Dr. rer. nat. Susanne Pedersen

Der gläserne Bürger und Patient

„e“ wie „electronic“

Die Möglichkeiten des World Wide Webs in Verbindung mit anderen Informationstechnologien scheinen unbegrenzt. Hardware ist so günstig wie noch nie. Die Rechner können über Funkverbindungen inzwischen ohne Probleme kabellos miteinander vernetzt werden. Über das Internet gelingt dies weltweit. Problemlos? Wohl kaum, wenn es um Datenschutz und Datensicherheit geht. Die bequemen Funkverbindungen lassen sich relativ leicht „abhören“ und damit ausspionieren. Mit der so genannten IP-Adresse des Rechners hinterlässt jeder Nutzer im Internet Spuren. Kaum einem User ist bewusst, welche Aktionen im Netz protokolliert werden, wie Persönlichkeitsprofile von diesem erstellt werden und wo des Anwenders oftmals unachtsam eingegebenen Daten gespeichert und weiterverteilt werden.

Datenschutz

Datenschutz bezeichnete ursprünglich den Schutz personenbezogener Daten vor Missbrauch. Der Begriff wurde gleichgesetzt mit Schutz der Daten, Schutz vor Daten oder auch Schutz vor „Verdatung“. Im englischen Sprachraum spricht man von „privacy“ (Schutz der Privatsphäre) und von „data privacy“ (Datenschutz im engeren Sinne). Im europäischen Rechtsraum wird in der Gesetzgebung der Begriff „data protection” verwendet.

Heute wird der Zweck des Datenschutzes darin gesehen, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt wird. Datenschutz steht für die Idee, dass jeder Mensch grundsätzlich selbst entscheiden kann, wem wann welche seiner persönlichen Daten zugänglich sein sollen.

> Der Datenschutz will den so genannten gläsernen Menschen verhindern.

Die Bedeutung des Datenschutzes ist seit der Entwicklung der Digitaltechnik stetig gestiegen, weil Datenerfassung, Datenhaltung, Datenweitergabe und Datenanalyse immer einfacher werden. Technische Entwicklungen wie Internet, E-Mail, Mobiltelefonie, Videoüberwachung und elektronische Zahlungsmethoden schaffen neue Möglichkeiten zur Datenerfassung. Interesse an personenbezogenen Informationen haben sowohl staatliche Stellen als auch private Unternehmen. Sicherheitsbehörden möchten beispielsweise durch Rasterfahndung und Telekommunikationsüberwachung die Verbrechensbekämpfung verbessern, Finanzbehörden sind an Banktransaktionen interessiert, um Steuerdelikte aufzudecken. Unternehmen versprechen sich von Mitarbeiterüberwachung (Arbeitnehmerdatenschutz) höhere Effizienz, Kundenprofile sollen beim Marketing helfen und Auskunfteien die Zahlungsfähigkeit der Kunden sicherstellen (Verbraucherdatenschutz, Schufa, Kreditreform). Dieser Entwicklung steht eine gewisse Gleichgültigkeit großer Teile der Bevölkerung gegenüber, in deren Augen der Datenschutz keine oder nur geringe praktische Bedeutung hat.

Vor allem durch die weltweite Vernetzung, insbesondere durch das Internet, nehmen die Gefahren hinsichtlich des Schutzes personenbezogener Daten laufend zu („Das Internet vergisst nicht.“). Datenschützer müssen sich deshalb zunehmend mit den grundlegenden Fragen des technischen Datenschutzes (Datensicherheit) auseinandersetzen, wenn sie Erfolg haben wollen.

Datensicherheit

Datensicherheit hat das Ziel, Daten jeglicher Art in ausreichendem Maße vor Verlust, Manipulationen, unberechtigter Kenntnisnahme durch Dritte und anderen Bedrohungen zu schützen. Dabei unterscheidet man in der Regel die Schutzziele Vertraulichkeit, Verfügbarkeit, Integrität und Verbindlichkeit. Anforderungen zu Datensicherheit von personenbezogenen Daten ergeben sich aus dem gesetzlichen Datenschutz, der in Deutschland im Bundesdatenschutzgesetz (BDSG) geregelt ist. Datensicherheit umfasst aber auch andere Daten, z. B. Vertragsdaten, Bilanzdaten oder Forschungsergebnisse.

> Datensicherheit ist eine Voraussetzung für Datenschutz.

Nur wenn geeignete Schutzmaßnahmen getroffen werden, kann man davon ausgehen, dass vertrauliche bzw. personenbezogene Daten nicht in die Hände von Unbefugten gelangen. Hierbei spricht man in der Regel von technischen und organisatorischen Maßnahmen zum Datenschutz, welche auch in der Anlage zum § 9 BDSG beschrieben sind. Häufig befindet sich eine Beschreibung der Datensicherheit in einem Datenschutzkonzept oder Sicherheitskonzept.

Maßnahmen zur Datensicherheit umfassen unter anderem die physische bzw. räumliche Sicherung von Daten, Zugriffskontrollen, das Aufstellen fehlertoleranter Systeme und Maßnahmen der Datensicherung und die Verschlüsselung. Wichtige Voraussetzung ist die Sicherheit der verarbeitenden Systeme. Ein effektives Sicherheitskonzept berücksichtigt jedoch neben technischen Maßnahmen auch organisatorische und personelle Maßnahmen, wie z. B. das Schaffen geeigneter Organisations- und Managementstrukturen oder die Schulung und Sensibilisierung von Personen.

Einzug des „e“ wie „electronic“ in viele Bereiche

Die Möglichkeiten der Vernetzung, des Internet, des Mobilfunks usw. finden inzwischen Einzug in vielen Bereichen des Lebens. Dies verbirgt sich letztlich hinter den Schlagworten eBusiness, eCommerce, eBanking, eLearning, eGovernment und eHealth, um nur ein paar wichtige Gebiete zu nennen. In dieser Richtung wird in den nächsten Jahrzehnten einiges auf uns zukommen. Die Vorteile sind verlockend, aber werden auch immer der Datenschutz und die Datensicherheit optimal sichergestellt?

Beispiel E-Government

Einheitliche Steuer-Identifikationsnummer

Ab 2006 wird für jeden Einwohner der Bundesrepublik Deutschland eine einheitliche Steuer-Identifikationsnummer vergeben, die ihn von der Geburt bis zum Tode begleitet.

Arbeits- und Sozialämter können seit 1999 beim Bundesamt für Finanzen anfragen, ob Bezieher von sozialen Leistungen ihren Banken Freistellungsaufträge erteilt haben. Alle Geldinstitute müssen nämlich dieser Behörde die Freistellungsaufträge ihrer Kunden melden. Über die Höhe des angelegten Geldes oder Höhe der Freistellungsaufträge wird da-

Dr. rer. nat.
Susanne Pedersen

Studium der Wirtschaftsmathematik in Ulm, seit 1999 in eigener Praxis als Heilpraktikerin mit den Schwerpunkten Elektroakupunktur nach Dr. Voll, Orthomolekulare Medizin, Ausdauersport- und Dorntherapie tätig. Durch enge Zusammenarbeit mit der Zahnarztpraxis ihres Mannes Dr. med. dent. Jürgen Pedersen Einbeziehung von Zähnen und zahnärztlichen Werkstoffen in Diagnostik und Therapie. 2005 Promotion in Medizininformatik zum Dr. rer. nat. mit dem Schwerpunkt „Interoperabilität im Gesundheitswesen". Sie betreut in CO'MED die ständige Rubrik „Gesundheitspolitik".

Kontakt:
Quellental 2, D-26340 Neuenburg
Tel.: 04452 / 1299
praxis.pedersen@t-online.de

bei keine Auskunft gegeben. Ausgelöst durch die Terroranschläge in den USA am 11. September 2001 wurde diese Regelung auf Kontenstammdaten im Jahr 2002 erweitert. Seither müssen alle Geldinstitute einer Konten-Evidenz-Zentrale (KEZ) sämtliche Konten und Depots aller Bankkunden melden. Zu den Kontenstammdaten zählen im Moment Name und Adresse des Kontoinhabers, das Geburtsdatum, Verfügungsberechtigte sowie Zeitpunkt von Eröffnung / Schließung und die Art des Kontos. Der Kontoinhaber wird „netterweise" nachträglich informiert, ob die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) über die KEZ bei den Banken eine Abfrage der Kontostammdaten getätigt hat. Seit 2004 sind alle Geldinstitute verpflichtet, allen Inhabern der etwa 500 Millionen Konten jährlich eine Aufstellung über alle Kapitaleinkünfte (Zinsen aus Sparbüchern und Bundesschatzbriefen, Dividenden usw.) auszustellen. Diese „Erträgnisaufstellung" wird allen Kunden automatisch einmal im Jahr zugeschickt, die Banken melden die Kapitaleinkünfte nicht dem Finanzamt, sondern dem Kunden. Die Finanzämter sind aber berechtigt, die Aufstellung von jedem Steuerpflichtigen einzufordern.

Die KEZ erhält durch die einheitliche Steuer-Identifikationsnummer extrem viele neue Möglichkeiten des schnellen Datenabgleichs. So haben eben nicht nur Finanzämter Zugriff auf die Daten der KEZ, sondern beispielsweise auch Sozialämter und Arbeitsagenturen. Die Daten müssen täglich aktualisiert zum automatisierten Zugriff bereitgehalten werden. Eine beunruhigende Vorstellung!

eCard-Strategie der Bundesregierung

Die Bundesregierung plant mit dieser Strategie eine einheitliche und abgestimmte Nutzung von Chipkarten im eGovernment, eBusiness und im elektronischen Rechtsverkehr. Als wesentliche Stützpfeiler werden die qualifizierte elektronische Signatur und die elektronische Authentisierung genannt. Eine elektronische Signatur ist quasi eine digitale Unterschrift.

Eine qualifizierte elektronische Signatur ist eine elektronische Unterschrift, die ein Zertifikat („öffentlicher Schlüssel") von einem verlässlichen Zertifizierungsdienst verwendet. Unter einem Zertifikat ist dabei eine elektronische Bescheinigung zu verstehen, mit der ein Signaturprüfschlüssel einer Person zugeordnet und die Identität dieser Person bestätigt werden kann (vgl. § 2 Nr. 6 Signaturgesetz). Für die qualifizierte elektronische Signatur muss der Zertifizierungsanbieter nach deutschem Recht die §§ 4 bis 14 Signaturgesetz einhalten. Außerdem muss das Zertifikat einen gesetzlich vorgeschriebenen Mindestinhalt haben (§ 7 Signaturgesetz). Sinn dieser Regelungen ist insbesondere, die Identität des Zertifikatinhabers sicherzustellen und die sichere Aufbewahrung und Verfügbarkeit des Zertifikats zu gewährleisten. Die qualifizierte elektronische Signatur ist also deshalb „qualifiziert", weil sie auf einem sicheren (im Hinblick auf die Identifikation des Inhabers) Zertifikat aufbaut.

Authentisierung ist das Nachweisen einer Identität, die Authentifizierung deren Überprüfung. Die Identität einer Person oder auch eines Programmes wird dabei an Hand eines bestimmten Merkmals überprüft. Dies kann zum Beispiel mit einem Fingerabdruck, einem Passwort oder einem beliebigen anderen Berechtigungsnachweis geschehen. Im Englischen wird zwischen den beiden Begriffen nicht unterschieden, das Wort „authentication" steht für beides.

Die erste Einführung der elektronischen Steuererklärung ELSTER vor einigen Jahren war eine Katastrophe. Das Programm war gerade zum Herunterladen bereitgestellt worden, als nach wenigen Wochen offiziell davor gewarnt wurde, die Steuererklärung auf diesem Wege zu erledigen – und das auf Grund gravierender Sicherheitsmängel! Inzwischen soll das System ausgereift sein und wird seit 2002 kräftig genutzt. Ab diesem Jahr sollen deutliche Verbesserungen eingeführt werden. Geplant ist, dass eine elektronische Authentisierung als auch eine qualifizierte Signatur unterstützt werden sollen. Derzeit läuft das Verfahren zweigleisig, einmal elektronisch und zusätzlich stark verkürzt in Papierform.

Ihre Meldedaten

Ein blühender Handel mit ihren persönlichen Daten. Glauben Sie nicht? Jeder Bürger ist gesetzlich verpflichtet, sich am Wohnort beim zuständigen Einwohnermeldeamt anzumelden. Die Daten werden elektronisch erfasst und gespeichert. Gegen eine Gebühr verkauft dieselbe Behörde ihre Adressdaten an jeden Interessenten. Demnächst bei einigen Städten und Gemeinden noch einfacher und direkt über so genannte Internetportale. Hinter vorgehaltener Hand spricht man von einem guten Geschäft.

Beispiel E-Health

Elektronische Gesundheitskarte

Auf dem diesjährigen 22. Chaos Communication Congress des Chaos Computer Clubs in Berlin war man sich einig: Die Gesundheitstelematik birgt neben Chancen auch gewaltige Risiken. So sind Datenschutz und Datensicherheit bei der elektronischen Gesundheitskarte (eGK) nicht wirklich gewährleistet. Der Informatiker Thomas Maus, der viel Erfahrung auf diesem Gebiet vorweisen kann sowie als wichtiger Kritiker nicht nur von der Bundesärztekammer gesehen wird, sieht die Risiken in unüberschaubaren Gefahren für die ärztliche Schweigepflicht, das Haftungsrisiko für Ärzte und die Intimsphäre der Patienten. Der Nutzen stünde in keinem Verhältnis zu diesen Gefahren sowie zu den Kosten, die Maus auch deutlich zu niedrig angesetzt sieht.

Beispiel Nutzen: Das so genannte E-Rezept soll Verordnungsmissbrauch, Medienbruch und Mehrfacherfassung vermeiden und so zu einer Zeit- und Kostenersparnis in Praxis und Apotheke führen. Fakt ist, dass ein Verbindungsaufbau mit einer Authentisierung bereits 40 bis 45 Sekunden verschlingt. Geplant ist, dass der Arzt mit seiner Arztkarte das Rezept elektronisch signiert, wobei nicht klar ist, ob je Rezept oder sogar je Position. Wie soll das E-Rezept auf die Patientenkarte kommen? Müssen also Patient und Arzt dafür anwesend sein? Klingt nicht nur unpraktikabel, sondern ist bei durchschnittlich 100 Rezepten pro Tag in einer Praxis unmöglich. Der Arzt wäre über eine Stunde nur mit dem Signieren der eRezepte beschäftigt und mit Verwaltungstätigkeit gebunden, was bisher zum großen Teil von Personal bewältigt werden kann. Die Arztkarte darf der Arzt schon aus Haftungsgründen nicht dem Personal überlassen.

Maus stellt auch zu Recht die Frage, wie sich wohl der Apotheker die verordneten Medikamente vom Computer bis zu den Lagerschränken merken soll. Zurzeit nimmt er einfach das Papierrezept mit. Fraglich ist auch eine Rezepteinlösung im Ausland oder durch eine andere Person. In den offiziellen Sicherheitsanforderungen wird übrigens ein durchgängiges nicht-elektronisches Ersatzverfahren gefordert.

Laut Maus und beispielsweise der Gesellschaft für Informatik sind auch folgende wesentliche Punkte nicht ausreichend abgeklärt: Welche Risiken gibt es bezüglich des unbefugten Zugriffs auf Patientendaten, bezüglich der Manipulation von Patientendaten, bezüglich

der Fälschung elektronischer Arztunterschriften und bezüglich des unbefugten Zugriffs auf die Praxis- und Klinik-Informationstechnologie?

> Die Vertraulichkeit der Patientendaten ist hochsensibel, äußerst wertvoll und damit ein hochattraktives Angriffsziel.

Dagegen fallen die Meldedaten weit abgeschlagen zurück.

Ein Satz noch zur Wirtschaftlichkeit: Die kalkulierten Erstinvestitionskosten in Höhe von 140.000 EUR für zwei Krankenhäuser sind beim Modellversuch in Trier mit 450.000 EUR deutlichst überschritten worden. Die „Suppe" hat übrigens der Steuerzahler in Rheinland-Pfalz ausgelöffelt.

Fazit

„Big Brother is watching you" ist die bittere Realität in unserer heutigen Zeit. Ich bin überzeugt, dass sich durch den Einsatz der elektronischen Datenverarbeitung in Verbindung mit den Möglichkeiten der Vernetzung und Mobilität nicht mehr gewährleisten lässt, was wann mit unseren persönlichsten Daten passiert. Die Aspekte Datenschutz und Datensicherheit hinken leider oftmals den neuen technischen Möglichkeiten hinterher oder werden schlicht vernachlässigt. Sie sind schließlich recht teuer und steuern nichts zur Funktionalität bei, im Gegenteil, sie behindert sie eher. Daher ist es höchste Zeit, ein besonders Augenmerk auf den Schutz der persönlichen Daten zu richten.

Damit Sie nun nicht nur mit schlechten Gedanken diese Artikellektüre beenden, noch etwas zum Schmunzeln. Der National Health Service im britischen Königreich rät den Staatsbürgern, öfter und aktiver Sex zu haben, so genanntes „Sexercise". Durch diese Mischung aus Sex und Exercise ließen sich Herzkrankheiten und Krebs wirksam bekämpfen. Vielleicht weitere Ansätze, uns abzulenken? Na, wenn das keine Aussichten sind…

Literaturhinweise

http://de.wikipedia.org/wiki/Datenschutz

http://de.wikipedia.org/wiki/Datensicherheit

Bundesministerium für Wirtschaft und Technologie: Chipkartenstrategie der Bundesregierung (eCard-Strategie). http://www.bmwa.-bund.de/redaktion/inhalte/pdf/e/ecard-strategie,property=pdf.pdf

http://de.wikipedia.org/wiki/Qualifizierte_elektronische_Signatur

http://de.wikipedia.org/wiki/Authentisierung

Franz Josef Wilde: Elektronische Gesundheitskarte – 1984 reloaded. zm 96, Nr. 3, Febr. 2006

Thomas Maus: „Elektronische Gesundheitskarte und Gesundheitstelematik – 1984 reloaded?. 22. Chaos Communication Congress, Berlin 2005, http://events.ccc.de/congress/2005/fahrplan/events/546.en.html Nordwest-Zeitung, 13.02.2006