüsselung und Sicherheitsstandards vorhanden ist. Weiterer möglicher Grund könnte das Ausweichen auf legale Plattformen sein. Insgesamt erfolgte eine Sensibilisierung der Kunden zum Thema Filesharing und die damit einhergehende Abmahnwelle von Rechteinhabern oder deren Dienstleistern.

Bei der Deutschen Telekom sind im Jahr 2011 Beschwerden von Nutzern, deren Daten an Dritte weitergegeben wurden, ebenfalls zurückgegangen. Zur Ursache dieses Rückgangs gibt es keine gesicherten Erkenntnisse. Grund dafür könnte unter anderem der von der Deutschen Telekom entworfene Ratgeber zum

Datenschutz für Kunden sein, der auf Datenschutz- und Sicherungsmaßnahmen für Endgeräte hinweist.

Telekommunikationsüberwachung nach § 110 TKG.

Verschiedene Gesetze des Bundes und der Länder verpflichten 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 Strafverteilung (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 bundesweit für den Mobilfunk.

2.5.8. Weiterentwicklung der Beauskunftung.

Die Gründung der Telekom Deutschland GmbH im Jahr 2010 machte es erforderlich, Unterschiede im Prozess der Auskunftserteilung bei der T-Mobile GmbH einerseits und bei der Deutschen Telekom AG (T-Home) andererseits zu identifizieren sowie 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, hat die Deutsche Telekom ihre Beauskunftungsstrategie gegenüber staatlichen Stellen im Jahr 2011

überarbeitet. Ziel war und ist es, eine verlässliche Handlungsmaxime zur Beauskunftung an berechnigte staatliche Stellen zu besitzen. Das Projekt wurde im Lauf des Jahres 2011 realisiert; seine Ergebnisse wurden im Februar 2012 dem Datenschutzbeirat der Deutschen Telekom vorgestellt. Der Datenschutzbeirat stellte fest, dass die Beauskunftung an staatliche Stellen auf Basis klar erkennbarer Rechtsgrundlagen sehr strukturiert und dokumentiert erfolgt. Hiervon unabhängig setzt sich die Deutsche Telekom auch weiterhin für eine Präzisierung und bundesweite Vereinheitlichung der gesetzlichen Rahmenbedingungen der Beauskunftung ein.

2.6. Forschung und Entwicklung.

Die Deutsche Telekom setzt bei der Entwicklung von innovativen Lösungen und Produkten nicht nur auf hauseigene Kompetenzen. Vielmehr sucht sie über den Schulterschluss mit wissenschaftlichen Einrichtungen Impulse aus neuen Blickwinkeln, die wichtiger Bestandteil der Innovationsstrategie des Unternehmens sind. Dabei berücksichtigen sowohl interne Entwickler als auch Wissenschaftler die Aspekte des Datenschutzes und der Datensicherheit bereits in den Machbarkeitsstudien – also noch vor Beginn der Entwicklungsphase eines Services oder Produkts.

Wichtige Einrichtung in Forschung und Entwicklung sind die Telekom Innovation Laboratories (T-Labs), die 2005 gemeinsam mit der Technischen Universität Berlin gegründet wurden.

Datenschutz und Datensicherheit für Privat- und Geschäftskunden haben in der Forschungsarbeit der T-Labs einen hohen Stellenwert – einige Beispiele aus dem Jahr 2011 und den ersten Wochen des Jahres 2012:

- Die Deutsche Telekom startete zur CeBIT 2012 mit der dritten Version von Simko (Sichere mobile Kommunikation), einem neuen Standard für sicheres Arbeiten unterwegs. Simko ist zum einen ein extrem sicheres Smartphone, zum anderen ein Betriebsmodell für die Sicherheit von Daten und den Abhörschutz von Telefongesprächen. Mails, Kontakte, Termine, SMS, Fotos, Tonaufnahmen und Telefonate sind komplett verschlüsselt und verlassen die Infrastruktur eines Kunden nicht. T-Systems und die Telekom Innovation Laboratories entwickelten gemeinsam eine sichere Softwarearchitektur für Smartphones, eine Art

„Fort Knox“ für Datenschutz im Telefon. So genannte Mikrokerne erlauben es, zwei sichere „Welten“ in einem Gerät anzulegen: Eine offene und eine hochsichere geschäftliche. Selbst bei Verlust oder Diebstahl bleiben die Informationen dank Verschlüsselung auf dem Smartphone geschützt. Dieser Aufbau erlaubt auch ein Ausweiten der bisherigen Simko-Lösung auf Tablets und Notebooks.

- **SmartSenior:** Intelligente Assistenzsysteme für Senioren helfen älteren Menschen, zu Hause möglichst lang ein unbeschwertes und selbstbestimmtes Leben zu führen. Die T-Labs leiten das Forschungsprojekt SmartSenior des Bundesministeriums für Bildung und Forschung. Ziel ist es, ein integriertes Gesamtkonzept aus Gesundheits-, Sicherheits-, Service- und Kommunikationslösungen mit einheitlichen, intuitiven Bedienoberflächen zu entwickeln. Damit soll die digitale Kommunikation und die Datenverarbeitung des Assistenzsystems geschützt werden, um zum Beispiel Gesundheitsdaten mit dem ambulanten Pflegedienst sicher austauschen zu können. Um bereits in der Entwicklungsphase für Testnutzer den Datenschutz und die Datensicherheit zu gewährleisten, hat die Deutsche Telekom 2011 einen großen Feldversuch vorbereitet. Dazu erarbeiteten die Entwickler mit den Datenschutzbeauftragten der beteiligten Partner Verfahren, die 2012 den datenschutzkonformen Testbetrieb sicherstellen sollen.
- **Erkennen von Unregelmäßigkeiten in Datensätzen:** In einem Forschungsprojekt untersuchte die Deutsche Telekom Daten mittels Methoden aus dem Bereich maschinenbasierten Lernens und künstlicher Intelligenz. Die Ziele sind zum Beispiel die Früherkennung von Server-Ausfällen oder die Missbrauchserkennung in Internetportalen. Die für diese Szenarien benötigten Testdaten erfordern ein hohes Maß an Anonymisierung. Das gewährleistete die Deutsche Telekom in enger Kooperation mit den Dateneignern und dem Konzerndatenschutz.
- **Datenspeicherung in Cloud-Lösungen:** Unternehmen und Verbraucher können Software heutzutage nach Bedarf über das Internet beziehen. Bei diesen so genannten Cloud-Lösungen liegen Daten physisch auf Servern, die weltweit verteilt sein können. Geschäftskundendaten, Produkt- oder Abrechnungsdaten unterliegen damit häufig unterschiedlicher Gesetzgebung und Einsichtnahme durch Behörden. Die Deutsche Telekom entwickelt in einem Forschungsprojekt permanent

Technologien und Lösungen weiter, um die wachsenden datenschutzrechtlichen Anforderungen von Firmen und Privatkunden zu gewährleisten.

- **SIM-Authentifizierung:** In einem Forschungsprojekt entwickelt und erprobt die Deutsche Telekom die Nutzung der SIM-Karte für eine sichere Authentifizierung von Internetdiensten. Anwender sollen über ein Smartphone einen besser gesicherten und einfacher zu handhabenden Zugang etwa zu ihrem E-Mail-Postfach erhalten. Dazu kann die Eingabe eines Passworts durch die Benutzung einer kurzen PIN ersetzt werden. Gleichzeitig können auch die Mobilfunknummern anonymisiert werden, so dass Werbe-SMS und Anrufe unter der vom Internetdienst abgespeicherten Rufnummer nicht möglich sind.


Neben der Forschung in den T-Labs arbeitet die Deutsche Telekom mit öffentlichen und privaten Wissenschaftsorganisationen, Forschungseinrichtungen, Hochschulen und Unternehmen zusammen. Sie unterstützt die Stiftungsprofessur „Mobile Business & Multilateral Security“ (www.m-chair.net) der Goethe-Universität Frankfurt am Main, die sich mit Fragen des Datenschutzes in der mobilen Kommunikation von morgen im Rahmen verschiedener europäischer Projekte beschäftigt:

- Das Projekt „Picos“ hat untersucht, wie Nutzer ihre Privatsphäre schützen können, wenn sie mit mobilen Endgeräten wie Smartphones soziale Netzwerke nutzen. Bisher existieren nur wenige Möglichkeiten für Nutzer, den Zugriff auf persönliche Daten und Inhalte je nach Situation einzuschränken. Ziel des Projekts ist es, ihnen Werkzeuge an die Hand zu geben, um jederzeit einfach selbst bestimmen zu können, welche Orts- und Kontextinformationen sie preisgeben wollen. Dazu zählen auch partielle Identitäten, mit denen Nutzer mit verschiedenen Pseudonymen auftreten können. Die in Picos entwickelten Konzepte wurden in zwei mobilen Applikationen implementiert und von Nutzern evaluiert.
- Das Projekt „PrimeLife“ entwickelt Konzepte und Technologien für eine datenschutzfreundliche Gestaltung von Identitätsmanagementsystemen. Der Stiftungslehrstuhl entwickelte darin unter anderem eine Methode zur ökonomischen Bewertung von Funktionen zum Schutz der Privatsphäre. Bisher war die Monetarisierung von Kundeninformationen, die Unternehmen aus ihren Kommunikationsdienstleistungen gewinnen, das

Geschäftsmodell vieler Telekommunikationsanbieter. Doch welchen Wettbewerbsvorteil erzielen Unternehmen, wenn sie ihren Kunden datenschutzfreundliche Funktionalitäten bereitstellen? Ein Beispiel ist ein Konzept für ein Identitätsmanagement, das über die reine Erfüllung rechtlicher Vorgaben hinausgeht und sich an den Datenschutzbedürfnissen der Nutzer orientiert.

2.7. Ausblick Datenschutz und Datensicherheit 2012.

In den vergangenen Monaten und Jahren hat sich die Deutsche Telekom nicht nur im Datenschutz einen Namen aufgebaut. Auch im Bereich der Cybersicherheit sind die Experten des Unternehmens mittlerweile gerne gesehene Gäste auf nationalen und internationalen Symposien und angesehenen Partner von Wirtschaft, Politik und Behörden. Besonders der Gedanke, Sicherheit und Datenschutz von vornherein in die Entwicklung von Prozessen und Produkten zu integrieren (Privacy and Security by Design), hatte 2011 breites Gehör gefunden. Ebenso stießen die 2010 entwickelten und 2011 ausgebauten Frühwarnsysteme der Deutschen Telekom zur Erkennung von Angriffsmustern aus dem Netz auf große Aufmerksamkeit. Auf dem Gebiet der Frühwarnung und Erkennung von Cyberangriffen wird auch im Jahr 2012 mit Neu- und technischen Weiterentwicklungen der Deutschen Telekom zu rechnen sein: Täglich tauchen weltweit 50.000 bis 60.000 neue Viren, Trojaner oder Würmer auf, die als Schadsoftware Endgeräte befallen. Diese hohe Anzahl erfordert künftig Sicherheitstechnologien und -systeme, die eine valide Erkennung in Echtzeit ermöglichen.

Die Deutsche Telekom wird im Jahr 2012 ihre Frühwarnsysteme wie die „Honeypot-Systeme“ (siehe Seite 40) weiter ausbauen, um Angriffsmuster und neue Trends bei Cyberangriffen zu erkennen. Dabei setzt das Unternehmen darauf, seine Technik anderen Unternehmen und Organisationen zur Verfügung zu stellen und die jeweiligen Erkenntnisse zum Online-Schutz der Kunden zusammenzuführen. Dazu wird die Deutsche Telekom 2012 unter anderem ihre mobilen Honeypots  aufstocken, mit der das Unternehmen als erster Telekommunikationsanbieter in Europa netzseitige Angriffe auf Smartphones analysieren konnte.

Fehlende Informationen über potentielle Sicherheitslücken bleiben auch 2012 eine der Hauptursachen für erfolgreiche Cyber-



Dank ausgeklügelter Frühwarnsysteme kann die Deutsche Telekom Angriffsmuster aus dem Netz erkennen. Auch in Zukunft arbeitet sie am Ausbau dieser Systeme.

Angriffe auf Unternehmen und Kunden. Die Deutsche Telekom setzt heute bereits verstärkt auf Kooperationen mit öffentlichen wie privaten Organisationen, um aus Angriffen zu lernen. Diese Zusammenarbeit könnte sich künftig zu einer Veröffentlichung von Sicherheitsstandards entwickeln, die der Fachwelt und Online-Community vorgestellt werden. Mit diesem Ansatz möchte die Deutsche Telekom die kritische Auseinandersetzung mit der Netzgemeinde suchen und auch Kritiker und Experten einladen, gemeinsam bessere Sicherheitsstandards und Schutzkonzepte zu entwickeln.


In Zusammenarbeit mit anderen Providern und Geräteherstellern setzt die Deutsche Telekom 2012 auf gemeinsame Bestrebungen der Branche, nicht nur die Endgeräte, sondern die Informationen und Daten selbst in den Mittelpunkt von Schutzmaßnahmen zu stellen. Die Datensicherheit im Internet sollte in Zukunft auch in der Information selbst enthalten sein – vergleichbar dem heutigen digitalen Rechtsmanagement von Arbeitsdokumenten. Die Deutsche Telekom führt dazu Gespräche mit unterschiedlichen Herstellern, um mit ihnen neue Lösungsansätze für die Produkte von morgen zu entwickeln.

Angesichts der hohen Bedrohungslage durch Angriffe aus dem Netz und eines immer größer werdenden Bewusstseins der Bevölkerung für Cybergefahren können es sich Hersteller und Anbieter nicht mehr leisten, ihre Produkte ohne neueste Schutztechnologien zu entwickeln oder ohne ausreichende Sicherheitstests zu veröffentlichen. Die Deutsche Telekom wird ihr im Jahr 2011 international eingeführtes PSA-Verfahren (Privacy and Security Assessment, siehe Seite 41) weiter entwickeln. Dieses Verfahren integriert die Anforderungen an technische Sicherheit und Datenschutz vom ersten Entwicklungsschritt an in die Produkt- und Systementwicklung. Jährlich durchlaufen aktuell mehr als 2.000 Projekte das PSA-Verfahren, und es gewinnt in der Fachwelt zunehmend Vorbildcharakter. Die Deutsche Telekom wird sich darüber hinaus auch weiterhin bei ihren Partnern und Lieferanten einsetzen, technische Sicherheit und Datenschutz als Design-Kriterium für Produkte sowie Services fest zu verankern. Vor der Markteinführung sollen digitale Sicherheitstests obligatorisch werden. Anbieter- und herstellerübergreifend lassen sich so Schutzniveaus von Produkten und Services erhöhen, um Kunden vor Cyberkriminalität und Internetgefahren zu schützen.

Neben dem weiteren Ausbau und der Etablierung von technischen Sicherheitsmaßnahmen setzt die Deutsche Telekom im Jahr 2012 ihre breit gefächerten Maßnahmen im Datenschutz fort. Nur sensibilisierte Mitarbeiter und Nutzer sind langfristig in der Lage, den sicheren und vertrauensvollen Umgang mit der Online-Welt zu gewährleisten. Das Unternehmen hat dazu unter anderem ein Projekt gestartet, in dem Kinder und Jugendliche, aber auch deren Erziehungsberechtigte, frühzeitig an den Umgang mit dem Internet und seiner Chancen sowie Risiken herangeführt werden.

Sicherheit und Datenschutz in der Cloud wird ebenso eines der wichtigen Themen der Deutschen Telekom sein. Cloud-Lösungen sind bereits heute integraler Bestandteil vieler IT-Modelle von Unternehmen. Auch immer mehr private Nutzer wollen Daten und Software nicht mehr auf dem Computer zu Hause oder dem Smartphone speichern. Dabei wollen sie sich zu Recht auf die hohen Datenschutz- und Sicherheitsstandards der Deutschen Telekom verlassen. Übergreifende Sicherheitsstandards will das Unternehmen durch die Entwicklung einheitlicher Zertifizierungsansätze von Cloud-Services erreichen. Sie wird dazu im Jahr 2012 die Initiativen des Branchenverbands Bitkom und des Bundesamts

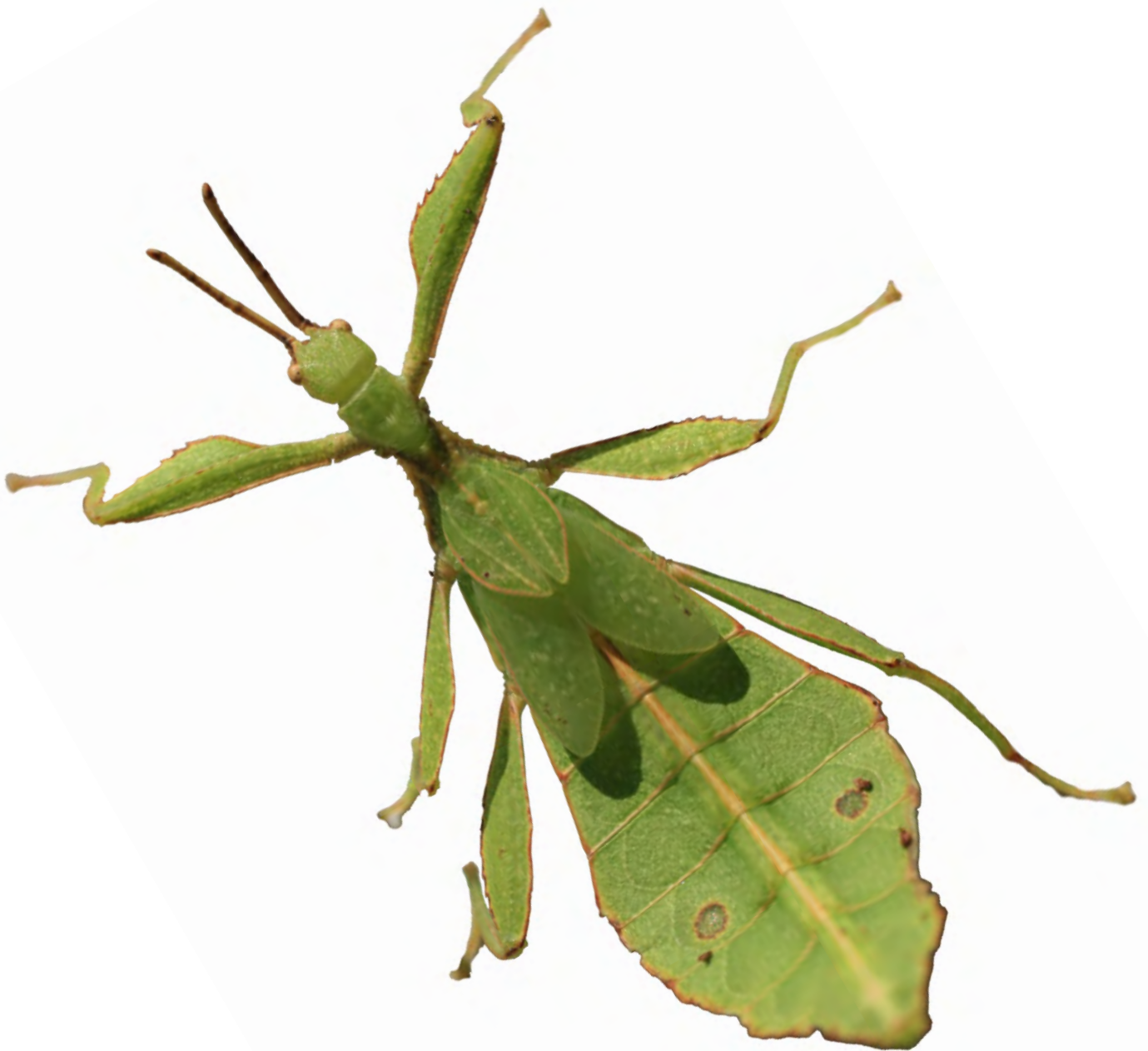
für Sicherheit in der Informationstechnik in Deutschland aktiv unterstützen sowie sich für die Etablierung unabhängiger Sicherheitszertifizierungen von Cloud-Dienste engagieren.

Im Bereich Gesetzgebung wird sich im Jahr 2012 beim Datenschutz einiges tun: Die Deutsche Telekom befasst sich mit der Umsetzung von neuen gesetzlichen Regelungen, wie etwa dem Telekommunikationsgesetz . Sie bereitet sich aber auch intensiv auf die erwartete Neuregelung zum Beschäftigtendatenschutz vor und bringt sich weiterhin konstruktiv in die Diskussionen mit ein.

Gleichzeitig wurde zum Jahresbeginn 2012 der erste Entwurf einer einheitlichen Datenschutzregelung für Europa, die EU-Datenschutzverordnung, vorgelegt. Durch den Harmonisierungsansatz bringt sie sehr viele positive Aspekte und Impulse für die Wirtschaft, aber auch für die Bürger Europas mit sich. Diesen Ansatz wird die Deutsche Telekom weiter unterstützen und dazu den Dialog mit Vertretern des Europäischen Parlaments suchen, um in der Unternehmenspraxis erkannten Regelungsbedarf vorzutragen.


Im Bereich Gesundheitswesen wird zudem ein besonderer Schwerpunkt in der Begleitung der neuen Geschäftsmodelle der Deutschen Telekom liegen. Das bringt eine Betrachtung der dafür geltenden gesetzlichen Rahmenbedingungen wie etwa des deutschen Strafgesetzbuchs mit sich, das zum Beispiel die Zugänglichmachung von Krankendaten für Dritte strafbewehrt untersagt. Solche Regelungen müssen im Lichte der heutigen Sicherheits- und Schutzmechanismen möglicher Geschäftsprozesse und Verarbeitungen in der IT neu betrachtet werden. Das Maß aller Dinge ist und bleibt dafür aber der hohe Anspruch an die Integrität und den Schutz der Patientendaten.

Wer sich gut tarnt, wird nicht entdeckt.
Die Deutsche Telekom setzt bei Datenschutz und
Datensicherheit darauf, sich nicht zu verstecken.



3.1. Privatkunden.

Gesetzliche Regelungen.

Nachdem sich der Vermittlungsausschuss von Bundesrat und Bundestag auf eine Novellierung des Telekommunikationsgesetzes einigte, soll das neue Gesetz im zweiten Quartal 2012 in Kraft treten. Zu den Änderungen des Telekommunikationsgesetzes zählt im Bereich Verbraucherschutz etwa, dass kostenpflichtige Warteschleifen bei Sonderrufnummern nicht mehr eingesetzt werden. Die Handhabung von so genannten Lokalisierungsdiensten (Location Based Services ) ist in § 98 Telekommunikationsgesetz geregelt. Ohne vorherige Einwilligung der Nutzer dürfen Diensteanbieter Standortdaten weder verarbeiten noch an Zusatzdiensteanbieter weiterleiten.

Desweiteren werden in § 98 Telekommunikationsgesetz zusätzliche Informationspflichten mit dem Ziel eingeführt, sensible Daten besser zu schützen und damit die Rechtsposition des Verbrauchers zu stärken. Hierzu gehört unter anderem die Verpflichtung, bei jeder Fremddortung des Mobilfunkendgerätes dem Nutzer anzuzeigen, dass er geortet wird. Diese Änderungen schaffen mehr Transparenz und Rechtssicherheit für Verbraucher.

Im Rahmen der Umsetzung europäischer Vorgaben wurden die Berichtspflichten von Telekommunikationsanbietern zu Datenschutzvorfällen erweitert. §109a Telekommunikationsgesetz sieht vor, Verletzungen des Datenschutzes unverzüglich mitzuteilen, sofern dadurch schwerwiegende Beeinträchtigungen der Verbraucher entstehen. Diese erweiterten Informationspflichten über Datenschutzverletzungen schaffen eine höhere Transparenz bei Datensicherheit und -schutz. Gegenüber den bestehenden Meldepflichten müssen die Telekommunikationsunternehmen nun nicht mehr nur dann informieren, wenn Daten unberechtigt an Dritte übermittelt wurden, sondern zum Beispiel auch, wenn Daten intern beim Provider unberechtigt gelöscht oder verändert wurden. Die Deutsche Telekom berichtete bereits weit vor einer gesetzlichen Verpflichtung und in Deutschland als erstes Unternehmen freiwillig über Datenvorfälle. Daher sieht sich die Deutsche Telekom für die neuen Berichtspflichten gut vorbereitet. Die erzielten Ergebnisse zur Verbesserung des Verbraucher- und Datenschutzes bewertet die Deutsche Telekom als sehr positiv. Hervorzuheben ist auch die Streichung des § 92 Telekommunikationsgesetz, der die Anforderungen an die Übermittlung von personenbezogenen Daten an nicht öffentliche Stellen im EU-Ausland geregelt hat. Durch die



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

Datenschutz ist zwar weltweit Thema – allerdings meistens nur jeweils auf Ebene jedes einzelnen Landes. Brauchen wir nicht einen übergreifenden Blick auf den Datenschutz? Müssen wir die Länderbarrieren nicht überdenken?

Die Diskussion, wie man vor dem Hintergrund von einzelnen Länderegelungen zu weltweit gültigen und verlässlichen Datenschutz-Standards kommt, wird aktuell vehement geführt. Hier zu einem positiven Ergebnis zu gelangen, ist unerlässlich für den Erfolg der gesamten Internet- und IT-Wirtschaft, weltweit. Geschäftsmodelle dürfen nicht an Ländergrenzen Halt machen. Unterschiedliche Datenschutzgesetze können aktuell jedoch genau dazu führen. Ein weltweit hoher, transparenter und verlässlicher Standard würde vollkommen neue Ansätze ermöglichen und gleichzeitig eine vertrauensbildende Maßnahme für den Kunden bedeuten. Der Kunde muss wissen, dass er mit seinen persönlichen Informationen weltweit gut aufgehoben ist. Nur dann wird er die neuen Geschäftsmodelle auch nachhaltig nutzen.

Besonders die Europäische Union hat 2011 und 2012 mit ihrer geplanten Novelle der EU-Datenschutzrichtlinie in Form einer Verordnung einen wesentlichen Schritt in Richtung eines harmonisierten Datenschutzrechts gemacht. Zumindest innerhalb Europas. Eine solche Harmonisierung war längst überfällig, um zum einen Transparenz für die Kunden zu schaffen, zum anderen aber auch einheitliche Wettbewerbsbedingungen für Unternehmen. Im nächsten Schritt sollten Ansätze wie die geplante Verordnung weltweit Schule machen. Im besten Einklang der Wirtschaft, der Verbraucher und des Datenschutzes.

Streichung ergeben sich Erleichterungen für den Datentransfer von Telekommunikationsdaten, da hier bisher besonders strenge Restriktionen galten, die weit über das allgemeine Schutzniveau des Bundesdatenschutzgesetzes hinausgingen. Der Name und die Adresse eines Telekommunikationsteilnehmers durften bislang zum Beispiel nicht an eine ausländische Konzerntochter übermittelt und dort verarbeitet werden. Mit Inkrafttreten des Gesetzes gelten im Bereich des internationalen Datentransfers für alle Branchen nunmehr einheitlich die Regelungen des Bundesdatenschutzgesetzes. Danach dürfen Telekommunikationsdaten im Ausland gemäß den allgemeinen Datenschutzvorschriften verarbeitet werden – eine Lösung, für die auch die Deutsche Telekom plädierte. Dies eröffnet der Telekommunikationswirtschaft die Möglichkeit, gleichberechtigt im internationalen Wirtschaftsverkehr zu handeln.

Speicherung und Sicherheit von Kundendaten.

Pro Jahr speichert und verarbeitet die Deutsche Telekom die Daten von fast 60 Millionen Privatkunden in Festnetz und Mobilfunk. Die Datenspeicherung erfolgt zur technischen Erbringung und Abrechnung der Dienstleistungen und ist in den Datenschutzhinweisen des Konzerns beschrieben. Die Speicherfristen hat jeweils der nationale Gesetzgeber festgelegt.

Der Konzern ist sich seiner Verantwortung im Umgang mit diesen hoch sensiblen Daten bewusst. Der Schutz dieser Daten steht für die Deutsche Telekom an oberster Stelle.

Speicherung von Funkzellen.

Die Deutsche Telekom speichert die Funkzelle, in der sich ein Mobiltelefon aktuell befindet. Dies geschieht aus technischen Gründen; ein Mobiltelefon ist so schneller und leichter erreichbar. Sobald ein Mobiltelefon die Funkzelle wechselt, wird der alte Standort überschrieben. Aus dieser Speicherpraxis ergibt sich, dass im Nachhinein kein Bewegungsprofil eines Mobiltelefons erstellt werden kann. Ebenso wenig ist es möglich, Standorte eines Handys in der Vergangenheit zu recherchieren, wenn kein Kommunikationsvorgang stattgefunden hat. Wenn hingegen mit einem Handy kommuniziert wurde, ist die Funkzelle zum Zeitpunkt des entsprechenden Vorgangs Bestandteil der Verkehrsdaten und wird 30 Tage lang gespeichert. Innerhalb dieses Zeitraums können diese Daten nachträglich beauskunftet werden.

Datenspeicherung.

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 Verbindung der Telekommunikationspartner. Danach werden sie zum Zweck der Abrechnung mit dem Kunden oder mit anderen Dienstleistern 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-Kartenummer 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

Verkehrsdaten – Die Speicherfristen auf einen Blick:

Verkehrsdaten, die zur Herstellung und Aufrechterhaltung einer Verbindung und für die Erstellung der Abrechnung notwendig sind, sichert die Deutsche Telekom 30 Tage. Das Unternehmen arbeitet an einer Verkürzung dieser Speicherdauer für Daten, die nicht für Abrechnungszwecke benötigt werden. Zur Aufrechterhaltung des technischen Betriebs und zur Störungsbeseitigung ist allerdings auch für diese Information eine Mindestspeicherdauer erforderlich. Abrechnungsdaten werden bis zu 80 Tage gespeichert, sofern ein Kunde keine sofortige Löschung nach Rechnungsversand wünscht. IP-Adressen, die als Verbindungsdaten beim Internetsurfen vorgehalten werden, löscht die Deutsche Telekom bereits nach sieben Tagen. Daten, die zur Abrechnung mit Service-Providern notwendig sind, speichert sie aus abrechnungstechnischen Gründen sechs Monate und ausschließlich in anonymisierter Form.

Konzernweite Einwilligungsklausel zur Nutzung von Kundendaten.

Die Deutsche Telekom informiert wie zahlreiche andere Unternehmen ihre Kunden über neue oder verbesserte Produkte und Dienste. Hierfür nutzt sie unter strengen Voraussetzungen vorliegende Kundendaten wie Name und Telefonnummer sowie die bislang genutzten Produkte: Eine Ansprache darf nur erfolgen, wenn der Kunde vorher explizit 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 bei Unterzeichnung des Auftragsformulars, telefonisch mit anschließendem Bestätigungsschreiben oder online. Zudem haben Kunden die Möglichkeit, die erteilte Einwilligung zu widerrufen, für den Fall, dass sie eine kundenindividuelle Ansprache nicht mehr erhalten möchten. Die Kunden der Deutschen Telekom können darüber hinaus ihren Einwilligungsstatus im Kundencenter-Portal unter www.telekom.de jederzeit einsehen und ändern.

Datenschutzlösung für anonymes Internetsurfen mit IPv6.

Die Deutsche Telekom stellte im November 2011 als erstes Telekommunikationsunternehmen eine Lösung für anonymes Surfen mit dem neuen Internetstandard IPv6 vor. Über ein dreistufiges Verfahren können die zwei unterschiedlichen Bestandteile der 2012 wirksam werdenden IP-Adressen zuverlässig für Dritte verschleiert werden. IP-Adressen werden bei der Nutzung des Internets vergeben und sind Voraussetzung fürs Surfen im Netz mit dem jeweiligen Endgerät (zum Beispiel PC, Laptop, Smartphone). Mit der entwickelten Datenschutzlösung kann der Nutzer selbst entscheiden, wie anonym er durchs Internet surfen und seine Identität verschleiern will. Damit leistet die Deutsche Telekom mehr als das aktuelle Recht fordert. Notwendig wird die Anonymisierung nach Auffassung der Deutschen Telekom, weil der in der Einführung befindliche Internetstandard IPv6 so viele IP-Adressen bereitstellen wird, dass jeder Nutzer mit all seinen denkbaren Endgeräte weltweit mit IP-Adressen versorgt werden kann. Technisch könnte jeder Nutzer und jedes seiner Endgerät seine Adresse dauerhaft behalten, so dass es über diese permanente Adresse eindeutig identifizierbar wäre. Damit wäre es theoretisch möglich, detaillierte Bewegungs- und Nutzerprofile zu erstellen, wovon die Lösung der Deutschen Telekom schützt.

Die neuen IPv6-Adressen bestehen aus zwei Teilen (Netzpräfix und Endgeräteanteil) mit jeweils 64 Bit Länge. Das Schutzmodell besteht aus drei Stufen: Die ersten beiden Stufen wirken auf den von der Deutschen Telekom vergebenen Netzpräfix. In der ersten Stufe erhalten somit alle Endgeräte, die an einen Internet-Zugangsrouten der Deutschen Telekom (Speedport) angeschlossen sind, regelmäßig zufällige neu gewählte Netzpräfixe zugewiesen. Diese Funktion wird werksseitig voreingestellt. Zweitens integriert die Deutsche Telekom in die Konfigurationseiten ihrer vertriebenen Router einen so genannten „Privacy Button“. Per Mausklick erhält der Nutzer ein vollständig neues IPv6-Präfix zugewiesen. Diese Neuvergabe kann manuell oder automatisch zu einem festgelegten Zeitpunkt erfolgen. Drittens wird bei den meisten modernen Endgeräten der Endgeräte-Anteil der IP-Adresse automatisch durch eine Zufallslogik verschleiert. Die Deutsche Telekom wird ihre Kunden über die Möglichkeiten zum anonymisierten Surfen informieren. Die Produkteinführung ist für 2012 geplant. Während der Umstellungszeit werden der bisherige Standard IPv4 sowie der neue IPv6 unterstützt.

Die Deutsche Telekom stellte die Lösung auf der Datenschutztagung Dafta im November 2011 einem Fachpublikum in Köln vor, ebenso im November auf einem IPv6-Symposium des Bundesbeauftragten für Datenschutz und Informationssicherheit, Peter Schaar. Sowohl die Reaktionen der Fachexperten als auch des Bundesdatenschutzbeauftragten waren positiv.

Sicherheit beim Telefonieren im GSM-Netz.

Der Kryptografie-Spezialist Karsten Nohl stellte auf einer Sicherheitskonferenz des Chaos Computer Clubs in Finowfurt in Brandenburg im August 2011 die technische Möglichkeit vor, unter bestimmten Rahmenbedingungen den geschützten Datenverkehr im weltweit standardisierten GSM-Netz entschlüsseln zu können. Seine Hacking-Versuche erreichten hohes Medieninteresse und bezogen sich auf Mobilfunknutzer, die Daten speziell über den GPRS-Standard im GSM-Netz senden. Die Deutsche Telekom verfolgt solche Versuchsanordnungen mit großem Interesse. Die Abhörsicherheit in den Netzen der Deutschen Telekom ist hoch. Es bedarf krimineller Energie, um die vorhandenen Sicherheitssysteme zu überwinden. Die Wahrscheinlichkeit des Abhörens oder auch Abrufens von Datenkommunikation ist für Kunden damit gering und stellt mehr eine theoretische technische Möglichkeit dar als ein Alltagsszenario.

Die Sicherheit des weltweiten Mobilfunkstandards GSM ist jedoch nicht nur das Anliegen einzelner Hersteller und Netzbetreiber – sie muss branchenweit gewährleistet werden. Die Deutsche Telekom engagiert sich deshalb zum Beispiel innerhalb der globalen Organisationen GSMA (Industrievereinigung der GSM-Mobilfunkanbieter) und 3GPP (Kooperation weltweiter Standardisierungsgremien im Mobilfunk) für die Weiterentwicklung von Sicherheitsstandards.

Das Unternehmen verbessert – dem technischen Fortschritt entsprechend – permanent seine Sicherheitssysteme und erhöht die Standards heutiger und künftiger Systeme. So arbeitet die Deutsche Telekom unter anderem an der flächendeckenden Einführung des Verschlüsselungsalgorithmus A5/3 in ihren GSM-Netzen, der noch höhere Sicherheitsstandards erfüllt. Es handelt sich dabei um einen Algorithmus, der aus den UMTS-Netzen abgeleitet ist. Gleichwohl ist eine netzseitige Zwangsaktivierung der neuen Verschlüsselungsalgorithmen nicht ohne weiteres möglich, da ansonsten ältere Mobiltelefone aufgrund von technischen Inkompatibilitäten nicht mehr verwendet werden könnten.

Für besonders sicherheitsempfindliche Bereiche bietet die Deutsche Telekom mit der Lösung Simko die Möglichkeit, Telefongespräche zwischen zwei Endgeräten hochwirksam zu verschlüsseln.

GSM.

GSM (Global System for Mobile Communications) ist ein Standard für voll-digitale Mobilfunknetze, die hauptsächlich für Telefonie, aber auch für Datenübertragung sowie Kurzmitteilungen (Short Messages, SMS) genutzt werden. Die Zielsetzung von GSM war es, Teilnehmern ein europaweites mobiles Telefonsystem anzubieten, das mit ISDN oder herkömmlichen analogen Telefonnetzen kompatible Sprachdienste anbot. In Deutschland wurde es 1992 eingeführt und ist heute der weltweit am meist verbreitete Mobilfunkstandard. Später folgten Erweiterungen des Standards zur schnelleren Datenübertragung wie etwa HSCSD, GPRS oder EDGE. Die Industrievereinigung GSMA vertritt weltweit rund 800 Mobilfunkanbieter und hat sich zur Aufgabe gesetzt, den GSM-Mobilfunk weiter zu entwickeln und gemeinsam netzwerkübergreifenden Standards zu erarbeiten.


Sicherheit und Datenschutz für Nutzer der Telekom Cloud.

Als ein führender Anbieter von Cloud-Lösungen, mit denen Privatanwender, Unternehmen und öffentliche Verwaltungen Rechenleistung und Speicherkapazitäten auf Knopfdruck über das Internet – der so genannten IT-Wolke – beziehen können, hat die Deutsche Telekom im Jahr 2011 die Telekom Cloud für Privatkunden in Deutschland vorgestellt. Sie ist Bestandteil des sogenannten „Cloud Store“, in dem die Deutsche Telekom neben Privatkunden Lösungen auch für kleinere Unternehmen und Großkunden anbietet.

Überall dort, wo das Internet und damit die online bereitgestellten Dienste der Deutschen Telekom zur Verfügung stehen, können Kunden ihre Dateien und Anwendungen nutzen. Und das über alle Endgeräte: Ob PC, Notebook, Tablet PC, Smartphone oder Fernseher – mit der Telekom Cloud sind Anwender nicht mehr an technische Plattformen gebunden. Privatkunden legen beispielsweise ihre Fotos, Musik, E-Mails oder Videos im virtuellen Mediencenter ab und greifen über das Internet verschlüsselt auf die Daten zu. Dabei stehen ihnen 25 Gigabyte Speicherplatz aus dem Netz zur Verfügung. Für die Verfügbarkeit der Dienste sorgt das Breitbandnetz der Deutschen Telekom.

Weil die Daten ausschließlich auf in Deutschland stehenden Servern gespeichert werden, unterliegen sie den strengen deutschen Datenschutzbestimmungen. Die Rechenzentren der Deutschen Telekom erfüllen modernste Schutzanforderungen, die ein hohes Maß an Sicherheit und Datenschutz garantieren. Alle im Mediencenter gespeicherten Daten sind vor Verlust geschützt, da die Inhalte nicht nur auf den Geräten des Nutzers, sondern auch auf den Servern der Deutschen Telekom gesichert sind. Im Jahr 2011 wurde das Mediencenter der Deutschen Telekom hinsichtlich Datenschutz und -sicherheit durch den TÜV Saarland geprüft und zertifiziert. Telekom Cloud Services, die kostenpflichtig sind, werden über die Telekom-Rechnung abgerechnet. Die Angabe von Kreditkartendaten ist also nicht nötig. Auch das trägt zu Datenschutz und Sicherheit bei.

Alle Services der Telekom Cloud durchlaufen bereits in der Entwicklung das konzernweit eingeführte PSA-Verfahren (Privacy and Security Assessment, siehe Seite 41). Es garantiert, dass die Anforderungen an technische Sicherheit und Datenschutz bereits fester Bestandteil der Produkt- und Systementwicklung sind. Dazu gehörte im Vorfeld die Umsetzung produktspezifischer

Sicherheitsanforderungen wie etwa der verschlüsselte Datenaustausch mit der Cloud genauso wie Sicherheitsüberprüfungen in Form von Penetrationstests  sowie die Überprüfung der Erfüllung gesetzlicher und unternehmenspolitischer Anforderungen. Cloud-Services bieten zahlreiche Möglichkeiten, die Telekom Cloud auch mit einzelnen Produkten von Partnerunternehmen zu kombinieren. Die Deutsche Telekom hat dazu im Jahr 2011 ihre Richtlinien weiter ausgebaut, um auch bei Kooperationspartnern und Dienstleistern ein einheitliches Datenschutz- und Sicherheitsniveau zu gewährleisten.

Datenschutzfreundliche „Zwei-Klick-Lösung“ für Like-Buttons.

Das Empfehlen von Web-Seiten über soziale Netzwerke verzeichnet eine steigende Beliebtheit. Nutzer von sozialen Netzwerken wie etwa Facebook können zum Beispiel durch einen Klick auf das „Gefällt-mir“-Symbol ihre vernetzten Freunde auf eine interessante Seite aufmerksam machen. Generell übermitteln diese Buttons Daten von Besuchern, auch wenn sie nicht beim sozialen Netzwerk angemeldet waren. Die Deutsche Telekom hat eine datenschutzfreundliche Lösung entwickelt, die nicht unfreiwillig personenbezogene Daten von Lesern ihrer Web-Seiten an die jeweilige Netzwerkplattform sendet. Der Telekommunikationskonzern bietet den Nutzern einen modifizierten „Gefällt-mir“-Button auf den unternehmenseigenen Web-Seiten an. Die Telekom-Lösung basiert auf der so genannten Zwei-Klick-Lösung, die bereits in der Fachwelt und von vielen Datenschützern anerkannt ist. Diese zweistufige Lösung übermittelt Daten nur mit Zustimmung der Nutzer: Automatisch überträgt dieser Button keine Daten an Dritte. Erst wenn der Nutzer die so genannte „Gefällt mir“-Empfehlungsschaltfläche aktiviert, gibt er seine Zustimmung zur technischen Kommunikation mit dem jeweiligen Server des sozialen Netzwerks. Der Button ist dann aktiv und baut eine Verbindung auf. Mit dem zweiten Klick wird die Empfehlung übermittelt.

Prüfung der Datenlöschung bei der Endgeräte-Reparatur.

In Deutschland erhalten Kunden im Reparaturfall eines Endgeräts (zum Beispiel Smartphone) unmittelbar ein funktionsfähiges Gerät aus dem Austauschpool der Deutschen Telekom. Das defekte Modell übersendet die Deutsche Telekom für die Instandsetzung zum Hersteller oder zu einem ihrer Reparaturdienstleister. Der Kunde ist in diesem Prozess verpflichtet, persönliche Daten von seinem Mobiltelefon zu löschen, bevor er es in einem T-Shop abgibt oder postalisch verschickt. Ebenso sind auch die Hersteller und Reparaturdienstleister vertraglich zum Löschen von Daten

verpflichtet, die sich möglicherweise noch auf dem Gerät befinden. Die Deutsche Telekom hat den gesamten Löschprozess wie im Berichtsjahr 2010 angekündigt untersucht. Die Überprüfung ergab, dass die datenschutzkonforme Löschung aller Kundendaten Teil des Standardprozesses für Reparaturen ist, dem sämtliche Hersteller und Reparaturdienstleister vertraglich unterliegen: Jedes Endgerät durchläuft dazu nach der Reparatur eine Ausgangskontrolle sowie einer abschließenden Zusatzüberprüfung, ob Kundendaten noch auf dem Gerät vorhanden sind. Im Rahmen der Überprüfung entstanden ebenso überarbeitete Musterverträge für Hersteller und Reparaturdienstleister, um die Abbildung und Einhaltung der Datenschutzanforderungen konzernweit zu standardisieren. Sollten Kunden vergessen, ihre Daten auf dem Endgerät vor Abgabe zur Reparatur zu löschen, gewährleistet das mehrstufige Lösch- und Kontrollkonzept der Deutschen Telekom die erfolgreiche Einhaltung datenschutzrechtlicher Anforderungen: Unter den 500.000 Austauschfällen im Jahr 2011 gab es nur zehn dokumentierte Kundenmeldungen zu einem fehlerhaften Löschvorgang.

Installation der Software Carrier IQ durch Smartphone-Hersteller.

In Deutschland berichteten Wirtschafts- und Tagesmedien Ende 2011 verstärkt über die Software „Carrier IQ“, die auf Smartphones verschiedener Hersteller produktionsseitig installiert ist. Dabei handelt es sich um eine Software zur Qualitätssicherung von Herstellern und Netzbetreibern. Diese kann bei definierten Ereignissen verschiedene Gerätedaten protokollieren. Die Anwendung lässt sich auf die Bedürfnisse verschiedener Hersteller und Netzbetreiber anpassen, was Datenschutzexperten kritisieren. Die Deutsche Telekom nutzt die Software Carrier IQ nicht und erfasst darüber auch keine Daten.

Überprüfung des Sicherheitskonzepts der Telekom Deutschland GmbH.

Bei technologischen und/oder organisatorischen Änderungen unterliegt die Deutsche Telekom der Verpflichtung, das generell geforderte Sicherheitskonzept nach § 109 Telekommunikationsgesetz den entsprechenden Änderungen 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



Beim Klicken des „Gefällt mir“-Buttons sozialer Netzwerke werden Daten von Besuchern übermittelt. Bei der so genannten „Zwei-Klick-Lösung“ werden Daten nur mit Zustimmung des Nutzers gesendet.

daher ein modifiziertes Sicherheitskonzept für die Telekom Deutschland GmbH aus den bereits bestehenden Einzelkonzepten entwickelt. Die Deutsche Telekom hat das Sicherheitskonzept im Oktober 2010 der Bundesnetzagentur als ihrer Aufsichtsbehörde im deutschen Markt vorgelegt. Im März 2011 bescheinigte die Behörde die Funktionsfähigkeit des Sicherheitskonzepts. Im dritten und vierten Quartal des gleichen Jahres überprüfte die Aufsichtsbehörde auch die Umsetzung an ausgewählten Standorten. Dabei wurde nur eine Empfehlung zur Anbringung eines Sichtschutzes an einem Gebäude ausgesprochen und umgehend von der Deutschen Telekom umgesetzt.

Deaktivierung von Massenspeichergeräten und externer Kommunikationsmöglichkeit.


In den Call Centern, die im Auftrag der Deutschen Telekom Kundenservice betreiben, sind die Mitarbeiter am Arbeitsplatz mit Computern ausgestattet, die über USB-Anschlüsse verfügen. Diese Anschlüsse sind in den Call Centern standardmäßig gesperrt, um das Speichern von Daten auf einem externen USB-Speichermedium und so eine unbefugte Weitergabe von Kundendaten zu verhindern. Bei einer Prüfung stellte die Deutsche Telekom fest, dass bei unter einem Prozent der Geräte im Kundenservice die

USB-Speichersperre nicht inaktiv war. Das Unternehmen beseitigte die Schwachstelle unmittelbar. Darüber hinaus hat die Deutsche Telekom bei den beauftragten Call Centern zur weiteren Erhöhung der Sicherheit den Mailversand nach Extern und das Aufrufen von nicht zur Aufgabenerfüllung notwendigen Internetseiten technisch unterbunden (siehe auch Seite 44).

Regulierung von Datenzugriffen durch Telekom Shop Partner.

In Deutschland übernehmen für die Deutsche Telekom den Vertrieb unter anderem ihr Tochterunternehmen Telekom Shop Gesellschaft mbH und deren Partner. Dieses Vertriebsgeschäft erfolgt auf Basis strenger Datenschutzvereinbarungen (Vereinbarung zur Auftragsdatenverarbeitung gemäß §11 Bundesdatenschutzgesetz) ausschließlich in Ladenlokalen. Die Telekom Shop Partner haben Zugriff auf eine zentrale Kundendatenbank, um Kunden der Deutschen Telekom zu Vertrags- und Produktfragen betreuen zu können. Der Zugriff auf die Kundendaten ist klar geregelt und nur für die Betreuung von Kunden im Ladengeschäft zugelassen. Die Kundendatenbank hat im Jahr 2011 bei einigen wenigen Vertriebspartnern von der Normalnutzung abweichende Zugriffsraten indiziert, die interne Prüfverfahren in Gang setzten. Das Ermittlungsergebnis ergab, dass die Datenbank nicht nur zur vereinbarten Kundenbetreuung, sondern auch zu einer vertraglich nicht vorgesehen Provisionskontrolle genutzt wurde. Eine Abmahnung der Vorfälle war nur in den Fällen möglich, in denen die Ermittlungsergebnisse rechtzeitig vorlagen. Zum Missbrauch der unberechtigt aufgerufenen Kundendaten ist es nach bisherigen Erkenntnissen nicht gekommen. Die Deutsche Telekom hat den internen Ermittlungsprozess verkürzt, um künftig unerlaubte Datenbankzugriffe noch schneller mit einer Abmahnung ahnden zu können. Alle Vertriebspartner sind in einem Schreiben sensibilisiert und an die datenschutzrechtlichen Bestimmungen erinnert worden.

Führen von Leistungsnachweisen im Telefonvertrieb.

Die Deutsche Telekom hat nach einem Hinweis eines regionalen Betriebsrates das Führen von individuellen Leistungsnachweisen im Telefonvertrieb einer datenschutzrechtlichen Überprüfung unterzogen. In einzelnen Call Centern  erfasst und verarbeiteten Teamleiter personenbezogene Daten, um die Erreichung von Umsatzzielen und Verkaufszahlen einzelner Teammitglieder zu dokumentieren. Diese Angaben speicherten sie außerhalb geschützter EDV-Anwendungen in einer Excel-Datei am Computer ihres Arbeitsplatzes. Ebenso dokumentierten Mitarbeiter den Fort-

schritt einzelner Vertriebsgespräche gegenüber ihrem Teamleiter in einer Excel-Datei, um ihren Beitrag zum Umsatzziel der Abteilung nachzuweisen. Die Deutsche Telekom hat sich mit den Fachabteilungen und Mitbestimmungsgremien verständigt, die betrieblich erforderlichen Kennzahlen mittels eines EDV-Programms „KPI-Viewer“ berechtigten Nutzergruppen bereitzustellen. Diese erhalten damit einen rollenbasierten Zugriff auf die Kennzahlen, so dass sie die nur für ihre Aufgaben relevanten Daten einsehen können. Eine Einsicht in personenbezogene Leistungskennzahlen ist nicht möglich. Diese Regelungen zum Führen von Leistungsnachweisen in Call Centern hat die Deutsche Telekom in eine Gesamtbetriebsvereinbarung eingebracht, um unternehmensweit eine datenschutz- und rechtskonforme Handhabung sicherzustellen. In der Übergangsphase gelten festgelegte Sicherheitsmaßnahmen und Verfahren, die sicherstellen, wer und wie die Kennzahlen elektronisch erfasst und eingesehen werden. Alle betroffenen Bereiche sind inzwischen aufgefordert, noch vorhandene papiergeführte Listen unverzüglich zu vernichten bzw. elektronisch vorliegende Versionen unwiederbringlich zu löschen. Die Einführung des Programms „KPI-Viewer“ soll 2012 abgeschlossen sein.

Unerlaubter Server-Zugriff bei ImmobilienScout24.

Beim Portalbetreiber ImmobilienScout24 haben sich Unbekannte unbefugt einen externen Zugriff auf einen der Unternehmensserver verschafft. Davon betroffen waren Adress- und Kontaktdaten, Kundennummern und Namen sowohl von gewerblichen als auch privaten Anbietern. Es handelte sich dabei um Daten, die in der Regel auf der Web-Seite von ImmobilienScout24 standardmäßig angezeigt werden und für die Kontaktinformationen der Anbieter im Zuge des Inserierens von Immobilien nötig sind. Darüber hinaus waren auch Daten aus Kontaktformularen betroffen. Hierbei handelte es sich beispielsweise um Kataloganforderungen oder Infoanfragen. Es wurden keine Bank- oder Finanzdaten entwendet. ImmobilienScout24, ein Tochterunternehmen der Deutschen Telekom, hat den unberechtigten Zugangsweg umgehend gesperrt und die Sicherheit der angegriffenen Server wiederhergestellt. Anbieter und Nutzer wurden informiert. Das Unternehmen hat Strafanzeige gegen Unbekannt bei der Staatsanwaltschaft Berlin gestellt.

Technische Störung im Kundenportal von T-Online.

Im September 2011 hat die Deutsche Telekom Unregelmäßigkeiten an Schnittstellen von IT-Systemen festgestellt, die den Betrieb des Kundenportals von T-Online im Internet sicherstellen. Ein



Die Wolke hat längst Einzug gehalten in eine zeitgemäße IT-Infrastruktur. Für Privat- und Geschäftskunden bietet Cloud Computing zahlreiche Vorteile.

Kunde hatte reklamiert, dass er im passwortgeschützten Bereich des Portals beim Einsehen seiner Bestellung Daten anderer Kunden angezeigt bekam. Vorsorglich wurden daraufhin die entsprechenden Funktionen des Kundencenters vorübergehend deaktiviert. Als Ursache der Fehlfunktion konnte ein Datenfehler in einem Software-Release analysiert werden, der theoretisch bei 300 Kundendatensätzen zu einer fehlerhaften Datenanzeige hätte führen können. Die Störung wurde in enger Zusammenarbeit mit dem Konzerndatenschutz innerhalb weniger Stunden beseitigt. Während der Wartungsarbeiten stand Kunden die telefonische Kundenbetreuung zur Verfügung. Nach bisheriger Kenntnis kam es vor Sperrung des Kundenportals bei zehn Kunden zu fehlerhafter Darstellung der Kundendaten, ein Missbrauch von Rechnungsdaten ist nicht bekannt. Die betroffenen Kunden erhielten von der Deutschen Telekom über den Vorgang eine schriftliche Benachrichtigung.

Fehlerhafte Dokumentenzustellung an eine Kanzlei.

Von 14. April 2011 bis 10. Mai 2011 wurden in Folge eines Arbeitsfehlers sechs E-Mails mit Unterlagen von drei Kunden, die Zahlungsansprüche gegen die Telekom Deutschland GmbH gerichtlich geltend machen, an eine falsche E-Mail-Adresse ge-

schickt. Im Anhang der E-Mails befanden sich Kopien der strittigen Rechnungen, Mobilfunkverträge und Kontoauszüge. Die Rechnungen enthielten Anschrift, Kundennummer und Bankdaten. Nach Bekanntwerden des Fehlers hat das Unternehmen den irrtümlichen Empfänger unverzüglich gebeten, die nicht für ihn bestimmten E-Mails zu löschen. Die Deutsche Telekom informierte die betroffenen Kunden über den Vorfall und kontaktiert sie bezüglich der möglichen Vergabe einer neuen Kundennummer.

3.2. Geschäftskunden.

Zertifizierung als Diensteanbieter für De-Mail.


Die Deutsche Telekom hat im zweiten Quartal 2012 den Service De-Mail  eingeführt, nachdem sie ihre Zertifizierung als De-Mail-Anbieter vom Bundesamt für Sicherheit in der Informationstechnik erhalten hat. De-Mail ist ein Dienst für den einfachen, sicheren und nachweisbaren Austausch von elektronischen Nachrichten. Für die erforderliche Zertifizierung überprüfte ein externer Auditor die Unternehmensbereiche der Deutschen Telekom, die etwa für die Einhaltung des Datenschutzes sowie für das Registrieren und die Identifikationsüberprüfung von Personen, die De-Mail nutzen wollen, verantwortlich sind. Für die technische Sicherheit von De-Mail überprüfte das Bundesamt die IT-Systeme der Deutschen Telekom und verlieh die Akkreditierung. In Ergänzung zur externen Zertifizierung hat die Deutsche Telekom das Produkt De-Mail intern ebenso erfolgreich überprüft. Ziel war es, die Peripherie-Systeme, die mit dem amtlichen De-Mail-System kommunizieren, einer strengen Kontrolle unter Beachtung der konzerneigenen Datenschutzbestimmungen zu unterziehen.

Die De-Mail verbindet die Vorteile der E-Mail mit der Zuverlässigkeit eines Briefs. Im Vergleich 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:///>).

- 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 einer Quersumme aus einer langen Zahl durch Addieren der einzelnen Ziffern. 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.

Cloud Computing.

Cloud Computing  ist heute innerhalb einer zeitgemäßen IT-Infrastruktur nicht mehr wegzudenken und bietet Nutzern zahlreiche Vorteile. Für Geschäftskunden stehen enorme Kosteneinsparungen an erster Stelle. Darüber hinaus können Unternehmen Kosten flexibilisieren und ihre IT entsprechend Bedarf bei schwankender Auslastung besser skalieren. Für die Anbieter von Cloud-Produkten bringen diese Angebote Herausforderungen mit sich, insbesondere bei der technischen Bereitstellung und der Gewährleistung der Sicherheit. Die Deutsche Telekom hat 2011 einen so genannten „Cloud Store“ eingerichtet, in dem sie ihre Angebote für Privatkunden, kleinere Unternehmen und Großkunden bündelt. Sämtliche Cloud-Angebote unterliegen dabei hohen Sicherheitsanforderungen.

Bei der Deutschen Telekom werden Sicherheit und Datenschutz durch eine konzernweite übergreifende Zusammenarbeit verschiedener Bereiche gewährleistet. Bereits bei der Entwicklung der Dynamic Computing Services floss konzernweites Fachwissen ein. So entwickelte der Bereich IT-Sicherheit die technischen Sicherheitsanforderungen. Der Bereich Datenschutz stellte im Rahmen des Privacy and Security Assessment (PSA-Verfahren, siehe Seite 41) sicher, dass der Schutz der verarbeiteten und gespeicherten Daten Priorität hat.

Beim Cloud Computing lagern alle Daten und Anwendungen in Rechenzentren. Wie sicher diese sind, hängt von den jeweiligen Cloud-Anbietern ab. Die Telekom Rechenzentren sind sicherheits-

zertifiziert. T-Systems – als Betreiber der Rechenzentren – bietet bereits seit 2005 Cloud-Dienste für Großkunden an. Die Telekom-Tochter hält weltweit 90 hochsichere Rechenzentren. Besonders die Standorte in Deutschland unterliegen strengen rechtlichen Datenschutzbestimmungen sowie EU-Regularien. Dank hoher Sicherheitsstandards für die Rechenzentren wehrt T-Systems zudem Hacker-Angriffe sowie Viren und Trojaner ab. Ständige Pflege und automatische Updates halten die Sicherheitsvorkehrungen auf dem aktuellsten Stand.

Auf Kundenwunsch kann der Dienstleister die Daten beim Transport durchs Netz zusätzlich verschlüsseln. Wichtig auch: die Verfügbarkeit der Cloud-Services. Würde ein Rechenzentrum aufgrund einer lokalen Katastrophe oder eines gezielten Angriffs ausfallen, kann ein „Zwilling“ den Betrieb übernehmen. Bei diesem „TwinCore“ genannten Angebot für Geschäftskunden ist jedes Rechenzentrum komplett gespiegelt. Aber auch in jedem einzelnen Rechenzentrum erhöht die Deutsche Telekom die Ausfallsicherheit durch Redundanz, um sich gegen den Ausfall einzelner Systeme innerhalb des Rechenzentrums zu schützen.

Die Deutsche Telekom hat sich als Anbieter von Cloud basierten Geschäftsmodellen intensiv an der politischen Diskussion um Sicherheit und Datenschutz in der Wolke beteiligt. Sowohl auf europäischer als auch auf nationaler Ebene waren unterschiedliche Vertreter des Unternehmens in Arbeitsgruppen, etwa bei der Europäischen Kommission oder auch im Rahmen des IT-Gipfelprozesses aktiv. Die Deutsche Telekom hat bei ihren Aktivitäten im verbandlichen und politischen Raum immer folgende Ziele definiert:

- Steigerung der Transparenz gegenüber Nutzern/Anwender zu datenschutzrechtlichen und sicherheitsrelevanten Regularien
- Hoher Investitionsbedarf in Sicherheit
- Schaffung von Orientierungspunkten, wie etwa Datenschutz- und Sicherheits-Zertifizierungen oder Gütesiegel für Cloud basierte Lösungen

Smart Metering/Smart Grids

Immer mehr Stromkunden werden zu Stromproduzenten. Inzwischen entspricht die installierte Leistung dezentraler Photovoltaikanlagen der von 25 Kernkraftwerken – mit einem



Smart Metering zeigt, was sich im Stromnetz gerade tut – Basis für ein intelligentes Stromnetz.



Unterschied: Sonne und Wolken steuern diese 25 Kernkraftwerke und bringen das Stromnetz aus dem Takt. Denn die Leistung schwankt erheblich. Digitale Zähler machen deutlich, was sich im Stromnetz gerade tut. Dies ist die Basis für ein intelligentes Stromnetz, das sich selbst steuert. Die übertragenen Verbrauchsdaten sind aber sensibel. Erstens lassen sie Rückschlüsse auf den Kunden zu, zweitens besteht die Gefahr von Manipulationen des gesamten Stromnetzes. Daher ist hier die Gewährleistung eines hohen Datenschutz- und Datensicherheitsniveaus von besonderer Bedeutung.

Die Deutsche Telekom hatte bereits in ihrer „Modellstadt“ T-City Friedrichshafen von 2007 bis 2012 den Einsatz von Smart Metering getestet und daraufhin die Sicherheit des Systems weiter verbessert. So hat die Telekom etwa entschieden, abrechnungsrelevante Daten von Steuersignalen für das vernetzte Haus zu trennen. Dafür gibt es zwei Infrastrukturen: Eine besonders sichere Kommunikationsbox, die alle Verbrauchsdaten aus dem Haus überträgt sowie eine Home-Management-Box, die Informationen ins Haus bringt.

Ebenso legt die Deutsche Telekom Wert auf gesicherte Rechnungslegung: Das Unternehmen überträgt hierfür Monatswerte

an die Energieversorger. Die Auslesefrequenz entspricht hierbei exakt dem Vertrag zwischen Energieversorger und Endverbraucher. Vereinbart der Endverbraucher etwa eine 15-minütige Auslesung, so wird genau diese Auslesefrequenz umgesetzt. Manipulationen beugt die Telekom dreifach vor. Die Werte werden verschlüsselt gespeichert und über einen gesicherten Transportkanal übermittelt. Außerdem sind weder Zähler noch andere Komponenten aus dem Internet erreichbar. Die Deutsche Telekom bietet also eine Infrastruktur für sicheren Datentransfer an.

Der Gesetzgeber hat ebenfalls reagiert und beim Bundesamt für Sicherheit in der Informationstechnik die Ausarbeitung eines generellen Schutzprofils sowie einer technischen Richtlinie für Smart Metering in Auftrag gegeben. Eine finale Version dieser Richtlinie wird für Juli 2012 erwartet. Sie soll das intelligente Messen, Auslesen und Übertragen des Stromverbrauchs im Haushalt regeln. Diese Richtlinie fokussiert sich derzeit aber nur auf die Steuereinheit im Haus des Kunden.

Die Deutsche Telekom sieht an dieser Stelle Handlungsbedarf: Smart Metering bedarf einer Ende-zu-Ende-Betrachtung der gesamten Systeme, Prozesse, Nutzungsszenarien und Marktrollen vor dem Hintergrund intelligenter Stromnetze. Mit ihrer jahrelangen Erfahrung als Netzbetreiber hat sie sich als Dialogpartner zur Umsetzung einer solchen Betrachtung angeboten und konkrete Vorschläge zur Sicherstellung eines hohen Sicherheitsniveaus für Smart Metering  und Smart Grids  gemacht.

Datenschutz-Leitfaden im Geschäftsfeld Gesundheit

Das Gesundheitswesen unterliegt zahlreichen datenschutzrechtlichen Bestimmungen. Einerseits, um personenbezogene Sozial-, Patienten- sowie Behandlungsdaten zu schützen, andererseits, um die rechtskonforme Anwendung von Medikamenten, Heil- und Behandlungsmethoden zu gewährleisten. Die Deutsche Telekom übernimmt mit ihren Produkten und Lösungen für das Gesundheitswesen eine Vorreiterrolle. Mit diesem Anspruch geht auch die Verantwortung einher, Gesundheitseinrichtungen wie Krankenhäuser und Kliniken jederzeit datenschutzkonforme Lösungen anbieten zu können und sie zu beraten, wie sie die Daten ihrer Patienten schützen. Daher wurde 2011 für das Segment Krankenhäuser ein Leitfaden zum Umgang mit sensiblen Gesundheits- und Sozialdaten

entwickelt. Es ist geplant, dass der Leitfaden um exemplarische Best Practice Ansätze ergänzt werden soll.

Zielgruppen des Leitfadens sind Kunden, Vertrieb und Vertriebsprojektmanager. Der Leitfaden dient der Sensibilisierung, Orientierung und Information hinsichtlich der datenschutzrechtlichen Anforderungen im Bereich E-Health und unterstreicht die Datenschutz-Leistungsfähigkeit/-Kompetenz des Konzerns im Lösungsgeschäft. Das Dokument behandelt unter anderem datenschutzrechtliche Rahmenbedingungen, in seiner Weiterentwicklung spezifische Lösungsansätze sowie Vorgehensweisen etwa für die Umsetzung von Outsourcing-Projekten oder die Auftragsdatenverarbeitung. Insbesondere die Beauftragung externer Dienstleister stellt Krankenhäuser vor komplexe Datenschutzerfordernungen. Der Leitfaden kann als Vorlage für weitere Geschäftsfelder dienen.

Smart Metering.

Smart Metering ist ein wesentlicher Bestandteil von intelligenten Stromnetzen und liefert den Versorgern Informationen, wann, wo und wie viel Strom dezentral in die Netze fließt und wie viel Strom die Endverbraucher abnehmen. Der Gesetzgeber schreibt seit 2010 die Installation von Smart Metern in Neubauten und bei Sanierungen vor.

Die Deutsche Telekom bietet mit Metering Services eine modular aufgebaute Datenkommunikationslösung an. Diese richtet sich an Wohnungswirtschaft, Messstellenbetreiber, Energieversorger, Vertriebsgesellschaften und Verteilnetzbetreiber. Geschäftskunden können an diese Kommunikationslösung ihre Smart Meter anbinden und verfügen so über die Infrastruktur zum Lesen und Transport der Daten. Auch Endverbraucher profitieren von den intelligenten Stromzählern: Die Kunden können genau nachvollziehen, wie viel Strom sie verbrauchen – nach Wunsch aufgeschlüsselt nach Stunden, Tagen, Wochen, Monaten oder Jahren. Damit können Vergleiche mit Vergangenheitswerten vorgenommen oder künftig interaktive Angebote genutzt werden, wie etwa Verbrauchsprognosen, Tarifoptimierung oder Benachrichtigungsdienste, die sich beim Überschreiten definierter Werte melden. Smart Metering findet Verwendung bei Strom, aber auch bei Gas, Wasser oder Wärme.

3.3. Beschäftigte.

Der Beschäftigtendatenschutz regelt den Umgang mit Daten von Arbeitnehmern und Beamten, unabhängig davon, ob dieser automatisiert oder nicht automatisiert erfolgt. Die Regelung zum Beschäftigtendatenschutz gibt den Rahmen vor, in dem Mitarbeiterdaten rechtlich zulässig verarbeitet werden dürfen: Dieser umfasst die Voraussetzungen für die Verarbeitung dieser Daten durch den Arbeitgeber sowie den Schutz der Mitarbeiterdaten vor unberechtigter externer und interner Nutzung. Neben den Rahmenbedingungen für berechnete betriebliche Verwendungen im Zuge der Begründung oder Durchführung eines Beschäftigungsverhältnisses regelt der Arbeitnehmerdatenschutz auch die Verwendung der Mitarbeiterdaten zur Ermittlung von Straftaten. Insbesondere die elektronisch vernetzte Arbeitswelt führt zu komplexen Anforderungen von individuellen Schutzinteressen seitens Gesetzgeber, Mitarbeitern, Kunden und dem Unternehmen als Arbeitgeber.

Die Bundesregierung beschloss im Jahr 2010 einen Gesetzentwurf zum Schutz von Arbeitnehmerdaten. Im Berichtszeitraum erfolgte im Februar 2011 die erste Lesung des so genannten Beschäftigtendatenschutzgesetzes im Parlament. Eine weitere Beratung und die Verabschiedung des Gesetzentwurfs werden für das Jahr 2012 erwartet. Die Deutsche Telekom befürwortet die Gesetzesinitiative, weil sie mehr Rechtssicherheit herstellt.

Ermittlungen gegenüber Beschäftigten.

Die Deutsche Telekom hat sich strenge Ermittlungsgrundsätze zur Auswertung von Mitarbeiterdaten auferlegt, die über die gesetzlichen Vorgaben hinaus gehen. Nur unter äußerst eingeschränkten Bedingungen dürfen personenbezogene Daten zum Zwecke der Leistungs- und Qualitätskontrolle sowie zur Aufdeckung und Verfolgung von Fehlverhalten von Mitarbeitern ausgewertet werden. Noch vor jeder Untersuchung von Mitarbeiterdaten prüft die Deutsche Telekom jeweils das Vorliegen eines strafrechtlich relevanten Anfangsverdachts. Die Ermittlungsgrundsätze sind rechtlich allgemein anerkannt, unterliegen aktuellen Rechtsprechungen und geben Mitarbeitern sowie Führungskräften die notwendige Handlungssicherheit.

Im Vergleich zur geltenden Rechtslage werden die Persönlichkeitsrechte der Beschäftigten deutlich aufgewertet. Gleichzeitig behält der Arbeitgeber die notwendigen Befugnisse, um auch weiterhin dienstliches Fehlverhalten, Korruption und Datendiebstahl bekämpfen zu können. Trotz allem bietet eine Normierung bis ins kleinste Detail durch den Gesetzgeber Potenzial zur Überregulierung. Sie ist daher mit der gebotenen Weitsicht anzugehen. Grundsätzlich bietet bereits die aktuelle Gesetzeslage ausreichend Handlungsspielraum für die Schaffung einer datenschutzfreundlichen Unternehmenskultur und einer partnerschaftlichen Zusammenarbeit im Betrieb.

Vereinbarungen, Standardisierung und Organisationsabläufe.

Im Jahr 2011 hat die Deutsche Telekom verschiedene Maßnahmen umgesetzt, um den Interessenausgleich von Arbeitgeber und Arbeitnehmer im Beschäftigtendatenschutz sicherzustellen. Neben dem Schutz von personenbezogenen Daten stand ebenso die Verhinderung von Missbrauch von Beschäftigtendaten im Mittelpunkt.

- Künftig vereinheitlicht die Deutsche Telekom die technische Büroausstattung von rund 130.000 Beschäftigten in Deutschland. Ziel ist es, die Arbeitsplätze mit einheitlicher Hard- und Software an 1.750 Standorten zu modernisieren und die Produktivität zu steigern. Die Grundlage bildet eine standardisierte IT-Infrastruktur mit einheitlicher Basisausstattung für alle Mitarbeiter. Im Jahr 2011 erreichte die Deutsche Telekom einen Meilenstein in dem Projekt: Die Benutzerdaten sämtlicher Mitarbeiter sind aus unterschiedlichen Systemen datenschutzkonform zusammengeführt worden. Ein Benutzer- und Berechtigungsmanagement stellt sicher, dass die Zugriffsrechte nach dem „Need-to-know“-Prinzip zentral verwaltet werden. Durch diese rollenbasierte Rechteverwaltung wird sichergestellt, dass Mitarbeiter nur auf die Daten zugreifen dürfen, die sie für ihren Aufgabenbereich benötigen. Auch für den Mitarbeiter sind Verbesserungen erreicht worden. Diese umfassen unter anderem:
 - Transparenz bei Benutzeridentität und Zugriffsrechten: Ein Intranet-Portal zeigt dem Mitarbeiter in einem geschützten Bereich an, welche Informationen zu seiner Benutzerkennung hinterlegt sind. Das sind etwa Zugriffsberechtigungen auf IT-Anwendungen, Zugehörigkeiten zum Organisationsbereich, Büroanschrift oder die Telefonnummer.

- Schutz beim Druck vertraulicher Dokumente: Von jedem Arbeitsplatz aus ist das Drucken und Scannen an zentralen Druckterminals möglich. Mit Einführung einer neuen Technik erfolgt ein Ausdruck erst, wenn der Mitarbeiter diesen am Drucker selbst mit einer Chipkarte freischaltet. Somit verbleiben keine vertraulichen Ausdrücke wie Kunden- oder Personaldaten unbeobachtet im Druckterminal, und die Mitarbeiter können selbst bestimmen, wann sie ihre Dokumente abholen.
- Datenschutz beim Arbeiten im Telekom Social Network: Mitarbeitern der Deutschen Telekom steht ein internes soziales Netzwerk zur Verfügung. Diese Social-Media-Plattform stellt den Nutzern verschiedene Funktionen zur virtuellen Zusammenarbeit wie etwa Diskussionsforen, Dokumentablagen, Nachrichtenversand oder die Bildung virtueller Arbeitsgruppen bereit. Für diese Funktionalitäten werden persönliche Daten erhoben und verarbeitet, die sich in Pflichtangaben und freiwillige Angaben aufteilen. Die Deutsche Telekom hat festgelegt, dass die Pflichtangaben auf ein Minimum beschränkt sind und jeder Mitarbeiter selbst entscheidet, welche Daten er darüber hinaus angibt und über das soziale Netzwerk austauschen will. Bei der Erstbenutzung des Telekom Social Network erhält jeder Mitarbeiter nur Basis-Nutzerrechte. Er kann seinen Zugang löschen und damit den Personenbezug seiner Inhalte aufheben. Ihm stehen Datenschutzhinweise zur Verfügung, um Transparenz im Umgang mit Inhalten und Daten auf der Social-Media-Plattform zu gewährleisten. Der Konzerndatenschutz erstellte einen Mustervertrag für alle deutschen und ausländischen Tochtergesellschaften, um für deren Mitarbeiter den rechts- und datenschutzkonformen Umgang mit dem Telekom Social Network einheitlich zu gewährleisten.
- Datenschutz bei der Revision: Die Deutsche Telekom hat die Aufgabenbereiche der Revision konzernübergreifend organisiert. Dazu wurden diese Unternehmensfunktionen aus einzelnen Konzerngesellschaften zentral zusammengelegt. Im Rahmen dieser so genannten Funktionsübertragung erarbeitete die Deutsche Telekom einen Mustervertrag, um die datenschutzkonforme Verwendung von Mitarbeiterdaten im Rahmen der Revisionstätigkeiten sicherzustellen.
- Datenschutz im Betrieblichen Eingliederungsmanagement: Die Deutsche Telekom hat den datenschutzkonformen Informationsaustausch zwischen den Beteiligten im Betrieblichen

Eingliederungsmanagement ausgebaut. Aufgrund des Informationsinteresses der Arbeitnehmervertretung war es notwendig zu regeln, in welchem Umfang selbige Daten über die Mitarbeiter erhält, die Anspruch auf eine Wiedereingliederung nach gesundheitlich bedingter Abwesenheit haben: Ist ein Mitarbeiter etwa mehr als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig, muss der Arbeitgeber prüfen, ob der Mitarbeiter eine solche Maßnahme nutzen kann. Er ist über eine entsprechende Arbeitsplatzgestaltung zu informieren, gleichzeitig hat die Arbeitnehmervertretung einen Informationsanspruch. Die Deutsche Telekom hat mit der Regelung ihre Datenschutzverpflichtungen gegenüber den Mitarbeitern mit den Informationsbedürfnissen der Arbeitnehmervertretung in Einklang gebracht.

Informationsbesuche der Datenschutzaufsicht zur elektronischen Personalakte.


Während der Bundesbeauftragte für den Datenschutz für die datenschutzrechtlichen Fragestellungen der Beamten der Deutschen Telekom zuständig ist, obliegt dies für die Angestellten unter anderem dem Landesdatenschutzbeauftragten Nordrhein-Westfalen. Die Deutsche Telekom stellte im Berichtszeitraum 2011 beiden Aufsichtsbehörden die neue Personalaktenrichtlinie des Konzerns vor: Seit 1. Dezember 2011 werden Personalunterlagen nur noch als elektronische Personalakte geführt.

Die Beauftragten verschafften sich einen Eindruck zu aktuellen Themen:

- Die qualifizierte elektronische Signierung (QES) von Dokumenten in der elektronischen Personalakte wird nach den Anforderungen des Bundesfinanzministeriums in einem aktuellen Projekt umgesetzt. Die QES dient zur Sicherstellung der Rechtswirksamkeit und Gültigkeit von elektronischen Dokumenten. In den elektronischen Personalakten der Beamten werden dazu fast 2,4 Millionen Dokumente hinsichtlich Löscho- und Aufbewahrungsfristen überprüft. Dieser Überprüfung lagen konkrete Anforderungen der Aufsichtsbehörden zugrunde, um die datenschutzgerechte Entsorgung der Papierakten von Beamten durchzuführen.
- Die physikalische Löschung in den Software-Systemen zur Personalverwaltung wird teilweise erst zu Jahresbeginn 2013 abgeschlossen sein, was die Aufsichtsbehörden als

kritisch beurteilen. Die Dauer des Verfahrens ergibt sich aus technischen Gründen, die in der Version der verwendeten SAP-Software liegen. Der Bundesdatenschutzbeauftragte ist darüber in Kenntnis gesetzt. Die Aufsichtsbehörde und die Deutsche Telekom arbeiten gemeinsam an einer schnelleren Lösung. In anderen Software-Systemen ist die Umsetzung der Datenlöschung bereits beauftragt. Beide Aufsichtsbehörden hoben die gute und konstruktive Zusammenarbeit hervor.

Unzulässige Auswertung in der Personalverwaltungssoftware.

Im Datenschutzkonzept  der bei der Deutschen Telekom eingesetzten Software für die Personalverwaltung sind zulässige Auswertungen und dafür autorisierte Nutzer festgelegt. Eine Konzernbetriebsvereinbarung regelt, welcher Nutzer welche Personaldaten abfragen darf. Eine Routineprüfung ergab, dass neu installierte Software-Funktionen zu unzulässigen Auswertungsmöglichkeiten führten. Die Deutsche Telekom hat daraufhin Berechtigungskonzepte entwickelt und damit die Auswertungsabfragen so angepasst, dass sie dem Datenschutzkonzept der Software und den Konzernregelungen entsprechen.

Fehlerhafter E-Mail-Versand im Bereich Fuhrpark-Management.

Einer Reihe von Mitarbeitern stellt die Deutsche Telekom gegen eine Gehaltsumwandlung ein Geschäftsfahrzeug zur Verfügung, das von der Tochtergesellschaft DeTeFleetServices GmbH bereitgestellt wird. Beim jährlichen, automatisierten Versand der elektronischen Abrechnungen ist ein systemtechnischer Fehler eingetreten: E-Mails enthielten den Empfängernamen des vorherigen Versandvorgangs. Unbeabsichtigt sind Abrechnungsinformationen so falschen Empfängern zugeordnet worden. Der Fehler wurde umgehend erkannt und abgestellt. Die Betroffenen erhielten ein Entschuldigungsschreiben mit Informationen über den Fehler sowie dessen Behebung.

Rechtskonforme Regelungen zur Datenverarbeitung einer Einkaufssoftware.

Die Einkaufsanwendung eBest (Electronic Buying and E-Commerce System Telekom) gehört zum Einkaufssystem der Deutschen Telekom. Nach einigen Funktionserweiterungen erfolgte eine Routineüberprüfung des Datenschutzkonzepts der Software. Dabei stellte sich heraus, dass verschiedene Konzerngesellschaften eBest nutzen, für diese organisationsübergreifende Datenverarbeitung jedoch keine vertragliche Regelung vorlag. Bei diesen Daten handelte es sich zum Beispiel um Bestellinformationen wie Mitarbeiter-


name oder Lieferanschrift, die zur Bestellabwicklung über das Einkaufssystem zwischen den Konzernunternehmen ausgetauscht werden. Die Deutsche Telekom schloss die Lücke durch die Ausarbeitung der fehlenden Verträge sowie die Überarbeitung des Datenschutz- und Sicherheitskonzepts für eBest.

3.4. Internationale Entwicklungen.

Gesetzliche Regelungen.

▪ Novellierung der EU-Datenschutzrichtlinie.

Die EU-Kommission hat die europäische Datenschutzrichtlinie überarbeitet und dem europäischen Rat und dem Parlament einen Entwurf unterbreitet. Dieser soll den Rechtsrahmen zum Schutz personenbezogener Daten in der EU schaffen und als Verordnung in Kraft treten. Als Verordnung erzielt sie im Gegensatz zur bisherigen Richtlinie unmittelbare Wirkung, weil sie nicht erst durch die EU-Mitgliedsstaaten in nationales Recht umgesetzt werden muss. In Folge entstünde in Europa eine einheitliche und harmonisierte Regelung zum Datenschutz, was für Unternehmen die internationale Geschäftstätigkeit unter Beachtung der Datenschutzbestimmungen erleichtern und den Verbraucherschutz stärken würde.

Die EU-Verordnung setzt teils auf existierende Vorschriften auf, wie sie bereits seit 2009 im deutschen Datenschutzrecht bestehen. Zu den Neuerungen zählen insbesondere die einheitliche Zuständigkeit einer Aufsichtsbehörde für einen Konzern, die Anwendbarkeit der Verordnung auch für Unternehmen mit Sitz außerhalb der EU sowie die Einführung des Datenschutzbeauftragten in Unternehmen in der gesamten EU. Ebenso neu ist die Möglichkeit, nicht mehr für jede einzelne „Legaleinheit“ einen Datenschutzbeauftragten ernennen zu müssen, sondern übergreifend einen Konzerndatenschutzbeauftragten berufen zu können. Auch die einheitliche Regelung zur Verständigung von Betroffenen bei Verletzung der Sicherheit personenbezogener Daten oder bei deren Missbrauch (Data Breach Notification)  ist vorgesehen. Zum letzten Punkt besteht im deutschen Datenschutzrecht bereits eine Vorschrift, die von der Deutschen Telekom umgesetzt wird.

Die Deutsche Telekom sieht in der Novellierung eine notwendige Harmonisierung der Datenschutzregelungen in Europa

und begrüßt die Stärkung des Schutzes von Betroffenen. Gleichzeitig besteht aus Sicht der Deutschen Telekom noch Handlungsbedarf bei zahlreichen ungenauen Vorschriften, bei denen sich die EU-Kommission Ausführungsbestimmungen vorbehält. Beispielsweise will sie datenschutzspezifische Zertifizierungen fördern, lässt jedoch die Frage nach Standards und Verfahren unbeantwortet. Die Deutsche Telekom plädiert an dieser Stelle für eine Beteiligung der Wirtschaft, um eine praxisnahe Umsetzung zu ermöglichen. Nach Abschluss der Beratungen in Parlament und Rat soll die neue EU-Datenschutzverordnung voraussichtlich 2013 in Kraft treten.

▪ **Weitere neue gesetzliche Regelungen und Initiativen.**

Doch nicht nur auf EU-Ebene gab es Neuigkeiten. Russland hat sein Datenschutzgesetz überarbeitet, insbesondere in Bezug auf internationale Datenübermittlungen. Ähnlich wie innerhalb der Europäischen Union war die Übermittlung in ein

Internationale Datenschutz-Gremien.

Die International Privacy Circles (IPCs, jetzt: International Privacy Leadership Teams) 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 Teams ist darüber hinaus die Vermittlung eines einheitlichen Wissensstands etwa 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. Hier werden 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.

Drittland nur dann möglich, wenn im Drittland ein adäquates Datenschutzniveau festgestellt wurde. Wie dies festzustellen ist, wurde mit der Novelle konkretisiert. Auch in einzelnen EU-Mitgliedsländern wurden Datenschutzgesetze überarbeitet, etwa in Ungarn. Die Änderungen haben weitreichende Konsequenzen für multinationale Unternehmen. So ist weiterhin die Unterbeauftragung im Rahmen der Datenverarbeitung nicht erlaubt. Bindende Konzernregelungen – wie etwa der Privacy Code of Conduct (G) der Deutschen Telekom – werden nicht anerkannt und die Übermittlung von personenbezogenen Daten aus Ungarn in das Ausland ist ohne Einwilligung weiterhin untersagt.

Auch für die Telekom hat die Bestätigung dieser harten Regelung Konsequenzen, da die ungarische Tochter internationale Konzerninfrastrukturen etwa für einheitliche Datenschutzzuschulungen nicht nutzen kann. Auch weicht das neue Gesetz dahingehend von der EU-Datenschutzrichtlinie ab, dass in Ungarn verarbeitete Daten immer dem ungarischen Datenschutzgesetz unterliegen, auch wenn diese im Ausland erhoben wurden. Dies kann zu einer Kollision mit den gesetzlichen Bestimmungen im Ursprungsland führen.

Maßnahmen länderübergreifender Zusammenarbeit.

Vom 28. bis 29. Juni 2011 fand der jährliche International Privacy Circle (IPC, künftig Zusammenkunft des International Privacy Leadership Teams) und International Data Protection Day statt. Im Unterschied zu den vergangenen Veranstaltungen fand der IPC dieses Mal nicht regional, sondern zentral in der Bonner Konzernzentrale der Deutschen Telekom statt. So bot sich erstmals allen Datenschutzverantwortlichen der internationalen Geschäftseinheiten die Gelegenheit des persönlichen Kennenlernens und Erfahrungsaustausches. Der Zirkel ist ein zentrales Forum, auf dem Kenntnisse und Meinungen zu Datenschutzthemen wie etwa Anforderungen zur internationalen Auftragsdatenverarbeitung, interne Kontrollsysteme oder Ergebnisse der internationalen Basisdatenschutzaudits ausgetauscht werden. Abgerundet wurde die Veranstaltung durch den International Data Protection Day, der anders als der Workshop-orientierte Privacy Circle strategische Themen betrachtete.

Ende 2010 priorisierte die Deutsche Telekom Themen im Rahmen der Datenschutz-Taskforce: Diese Themen, der Rollout des internationalen Privacy und Security Assessments (PSA), internationale Datenschutz-Schulungen und internationale

Auftragsdatenverarbeitung, wurden im Laufe des Jahres entwickelt und umgesetzt. Im Rahmen der Auftragsdatenverarbeitung wurden neue Vorlagen für verschiedene Projektkonstellationen erstellt, um die Fachbereiche effizienter unterstützen zu können. Die internationalen Schulungen werden zukünftig schrittweise in Zusammenarbeit mit den Landesgesellschaften in die jeweiligen Sprachen übersetzt. Das internationale Intranet wurde im Rahmen eines gemeinsamen Relaunch-Projektes im Vorstandsbereich Datenschutz, Recht und Compliance komplett neu erstellt. So finden sich nun Informationen, Newsletter und Unterlagen in einem einheitlichen und übersichtlichen Design.

Revisionsprüfung des internationalen Datenschutzes.

Die Konzernrevision hat im August und September 2011 die internationale Datenschutzstrategie im Konzern der Deutschen Telekom geprüft. Dabei wurden die Umsetzung des Privacy Code of Conduct, des internationalen Governance & Cooperation Models und die daraus abzuleitenden Pflichten und Prozesse in den internationalen Geschäftseinheiten betrachtet. Als Ergebnis wurde die erfolgreiche Umsetzung des Privacy Code of Conduct in über 90 Prozent der internationalen Geschäftseinheiten und der Rollout des Governance Modells als positiv gewertet. Die Weiterentwicklung des Governance & Cooperation Modells sowie die vollständige Umsetzung des Privacy Code of Conduct über die nächsten Jahre wurde empfohlen.

Um den Empfehlungen zu entsprechen, ist ein Maßnahmenkatalog ausgearbeitet worden, dessen Umsetzung im Laufe des Jahres 2012 angegangen wird. So soll etwa die Aufgabenstellung für den jeweiligen Datenschutzbeauftragten in einer nationalen Geschäftseinheit und der damit verbundene Umsetzungsprozess zukünftig zusätzlich in einer vereinfachten Prozessübersicht dargestellt werden. Dies optimiert den Übergang bei einem Wechsel des Datenschutzbeauftragten und gestaltet die Einarbeitungsphase noch effizienter. Zugleich wurde ein Zeit- und Informationsablauf zwischen den Geschäftseinheiten und der Konzernzentrale definiert, um die Unterstützungsmöglichkeiten des Konzerndatenschutzes während des Übergangs zu optimieren. Darüber hinaus soll die funktionale Führung der dezentralen Datenschutzstruktur durch den Konzerndatenschutz ausgebaut und die bestehende Verzahnung zwischen Konzern und den Geschäftseinheiten verstärkt werden. Dabei wird auf die bereits existierenden Abstimmungsprozesse aus dem Governance & Cooperation Model aufgesetzt.

Das im Jahr 2011 komplett überarbeitete internationale Datenschutz-Intranet, das Dokumente, Informationen und Schulungen zum internationalen Datenschutz bereitstellt, wird weiter ausgebaut. Außerdem wurde empfohlen, über diese Plattform weitere zukünftige Schulungen und Weißbücher für die Geschäftseinheiten bereitzustellen. Als zentrales Online-Kommunikationsmedium wird das Intranet verstärkt Rahmeninformationen wie die internationale Datenschutzstrategie und daraus abgeleitete Inhalte zur Verfügung stellen. Das erfolgreich eingeführte Datenschutz- und Datenschutzvorfall-Reporting wird als kombiniertes Berichtswesen weiterentwickelt. Der in den vergangenen Jahren beschrittene Weg im internationalen Datenschutz wurde als positiv bewertet. Dieser Weg solle kontinuierlich weiterentwickelt und an neue Anforderungen angepasst werden.

Internationaler Standard beim Tracking.

Ausgehend von der Federal Trade Commission in den USA wurde eine breitere Debatte auf internationaler Ebene über Tracking-Mechanismen im Internet und die fehlende Möglichkeit für Nutzer, sich einem Tracking zu entziehen losgetreten. Auf Ebene des World Wide Web Consortium (kurz: W3C), einem Gremium zur Standardisierung der das World Wide Web betreffenden Techniken, wurde eine Arbeitsgruppe installiert. Diese verfolgt das Ziel, einen internationalen Standard zu erreichen, der es den Internetnutzern überlässt, sich verfolgen zu lassen oder ein Tracking zu unterbinden. Die Deutsche Telekom sieht hier dringenden Handlungsbedarf. Dies gilt in besonderem Maße für Mechanismen wie die EU-Cookie-Richtlinie sowie die Vorschläge zur Novellierung des Telemediengesetzes. Die Deutsche Telekom wird sich an der Diskussion auch weiterhin intensiv mit dem Ziel beteiligen, dass damit auch nationale und europäische Datenschutzerfordernisse erfüllt werden können.

Audits an ausländischen Standorten.

T-Systems ist die Geschäftskundensparte der Deutschen Telekom. Sie bietet IT-Dienstleistungen im In- und Ausland an. Im Jahr 2011 wurden mehrere ausländische Standorte der T-Systems hinsichtlich der Gewährleistung eines angemessenen Datenschutzniveaus überprüft, so etwa in Brasilien, Malaysia und Südafrika. Diese Audits werden als Point of Production-Audits (PoP-Audits) bezeichnet. Hierbei wurde ein unterschiedliches Niveau vorgefunden und dementsprechend die Umsetzung von Maßnahmen festgelegt und verfolgt. Des Weiteren wurden



Die Deutsche Telekom verbessert ihre internationale Zusammenarbeit ständig.

Re-Audits zur Überprüfung der Umsetzung vereinbarter Maßnahmen aus den vorherigen Audits durchgeführt.

Bei den Privacy Code of Conduct-Audits (PCoC-Audits) wird die Einhaltung des Datenschutzkodex innerhalb des Konzerns überprüft. Dabei wurden die Ergebnisse des internationalen Basisdatenschutzaudits herangezogen. Dies geschah etwa bei der T-Mobile Polen, der Telekom Kroatien, der Magyar Telekom, der T-Mobile Tschechien sowie im Bereich der OTE in Griechenland und der Romtelecom in Rumänien. Auch hier waren die Ergebnisse heterogen. Neben der Definition von Maßnahmen wurden Einheiten, deren Struktur sich im Aufbau befindet, im Hinblick auf die personelle und organisatorische Positionierung durch die Deutsche Telekom unterstützt. Entsprechende Re-Audits wurden ebenfalls festgelegt.

Weiterentwicklung des Datenschutzes bei Hrvatska Telekom.


Bei einem Besuch des Datenschutzbeauftragten der Deutschen Telekom beim CEO der Hrvatski Telekom wurde im Oktober 2011 die Datenschutzstrategie der kroatischen Konzerntochter konkretisiert. Dabei wurden die Datenschutzvorgaben aus dem Governance Model vereinbart, die Umsetzung von Maßnahmen aus vorangegangenen Audits besprochen sowie die Umsetzung

des PSA-Verfahrens erläutert. Außerdem wurde vereinbart, die Datenschutzorganisation der Hrvatska Telekom um weiteres Fachpersonal auszubauen, wodurch die Zusammenarbeit mit der internen IT-Abteilung im Rahmen von Projekten noch effizienter gestaltet wird.

Everything Eyewhere.

Zum 1. Juli 2010 hatten 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 entsprechenden Maßnahmen und Entscheidungen zur Einhaltung des systemseitigen Datenschutzes bei der Systemmigration wurden 2011 begleitet. Es wurden Fristen festgelegt, die einen datenschutzkonformen Übergang ermöglichen.

Attacke auf Home Gateways bei Slovak Telekom und Romtelecom.

Massenhafte Angriffe auf die Home Gateways (DSL Router) der Endkunden verursachten im Februar 2011 bei der Slovak Telekom und bei der Romtelecom erhebliche Störungen im Internet Zugangsgeschäft. Die Hacker nutzten einen unsicheren Administrationszugang der von den betroffenen Landesgesellschaften verwendeten Endgeräte, um die Einstellungen für den Domain Name Service (ein Dienst zur Namensauflösung im Internet) zu manipulieren. Hierdurch wurde der Internetverkehr der betroffenen Endkunden teilweise auf andere Ziele umgeleitet. Auf diese Weise wurde versucht, Schadsoftware zu verbreiten (beispielsweise ein Botnetz zu etablieren, um verteilte Denial-of-Service Angriffe  durchführen zu können) und Zugangsdaten zu Diensten zu erschleichen (sog. Phishing Angriffe).

Durch die Angriffe wurden auch einzelne Infrastrukturkomponenten der beiden Landesgesellschaften stark belastet, so dass auch Kunden von Ausfällen betroffen waren, deren Home Gateways nicht direkt angegriffen wurden. Betroffene Geräte wurden per Fernwartung identifiziert und die manipulierten Konfigurationseinstellungen korrigiert. Zudem wurde die Schwachstelle beseitigt. Die Deutsche Telekom hat Slovak Telekom und Romtelecom in ihrem Vorgehen unterstützt.



Thomas Tschersich,
Leiter IT-Sicherheit der
Deutschen Telekom AG

Ein neues Credo der Cybersicherheit lautet „Analyse vor Prävention“. Ist das nicht paradox?

Zunächst mag dieser Gedanke in der Tat paradox klingen. Das Paradoxon löst sich allerdings auf, wenn man es differenziert betrachtet: Das eine dem anderen voranzustellen, bedeutet nicht, das andere zu lassen! Natürlich sind für eine funktionierende Cybersicherheit beide Faktoren wichtig, Prävention und Analyse. In einer Zeit, in der digitale Bedrohungen immer mehr zunehmen und neue Angriffe nach neuen Mustern auf der Tagesordnung stehen, verschieben sich allerdings die Schwerpunkte. Wir müssen uns darüber im Klaren sein, dass wir nicht einfach einen starren, virtuellen Zaun um unsere Infrastrukturen errichten können.

Um zu wissen, wie wir Bedrohungen entgegenwirken können, müssen wir vielmehr untersuchen, wie diese Bedrohungen aussehen! Und da kommt die Analyse ins Spiel, deren Ergebnisse dann natürlich wieder in präventive Maßnahmen einfließen müssen.

Die Deutsche Telekom hat in den vergangenen Monaten Frühwarn- und Analysensysteme wie ihre Honey Pots oder das CERT weiter ausgebaut. Gleichzeitig setzt sie auf Einbindung von Sicherheit und Datenschutz ab dem ersten Entwicklungsschritt von Projekten und auf digitale Sicherheitstests vor der Markteinführung eines Produktes. Aber das alles ist immer nur eine Momentaufnahme. Uns ist klar: Die richtige Balance zwischen Analyse und Prävention ist der Weg, den wir gehen wollen und müssen.

3.5. Systeme und Prozesse.

Das Jahr 2011 war ein Jahr der breiten öffentlichen und politischen Diskussion zum Thema Datenschutz und Datensicherheit (siehe Seite 10). Die Deutsche Telekom erachtet das breite gesellschaftliche und politische Bewusstsein für diese Themen als ausgesprochen fruchtbar für die konstruktive Weiterentwicklung der bestehenden und angedachten nationalen und internationalen Schutz- und Sicherheitskonzepte. Das Unternehmen legt in der Debatte allerdings Wert auf Offenheit: Es muss stets deutlich gemacht werden, dass eine absolute Sicherheit von Daten nicht möglich ist. Es kann immer nur darum gehen, Systeme und Prozesse so sicher wie möglich, nötig und gewünscht zu gestalten.

Die Deutsche Telekom hat auf diesem Gebiet auch 2011 wichtige Meilensteine erreicht. Sie hat ihre Frühwarnsysteme weiter ausgebaut, mit deren Hilfe sie neue Angriffsmuster aus dem Netz erkennen, auswerten und zur Verbesserung der eigenen Systeme nutzen kann (siehe Seite 40). Gleichzeitig hat sie ein konzernweit eingesetztes Verfahren weiter etabliert, das Datenschutz und Datensicherheit von Beginn an in die Entwicklung von Produkten und Systemen einbezieht und berücksichtigt (siehe Seite 41). Darüber hinaus hat das Unternehmen auch 2011 mit Zertifizierungen durch unabhängige Institute den Nachweis erbracht, dass es die relevanten Normen und Standards erfüllt. Experten bescheinigen dem Unternehmen ein vorbildliches Sicherheitsniveau. Zentraler 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.

Sicherheitsmanagement der Deutschen Telekom.

Der Vorstand der Deutschen Telekom ist 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 2011 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 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 ist seit 2010 gemäß ISO 27001 (siehe Seite 45) zertifiziert und erfüllt damit den wichtigsten internationalen Standard.

Das Sicherheits- und Datenschutzmanagement fußt auf folgendem Regelungsrahmen:

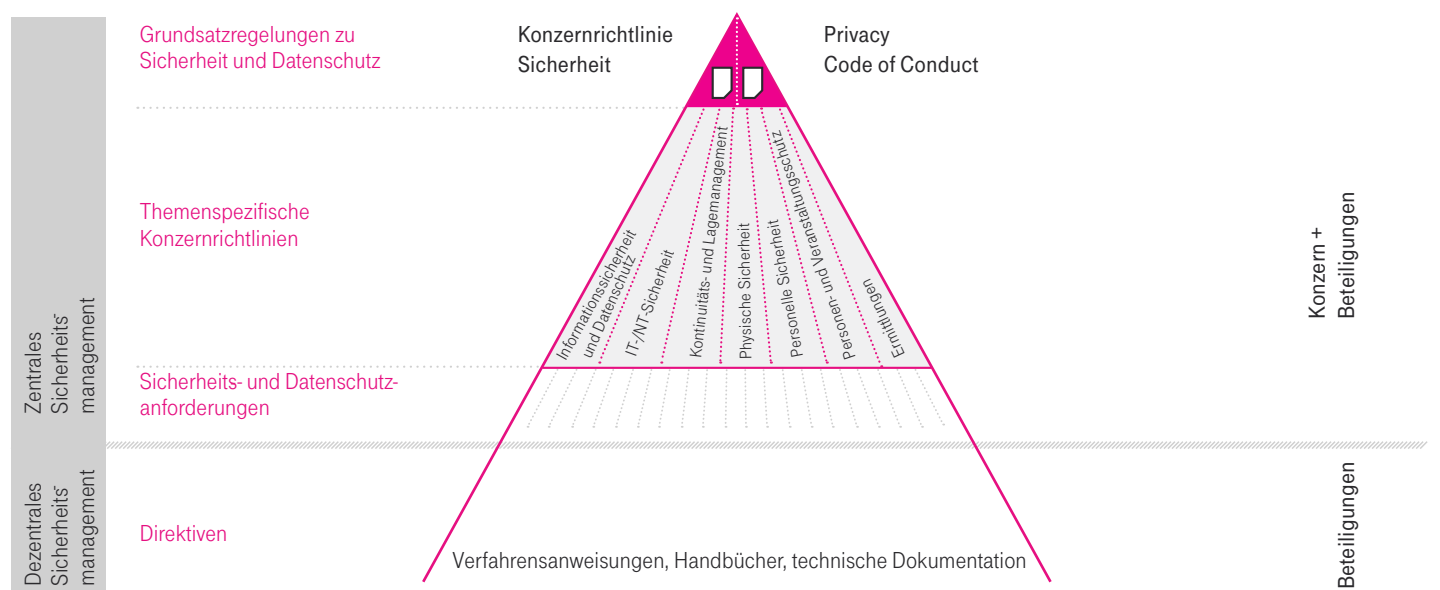
An der Spitze des Regelungsrahmens stehen die beiden grundlegenden Dokumente zu Datenschutz und Sicherheit der Deutschen Telekom: Der „Privacy Code of Conduct“ enthält die internen Anforderungen des Umgangs mit personenbezogenen Daten (allgemeine Datenschutzbestimmungen), die „Konzern-

richtlinie Sicherheit“ die sicherheitsrelevanten Grundsätze des Konzerns. Der Privacy Code of Conduct und die 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

Die 2010 überarbeiteten Regelwerke des Zentralen Sicherheitsmanagements sind 2011 in Deutschland und in den internationalen Beteiligungen sukzessive eingeführt worden. Dieser Prozess ist weitestgehend abgeschlossen. In den einzelnen

Regelungsrahmen zu Sicherheit und Datenschutz.





In den so genannten Honigtöpfen der Deutschen Telekom hinterlassen Angreifer den digitalen Fingerabdruck ihres Angriffsmusters.

Einheiten werden sie durch lokale Regelungen ergänzt und ausgestaltet. In Deutschland sind die Richtlinien in den Gesellschaften Deutsche Telekom AG und Telekom Deutschland GmbH bereits im Jahr 2010 in Kraft getreten.

Frühwarnsysteme.

Als größter Anbieter von Kommunikationsdienstleistungen in Deutschland sind die Deutsche Telekom und ihre Kunden ein prominentes Ziel für Cyberangriffe. Die Möglichkeit solcher Angriffe bringt immer wieder neue Herausforderungen mit sich. Um hierauf zu reagieren, hat die Deutsche Telekom ein Frühwarnsystem auf- und seither kontinuierlich ausgebaut. Schon bei der Konzeption des Frühwarnsystems wurden die strengen deutschen datenschutzrechtlichen Maßstäbe berücksichtigt. Das System zielt darauf ab, Informationen über Angreifer zu ermitteln, neue Angriffe zu erkennen und bessere Abwehrstrategien zu entwickeln. Weiterhin wird es damit möglich, frühzeitig Anpassungsbedarfe der Sicherheitsmechanismen zu erkennen und diese zu implementieren. Sind Telekomkunden von Cyberattacken betroffen, informiert das Unternehmen die Betroffenen. Grundsätzlich gilt die Maxime, dass die Qualität eines Frühwarnsystems umso besser ist, je mehr Datenquellen und -material für die Analysen zur Verfügung stehen. Daher verknüpft die Deutsche Telekom ihr

Bild der Sicherheitslage im Internet, das rein auf eigenen, selbst generierten Informationen basiert, mit allgemein verfügbaren Herstellerinformationen und Erkenntnissen von Behörden.


Lockvogelsysteme – Honeypots.

Zentraler Bestandteil des Frühwarnsystems sind so genannte Honeypots (englischer Begriff für Honigtöpfe). Sie stellen aus dem Internet erreichbare Serversysteme dar, die jedoch isoliert von der eigentlichen Infrastruktur der Deutschen Telekom stehen. Diese Honeypots können daher selbst im Falle einer Kompromittierung nicht zu einer Gefährdung für die konzerneigene Infrastruktur werden. Einige dieser Honeypot-Systeme sind selbstlernend, das bedeutet, dass unbekannte Angriffe aufgezeichnet, analysiert und danach automatisch vom Frühwarnsystem erkannt werden. Die Deutsche Telekom hat im April 2010 mit dem Aufbau solcher Honeypot-Systeme begonnen. Ursprünglich sollten sie nur Rückschlüsse auf Angriffe auf Internet-Applikationen des Unternehmens ermöglichen. Heute verwendet die Deutsche Telekom die Daten für verschiedene Zwecke weiter, etwa zur Information von Endkunden und anderer Internet-Diensteanbieter.

In Ergänzung der bestehenden Honeypot-Systeme für Internet-Applikationen betreibt die Deutsche Telekom seit Dezember 2010 verschiedene Secure Shell Honeypots (SSH). Diese simulieren SSH-Server und ermöglichen es, den Ablauf eines Angriffs aufzuzeichnen und dabei die eingesetzten Schadprogramme auf Authentisierungsinformationen für eine spätere Analyse zu sammeln.

Als erster Provider in Europa hat sich die Deutsche Telekom entschieden, Honeypots zu entwickeln, die die Betriebssysteme für Smartphones (Android und iOS (für iPhone)) simulieren. Dabei sollen Angriffe auf solche Smartphones erkannt und hieraus Abwehrmaßnahmen entwickelt werden. Diese neue, angepasste Form von existierenden Honeypots auf Basis unter anderem der Open Source-Software Kippo zeigt, dass systematische Angriffe gegen offene Systeme im Mobilfunknetzen heute zum Alltag gehören.

Die Deutsche Telekom pflegt einen engen Austausch mit anderen Providern, die mit vergleichbaren Systemen arbeiten, die sie zum Teil von der Deutschen Telekom übernommen haben. Zum Netzwerk gehört unter anderem die von der Bundesregierung geförderte „Anti-Botnet-Initiative“, die zum Ziel hat, die Anzahl verseuchter Endkunden-Computer zu reduzieren.

Seit ihrer Einrichtung im April 2010 haben die Honeypots mehr als 12 Millionen Angriffe von Hackern erkannt (Stand März 2012). Die so gewonnenen Einblicke über Angriffsarten und -methoden hat die Deutsche Telekom genutzt, um erfolgreiche Angriffe auf ihre realen IT-Systeme abzuwenden und Kunden zu informieren, deren Rechner Teil eines Botnetzes  und damit fremdgesteuert sind.

Ihr Frühwarnsystem verbessert die Deutsche Telekom ständig, um den bestmöglichen Schutz der Kunden- und der eigenen Daten zu gewährleisten.

Telekom-CERT.

Das Cyber Emergency Response Team (CERT) der Deutschen Telekom ist innerhalb der Deutschen Telekom für das internationale Cyber Incident Management – also das Management von Internetsicherheitsvorfällen für alle Informations- und Netzwerktechnologien des Konzerns – zuständig. Dadurch übernimmt es die wichtige Aufgabe, das Unternehmen und dessen Kunden vor Gefahren aus dem Internet zu schützen. Es bildet die zentrale Anlaufstelle für die Meldung von Vorfällen und etabliert Mechanismen zur Früherkennung von Angriffen auf intern und extern erreichbare Systeme.

Die Aufgaben des CERTs umfassen:

- Cyber Incident Management: Koordination und Management von kritischen Sicherheitsvorfällen
- Strategic Threat Radar: Verantwortung und Pflege eines Bedrohungsradars zur Identifizierung von Bedrohungen im Kontext mit aktuellen und zukünftigen Kerntechnologien des Konzerns
- Advisory Management: Bewertung und Verteilung von Sicherheitshinweisen innerhalb des Konzerns, sowie Monitoring der Implementierung von kritischen Sicherheits-Updates
- Vulnerability Scanning: Regelmäßige Durchführung von Sicherheitsscans der aus dem Internet erreichbaren Portale und Systeme
- Central Interface: Zusammenarbeit mit den Strafverfolgungsbehörden sowie Schnittstellenfunktionen zu national und international relevanten Gremien und Behörden für IT-Sicherheit

Im Jahr 2011 hat das Telekom CERT Hinweise zu 1.174 Schwachstellen in Softwarekomponenten, die auch in der Deutschen Telekom verwendet werden, an interne Betriebseinheiten gesandt. Dies ist ein minimaler Anstieg im Vergleich zum Vorjahr. Die Bewertung der Sicherheitshinweise hinsichtlich ihrer Kritikalität zeigt einen im Wesentlichen gleichbleibend hohen Anteil von kritischen oder hochkritischen Schwachstellen.

Viele der Hinweise adressieren Schwachstellen, die zu Denial-of-Service-Angriffen oder so genannten Drive-by-Infektionen führen können. Bezüglich der betroffenen Betriebssysteme ist kaum ein Unterschied zu den Vorjahren festzustellen. Aufgrund der Marktdurchdringung von Unix- und Windows-Systemen weisen beide Plattformen beinahe den gleichen Anteil von Schwachstellen auf: Im direkten Vergleich sind es bei Unix 48 Prozent und bei Windows-Systemen 43 Prozent.

Im Rahmen des Strategischen Bedrohungsradars werden Trends, Innovationen sowie aktuelle und zukünftige Technologien auf ihr Bedrohungspotenzial hin untersucht und bewertet. Der Radar versetzt das Management der Deutschen Telekom frühzeitig in die Lage, Cyberbedrohungen hinsichtlich ihrer Auswirkungen zu beurteilen und Gegenmaßnahmen zu entwickeln.

Im besonderen Fokus des Telekom CERT steht derzeit die Bedrohung Advanced Persistent Threat (APT). Zu diesem Thema hat das Telekom CERT ein Projekt gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) aufgesetzt. In diesem soll erarbeitet werden, welche Sicherheitstechnologien und -prozesse geeignet sind, um umfassend gegen solche Bedrohungen zu schützen. Die Ergebnisse werden der Allgemeinheit zur Verfügung gestellt.

Privacy and Security Assessment (PSA-Verfahren).

Die Bereiche Datenschutz und Datensicherheit leisten innerhalb der Deutschen Telekom wichtige Grundlagenarbeit für verlässliche Produkte, die den Anforderungen an Sicherheit und Datenschutz genügen. Schon 2010 haben sie das so genannte Privacy and Security Assessment, kurz PSA-Verfahren, gemeinsam eingeführt, um zu gewährleisten, dass alle Projekte innerhalb des Konzerns die Anforderungen für technische Sicherheit und Datenschutz vom ersten Entwicklungsschritt an erfüllen.

Das Verfahren adressiert folgende Ziele:

- Sicherstellung der datenschutzspezifischen Rechtskonformität von allen Produkten, Systemen und Plattformen
- Einheitliches und adäquates Sicherheits- und Datenschutzniveau in allen Produkten, Systemen und Plattformen, die aktualisiert oder neu erstellt werden.
- Integriertes Verfahren für technische Sicherheit und Datenschutz als Bestandteil der Produkt- und Systementwicklungsprozesse.
- Der Projektkomplexität und Kritikalität angepasstes Betreuungsniveau durch die Einführung einer Kategorisierung zu Beginn jedes Entwicklungsprojekts.

Die Anwendung des PSA-Verfahrens ist verbindlich für alle deutschen Gesellschaften sowie für länderübergreifende Projektvorhaben der Deutschen Telekom, sofern sie aus Deutschland umgesetzt werden. Der internationale Rollout des Verfahrens konnte im Jahr 2011 weit vorangetrieben werden. Der Abschluss der Maßnahme ist für die Jahre 2012/2013 geplant.

Anhand eines Kategorisierungs-Werkzeugs wird einem Projekt zu Prozessbeginn die technische Sicherheits- und Datenschutzrelevanz nach der Kategorisierung A, B und C zugeordnet. Danach richtet sich die Betreuungstiefe. Je kritischer ein Projekt ist, desto umfassender ist der Beratungs- und Betreuungsansatz durch Datenschutz- und Sicherheitsexperten. Auf diese Weise wird ein optimaler Ressourceneinsatz bei allen Beteiligten sichergestellt. Die am Prozess Beteiligten sind neben den Datenschutz- und Sicherheitsexperten die Projektleiter und Systemverantwortlichen. Am Ende eines Entwicklungsprozesses, der mit dem PSA-Verfahren begleitet wurde, stehen immer ein Sicherheitstest und eine Datenschutzfreigabe.

Die Deutsche Telekom fordert immer wieder öffentlich, Sicherheit und Datenschutz als Designkriterium von Produkten und Prozessen verbindlich vorzuschreiben.

Runder Tisch „Sicherheit im Vertrieb“.

Im Rahmen des 2010 initiierten Vertriebsprojekts „Risikomanagement in Vertrieb & Service“ hat die Deutsche Telekom einen

Runden Tisch „Sicherheit im Vertrieb“ eingerichtet. Dieser unterstützt als Beratungs- und Informationsgremium die Geschäftsführung der Telekom Deutschland GmbH bei vertriebsrelevanten Betrugsfällen. Darunter fallen etwa Prämien- und Provisionsbetrug, Zugangs- und Datenmissbrauch, Einsatz nicht autorisierter Vertriebspartner, Missbrauch bei der Aktivierung von Prepaid-Karten und die Trennung von Endgerät und SIM-Karte.

Der Runde Tisch bündelt und koordiniert die Aktivitäten mit Bezug zu Betrugsfällen und stellt so die vertriebskanalübergreifende Transparenz sicher. Zudem forciert und koordiniert er die nachhaltige Umsetzung aller aus den oben genannten Betrugsfällen erforderlichen Maßnahmen. Darüber hinaus werden zur Reduktion von Sicherheitsrisiken entsprechende präventive Maßnahmen empfohlen.

Der Runde Tisch hat bei festgestelltem Fehlverhalten eine Empfehlungskompetenz im Hinblick auf erforderliche Sanktionen und einzuleitende Maßnahmen. Insbesondere initiiert er bei Betrugsfällen die Sanktionierung von Vertriebspartnern. Sanktionierungen können Abmahnungen und Provisionsrückforderungen sein, aber auch straf- oder zivilrechtlicher Konsequenzen nach sich ziehen.

Der Bereich Group Business Security (GBS) stellt den Vorsitzenden des Runden Tisches. Ein ausgewogenes Stimmrecht zwischen vertriebslichen und nicht vertriebslichen Bereichen stellt die Parität des Gremiums sicher.

Datenschutz-Orientierung für neue Geschäftsfelder.

Mit der neuen Strategie „Verbessern – Verändern – Erneuern“, die René Obermann im Frühjahr 2010 vorstellte, legt die Deutsche Telekom einen Fokus auf Wachstum durch neue, intelligente Netzlösungen und Angebote in Geschäftsfeldern wie Energie, Gesundheit oder dem Automobilbereich. Gerade neue Geschäftsfelder benötigen Hinweise, wie die Belange des Datenschutzes in ihre Geschäftsmodelle spielen können, geht es dabei doch immer auch um das Verarbeiten personenbezogener Daten, deren Schutz die Deutsche Telekom hohen Wert beimisst. Hierfür erstellte die Deutsche Telekom 2011 „Leitplanken“, die die datenschutzrechtlichen Rahmenbedingungen der jeweiligen Projekte und Geschäftsfelder für diese spezifisch zusammenfasst und darstellt. Während diese Orientierungshilfen neuen Mitarbeitern eine erste Information geben, auf was in den einzelnen Bereichen be-

sonders zu achten ist, dienen sie bereits erfahrenen Mitarbeitern als abstrahierte Zusammenfassung der wesentlichen Rahmenbedingungen.

Auditierungen und Zertifizierungen.

Regelmäßig finden bei der Deutschen Telekom konzernweit Auditierungen und Zertifizierungen im Bereich des Datenschutzes und der Datensicherheit statt. Dabei greift das Unternehmen auf ein System von Prüfungen durch externe und interne Stellen zurück. Die Deutsche Telekom nimmt damit in der Telekommunikationsbranche eine Vorbildfunktion ein: Zertifizierungen für Unternehmensbereiche sind in der Telekommunikationsbranche noch die Ausnahme. 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. Prüfgegenstand ist die Einhaltung der Vorgaben des Konzerndatenschutzes. Die zweite Kategorie umfasst Audits von Systemen wie etwa der IT und Produkten. Darüber hinaus wird geprüft, ob die Organisationsstruktur und die internen Prozesse der Deutschen Telekom den aktuellen Datenschutz- und Sicherheitsanforderungen entsprechen. Zur dritten Kategorie gehören anlassbezogene Audits bei Vorfällen oder Verdachtsmomenten ebenso wie Abnahmeaudits zur Freigabe von priorisierten

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 von externen Auditoren durchgeführten Audits 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.

Projekten. Das bedeutet: Vor einer Produkteinführung wird geprüft, ob das neue Produkt alle geforderten und notwendigen Datenschutz- und Sicherheitsvorschriften erfüllt. Im Rahmen von Nominierungsaudits werden neue Vertriebspartner vor der Aufnahme von Geschäftsbeziehungen auditiert. In wiederkehrenden Regelaudits prüft die Deutsche Telekom bestehende Vertriebspartner.

Durchgeführte Audits.

Im Jahr 2011 haben die interne Revision, Konzerndatenschutz und Zentrales Sicherheitsmanagement insgesamt 220 Audits zu Datenschutz und Sicherheit durchgeführt: Ein großer Teil dieser Audits betrafen 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 mögliche Lücken zu identifizieren. Solche Lücken können etwa durch Sicherheitsmängel in Softwarelösungen entstehen, die, sobald sie erkannt sind, gemeinsam mit Industriepartnern beseitigt werden. Ein weiterer Schwerpunkt der durchgeführten Audits diente 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.

Audits im Bereich Vertrieb.

Im Jahr 2011 hat die Deutsche Telekom im Bereich Vertrieb 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. Im Jahr 2011 wurden im Vertrieb 28 Call Center, die nach den Vorgaben der Deutschen Telekom aktiv Kundenanrufe tätigen, erfolgreich durch den TÜV-Rheinland zertifiziert.

Zudem wurden im Jahr 2011 letzte Vorbereitungen getroffen, um 2012 auch die Call Center zertifizieren zu lassen, die im Auftrag der Deutschen Telekom Kundenservice betreiben. Hierzu musste zunächst für die PCs in den Call Centern eine eigene IT-Umgebung geschaffen werden, um die Nutzung von Internet und Mailverkehr einschränken zu können (siehe Seite 27). So konnte die Sicherheit der Kundendaten kontinuierlich auf sehr hohem Niveau verbessert werden. Gleichzeitig wurden die 2010 gestarteten Zertifizierungs- und Erhaltungsaudits von rund 350 Exklusivpartnern im Handel fortgesetzt.

Darüber hinaus verfolgte die Deutsche Telekom durch Kunden und Mitarbeiter gemeldetes nicht regelkonformes Verhalten von Vertriebspartnern und Mitarbeitern stringent und sanktionierte es. Ein 2010 eingeführtes Gremium, der Runde Tisch zur „Sicherheit im Vertrieb“ stellt hierfür die zentrale Koordinierungs- und Steuerungsstelle dar.

Standard-Datenschutzaudits.

Die Deutsche Telekom auditiert regelmäßig Prozesse und Systeme. Die wichtigsten im Bereich Datenschutz waren im Jahr 2011 folgende sogenannte TOP-Audits:

- **Auditierung Bonitätsprüfung:** Das Risikobewertungssystem der Telekom Deutschland GmbH bewertet das Risiko von Forderungsausfällen bei Geschäften mit Bestandskunden und Vertriebspartnern. Das Audit brachte Mängel zum Beispiel im Rollen- und Berechtigungskonzept oder beim Löschkonzept zu Tage, die sukzessive behoben werden.
- **Audit ProKom:** Das System ProKom dient der Verwaltung und Bearbeitung von Verzeichniseinträgen der Telekommunikati-

onsteilnehmer. Das Audit ergab ein angemessenes Datenschutzniveau.

- **Audit Ermittlungsprozess:** 2011 wurde im dritten Jahr in Folge untersucht, ob die internen Ermittlungen innerhalb der Deutschen Telekom datenschutzkonform durchgeführt werden. Das Audit bestätigte, dass alle eingeleiteten Maßnahmen aus dem Vorjahresaudit umgesetzt wurden und sowohl Prozesse, als auch eingesetzte Verfahren den Anforderungen des Datenschutzes entsprechen.
- **Audit Prozess der Revisionsprüfungen:** Die Konzernrevision wurde auf die Einhaltung der datenschutzrechtlichen Rahmenbedingungen (Gesetze und konzerninterne Vorgaben) wie bereits im Vorjahr auditiert. Das Audit zeigte ein positives Ergebnis, alle Maßnahmen aus dem Vorjahresbericht wurden umgesetzt.
- **Audit Kundenmanagement im Mobilfunk:** Wie bereits im Jahr 2010 wurde das System für das Kundenmanagement im Mobilfunk mit erweitertem Umfang überprüft. Trotz erheblicher Verbesserungen an vielen Stellen ergaben sich einige Mängel, die bereits abgestellt wurden. Als eines der wichtigsten Systeme wird dieses System weiterhin jährlich auditiert.
- **Audit Kundenmanagement Festnetz:** Beim Audit des Systems zum Kundenmanagement im Festnetz wurden insbesondere die Benutzeroberfläche, die Archivierung und Löschung von Kundendaten sowie das Benutzerkonzept überprüft. Dabei ergaben sich keine kritischen Mängel. Einige der identifizierten kleineren Probleme im Löschkonzept wurden behoben.
- **SAP-HR-Basisaudit:** Prüfung der Erhebung und Verarbeitung von Mitarbeiterdaten, also etwa die Einhaltung der vereinbarten Zugriffsberechtigungen. Durch die Komplexität des Software-Systems und das sich stets wandelnde Umfeld, etwa durch Reorganisation oder Systemupdates, stellen sich Regelungsbedarfe heraus, auf die die Deutsche Telekom durch ihre betriebliche Organisation reagieren konnte. So konnten einige Kritikpunkte der Untersuchung kurzfristig beseitigt werden.
- **Audit Data Warehouse:** © Im Jahr 2011 erfolgte eine Überprüfung der Einhaltung datenschutzrechtlicher Vorgaben beim Data Warehouse für den Mobilfunk und für das Festnetz. Für die identifizierten Schwachstellen wie etwa teilweise fehlende

Verschlüsselung ist die Behebung eingeleitet beziehungsweise abgeschlossen.

- **Audit Missbrauchserkennungssysteme:** Für die Erkennung von Missbrauch und Leistungserschleichung durch Kunden oder Vertriebspartner betreibt die Deutsche Telekom mehrere Systeme. Diese wurden 2011 auditiert und bestätigten insbesondere, dass die Filtereinstellungen zur Erkennung von Missbräuchen datenschutzkonform gestaltet und protokolliert werden.
- **PCoC Audits bei deutschen Tochterunternehmen:** Bei den Tochterunternehmen Autoscout, Friendscout und Operational Services wurde die Einhaltung der allgemeinen Datenschutzbestimmungen der Deutschen Telekom, des Privacy Code of Conduct, kurz PCoC auditiert. Eine analoge Prüfung erfolgte bei internationalen Beteiligungen (siehe 37).

Gefundene Schwachstellen wurden und werden bei sämtlichen Audits geschlossen und die Umsetzung der Maßnahmen vom Konzerndatenschutz überprüft.

Ergebnisse des nationalen und internationalen Basis-Datenschutzaudits 2011.

Auch 2011 wurde das jährliche Basisdatenschutzaudit durchgeführt. Ziel des Audits ist die Messung des allgemeinen Datenschutzniveaus, das Erkennen von Verbesserungspotenzialen und die Ableitung von Gegenmaßnahmen. Hierzu wurden 40 Prozent der Konzernbeschäftigten aus Deutschland und 30 internationalen Beteiligungsunternehmen befragt. Eine Selbsteinschätzung der Datenschutzbeauftragten in den internationalen Beteiligungsunternehmen über die Einhaltung der Anforderungen aus dem Privacy Code of Conduct ergänzte das Basisdatenschutzaudit. Sowohl die Befragung der Mitarbeiter, als auch die Selbsteinschätzung der Datenschutzbeauftragten werden durch Stichprobenkontrollen überprüft.

Auf Konzernebene zeigt das Basisdatenschutzaudit 2011, dass die eingeführten Datenschutzmaßnahmen wirksam sind. Das relativ hohe Datenschutzniveau hat sich weiter verbessert. Die Beteiligungsquote stieg im gesamten Konzern von 43 Prozent auf 52 Prozent, in Deutschland lag sie sogar bei über 60 Prozent. Die hohe Sensibilität der Mitarbeiter für das Thema Datenschutz zeigte sich in der Frage, wie wichtig die Mitarbeiter das Thema

Datenschutz erachten. Hier stuften konzernweit 87 Prozent der Mitarbeiter das Thema Datenschutz als wichtig oder sehr wichtig ein. Dies ist ein gegenüber dem Jahr 2010 weiter gestiegener Wert, der sowohl in Deutschland als auch international ein ähnlich hohes Datenschutzbewusstsein zeigt.

Weitere geprüfte Themenbereiche wie etwa die Nutzung von Werkzeugen für die Verschlüsselung von Daten, die Entsorgung von Papier, die Teilnahme an Schulungen zum Thema Datenschutz sowie die Kenntnis der Prozesse und Meldewege zum Datenschutz zeigten einen hohen Sensibilisierungsgrad der Mitarbeiter. Für die untersuchten Bereiche wurden individuelle Ergebnisse bereitgestellt, die es den Einheiten ermöglichen, ihre Stärken und Schwächen zu analysieren und an Verbesserungen zu arbeiten.

Übergreifend zeigen sich lediglich Schwächen etwa im Bereich der Nutzung von vorhandenen E-Mail-Verschlüsselungsmechanismen oder in der Verpflichtung der Mitarbeiter auf das Daten- und Fernmeldegeheimnis bei internationalen Tochtergesellschaften. Wie auch bei den Audits zum Privacy Code of

ISO/IEC 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/IEC 27001-Zertifikaten erfolgt durch akkreditierte Zertifizierungsinstitute. Sie umfasst die Themen Dokumentenlenkung, ständige Verbesserung des Managementsystems, Management von organisationseigenen 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.

Conduct zeigt sich im internationalen Umfeld, dass es häufig an der ausreichenden Ausstattung der Datenschutzbeauftragten mit Personal, Zeit und Technik mangelt. An der Behebung der Schwächen arbeitet die Deutsche Telekom. Näheres zu Audits im Ausland siehe „Internationale Entwicklungen“, Seite 34.

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 des Rechnungsprozesses für Privatkunden durch den TÜVIT.

Nachdem bereits im Jahr 2010 der gesamte Abrechnungsprozess der Deutschen Telekom für Privatkunden im Festnetz durch den TÜVIT zertifiziert wurde (Datenschutz-zertifikat „Trusted Site Privacy“), befindet sich der Abrechnungsprozess für Privatkunden im Mobilfunk derzeit (Stand April 2012) im Zertifizierungsprozess.

Eine Prüfung nach den Trusted Site Privacy-Kriterien umfasst sowohl die Bewertung des Datenschutzes als auch eine Bewertung der IT-Sicherheit. Hierfür wurden bereits verschiedene IT-Systeme und -Schnittstellen auditiert und sicherheitstechnische Untersuchungen durchgeführt. Der Prozess umfasst das Erheben und Verarbeiten sämtlicher Daten, die über 35 Millionen Mobilfunkkunden täglich beim Telefonieren über Mobilfunk erzeugen. Die Zertifizierung wird für 2012 erwartet.

Zertifizierung der Telekom Shops.

Um ein gleichbleibend hohes Datenschutzniveau am Verkaufsort zu gewährleisten, finden in den Telekom Shops wiederholt Kontrollen mit dem Ziel der Einhaltung der Vorgaben zum Datenschutz statt. Seit 2009 unterzieht sich die Telekom Shop Vertriebsgesellschaft zudem regelmäßig einem Audit durch eine externe Prüfungsgesellschaft. Auch 2011 wurden die daten-

schutz- und sicherheitsrelevanten Prozesse in den Telekom Shops von der DEKRA Certification GmbH auditiert. Damit wurde der dreijährige Audit-Zyklus abgeschlossen. Die Telekom Shops können weiter das DEKRA Siegel „Datenschutz und Datensicherheit gemäß dem Bundesdatenschutzgesetz“  nachweisen.

Zertifizierungen nach internationalem Standard.

Im Jahr 2011 wurden die Zertifizierungen des Zentralen Sicherheitsmanagements und Teilen der T-Deutschland GmbH nach der internationalen Norm ISO/IEC 27001 bestätigt. Bei T-Systems wurde auch im Jahr 2011 der Prozess der Zertifizierung der deutschen Organisation und von 19 Landesgesellschaften fortgesetzt. Dies dient dem Erhalt des Dachzertifikats über die Einführung eines konzernweiten Informationssicherheits-Managementsystems. Insgesamt wurden im Jahr 2011 weltweit 188 ISO/IEC 27001-Audits durchgeführt.

3.6. Kommunikation nach innen und nach außen.

Der Umgang mit personenbezogenen Daten ist Vertrauenssache: Vertrauen der Kunden in das Unternehmen, dem sie ihre persönlichen Daten übergeben. Vertrauen aber auch der Deutschen Telekom gegenüber den Mitarbeitern, die mit diesen 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 gleichzeitig ihren Mitarbeitern Sicherheit im Umgang mit personenbezogenen Daten. Hierzu nutzt die Deutsche Telekom eine Vielzahl von Kommunikationsmitteln und -wegen, extern wie intern.


Kommunikation nach außen.

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 Daten. Die Deutsche Telekom nutzt verschiedene Medien zur Information und baut ihre Kommunikation stetig aus.

Bereits in den Jahren 2010 und 2011 hat die Deutsche Telekom den europäischen Datenschutztag zum Anlass für Informationen und Aktionen genommen. Der Datenschutztag 2012 am 28.




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

Januar stand im Zeichen des Datenschutzes für Kinder und Jugendliche. Der Konzerndatenschutzbeauftragte Claus-Dieter Ulmer gab mit einem neu konzipierten Vortrag an einer Schule den Startschuss für eine bundesweite Vortragsreihe, für die sich Schulen bei der Deutschen Telekom bewerben können. Im Mittelpunkt der interaktiven Vorträge und Diskussionen stehen Kinder und Jugendliche, die mit dem Internet und Social Media  aufwachsen. Sie sollen mit den Risiken und Gestaltungsmöglichkeiten zum Schutz ihrer Persönlichkeit vertraut gemacht werden. Insbesondere sollen sie dafür sensibilisiert werden, welche persönlichen Informationen sie preisgeben können oder besser nicht preisgeben.

Die Deutsche Telekom beteiligt sich intensiv an der öffentlichen und der Experten-Debatte um Datenschutz und Datensicherheit. Dabei steht für die Deutsche Telekom der transparente und fachlich fundierte Austausch von Ideen und Standpunkten im Mittelpunkt.

In Dialog treten war ein Ziel, das die Deutsche Telekom 2011 mit neuen Ansätzen verfolgt hat. Das Unternehmen entwickelte seinen Social Media Auftritt weiter und startete ein Unternehmensblog, das regelmäßig auch zu Fragestellungen des Datenschutzes und der Datensicherheit berichtet und Stellung bezieht. (<http://blogs.telekom.com/tags/datenschutz/>). So thematisierten

die Unternehmensblogger etwa die Vorratsdatenspeicherung  oder die Sicherheit von Smart Meters. In der neuen Rubrik "Management zur Sache" beziehen darüber hinaus Führungskräfte der Deutschen Telekom Stellung zu aktuellen Themen. Auch hier werden Datenschutz und Datensicherheit etwa mit einem Blick auf die geplante EU-Datenschutzverordnung oder die Sicherheit von Social Media beleuchtet.

Darüber hinaus setzt die Deutsche Telekom mit ihren telegraphen_events neue Impulse. Zu diesen Veranstaltungen lädt das Unternehmen Politiker, Blogger, Experten, Vertreter von Verbänden und Unternehmen in ihre Berliner Repräsentanz, um aktuelle Themen rund um Entwicklungen in der digitalen Welt zu diskutieren – Netzpolitik, Regulierung, Medienwandel, Produktinnovationen. Auch Datenschutz und Datensicherheit stehen häufig im Fokus. Im Vordergrund der Veranstaltung steht neben dem Austausch von Ideen der kontroverse Meinungs-austausch, um Zukunftsthemen der Telekom zu lancieren und Standpunkte frühzeitig zu besetzen, die auf der politischen Agenda auftauchen könnten. Zu einem "telegraphen_special" lud die Deutsche Telekom zur CeBIT 2012 in Hannover ein, wobei es um die sichere digitale Identität ging, wiederum ein Datenschutz- und Datensicherheitsthema.

Außerdem war die Deutsche Telekom Gastgeber eines Workshops von „Co:laboratory“, der in ihrer Berliner Repräsentanz im Juni 2011 stattfand. Die von Google ins Leben gerufene Initiative untersucht die Entwicklung des Verhältnisses von Privatheit und Öffentlichkeit in der Gesellschaft. Darüber hinaus hat die Deutsche Telekom sich an den öffentlichen Debatten zum Arbeitnehmerdatenschutz und zur EU-Datenschutzverordnung eingebracht. Zudem nehmen Verantwortliche der Deutschen Telekom immer wieder an diversen Expertenzirkeln, Fachevents und öffentlichen Veranstaltungen teil. Zu Themen des Datenschutzes und der Datensicherheit hat die Deutsche Telekom an mehreren Expertenanhörungen vor EU-Gremien und internationalen Organisationen teilgenommen.

Seit 2011 veröffentlicht die Deutsche Telekom online auch einen Bericht zur Sicherheitslage im Internet. Dieser Quartalsbericht ist abzurufen unter www.telekom.com/sicherheit.

Mit folgenden weiteren Maßnahmen richtete sich die Deutsche Telekom 2011 und Anfang 2012 an die Öffentlichkeit:

- Eine neue Auflage des Datenschutzratgebers zum sicheren Surfen im Netz
- Neugestaltung des Webauftritts zu Datenschutz und Datensicherheit mit Aufbau einer Ratgeberseite
- Verteilung von Datenschutzratgebern in Telekom Shops deutschlandweit
- Radiobeiträge zu Themen wie sicherer WLAN-Verschlüsselung oder zum sicheren Online-Shopping
- Messeauftritt der Deutschen Telekom auf der CeBIT im März 2012 mit Fokus auf den Sicherheitsaspekten des Cloud-Computing
- Darstellung der Frühwarnsysteme auf der CeBIT

Kommunikation nach innen.

Datenschutz und Datensicherheit können nur dann gewährleistet werden, wenn sich die Mitarbeiter der Deutschen Telekom darüber nicht nur in vollem Umfang bewusst, sondern darüber hinaus auch auf ihre Verantwortung vorbereitet und geschult sind. Dann können sie in Standard- ebenso wie in schwierigen Situation stets sicher agieren. Das Unternehmen legt besonderen Wert darauf, seinen Mitarbeitern kontinuierlich das dafür notwendige Wissen zu vermitteln. Die Deutsche Telekom verfolgt dabei die Strategie, insbesondere Führungskräfte von Anfang an bei der Datenschutzkommunikation zu den Mitarbeitern einzubinden. Führungskräfte sollen gegenüber ihren Mitarbeitern als Vorbilder agieren. Zudem stellt ein modulares Baukastensystem sicher, dass Mitarbeiter je nach Thema und Arbeitsbereich individuell geschult werden. So wird gewährleistet, dass Datenschutz und -sicherheit bei allen Mitarbeitern der Deutschen Telekom nachhaltig auf Resonanz treffen.

Im Jahr 2011 lag ein Schwerpunkt auf internationaler Ebene darauf, den Privacy Code of Conduct der Deutschen Telekom in ausländischen Konzerntöchtern weiter auszurollen, zu kommunizieren und die Mitarbeiter durch Schulungen mit den Leitlinien des Kodex vertraut zu machen. Ein zweiter Schwerpunkt, der in Deutschland und international durch Schulungen kommuniziert

Datenschutzkoordinatoren.

Eine Stütze der dezentralen Datenschutzorganisation in Deutschland sind die so genannten Datenschutzkoordinatoren: Mitarbeiter, die neben ihren regulären Aufgaben den Bereich Datenschutz bei der Einführung und Umsetzung der konzernweiten Datenschutzanforderungen unterstützen. Aktuell setzt die Deutsche Telekom etwa 100 Datenschutzkoordinatoren zur Unterstützung des Konzerndatenschutzes ein.

wurde, war das Privacy and Security Assessment, kurz PSA-Verfahren. Dieses Verfahren stellt sicher, dass Datenschutz und -sicherheit bei der Produkt- und Systementwicklung frühzeitig integriert sind (siehe Seite 41).

Ein weiterer Aspekt der Kommunikation nach innen war es, Mitarbeiter im Bereich Kundendatenschutz im Vertrieb zu schulen. Dies ist aufgrund der hohen Sensibilität des Bereichs ein Projekt, das auf mehrere Jahre angelegt ist. Darüber hinaus wurden alle Beschäftigten konzernweit im Rahmen des zweijährigen Turnus auf das Daten- und Fernmeldegeheimnis verpflichtet und für den Informationsschutz sensibilisiert.

Für die Kommunikation nach innen stehen diverse Schulungsformate und -medien zur Verfügung. Sie reichen vom klassischen Seminar im Schulungsraum mit persönlicher Anwesenheit über Webinare, Selbstlernen durch Online-Formate oder Schulungsmaterial, über Gespräche mit dem Vorgesetzten, einem Experten oder Besuche des Datenschutzbeauftragten. Welches Format oder Medium gewählt wird, orientiert sich an der Priorität des Lerninhalts, dem Vorwissen des Einzelnen, aber auch den Interessen der Mitarbeiter. Zudem liegen die Materialien auch im Intranet vor.

Im Mai 2011 wurden verschiedene Standorte der Deutschen Telekom in Deutschland von Vertretern des Konzerndatenschutzes besucht. Neben Workshops für die Mitarbeiter und Führungskräfte der Standorte wurden Gespräche mit Vertretern des Konzerndatenschutzes sowie den Datenschutzkoordinatoren angeboten, in denen es um die individuellen Besonderheiten der Standorte und der vom Personal wahrgenommenen

Aufgaben ging. Schließlich wurde die existierende Richtlinien-datenbank überarbeitet und als neues digitales Bücherregal im Intranet allen Mitarbeitern der Deutschen Telekom zur Verfügung gestellt.

Im Rahmen des Basisdatenschutzaudits (siehe Seite 45) verlieh die Deutsche Telekom auch im Jahr 2011 einen nationalen und internationalen Datenschutz-Award. Das Unternehmen zeichnete mit diesem Preis auf nationaler Ebene die drei Bereiche sowie international die drei Landesgesellschaften aus, die bei der Überprüfung am besten abgeschnitten haben.



Kommunikation nach innen wird bei der Deutschen Telekom über verschiedene Kanäle gepflegt. Wichtig ist die persönliche Ansprache der Adressaten.

Von einem dicken Panzer prallt einiges ab.
Oft bringen Impulse von außen jedoch entscheidende Ideen.



4.1. Aufgabe und Funktion.

Der Datenschutzbeirat der Deutschen Telekom ist ein Gremium, das den Vorstand berät. Er fördert den Austausch mit führenden Experten und Persönlichkeiten aus Politik, Lehre, Wirtschaft und Nichtregierungsorganisationen zu aktuellen, datenschutzrelevanten Herausforderungen. Zunehmend befasst er sich auch mit Themen der Datensicherheit. Der Datenschutzbeirat ist seit Februar 2009 tätig und erweitert die Datenschutz- und Sicherheitsorganisation der Deutschen Telekom um einen gesellschaftlich vielfältigen Blick von außen. Der Datenschutzbeirat ist frei von Weisungen und in seiner Meinungsfindung unabhängig.

Der Datenschutzbeirat bearbeitet ein umfangreiches Themenfeld: Er befasst sich mit Geschäftsmodellen und -prozessen zum Umgang mit Kunden- und Mitarbeiterdaten ebenso wie mit der IT-Sicherheit und der Angemessenheit ergriffener Maßnahmen. Darüber hinaus sind seine Themen internationale Aspekte des Datenschutzes sowie die Implikationen neuer gesetzlicher Regelungen. Auch die Beurteilung von allgemeinen Datenschutz- und Datensicherheitsmaßnahmen bei der Deutschen Telekom sowie die Erarbeitung von Vorschlägen und Empfehlungen an Vorstand und Aufsichtsrat zu entsprechenden Fragen gehören zu den Aufgaben des Beirats.

4.2. Zusammensetzung.

Die Mitglieder des Datenschutzbeirats werden von der Deutschen Telekom jeweils für zwei Jahre berufen. Um eine qualifizierte und kritische Reflexion von Datenschutz und Datensicherheit von außen zu gewährleisten, werden führende Datenschutzexperten aus unterschiedlichen Berufsgruppen und verschiedenen parteiischen Hintergründen berufen. Im Jahr 2011 wurde der Datenschutzbeirat für weitere zwei Jahre bestellt.

Zu seinen Mitgliedern zählen:

- Wolfgang Bosbach, CDU, MdB und Vorsitzender des Innenausschusses des Deutschen Bundestages
- 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)
- Dr. Konstantin von Notz, Bündnis 90/Die Grünen, MdB, Sprecher für Innen- und Netzpolitik, Obmann der Enquete-Kommission „Internet und digitale Gesellschaft“

- Gisela Piltz, MdB, stellvertretende Fraktionsvorsitzende der FDP-Bundestagsfraktion
- Gerold Reichenbach, SPD, MdB, stellvertretender Vorsitzender der Enquete-Kommission „Internet und digitale Gesellschaft“
- 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 Enquete-Kommission „Internet und digitale Gesellschaft“
- Halina Wawzyniak, Die Linke, MdB, stellvertretende Parteivorsitzende, Obfrau der Enquete-Kommission „Internet und digitale Gesellschaft“
- Prof. Dr. Peter Wedde, Professor für Arbeitsrecht und Recht in der Informationsgesellschaft, Direktor der Europäischen Akademie der Arbeit in der Universität Frankfurt am Main



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

Der Datenschutzbeirat der Deutschen Telekom arbeitet noch immer, auch wenn das Unternehmen sich im Datenschutz stark weiterentwickelt hat. Warum?

Die Deutsche Telekom hat 2009 den Datenschutzbeirat in einer Krisensituation eingerichtet. Seither hat sich das Unternehmen, auch mit Hilfe des Beirats, verändert. Der Konzern ist sensibler, selbstkritischer und umsichtiger in Sachen Datenschutz geworden: Das darf nicht dem Kostensparen geopfert werden. Will ein Unternehmen wie die Deutsche Telekom ein hohes Datenschutzniveau als Wettbewerbsvorteil herausstellen, erfordert dies ein starkes Gewicht des Themas auch und gerade in Zeiten der Umstrukturierung. Auch bei neuen Produkten kommt es mehr und mehr auf Datenschutz und Datensicherheit an. Die „Telekom Cloud“ muss ein Synonym für den Schutz der Persönlichkeitsrechte werden, um Markterfolg zu haben. Beides macht ein umso höheres Engagement des Beirats notwendig.

Neben dem Wandel innerhalb des Unternehmens spüren wir immer stärker den Einfluss, den äußere Entwicklungen auf unsere Arbeit ausüben, Veränderungen der Rechtslage, der technischen Optionen oder des gesellschaftlichen Bewusstseins beispielsweise. Längst stehen neben der Aufarbeitung von Fehlern der Vergangenheit die Dienstleistungen der Zukunft, neben „Datenschutzklassikern“ die Belange der Datensicherheit auf unserer Tagesordnung. Wir sehen, dass Unternehmen nur in engem Schulterschluss beider Disziplinen die adäquaten Schutz- und Sicherheitsanforderungen erfüllen und zunehmenden Bedrohungen Stand halten können. Auch dabei unterstützt der Beirat.

4.3. Beispiele seiner Arbeit im Jahr 2011.

Die Arbeit des Datenschutzbeirats ist geprägt von seiner Rolle als wichtiges Beratungsgremium des Vorstands der Deutschen Telekom. Die Unterstützung des Unternehmens im Vorhaben, in der Telekommunikationsbranche eine Vorreiterrolle bei Datenschutz und -sicherheit zu übernehmen, bildet einen ebenso wichtigen Tätigkeitsschwerpunkt.

Grundsätzlich kann der Beirat eigenständig Datenschutz- und Datensicherheitsthemen aufgreifen und entsprechende Vorschläge oder Empfehlungen für den Vorstand der Telekom erarbeiten. Durch diesen Freiheitsgrad befasste sich das Beratungsgremium 2011 neben Themen, die ihm vom Vorstand übertragen wurden, insbesondere auch mit Zukunftsthemen rund um den Datenschutz und die Sicherheit von Daten.

Insgesamt kam der Beirat 2011 zu vier Sitzungen zusammen. In ihnen beschäftigten sich die Mitglieder unter anderem mit den Datenschutzaspekten der strategischen Wachstumsfelder Gesundheit und Energie. Sie untersuchten die Datenschutzimplikationen internationaler Geschäftsmodelle und berieten über die Auswirkung von Schulungen im Konzern. Ein weiteres Beratungsfeld war das auch in der Öffentlichkeit aufmerksam verfolgte Thema „Packet Inspection“ beziehungsweise „Deep Packet Inspection“. Hierbei geht es um eine Technik zur Analyse von Datenpaketen, die Netzbetreiber für die Untersuchung von zwischen Servern und Rechnern ausgetauschten Daten benutzen (siehe Infokasten). Der Datenschutzbeirat überzeugte sich von der Einhaltung des Telekommunikationsgesetzes sowie der Transparenz über die Regeln zum Einsatz der Datenpaketanalyse im Konzern. Auf Empfehlung des Datenschutzbeirats wurden Informationen über die von der Deutschen Telekom eingesetzte „Packet Inspection“ im Internet veröffentlicht.

Packet Inspection/Deep Packet Inspection.

„Packet Inspection“ bezeichnet eine Technik zur Analyse von Datenpaketen, die Netzbetreiber für die Untersuchung von zwischen Servern und Rechnern ausgetauschten Daten benutzen. Sie werden eingesetzt für die Messung von Verkehrsströmen, zur Abwehr von Angriffen auf die Netzwerkinfrastruktur.

Die „Deep Packet Inspection“ ist eine Technik zur Datenpaket-Analyse, die auch Inhaltsdaten betrachtet. Diese Technik ist erforderlich, um etwa per E-Mail versendbare Viren zu entdecken. Beide Analyseformen führt die Deutsche Telekom automatisiert und ohne Einblicke der Mitarbeiter durch.

Die Deutsche Telekom ist wie jedes Telekommunikationsunternehmen dazu verpflichtet, unter bestimmten Voraussetzungen Auskunft über Verkehrs- und Bestandsdaten an staatliche Stellen zu geben und die Telekommunikation für staatliche Stellen zu überwachen. Dafür hat das Unternehmen 2011 einen neuen Handlungsleitfaden erarbeitet und dem Beirat vorgestellt. Ziel dieses Leitfadens ist es, Mitarbeitern in Zweifelsfällen eine klare und juristisch fundierte Richtschnur zu geben, wie sie der Informationsfreiheit, dem Schutz von Daten und Unternehmensinteressen sowie dem staatlichen Interesse an Gefahrenabwehr und Strafverfolgung gerecht werden können. Der Beirat hat den neuen Leitfaden in seiner ersten Sitzung 2012 zustimmend zur Kenntnis genommen und den Umgang der Deutsche Telekom zur Beaufkundung und Überwachung ausdrücklich gelobt.

Der Vorstand der Deutschen Telekom wird den konstruktiven Dialog mit dem Datenschutzbeirat fortsetzen, um seine Vorreiterrolle

bei Datenschutz und -sicherheit in der Branche weiter auszubauen. Der dazu notwendige kritische Blick externer Experten auf die Anforderungen an Datenschutz und IT-Sicherheit sowie deren Umsetzung im Konzern hat sich bewährt – damit die Kunden der Deutschen Telekom auch in Zukunft auf die Sicherheit aller Produkte und Services vertrauen können.



Ein Blick von außen bringt neue Einsichten und neue Ideen.

Die Natur hat perfekte Mechanismen gefunden,
ihr Wertvollstes zu schützen.

Die Deutsche Telekom hilft ihren Kunden, auch ihr Wertvollstes
in der digitalen Welt zu schützen – ihre Daten.



Das Internet ist aus unserem Leben kaum mehr wegzudenken: Wir erledigen unsere Einkäufe online, chatten mit Freunden auf einem anderen Kontinent, schauen Filme im Netz an – die Möglichkeiten sind schier endlos. Das allerdings leider nicht nur im Positiven, denn die Internetkriminalität boomt: Etwa alle vierzehn Sekunden gibt es ein neues Opfer, 54 Prozent der erwachsenen Onliner geben etwa an, bereits einen Computervirus gehabt zu haben. Einen hundertprozentigen Schutz vor Betrügern gibt es nicht, aber wir wollen Ihnen zeigen, wie Sie sich mit wenigen Handgriffen schützen und sicherer im Internet surfen können.

Unter www.telekom.com/ratgeber stehen Ihnen weiterführende Tipps und Hilfestellungen zur Verfügung. Dort erhalten Sie außerdem Informationen zu Datenschutz- und IT-Sicherheitsthemen, sowie zur aktuellen Bedrohungslage im Netz. Wenn Sie Fragen rund um Datenschutz oder IT-Sicherheit haben, können Sie über die Website oder per E-Mail (datenschutz@telekom.de) mit uns Kontakt aufnehmen.

5.1. 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 Virenschutzpro-

gramm 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.

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.

5.2. Gestaltung eines sicheren Passworts.

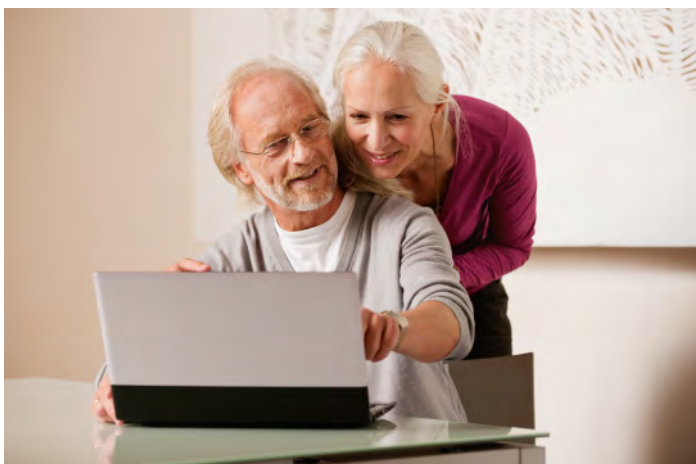
Ohne Passwort geht im Internet nicht viel. Und je besser ein Passwort ist, umso sicherer geschützt sind die Daten, die sich dahinter verbergen. Wer das Internet nutzt, benötigt Benutzernamen und Passwörter, um sich in den unzähligen Foren, Communities oder beim Online-Shopping anzumelden.

Spätestens beim fünften Passwort wird es da schwierig, den Überblick zu behalten. Hinzu kommt, dass ein sicheres Passwort nicht immer einprägsam ist. Aber es gibt Abhilfe.

Wie erstelle ich ein sicheres Passwort?

Die goldene Regel für ein sicheres Passwort: Es sollte von Außenstehenden nicht als sinnvolles Wort erkannt werden! Dafür gibt es einen einfachen Trick:

Einfach einen für Sie leicht zu merkenden Satz wählen und aus den Anfangsbuchstaben ein neues Wort bilden. Um das Passwort möglichst unknackbar zu gestalten ergänzen Sie den Satz durch Zahlen und Sonderzeichen. Beispielsweise: Meine Mutter kauft jeden Samstag 16 Eier auf dem Markt – §MMkjS16EadM!.



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

Als Untergrenze für ein sicheres Passwort empfehlen Experten 8 Zeichen, es kann aber auch deutlich länger sein. Grundsätzlich gilt: Je länger und komplexer ein Passwort ist, desto besser.

Bringen Sie Hacker zur Verzweiflung.

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

Erstellen Sie für jeden Zugang ein eigenes Passwort.

Eine weitere wichtige Vorsichtsmaßnahme: Verwenden Sie nach Möglichkeit für unterschiedliche Zugänge unterschiedliche Passwörter. Denn ab und an gelingt es Datendieben, komplette 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. Auf jeden Fall sollte das 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 Passwörter nie auf der Festplatte speichern oder auf einem Zettel in der Nähe des Computers notieren.

Ändern Sie wichtige Passwörter regelmäßig.

In regelmäßigen Abständen sollten Sie wichtige Passwörter ändern, um den Schutz vor Datendiebstahl zu erhöhen. Wir empfehlen, etwa alle drei Monate ein neues Passwort zu verwenden.

Wann benötige ich ein sicheres Passwort?

Möglicherweise benötigen Sie nicht immer ein Passwort, das höchsten Sicherheitsanforderungen entspricht. Bei einem Anglerforum etwa müssen Sie vermutlich nicht so vorsichtig sein wie beim Online-Banking.

Überlegen Sie 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 bei Online-Banking oder 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.

Generell gilt: Überlegen Sie sich gut, was es für Folgen hätte, wenn Ihr Passwort in die falschen Hände fallen würde – und treffen Sie danach Ihre Entscheidung, wie sicher Sie Ihr Passwort gestalten.

5.3. WLAN-Sicherheit für Zuhause.

Immer mehr Menschen nutzen drahtlose Funknetzwerke (Wireless Local Area Networks, kurz WLAN), um sich mit dem Internet zu verbinden.

Damit sich niemand ungewollt Zutritt zur Wohnung verschafft, schließen die meisten Menschen ihre Tür ab, wenn sie nach draußen gehen. Was im Offline-Leben selbstverständlich ist, ist auch Online unverzichtbar. Denn ein ungesicherter WLAN-Anschluss macht es Betrügern leicht, auf Kosten und in Verantwortung des Inhabers Dateien aus dem Netz herunterzuladen.

Außerdem: Besitzer von WLAN-Zugängen sind laut eines Urteils des Bundesgerichtshofs (BGH) vom 12. Mai 2010 (I ZR 121/08) dazu verpflichtet, ihren Zugang mit einem Passwort zu schützen.

Generell gilt: Jede drahtlose Verbindung bietet weniger Sicherheit als eine Netzwerkverbindung per Kabel. Bei der drahtlosen Verbindung werden die Daten per Funk an den Empfänger übermittelt und können abgefangen werden. Trotzdem müssen Sie nicht auf die Nutzung des drahtlosen Zugangs verzichten: In wenigen Schritten kann jeder sein WLAN vor Eingriffen und Datendieben schützen.



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

Sichern Sie Ihren WLAN-Router.

Router werden meist mit einem voreingestellten Netzwerknamen (SSID) ausgeliefert. Für eine sichere WLAN-Verbindung ist die Änderung der SSID sinnvoll, um Rückschlüsse auf den Hersteller des Routers zu erschweren. So können keine gerätespezifischen Sicherheitslücken ausgenutzt werden. Das Verbergen der SSID bringt keinen Sicherheitsgewinn, erhöht aber den Konfigurationsaufwand. Um die Konfiguration Ihres Telekom-Routers zu ändern, geben Sie in die Adresszeile Ihres Browsers <https://192.168.2.1> oder bei neueren Speedportgeräten <https://speedport.ip> ein und folgen dann den Anweisungen. Bei anderen Geräten folgen Sie den Anweisungen, die Sie im Handbuch Ihres Routers finden. Ändern Sie außerdem das voreingestellte Zugangspasswort für die Konfiguration Ihres Routers. Tipps zum Erstellen eines sicheren Passworts finden Sie im Kapitel „Gestaltung eines sicheren Passworts“.

Richten Sie eine Verschlüsselung ein.

Darüber hinaus ist es unverzichtbar, den WLAN-Zugang zu verschlüsseln und so für andere nicht zugänglich zu machen. Bei den meisten WLAN-Systemen geschieht dies über die Verschlüsselungsmethode WPA2-PSK (G). Dabei wird beim Verbindungsaufbau ein „Schlüssel“ (Passwort) gebraucht, um ins Netz zu kommen. Wichtig ist dabei, ein sicheres Passwort zu wählen und die vom Hersteller voreingestellten Passwörter zu ändern.

(Siehe „Gestaltung eines sicheren Passworts“, wobei hier ein deutlich längeres Passwort gewählt werden sollte).

Schalten Sie Ihr WLAN ab.

Außerdem: Wenn Sie Ihr WLAN nicht nutzen, sollten Sie es abschalten. Auf diese Art und Weise schützen Sie sich nicht nur vor Datendieben und ungewollter Nutzung ihres Zugangs für illegale Handlungen, sondern sparen auch Strom.

Tipp: Mit der kostenlosen Software Netzmanager der Deutschen Telekom sichern Sie ihr WLAN schnell und bequem ab. Der Netzmanager hilft Ihnen bei der Einrichtung einer sicheren Verschlüsselung, der Einrichtung einer SSID und eines sicheren Passwortes. Wählen Sie hierzu im Netzmanager den Menüpunkt „Routereinstellungen“ und „Funknetzwerk (WLAN)-Einstellungen“ ändern. Den Netzmanager können Sie unter www.telekom.de/netzmanager downloaden.

WLAN-Sicherheit für unterwegs.

Besonders wenn Sie mit ihrem Laptop öffentlich zugängliche HotSpots nutzen, sollten Sie die folgenden Tipps beachten, um Ihre Daten bestmöglich zu schützen.

Deaktivieren Sie Ihre Netzwerkfreigabe.

Wenn Sie HotSpots nutzen, sollte die Datei- und Verzeichnisfreigabe auf Ihrem mobilen Endgerät deaktiviert sein. In der Regel können Sie diese Freigabe in den Netzwerkeinstellungen Ihres Betriebssystems deaktivieren.

Bei HotSpot-Nutzung sollten Sie auf Ihrem Laptop nie mit einem Benutzerkonto angemeldet sein, das Administratorenrechte besitzt.

Aktivieren Sie Ihre Firewall.

Bevor Sie sich in ein fremdes WLAN einwählen, aktivieren Sie die Firewall Ihres Laptops. Im umfassenden Sicherheitspaket der Telekom ist eine intelligente 2-Wege Firewall enthalten, die neben dem eingehenden auch den ausgehenden Datenverkehr kontrolliert. Und so dabei hilft, 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 HotSpot, beispielsweise dem der Telekom, sehr ähnlich sind. Bei der Verbindung mit dem falschen HotSpot werden Sie aufgefordert, Informationen wie etwa Ihre Kreditkartennummer anzugeben, angeblich um ein neues HotSpot-Konto zu eröffnen. Diese Manipulationstechnik ist angelehnt an die Phishing-Technik, die in den Punkten „Sicheres Online-Banking“ und „Schutz vor Phishing-Angriffen“ erläutert werden. Als Schutz hilft hier nur die genaue Überprüfung der verwendeten Zertifikate.

Über die richtige Installation und Einrichtung eines sicheren WLAN-Zugangs können Sie sich außerdem unter <http://hilfe.telekom.de> informieren.

Worauf Sie beim mobilen Surfen mit Ihrem Smartphone achten sollten, erfahren Sie im Kapitel „Smartphone“.

Sicheres Online-Banking.

Immer mehr Menschen wickeln ihre Bankgeschäfte über das Internet ab. Praktisch: Diese Bankfiliale ist zu jeder Tages- und Nachtzeit erreichbar und kann bequem von zu Hause oder unterwegs mit dem Smartphone bedient werden.

So bequem das Online-Banking ist, es birgt auch Risiken! Sensible Daten wie die Persönliche Identifikationsnummer (PIN) und die Transaktionsnummer (TAN), die den Zugriff auf das Konto ermöglichen, fallen bei Unachtsamkeit immer wieder Betrügern in die Hände. Dies passiert sehr häufig durch Phishing-Angriffe, die nach Einschätzung des Bundeskriminalamts ein hohes Gefährdungs- und Schadenspotenzial besitzen.

Um Online-Banking möglichst sicher zu gestalten, wurden verschiedene Verfahren entwickelt:

- Chip-TAN-Verfahren: Mit einem kleinen Lesegerät, in das die EC-Karte gesteckt wird, werden für jede Transaktion eigene Transaktionsnummern (TAN) generiert. Die Nummer setzt sich aus dem im Lesegerät angezeigten Zifferncode, der EC-Karte,

der Kontonummer des Empfängers und dem Überweisungsbetrag zusammen. Werden Bestandteile des Codes wie zum Beispiel die Kontonummer des Empfängers geändert, bricht das System die Überweisung ab.

- Mobile-TAN-Verfahren: Der Kunde hinterlegt bei seiner Bank seine Handynummer. Will er eine Online-Überweisung tätigen, bekommt er eine SMS mit einer speziell für diese Transaktion gültigen TAN. Die TAN ist zeitlich begrenzt einsetzbar und gilt nur für die online eingegebenen Zielkonto-Daten und den eingegebenen Betrag.
- Die Secoder-Technik ist die neueste Sicherheitsentwicklung im Bereich Online-Banking. Der Secoder wirkt quasi wie eine Firewall für Chipkartenanwendungen. Möchten Sie das neue Secoder-Verfahren verwenden, fragen Sie bitte Ihre Bank, ob die Secoder-Funktionen schon unterstützt werden.
- Alternativ können Sie auch spezielle Software zum Online-Banking nutzen. Ein Beispiel hierfür ist die Banking Software der Telekom. Diese Software ist kostenlos und bietet den größtmöglichen Schutz vor Pharming und Phishing. Sie funktioniert bei den meisten Online-Banking-Plattformen.

Generelle Vorsichtsmaßnahmen:

- Bewahren Sie Ihre persönlichen Daten wie Passwörter, PIN und TAN immer an einem sicheren Ort auf!
- Speichern Sie diese nie auf Ihrem Computer ab!
- Verraten Sie niemandem Ihr Passwort! Seien Sie misstrauisch; Eine Bank wird Sie niemals per Mail nach Ihren Zugangsdaten fragen. Erhalten Sie dennoch ein Mail mit einer solchen Aufforderung, ist sie mit großer Wahrscheinlichkeit ein Fall von Phishing. Tipps wie Sie sich vor Phishing schützen können finden Sie unter „Phishing“.
- Wählen Sie ein sicheres Passwort! (siehe „Gestaltung eines sicheren Passwortes“)
- Verwenden Sie beim Online-Banking auf jeden Fall ein Passwort, das Sie nicht für andere Zwecke nutzen!

- Ändern Sie das Kennwort regelmäßig, um die Sicherheit zu erhöhen.
- Führen Sie Bankgeschäfte nur vom eigenen Endgerät im privaten Umfeld durch!
- Achten Sie darauf, sich nach Beendigung der Sitzung abzumelden und den Zwischenspeicher (Cache) Ihres Computers zu leeren.
- Wichtig: Benutzen Sie immer eine aktuelle Virenschutzsoftware und führen Sie Sicherheits-Updates durch, 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.
- Sperren Sie Ihren Zugang zum Online-Banking, wenn Ihnen etwas verdächtig oder ungewöhnlich erscheint! Dies können Sie telefonisch bei Ihrer Bank in Auftrag geben oder direkt im Online-Banking-Fenster veranlassen.

Unter der allgemeinen Nummer 116116 können Sie Ihren Online-Banking-Account jederzeit sperren lassen. Auch wenn Sie Ihr Handy, Ihre EC- oder Kreditkarte, Ihren Mitarbeiterausweis oder andere Zugangskarten verlieren, können Sie sie über diese Nummer sperren lassen.

5.4. Online-Shopping.

Bücher, Elektronik, Bekleidung und sogar Lebensmittel – fast alles lässt sich heutzutage in Online-Shops bestellen. Das Geschäft rechnet sich für beide Seiten. Der Käufer erspart sich den Weg zum Laden und zahlt dabei oft sogar weniger Geld. Der Verkäufer spart sich die Ladenmiete und benötigt nur ein Lagerhaus.

Eine Umfrage der Telekom hat ergeben, dass mehr als 80 Prozent der deutschen Internetnutzer ihre Einkäufe gerne bequem per Online-Shopping erledigen.

Was sollte man beim Online-Shopping beachten?

Traue nur dem, den Du kennst. Getreu diesem Grundsatz sollten Sie sich beim Online-Einkauf vorab über einen Shop informieren, in dem Sie einkaufen möchten. Kundenbewertungen und Beurteilungen in Foren können Fehleinschätzungen und möglichen Schäden vorbeugen.

- Achten Sie darauf, dass spätestens beim Einloggen und der Eingabe von Daten die Webadresse des Shops den Zusatz „s“ hinter dem http enthält – dieser weist auf eine sichere Verbindung hin. Wie beispielsweise „<https://www.telekom.de>“.
- Geben Sie die Adresse des Shops immer manuell im Browser ein und folgen nicht einem Link, der Sie eventuell auf eine unsichere Seite führt. So können Sie verhindern, dass Betrüger Ihre Daten und Passwörter abgreifen.
- Das Symbol eines geschlossenen Schlosses weist zusätzlich auf eine sichere Verbindung hin. Dieses befindet sich rechts unten in der Adresszeile des Browsers.
- Wählen Sie auf jeden Fall ein sicheres Passwort für Ihren Shop-Zugang. Wie Sie ein sicheres Passwort erstellen, erfahren Sie unter „Sicheres Passwort erstellen“.
- Verraten Sie niemandem Ihr Passwort! Seien Sie misstrauisch. Ein seriöser Shop wird Sie niemals nach Ihren Zugangsdaten fragen. Erhalten Sie dennoch ein Mail mit einer solchen Aufforderung, ist sie mit großer Wahrscheinlichkeit ein Fall von Phishing. Tipps wie Sie sich vor Phishing schützen können finden Sie unter „Phishing“.
- Wählen Sie eine sichere Zahlungsart, wie Bankeinzug, Rechnung oder Nachnahme. Oder nutzen Sie die Möglichkeit der Zahlung über einen Online-Zahlungsservice..

5.5. Smartphones – so surfen Sie sicher.

Mit Einführung von Smartphones ist das verbrauchte Datenvolumen deutlich gestiegen: Von 0,2 Millionen Gigabyte im Jahr 2005 auf 70 Millionen Gigabyte im Jahr 2010. Keine Frage – Smartphones erleben einen Siegeszug. Mit stetig steigenden

Verkaufszahlen werden sie allerdings auch ein immer interessanteres Ziel für Viren und andere Schadsoftware.

Sicher mobil im Netz – So geht's.

Die beste Software nutzt nichts, wenn sie veraltet ist, also sollten Sie Updates immer zeitnah einspielen. Das fällt leichter, wenn Sie nur die Anwendungen installieren, die Sie wirklich brauchen. Nicht mehr benötigte Anwendungen können Sie einfach deinstallieren.

Basisschutz ist kein Hexenwerk.

Zusätzlich sollten Sie ihr Smartphone immer mit einem Passwort versehen und die automatische Sperrung bei Inaktivität aktivieren. Außerdem können Sie einstellen, dass alle Daten auf dem Endgerät gelöscht werden, wenn das Passwort mehrfach falsch eingegeben wurde. In diesem Fall ist natürlich ein regelmäßiges Backup der eigenen Daten besonders wichtig; bei Smartphones ist es die Regel, dass beim Datenabgleich (Synchronisation) mit dem PC ein Backup erstellt wird.

Auch das Abschalten der verschiedenen Verbindungsmöglichkeiten wie Bluetooth, WLAN oder UMTS schützt vor ungewollten Eingriffen, wenn gerade keine Verbindungen darüber hergestellt werden müssen. Und es entlastet den Akku.

Wenn Sie nicht wollen, dass Ihr Smartphone Ihren Standort übermittelt, können Sie die Ortungs-Funktionen (z.B. GPS) einfach abschalten.

Sicherheit à la carte.

Smartphones werden mit unterschiedlichen Betriebssystemen betrieben („Windows Mobile“, „Symbian“, „iOS“, „Android“ oder „Windows Phone 7“). Je weiter verbreitet ein System ist, desto attraktiver ist es für Angreifer. Wie Sie welches System am besten schützen können, erfahren Sie unter www.telekom.com/ratgeber.

Daten von alten Endgeräten löschen.

Mit dem Kauf eines neuen Mobiltelefons stellt sich die Frage: Was tun mit dem alten Gerät? Die meisten landen entweder in der Schublade, werden an Familienmitglieder oder Freunde verschenkt oder verkauft. Aber was passiert mit den persönlichen Daten auf dem alten Handy? Reicht es, wenn sie gelöscht werden? Um sicherzugehen, dass Fremde Ihre entfernten Daten nicht

wieder herstellen können, sollte das Gerät am besten durch Überschreiben vollständig gelöscht werden. Dies geschieht bei unterschiedlichen Betriebssystemen auf verschiedene Art und Weise. Wie Sie private Daten von Ihrem Endgerät final löschen können, erfahren Sie unter www.telekom.com/ratgeber

5.6. So nutzen Sie Apps sicher.

Applications – kurz Apps – können eine ganze Menge: Schnell die nächste S-Bahn herausuchen, die aktuelle Wettervorhersage mitteilen oder Wartezeiten durch Mini-Spiele verkürzen. Einfache Tipps helfen, Apps sicher zu nutzen.

Was muss ich bei der Nutzung von Apps beachten?

Bei der Installation einer App wird meist angezeigt, auf welche Daten diese zugreifen kann. Damit die Anwendung Daten empfangen und versenden kann, steht dabei die Internetverbindung meist an erster Stelle. Einige Programme verlangen aber deutlich mehr Zugriff, zum Beispiel auf das Telefonbuch, Anrufprotokolle oder den Standort. Die meisten Smartphones bieten im Menüpunkt „Einstellungen“ die Möglichkeit, bestimmte Datenverarbeitungen, etwa den Export von Standortdaten, zu unterbinden. In manchen Fällen erlauben die Betriebssysteme aber keine Auswahl. Hier muss man sich auf die Weitergabe der Daten einlassen, oder auf die Installation der Software verzichten.

Problematisch: Apps, die etwa Vollzugriff auf das Telefonbuch erhalten. Die meisten Nutzer verwalten hier nicht nur Telefonnummern, sondern auch (E-Mail-) Adressen, Geburtstage oder Bilder ihrer Freunde oder Geschäftspartner. Im ungünstigsten Fall können diese Daten unbemerkt zum App-Entwickler weitergeleitet werden.

Wenn Sie sicher gehen wollen, lesen Sie sich vor der Installation die Informationen zur jeweiligen App durch. Besonders die zum Thema Datenschutz. Entscheiden Sie dann, ob Sie bereit sind, auf die Bedingungen des Entwicklers einzugehen.

Sollten Sie eine Verarbeitung Ihrer Daten feststellen, die weder im System angezeigt noch in den Nutzerinformationen aufgeführt wird, sollten Sie dies direkt an die Hotline des Anbieters des App-Stores melden. Die meisten App-Stores haben Regelungen, die eine heimliche Datenverarbeitung verbieten.

5.7. Spurenlos im Netz.

Cookies, IP Adressen ©, temporäre Internetdateien, Flash-Objekte, eindeutige Browserkennung, aufgerufene Websites und abgespeicherte Passwörter sind nur einige Spuren, die ein Nutzer im Netz oder auf seinem Rechner hinterlässt. Um sich und Ihre Daten vor diesem Sicherheitsrisiko zu schützen, sollten Sie einmal pro Monat umfassend aufräumen und Ihren Rechner von diesen Daten säubern. Wir sagen Ihnen, wie's geht.

Cookies löschen.

Web-Cookies sind weit verbreitet – ganze Internetseiten basieren darauf und funktionieren ohne sie nicht nutzerfreundlich. Cookies sind kleine Dateien, die von einer Internetseite auf Ihrem Computer gespeichert werden und Informationen wie beispielsweise persönliche Seiteneinstellungen, Anmeldeinformationen oder eine eindeutige Nutzerkennung enthalten. Damit kann das Surfen komfortabler werden.

Wenn Sie bei einem Online-Shop den Warenkorb benutzen oder die Sprache einer Webseite wechseln, werden hierzu Cookies verwendet. Doch Cookies können auch dazu dienen, ein vollständiges, personalisiertes Benutzerprofil anzulegen. Neben Web-Cookies gibt es Flash-Cookies und Super-Cookies, mit denen Informationen von einem Web- oder Werbeanbieter gespeichert



und abgerufen werden können. Wer das verhindern will, kann in den gängigen Browsern wie Internet Explorer, Firefox oder Opera für bestimmte Cookies selbst bestimmen, welche er akzeptiert und welche nicht. Bestimmte Browser bieten bereits heute die Möglichkeit, den Web- und Werbeanbietern von vornherein mitzuteilen, dass man nicht verfolgt werden möchte (siehe Screenshot Seite 64). Dieses Verfahren beruht auf der Do Not Track Standardisierungsinitiative, die von der Telekom und allen gängigen Browseranbietern unterstützt wird.

Wie Sie Cookies in Ihrem Browser blockieren können, erfahren Sie unter www.telekom.com/ratgeber

Kleine Helfer.

Es ist nicht einfach, alle Verkehrs- und Nutzungsdaten und Informationen zu finden und zu löschen. Aber es gibt Programme, die diese Arbeit fast komplett für Sie übernehmen:

▪ Spybot Search&Destroy

Der Malware-Schutz erkennt verschiedene Formen von Spyware, die sich auf dem Rechner einschleichen und versuchen, die Surfgewohnheiten des Nutzers auszuspionieren. Das Programm löscht alle Gebrauchsspuren wie etwa Surf- und Download-Verzeichnisse. Außerdem schließt es undichte Stellen im Browser und blockiert Einfallstore für Schadsoftware und bössartige Websites.

<http://www.safer-networking.org/de/mirrors/index.html>

▪ Ccleaner

Das Reinigungsprogramm versucht, überflüssige und potenziell verräterische Informationen vom Computer zu löschen. Es durchsucht unter anderem die zentrale Windows-Datenbank und Verzeichnisse, in denen typischerweise Daten wie Cookies abgelegt werden.

<http://www.piriform.com/ccleaner/download/standard>

Und was kann ich tun, wenn doch Informationen über mich im Netz stehen, die ich dort nicht haben will?

Fotos aus der Schulzeit, von wilden Partys, dem letzten Urlaub oder vom Wochenende: In sozialen Netzwerken teilen viele gern ihre Erinnerungen mit Freunden. Was kann man aber tun, wenn man selbst auf einem der Fotos abgelichtet ist und das Erlebte nicht mit anderen teilen möchte? Und woher weiß man, was im Internet über einen steht? Alle 1,5 bis 2 Sekunden wird irgendwo

auf der Welt eine neue Internetadresse registriert. Bei Millionen von Websites ist es schier unmöglich, den Überblick über veröffentlichte Informationen zu behalten.

In Kooperation mit der Deutschen Telekom AG startete mit www.rufnotse.de ein Dienst, der unliebsame Informationen aus dem Internet findet, auswertet und löschen lässt.

Das kostenpflichtige Angebot richtet sich an Privatpersonen, Eltern, Selbstständige und Firmen, die ein umfassendes Bild über ihr „Online-Ich“ haben möchten.

Anonym surfen mit IPv6.

Mit der Einführung des neuen Internetstandards IPv6 wird es künftig 340 Sextillionen neue IP-Adressen geben – genügend, um alle denkbaren Endgeräte weltweit mit einer dauerhaften IP-Adressen zu versorgen und sie damit auch klar einem Nutzer zuzuordnen.

Für anonymes Surfen mit dem neuen Internetstandard IPv6 hat die Deutsche Telekom eine Lösung entwickelt. Sie als Nutzer können dabei ab 2013 selbst entscheiden, wie anonym Sie durchs Netz surfen möchten. Die neuen IPv6-Adressen bestehen aus zwei Teilen: Der so genannten Netzpräfix, die vom Netzprovider zugeteilt wird, und dem Endgeräte-Anteil. Die Telekom-Lösung setzt in drei Schritten an beiden Teilen an:

- Grundschatz: Ist Ihr Endgerät an einen aktuellen Telekom-Router angeschlossen, erhält das Gerät regelmäßig einen Netzpräfix. Dieser wird nach dem Zufallsprinzip erstellt. Diese Funktion ist werksseitig in den Routern voreingestellt.
- Privacy Button: Auf den Webseiten (Firmware-Einstellungen des Routers) der von der Telekom vertriebenen Kundenrouter (Speedport) wird ein so genannter „Privacy Button“ installiert werden. Wird dieser angeklickt, erhalten Sie ein vollständig neues Netzpräfix. Diese Neuvergabe können Sie manuell vornehmen oder automatisch zu einem festgelegten Zeitpunkt.
- Privacy Extension: Zusätzlich wird auf den meisten modernen Endgeräten der zweite Teil der IP-Adresse, der Endgeräte-Anteil, automatisch durch eine Zufallslogik verschleiert. Bitte achten Sie immer darauf, dass diese Funktion auf Ihrem jeweiligen Endgerät aktiviert ist.

5.7. Phishing.

Durch gefälschte E-Mails und Internetseiten gelangen Kriminelle an sensible Daten: Sie angeln Passwörter sowie PINs und TANs.

Phishing ist eine Wortzusammensetzung aus den Begriffen „Password“ und „Fishing“ und bezeichnet das Abgreifen von Passwörtern sowie Persönlicher Identifikationsnummern (PIN) und Transaktionsnummern (TAN). 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. Um sich vor diesen Angriffen zu schützen, achten Sie auf die folgenden Punkte:

Schutz vor Phishing-Angriffen.

- Merken Sie sich die Unternehmen, mit denen Sie Geschäfte tätigen. Gehört der Absender nicht dazu, ist die E-Mail vielleicht betrügerischen Ursprungs und in jedem Fall Spam.
- Beachten Sie den Betreff: Banken und E-Mail-Provider werden für Rundschreiben niemals einen Betreff wie „Ihre_Konto_Überprüfung_JETZT“ benutzen.
- Sie können von einem Dienstleistungsunternehmen erwarten, dass man Ihren Namen kennt. Die meisten Phishing-Mails sind unpersönlich und enthalten höchstens Anreden, wie zum Beispiel „Sehr geehrtes Mitglied“ oder „Lieber Kunde der XY Bank“.
- Bei der Kommunikation folgen Dienstleistungsunternehmen bestimmten Regeln. 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 fragen Sie nach.
- Rechtschreib- oder Grammatikfehler sind in E-Mails generell nicht auszuschließen. Jedoch sollte alles, was über die Anzahl von einem Fehler hinausgeht, zu besonderer Vorsicht mahnen.
- Falsche oder fehlende Umlaute (ae anstatt ä) sind häufig ein Warnsignal.

- Ebenso unsinnig sind Aufforderungen, Schutzvorrichtungen wie Popup-Blocker oder Virens Scanner zu deaktivieren.
- Ziehen Sie mit dem Mauszeiger immer über die angegebenen Links, da auf diese Weise häufig die Zieladresse in der Statusleiste am Fensterboden erscheint. So können Sie prüfen, ob Sie der Link tatsächlich auf die gewünschte Seite führt.
- Aktivieren Sie die Phishing-Schutzvorrichtungen Ihres Browser-Programms. Standardmäßig sind die Browser ab Firefox 3 sowie Opera 9.5 und Internet Explorer 7 damit ausgerüstet.
- Immer wenn Sie persönliche Daten online eingeben möchten, sollten Sie ein neues Browser-Fenster öffnen. Nach Beendigung der Transaktion loggen Sie sich am besten sofort aus und schließen das Fenster.

Der beste Schutz vor Phishing-Mails: Ungelesen löschen!

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.
- Vorsicht bei unbekanntem Sicherheitszertifikaten! Zertifikate von Banken und seriösen Online-Shops sind den gängigen Browsern bekannt. Wenden Sie sich an Ihre Bank bzw. den Online-Shop, bevor sie das Zertifikat akzeptieren.
- Um sicherzugehen, dass Sie auf einer echten Seite sind, geben Sie die Adresse Ihrer Bank immer selbstständig in die Adresszeile Ihres Browsers ein und folgen keinem Link.
- Auf der Login-Seite werden von Ihrer Bank nie TAN-Codes abgefragt. Sollte das der Fall sein, setzen Sie sich bitte unverzüglich mit Ihrer Bank in Verbindung.



Unabhängige Webseiten informieren über die aktuelle Phishing-Gefahr.

Phishing-Radar.

Um Verbrauchern eine Möglichkeit zu geben, sich über Risiken zu informieren und Betrugsversuche schnell und unbürokratisch zu melden, haben das Bundesverbraucherministerium und die Verbraucherzentrale Nordrhein-Westfalen unter www.verbraucherfinanzwissen.de ein Phishing-Radar eingerichtet. Dort können Sie in einem Forum Phishing-Mails melden und so andere Nutzer warnen oder eine E-Mail mit einem Hinweis auf die Phishing-Mail an die Verbraucherzentrale senden.

5.8. Social Engineering.

Betrüger nutzen gezielt menschliche Eigenschaften und Schwächen, um an sensible Daten zu gelangen.

Was ist Social Engineering?

Social Engineering („Soziale Manipulation“) hat das Ziel, durch zwischenmenschliche Beeinflussung unberechtigt an private und sensible Daten zu gelangen. Täter spionieren das persönliche Umfeld ihrer Opfer aus und täuschen falsche Identitäten vor.

Wie kann ich mich dagegen wehren?

Die Abwehr von Social Engineering ist nicht leicht, da der Angreifer im Grunde positive menschliche Eigenschaften ausnutzt: Den

wichtigsten Beitrag zur Bekämpfung von Social Engineering liefert deshalb im konkreten Fall das Opfer selbst, indem es Identität und Berechtigung eines Ansprechenden zweifellos sicherstellt, bevor es weitere Handlungen vornimmt. Bereits die Rückfrage nach Name und Telefonnummer des Anrufers oder dem Befinden eines nicht existierenden Kollegen kann schlecht informierte Angreifer enttarnen. Auch scheinbar geringfügige und nutzlose Informationen sollten Unbekannten nicht offengelegt werden, denn sie könnten zusammen mit weiteren Angaben zum Abgrenzen eines größeren Sachverhalts dienen. Wichtig ist eine schnelle Warnung aller potenziellen weiteren Opfer; Erste Ansprechpartner sind die Sicherheitsabteilung des Unternehmens, die Kontaktadresse des E-Mail-Providers und Mitmenschen, deren Angaben zur Vorspiegelung falscher Tatsachen missbraucht wurden.

Folgende Punkte sollten Sie beachten:

- Ist die Identität des Absenders einer E-Mail nicht sicher, sollten sie stets misstrauisch sein.
- Bei Anrufen sollten auch scheinbar unwichtige Daten nicht sorglos an Unbekannte weitergegeben werden, da diese die so erhaltenen Informationen für weitere Angriffe nutzen können.
- Bei Antworten auf eine E-Mail-Anfrage sollten unter keinen Umständen persönliche oder finanzielle Daten preisgegeben werden, egal von wem die Nachricht zu kommen scheint.
- Keine Links aus E-Mails verwenden, die persönliche Daten als Eingabe verlangen. Stattdessen die URL selbst im Browser eingeben.
- Bei Unklarheit über die Echtheit des Absenders diesen nochmals telefonisch kontaktieren, um die Authentizität der E-Mail zu überprüfen.

Bot-Netze.

Ist Ihr Rechner Teil eines Bot-Netzes, kann er unbemerkt von Cyberkriminellen ferngesteuert werden und zum Beispiel Spam versenden oder andere Computer infizieren, wenn Sie online sind. Bot-Netze gelten als Grundlage von Internetkriminalität und sind eine der größten illegalen Einnahmequellen im Internet. Sie sind Netzwerke aus Computern, die nach einer Infektion mit Schadsoftware zusammengeschlossen werden.

Um sich und andere vor solchen Angriffen zu schützen, beachten Sie folgende Hinweise des Anti-Botnet-Beratungszentrums (www.botfrei.de/telekom):

- Überprüfen Sie Ihren Rechner auf Befall. Der DE-Cleaner auf www.botfrei.de/telekom findet mögliche Schädlinge und löscht sie.
- Installieren Sie aktuelle Service-Packs und Sicherheitsupdates für Ihr System und aktivieren Sie automatische Updates.
- Installieren Sie einen Virenschanner und aktualisieren Sie ihn regelmäßig.
- Verwenden Sie eine Firewall.

Unter www.botfrei.de/telekom erklärt das Anti-Botnet-Beratungszentrum des Bundesamts für Sicherheit in der Informationstechnik was Bot-Netze sind, welche Gefahren von ihnen ausgehen und wie man sich vor ihnen schützen kann.

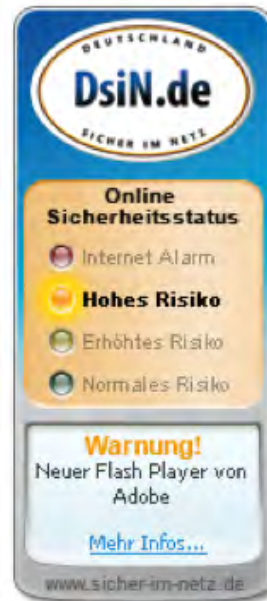
In den Rubriken „Informieren“, „Säubern“ und „Vorbeugen“ finden Sie alle Informationen, die Sie brauchen, um Ihren Computer dauerhaft gegen Schadprogramme zu sichern.

5.9. Das Sicherheitsbarometer.

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

Unter www.sicher-im-netz.de zeigt das Barometer die aktuelle Gefahrenlage in vier Stufen an:

- Die Stufe Blau wird als „Normales Risiko“ bezeichnet und informiert, wie sich Nutzer schützen sollten, damit der Grundschutz möglichst hoch ist.
- Die Stufe Grün wird als „Erhöhtes Risiko“ bezeichnet und soll vor akuten Bedrohungen warnen, deren Verbreitung oder Schadensausmaß allerdings begrenzt sind. Beispiele sind Phishing- oder Pharming-Angriffe von begrenztem Ausmaß.



- Die Stufe Gelb 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.

Unter www.t-online.de/sicherheit, den Serviceseiten der Deutschen Telekom, erhalten Sie Tipps, wie Sie sich gegen mögliche Gefahren schützen können. In Zeiten normaler

Risikolage, das heißt, wenn keine akuten Warnungen vorliegen, informiert Sie das Barometer über Basis-Sicherheitsmaßnahmen und sensibilisiert für aktuelle sicherheitsrelevante Themen oder Bedrohungen.

5.10. Verhalten im Sozialen Netzwerk.

Durch das Web 2.0 haben die Sozialen Netzwerke Einzug in unseren Alltag gehalten. Aber was sollte man dort beachten? Xing, Facebook, Google+, MySpace, StudiVZ und wie sie alle heißen. Um mit Freunden, Bekannten und Kollegen in Kontakt zu treten, geben viele in Sozialen Netzwerken wie selbstverständlich private Daten preis.

Das Internet ist zwar kein rechtsfreier Raum. Dennoch halten sich nicht alle an die geltenden Regeln, und vor allem gelten nicht in jedem Land dieselben Regeln: Datenschutzbestimmungen, das Recht am eigenen Bild oder Urheberrechte werden oft nicht ganz so ernst genommen. Deshalb ist es wichtig, sich vorab die Allgemeinen Geschäftsbedingungen und Datenschutzhinweise der Plattform-Betreiber genau anzuschauen.

Gestaltung des eigenen Profils.

- In erster Linie gilt es, möglichst keine persönlichen Daten wie E-Mail-Adressen, Telefonnummern, Messenger-Daten, Fotos etc.

allen zugänglich zu veröffentlichen. Denn wer viel über sich verrät, macht es anderen leicht, ihm beispielsweise Phishing-Nachrichten oder unerwünschte Werbung zukommen zu lassen.

- Den Zugriff auf das eigene Profil können Sie bei den Einstellungen einschränken. Am sichersten ist es, nur Freunden den Zugang zu erlauben.

Privatsphäre.

- Machen Sie sich mit den Privatsphäre-Einstellungen des Netzwerkes vertraut. Wie Sie in den verschiedenen Sozialen Netzwerken Ihre Privatsphäre richtig schützen, können Sie neben den Datenschutzhinweisen und Allgemeinen Geschäftsbedingungen der Community auch unter www.klicksafe.de nachlesen.
- Persönliche Daten sollten nur echten Freunden zugänglich gemacht werden.
- Manche Netzwerke bieten die Möglichkeit, Freunde in verschiedene Gruppen einzuteilen und ihnen unterschiedliche Freigaben zuzuteilen. So können Sie kontrollieren, wer welche Informationen einsehen kann.

Profilbilder und Fotoalben.

- Auch wenn es mittlerweile fast normal scheint, sich anhand von Fotos im Internet darzustellen, missachten einige Bilder die Regeln zum Schutz der Privatsphäre. Sie sollten sich gut überlegen, welche Fotos von sich Sie im Internet zeigen.
- Wenn Sie Fotoalben erstellen, sollten Sie darauf achten, nur direkten Freunden Zugang zu diesen Alben zu gewähren. Das kann einfach in den Albumeinstellungen vorgenommen werden.
- Grundsätzlich sollte man nur die Fotos hochladen, an denen man 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. (Siehe dazu „Rufnotse“)
- Da Sie selbst bestimmt nicht auf unvorteilhaften Bildern gezeigt werden möchten, sollten Sie auch die Privatsphäre von Freunden



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

und Bekannten respektieren und erst nach Absprache Bilder von ihnen ins Netz stellen. Beziehungsweise diese löschen, wenn man Sie darum bittet.

Freunde hinzufügen.

- Bevor Sie Freundschaftseinladungen annehmen oder an andere verschicken, sollten Sie gründlich prüfen, um wen es sich dabei handelt.

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 offen auf den Pinnwänden angegeben werden. Solche Informationen sollten nur privat, zum Beispiel per E-Mail oder Messenger ausgetauscht werden!

Melde- und Ignorierfunktion.

- Personen, Inhalte oder Gruppen, die gegen den Verhaltenskodex der Netzwerke verstoßen, sollten Sie unbedingt melden. Sie können dafür den Melde-Button auf Ihrer Profseite nutzen.

- 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 bei Ihrem Anbieter melden.

Adressbuch-Synchronisation.

Manche Netzwerke bieten die Möglichkeit, externe E-Mail-Adressbücher mit der Community zu verbinden. Die Seiten können anhand der Daten abgleichen, wer bereits Mitglied im Netzwerk ist und wer (noch) nicht. Was genau dann mit den Daten passiert, und ob und wie sie weiter genutzt werden, ist nicht klar.

Der Ton macht die Musik.

Zu analogen Zeiten gehörte es zur guten Erziehung, den „Knigge“ gelesen zu haben und anwenden zu können. Für die digitale Kommunikation gibt es ebenfalls Kommunikationsregeln: Unter www.eetiquette.de erfahren Sie mehr über virtuelles gutes Benehmen.

5.10. Sicherheit für Kinder im Internet.

Jugendliche zwischen 10 und 18 Jahren sind die am besten vernetzte Altersgruppe, 98 Prozent von ihnen nutzen das Internet. Mit 13 sind die meisten bereits täglich online.

Trotz des gewohnten Umgangs mit der digitalen Welt fehlt vielen Kindern und Jugendlichen das Wissen, wie sie sich und ihre Daten am besten schützen. Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) hat in einer Umfrage unter Jugendlichen herausgefunden, dass jeder Vierte Lücken im Wissen um sichere Daten im Netz hat.

Kein Wunder, dass Eltern um die Sicherheit ihrer Kinder besorgt sind. Um dieser Sorge vorzubeugen, können Sie Ihr Kind für den richtigen Umgang mit dem Internet sensibilisieren:

- Entdecken Sie das Internet gemeinsam!
- Sprechen Sie mit Ihrem Kind über seine Erfahrungen!
- Werfen Sie einen Blick auf den Bildschirm, wenn Ihr Kind am PC sitzt!
- Klären Sie Ihr Kind über mögliche Gefahren des Netzes auf!

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. Die Suchmaschine www.fragfinn.de schafft einen sicheren Surfraum für Kinder.

Kinder und Jugendliche sollten mit dem Umgang des Internets vertraut gemacht werden: Um das Potential des Netzes voll ausschöpfen zu können, brauchen sie neben entsprechenden Fähigkeiten vor allem Schutz!

- Vereinbaren Sie Regeln für die Internetnutzung und informieren Sie über Schutzvorrichtungen.
- Spezielle Filter, die Sie auf Ihrem Computer installieren können, sperren pornografische, gewaltverherrlichende oder rechtsradikale Seiten automatisch. Die Telekom bietet ihren Kunden unter www.telekom.de/kinderschutz software dafür eine kostenlose Lösung an.
- Erklären Sie Ihrem Kind, dass es keinesfalls persönliche Daten weitergeben sollte. Auch bei der Erstellung einer E-Mail-Adresse oder eines Namens für Chaträume sollte Ihr Kind ausschließlich auf Spitznamen zurückgreifen.



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.

- Sprechen Sie mit Ihrem Kind über die Risiken von realen Treffen mit Kontakten aus dem Netz. Im Internet kennengelernte Personen sollte Ihr Kind nur nach Rücksprache mit Ihnen treffen. Kinder können nicht erkennen, ob eine Person gut gemeinte Absichten hat.
- Diskutieren Sie den Wahrheitsgehalt von Inhalten mit Ihren Kindern!
- Ermutigen Sie Ihr Kind zu guter Netiquette! Tipps dazu gibt's unter www.eetiquette.de.
- Weitere umfassende Informationen zum Thema „Kinder sicher im Netz“ finden Sie unter www.klicksafe.de. Im Auftrag der Europäischen Kommission will eine weitere Seite die Medienkompetenz im Umgang mit dem Internet fördern. Unter www.watchyourweb.de finden Kinder, Jugendliche und Eltern Datenschutztipps speziell für Internet-Gemeinschaften.

Weiterführende Infos und Angebote gibt es unter anderem hier:

- www.klick-tipps.net
- www.ein-netz-fuer-kinder.de
- www.fragfinn.de
- www.klicksafe.de
- www.watchyourweb.de
- www.blinde-kuh.de (Suchmaschine)
- www.internauten.de (Kinder-Portal)
- www.jugendinfo.de/cyberbullying (Tipps für Kinder gegen Mobbing)
- www.netzcheckers.de (Jugend-Portal)
- www.schau-hin.info

Funktionierende Schutz-Strukturen müssen wachsen und dabei gepflegt werden.

Die Deutsche Telekom arbeitet kontinuierlich an der Verbesserung von Datenschutz und Datensicherheit.



6.1. Besondere Maßnahmen in Datenschutz und Datensicherheit seit 2008.

Die Deutsche Telekom hat in den vergangenen Jahren und Monaten Maßnahmen entwickelt, die dazu beitragen sollen, das Niveau von Datenschutz und Datensicherheit im Konzern weiter zu erhöhen und entsprechende Systeme und Prozesse permanent zu verbessern.

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. Weiterer Schwerpunkt ist der Austausch mit anderen Unternehmen, Experten und staatlichen Stellen.

Das hat die Deutsche Telekom getan.

- Ende 2011: Vorstellung eines Verfahrens, wonach auch unter IPv6 das Internet weitestgehend anonym genutzt werden kann.
- 2011: Ausweitung des Verfahrens zur Gewährleistung von Datenschutz und Datensicherheit ab dem ersten Planungsschritt von Prozessen und Produkten auf ausländische Tochtergesellschaften.
- Mitte 2010: Einführung eines einheitlichen Sicherheits- und Datenschutzverfahrens mit standardisierten Dokumenten für die deutschen Konzerngesellschaften (PSA-Verfahren).
- Ende 2009: Vorstandsbeschluss zur restriktiven Handhabung von Prozess- und Einzelfallprüfungen im Mitarbeiterumfeld über § 32 BDSG hinaus.
- Mitte 2009: Etablierung einer eigenen Einheit, die sich ausschließlich auf Auditierungen zum Datenschutz spezialisiert.
- Februar 2009: Einrichtung eines Datenschutzbeirats mit führenden Datenschutzexperten aus Politik, Lehre, Wirtschaft und unabhängigen Organisationen.

- Veröffentlichung eines Datenschutzreports unter www.telekom.com/datenschutz, der über sämtliche aktuellen Vorkommnisse informiert.
- Frühjahr 2009: Veröffentlichung des ersten Datenschutzberichts als erster DAX 30-Konzern. Ziel: offene, transparente Kommunikation der Datenvorfälle und Maßnahmen zum Datenschutz.
- Neuausrichtung der Konzernsicherheit und der Steuerungsstrukturen „Vier-Augen-Prinzip“.
- 10-Punkte-Sofortmaßnahmenprogramm (März 2009).
- Oktober 2008: Schaffung des Vorstandsressorts Datenschutz, Recht, Compliance als erster DAX 30-Konzern. Mittlerweile sind andere DAX 30-Konzerne nachgezogen.

Verbesserter Datenschutz.

- Abschalten unsicherer Systeme.
- Einführung von Systembeschränkungen bei abgehenden Kundenanrufen durch Call Center, 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-Systemen, 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.

Austausch und Kooperation.

- Expertenaustausch über nationale und internationale Computer Emergency Response Teams.
- Teilen von Analysen aus Angriffen auf die dafür eingerichteten Frühwarnsysteme der Telekom.
- Meldung von erkannter Schadsoftware an Anti-Viren-Industrie.
- Teilen von Know How für Einrichtung des Cyber-Abwehrzentrums.
- Expertenbeteiligung an Sicherheitsübung „LÜKEX“.

Sensibilisierung der Öffentlichkeit.

- Kostenlose Datenschutzbroschüre unter www.telekom.com/datenschutz
- Neukonzeption und Erweiterung des Online-Angebots zu Datenschutz und Datensicherheit auf www.telekom.com
- Vorträge an Schulen zum sicheren Surfen im Netz.
- 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 Schadsoftware verseucht sind.
- Regelmäßige Radiobeiträge mit Tipps zum sicheren Surfen im Netz etc.
- Chat zu Datenschutz und Datensicherheit.

6.2. 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 Datenschutzschnittstellen 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 Richtlinien, Datenschutzanforderungen und Schulungen 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 recht-

lichen 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 Personalschutzes und des Schutzes von personenbezogenen Daten Dritter, die nicht Kunden 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.

6.3. 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, Aggregationssysteme 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.

6.4. 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.

Auskunftersuchen.

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.

Botnetze.

Botnetze sind Netzwerke aus Computern, die nach der Infektion mit Schadsoftware zusammengeschlossen werden. Ist ein Computer Teil eines Botnetzes, kann er unbemerkt auf ferngesteuerte Befehle von Cyberkriminellen reagieren und zum Beispiel Spam versenden oder andere Computer infizieren, wenn sie online sind.

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.

Call Center.

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/Dynamic Computing.

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.

Data Breach Notification.

„Data Breach Notification“ bezeichnet die Verständigung von Betroffenen bei Verletzung der Sicherheit personenbezogener Daten oder bei deren Missbrauch. Europäische Unternehmen unterliegen rechtlich der so genannten "Data Breach Notification Duty", einer Melde- und Informationspflicht gegenüber Aufsichtsbehörden und Kunden auf Grundlage einer EU-Richtlinie.

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.

Denial-of-Service-Angriffe.

Denial-of-Service-Angriffe sind Attacken aus dem Netz, die auf eine digitale Überlastung von Infrastruktursystemen abzielt, die in deren Folge zusammenbrechen.

Datenschutzkonzept.

Ein Datenschutzkonzept ist ein Dokument, das Auskunft über die Rechtmäßigkeit der Datenverarbeitung bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten enthält. Es gehört neben Fach-, Betriebs- und Sicherheitskonzept zur Dokumentation eines IT-Systems.

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.

Drive-by 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 Geooanwendungen einbinden, um so die Daten in interaktiven Karten darzustellen oder weiterzuverarbeiten. Beispiele für Geodatendienste sind Google Street View oder Microsoft Bing.

Forschungsunion.

Die Forschungsunion Wirtschaft – Wissenschaft ist das zentrale innovationspolitische Beratungsgremium zur begleitenden Umsetzung und Weiterentwicklung der Hightech-Strategie 2020 der deutschen Bundesregierung.

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.

Penetrationstest.

Ein Penetrationstest ist ein umfassender Sicherheitstest, um die Sicherheit möglichst aller Bestandteile und Anwendungen eines Netzwerks- oder Softwaresystems zu prüfen. Dazu setzen Sicherheitsexperten Werkzeuge und Methoden ein, die auch so genannte Hacker nutzen, um unbefugt in das System eindringen zu können (Penetration).

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 zu- beziehungsweise abgeschaltet werden.

Smart Metering.

Der Service umfasst das Auslesen, Verarbeiten, Darstellen sowie Fakturieren des Verbrauchs von Strom und 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.

Telekommunikationsgesetz.

Das Telekommunikationsgesetz ist die Rahmenrichtlinie für Telekommunikationsnetze und -dienste. Es regelt den Telekommunikationsmarkt und sorgt unter anderem für den allgemeinen öffentlichen Schutz und den individuellen Kundenschutz. Das Telekommunikationsgesetz legt darüber hinaus die Zuteilung von Frequenzen, die Nummerierung oder auch die Zulassung von Mehrwertdienstleistungen wie etwa 0900-Nummern fest.

Verkehrsdaten.

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

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 können.

6.5. 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 Vertriebsgesellschaft

Impressum.

Deutsche Telekom AG
Corporate Communications
D-53262 Bonn
Telefon 0228 181 4949
Telefax 0228 181 94004
www.telekom.com

Konzept:

Deutsche Telekom AG und
Beecken's Agentur für
Unternehmens-Kommunikation GmbH, Düsseldorf

Gestaltung und Produktion:

Beecken's Agentur für
Unternehmens-Kommunikation GmbH, Düsseldorf

Fotos:

Deutsche Telekom AG, Fotolia

Druck:

INDUSTRIEDRUCK GmbH, Ottendorf-Okrilla

KNr. 642 200 227

Kontakt.

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

Erleben, was verbindet.

