daten
schutz

XIX. Tätigkeitsbericht

des Landesbeauftragten
für den Datenschutz Niedersachsen
für die Jahre 2007 – 2008

Herausgeber: Der Landesbeauftragte für den Datenschutz Niedersachsen
~~Brühlstraße 9, 30169 Hannover~~ Prinzenstr. 5, 30159 Hannover
Postfach 221, 30002 Hannover

Verantwortlich: Joachim Wahlbrink

Layout: set-up design.print.media
Walderseestraße 7, 30163 Hannover

Druck: Landesvermessung und Geobasisinformation Niedersachsen
Podbielskistraße 331, 30659 Hannover

Zur besseren Lesbarkeit wird bei verallgemeinernden Substantiven lediglich das bestimmende grammatische Geschlecht verwendet. Selbstverständlich richtet sich dieser Bericht an die Angehörigen beider Geschlechter.

XIX. Tätigkeitsbericht

des Landesbeauftragten
für den Datenschutz Niedersachsen
für die Jahre 2007 – 2008

Inhaltsverzeichnis

Zu diesem Bericht

Die Broschüre, die Sie gerade in den Händen halten, ist der 19. Tätigkeitsbericht des Niedersächsischen Landesbeauftragten für den Datenschutz, der gesetzesgemäß im Zweijahres-Rythmus dem Niedersächsischen Landtag vorzulegen ist.
Was ist über die Jahre 2007 und 2008 aus der Sicht eines Datenschützers zu berichten? Sehr viel – und sehr viel mehr, als es zuvor erwartet wurde:

Das Thema Datenschutz ist endlich in den Chefetagen angekommen. Es hat sich gezeigt, dass die Missachtung seiner Regeln auch die Position von Topmanagern gefährdet.
Woher kommt dieser Wandel? Ich will hier jetzt nicht die Liste sattsam bekannter Sünder wiederholen. Im Ergebnis bestätigt sich wieder einmal die hohe politische Gestaltungskraft von Skandalen – 1 Skandal bewirkt mehr als 1000 Argumente.
Eine gerade bekanntgewordene Umfrage des Meinungsforschungsinstituts Emnid (August 2009) belegt das große und wachsende Misstrauen der Bevölkerung beim Umgang mit persönlichen Daten in der Wirtschaft. Die öffentlichen Hände, Verwaltungen und Regierungen, schneiden zwar besser ab, stehen aber auch nicht wirklich gut da.

Was ist zu tun, was am dringlichsten ?
Das seit Jahrzehnten geforderte Arbeitnehmerdatenschutzgesetz muss endlich her, um den Schutz der Privatsphäre in der Arbeitswelt zu sichern und auszubauen.
Die Verseuchung vor allem der Städte mit Überwachungskameras muss gestoppt werden. Hierbei ist insbesondere die Information der Bevölkerung über die langfristigen Schadensfolgen dieser Entwicklung zu intensivieren. Sicherheitsillusionen sind aufzudecken, auch wenn das politisch Überwindung kostet.
Das alles geht nur mit verstärkten personellen Kräften und finanziellen Mitteln. Niedersachsen hat im Jahre 2009 einen Anfang gemacht und den Datenschutz im privaten und wirtschaftlichen Bereich verstärkt. Trotzdem liegt Niedersachsen – wie bisher – im Ländervergleich weit hinten.
Die sich immer weiter beschleunigenden Innovationen im IT-Bereich lassen unübersehbare Felder entstehen. Die Datenschützer stehen dem weitestgehend machtlos gegenüber.
Auch deshalb wird im Schwerpunktthema dieses Berichts versucht, einen Einblick in den Bereich des technisch-organisatorischen Datenschutzes in einer Weise zu vermitteln, die schon einem interessierten, nicht erst einem darauf spezialisierten Leserkreis gerecht wird.

Beim weiteren Durchblättern werden Sie verschiedene Darstellungsstile finden.
Ich erhoffe mir dadurch einen leichteren Zugang bei der Lektüre der folgenden Seiten und danke für Ihr Interesse.

Joachim Wahlbrink
Landesbeauftragter für den Datenschutz Niedersachsen

1

Datenschutz im öffentlichen Bereich

Zusammenarbeit mit den kommunalen Datenschutzbeauftragten

Die Kooperation mit den behördlichen Datenschutzbeauftragten der Kommunen ist ein wichtiger Bestandteil unserer täglichen Arbeit. Ohne deren Unterstützung wäre die zeitnahe Umsetzung datenschutzrechtlicher Ziele vor Ort in einem Flächenland wie Niedersachsen nicht möglich.

Das Netzwerk NORDWEST, ein Zusammenschluss der behördlichen Datenschutzbeauftragten der Kommunen von Cuxhaven bis Osnabrück, von Emden bis Nienburg, bietet seit 2005 mit meiner Unterstützung sein Wissen und seine Hilfe bei datenschutzrechtlichen Belangen im Internet und bei jährlich stattfindenden Workshops an. Die Mitglieder des Netzwerkes arbeiten gemeinsam engagiert Problembereiche im Datenschutzalltag auf und tragen wirksam zur Stärkung und Verbesserung des Datenschutzes in der Region bei. Inzwischen hat das Netzwerk auch länderübergreifende Kontakte aufgebaut: Beim Erfahrungsaustausch der kommunalen Datenschutzbeauftragten des Landes Rheinland-Pfalz konnten die vom Datenschutzbeauftragten des Landes Rheinland-Pfalz eingeladenen Vertreter des Netzwerkes ihre Arbeit wirkungsvoll präsentieren.

Eine Umfrage des Netzwerkes im letzten Jahr hat ergeben, dass den kommunalen Datenschutzbeauftragten eine wirksame Aufgabenwahrnehmung im gesetzlich geforderten Umfang oftmals nicht möglich ist: Viele Datenschutzbeauftragte, die die Aufgabe nicht hauptamtlich ausüben, erfahren gerade **nicht** die Entlastung im jeweils erforderlichen Umfang von anderen Tätigkeiten. Das Interesse am Aufbau weiterer Netzwerke in den übrigen Landesregionen besteht, viele Datenschutzbeauftragten winken aber ab, weil sie allein schon die Bewältigung der täglichen Arbeit voll in Anspruch nimmt.

Vor dem Hintergrund, dass der Aufgabenbestand der Datenschutzbeauftragten durch die zunehmenden E-Government-Verfahren erheblich ausgeweitet wurde, reicht es künftig aus meiner Sicht nicht mehr aus, diese Aufgabe einem Bediensteten zusätzlich zu seinen sonstigen Aufgaben „zur Erledigung nebenbei“ zu übertragen. Zwar hat der Gesetzgeber der Forderung, in das Gesetz einen Rechtsanspruch auf Freistellung im erforderlichen Umfang aufzunehmen, auch im Hinblick auf die Organisationshoheit der Kommunen nicht entsprochen. In der Gesetzesberatung bestand jedoch Einvernehmen darüber, dass den Datenschutzbeauftragten angemessene zeitliche Ressourcen zur Verfügung stehen müssen, um ihre Aufgabe wirksam ausüben zu können.

Zwecks Klärung der Frage nach dem Umfang der erforderlichen Freistellung empfehle ich den behördlichen Datenschutzbeauftragten, schriftlich aufzulisten, welche Aufgaben mit welchen Zeitanteilen im Laufe eines gewissen Zeitraums anfallen, um bei Bedarf einen Nachweis ihrer Tätigkeiten vorlegen zu können.

Ich appelliere an die Kommunen, die Arbeit ihrer behördlichen Datenschutzbeauftragten zu unterstützen und ggf. die bestehenden Arbeitsbedingungen zu verbessern.

Das Niedersächsische Beamtengesetz

Es gab einmal …

gleiche personaldatenschutzrechtliche Regelungen im Niedersächsischen Beamtengesetz (NBG), die auf alle niedersächsischen Beamten, Angestellten und Arbeiter Anwendung fanden.

Um unterschiedliche Standards beim Schutz personenbezogener Daten im Dienst- oder Arbeitsverhältnis zu vermeiden, galten früher die für Beamtinnen und Beamte bestehenden spezialgesetzlichen Regelungen zum Personaldatenschutz auch für Angestellte und Arbeiter (Beschäftigte), die auf Grund eines Vertrages im öffentlichen Dienst stehen (vgl. §§ 101 bis 101 h i. V. m. § 261 Abs. 1 Nr. 2 NBG a. F.).

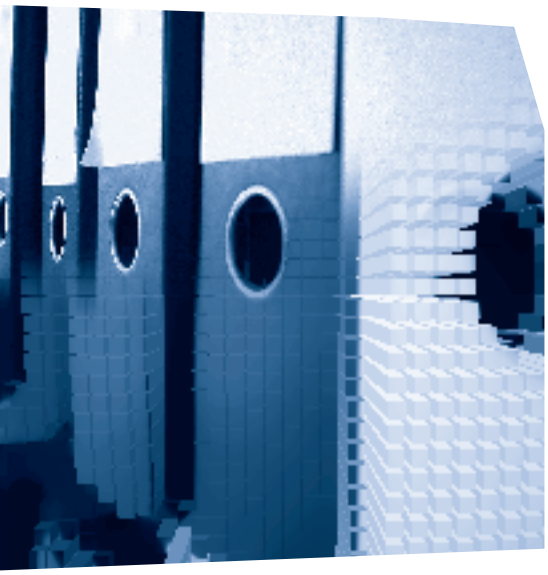
Gleiches Recht für alle, gilt dies nicht mehr seit dem 1. April 2009?

Seit der Novellierung des NBG durch Artikel 1 des Gesetzes zur Modernisierung des niedersächsischen Beamtenrechts vom 25. März 2009 (Nds. GVBl. S. 72) finden die im NBG spezialgesetzlich geregelten Vorschriften zum Personaldatenschutz keine Anwendung mehr auf Beschäftigte im öffentlichen Dienst. Für sie sind grundsätzlich die allgemeinen Regelungen des Niedersächsischen Datenschutzgesetzes (NDSG) heranzuziehen, da weder die jeweiligen Arbeitsverträge der Betroffenen noch die Tarifverträge (vgl. u. a. TVöD oder TV-L) ausreichende Regelungen zum Personaldatenschutz enthalten.

Wer meint, dass diese Lösung für die Belange der Beschäftigten ausreicht, sei darauf hingewiesen, dass die früher im NDSG existierenden personaldatenschutzrechtlichen Regelungen (vgl. § 24 NDSG, in der Fassung vom 17. Juni 1993) Ende 1997 gestrichen und in das NBG überführt worden sind.

Zu Hinweisen, dass demnächst mit einem Beschäftigtendatenschutzgesetz zu rechnen ist, vermag ich nur anzumerken, dass es trotz jahrelanger Forderungen der Datenschutzbeauftragten diesbezüglich bisher keine gesetzgeberischen Initiativen gegeben hat.

Die bis zum 1. April 2009 in Niedersachsen bestehende Rechtslage, die bereichspezifischen personaldatenschutzrechtlichen Regelungen in einem Spezialgesetz zusammenzuführen, hatte sich aus meiner Sicht durchaus bewährt. Der Rechtsprechung des Bundesverfassungsgerichts, das die Einschränkung des Rechts auf informationelle Selbstbestimmung nur auf Grund einer gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit und der Verhältnismäßigkeit entspricht, für zulässig erachtet (Urteil vom 15. Dezember 1983 – Volkszählungsurteil – BverfGE 65,1), wurde damit voll entsprochen.



Meine Empfehlung im Gesetzgebungsverfahren zur Novellierung des NBG lautete daher, die bisherige Regelung des § 261 Abs. 1 Nr. 2 NBG nicht zu streichen.

In der Praxis gestaltet sich die Rechtsanwendung im Hinblick auf die nunmehr unterschiedlich zu betrachtenden Personengruppen der Beamtinnen und Beamten sowie der sonstigen nichtverbeamteten Beschäftigten interessant. Beispielhaft ist hierzu der Fall der Vorgesetzteneinschätzung zu benennen:

Mit der Novellierung der Niedersächsischen Laufbahnverordnung (NLVO) vom 30. März 2009 (Nds. GVBl. S. 118) ist in § 2 Abs. 2 Nr. 6 ein neues Instrument zur Förderung von Personalentwicklungs- und Personalführungsmaßnahmen der Beamtinnen und Beamten aufgenommen worden: Eignung, Befähigung und fachliche Leistung der Beamtinnen und Beamten sollen verwendungs- und entwicklungsbezogen durch Personalentwicklungs- und Personalführungsmaßnahmen, wie z. B. durch die Einschätzung von Vorgesetzten durch ihre Mitarbeiterinnen und Mitarbeiter, gefördert werden.

Da die Vorgesetzteneinschätzung als Maßnahme in einer Rechtsvorschrift normiert worden ist, bedarf die Durchführung nicht der Zustimmung der oder des Betroffenen. Das Ergebnis der Vorgesetzteneinschätzung ist gemäß § 50 Satz 2 Beamtenstatusgesetz (BeamtStG) in die Personalakte der Betroffenen aufzunehmen.

Für nichtverbeamtete Beschäftigte besteht keine Erhebungsbefugnis für eine Vorgesetzteneinschätzung, deshalb ist diese nur mit freiwilliger Einwilligung der Betroffenen zulässig. Die freiwillige Einwilligung bezieht sich sowohl auf die Mitarbeiterinnen und Mitarbeiter als auch auf die Vorgesetzten.

Dies könnte dazu führen, dass nur noch Beamtinnen und Beamte ihre verbeamteten Vorgesetzten einschätzen dürfen…?

Ich bin sicher, dass im Laufe der Zeit noch weitere Fälle bekannt werden, in denen unterschiedliche Maßstäbe anzusetzen sind.

Zu begrüßen wäre eine gesetzliche Regelung, ähnlich wie z. B. im Gesetzentwurf zur Änderung dienstrechtlicher Vorschriften, Artikel 4, Änderung des Datenschutzgesetzes Nordrhein-Westfalen (DSG NRW), unter § 29 vorgesehen (vgl. LT-Drs. 14/8176 vom 17. Dezember 2008):

„Die beamtenrechtlichen Vorschriften über die Führung von Personalakten (§ 50 Beamtenstatusgesetz, §§ 84–92 des Landesbeamtengesetzes für das Land NRW) sind für alle nichtverbeamteten Beschäftigten einer öffentlichen Stelle entsprechend anzuwenden, soweit nicht die Besonderheiten des Tarif- und Arbeitsrechts hinsichtlich der Aufnahme und Entfernung von bestimmten Vorgängen und Vermerken eine abweichende Behandlung erfordern."

Neuauflage des Datenschutzgesetzes

„Da steht ja wirklich auch was Neues drin!“

Neue Auflage der Broschüre „Das Niedersächsische Datenschutzgesetz“ im Januar 2009 erschienen

Seit Jahresanfang steht allen datenschutzrechtlich Interessierten die dritte Auflage der Broschüre „Das Niedersächsische Datenschutzgesetz“ (NDSG) des Landesbeauftragten für den Datenschutz Niedersachsen mit umfangreichen Erläuterungen und Beispielen zum Thema Datenverarbeitung zur Verfügung.

Die überarbeitete Fassung hilft bei datenschutzrechtlichen Fragen. Sie gibt als Handbuch für den täglichen Gebrauch einen Überblick über das geltende Datenschutzrecht in Niedersachsen und bietet vielfältige Informationen mittels ausführlicher Hinweise und praktischer Tipps.

Neben redaktionellen Anpassungen, wie z. B. der Einarbeitung des § 25 a NDSG, sind als neue Hilfen ein Abkürzungs- und ein Stichwortverzeichnis eingefügt worden.

Hilfreich sind z. B. die neuen Ausführungen zur Auftragsdatenverarbeitung (vgl. Erläuterungen zu § 6 NDSG, Abgrenzung zur sog. „Funktionsübertragung“) oder zur Videoüberwachung (§ 25 a NDSG). Hierbei verweise ich insbesondere auf die Erläuterungen zu Videoattrappen (sog. „Dummies“), zur Überwachung von Wertstoffhöfen oder von nicht öffentlich zugänglichen Räumen in öffentlichen Gebäuden (Museen, Schulen).

Die Broschüre steht auf meiner Homepage als Download unter folgendem Link zur Verfügung:
http://cdl.niedersachsen.de/blob/images/C53014928_L20.pdf

„So wichtig wie nie zuvor“:

Entwicklung von Medienkompetenz bei Kindern und Jugendlichen

Das „Daten-Outing“ von Heranwachsenden in Netz-Communities (Chats, Foren, Blogs) birgt viele Gefahren. Durch das Einstellen von Fotos, Filmen, Adressen und Telefonnummern im Internet kann es zu erheblichen Persönlichkeitsverletzungen kommen. Oft kommt es zu kriminellen Nutzungen der Daten. Die Meldungen über missbräuchliche Verwendungen von Fotos und persönlichen Daten, die in sog. „soziale Netzwerke“ oder in Chat-Portale eingestellt wurden, und über Gewaltvideos im Internet und auf Handys, nehmen immer mehr zu.

Die Landesmedienanstalten bieten bereits in Zusammenarbeit mit der Polizei und anderen Stellen diverse Hilfestellungen für Kinder und Jugendliche sowie für deren Eltern an.
Um Schülerinnen und Schüler für das Thema „Datenschutz im Alltag und Beruf“ zu sensibilisieren, sind von mir Ende 2008 unter dem Motto „Was geht mich das an?“ 2.000 DVD mit einem Lehrfilm an Schulen und sonstige Bildungsträger in Niedersachsen verteilt worden.
Unter dem Aspekt, dass besonders Jugendliche die neuen Technologien intensiv nutzen, soll der von der Robert-Jungk-Oberschule in Kooperation mit der Carl-Zeisss-Oberschule in Berlin produzierte Film den Schülerinnen und Schülern der Oberstufe aufzeigen, wie Daten missbräuchlich verwendet werden können, und ihnen grundlegende Regeln zum Datenschutz im Alltag vermitteln. Anhand von sechs Filmszenen wird anschaulich dargestellt, in welchen Bereichen Datenschutzverstöße anfallen können. Mittels Erläuterungen der einzelnen Szenen durch Datenschutzexperten erhalten Jugendliche viele praktische Tipps zum souveränen Umgang mit ihren Daten.
Mein Dank geht an das Niedersächsische Kultusministerium, das mich bei der Verteilung der DVD unterstützt hat.
Seitens der Datenschutzbeauftragten des Bundes und der Länder sind im Laufe des nächsten Jahres weitere Aktionen, wie z. B. Unterrichtsmaterial zu dem Thema und Informationsveranstaltungen in Zusammenarbeit mit den für Jugendschutz zuständigen Institutionen, geplant.

Ergänzende Informationen:

zu diesem Thema finden Sie auf meiner Homepage unter folgendem Link:
http://www.lfd.niedersachsen.de/master/C54257318_N54257107_L20_D0_I560.html

Neue Handreichung

„Datenschutzrechtliche Grundlagen bei Auftragsdatenverarbeitung/Outsourcing in der öffentlichen Verwaltung“

der Datenschutzbeauftragten des Bundes und der Länder im November 2008 erschienen

Kostendruck, Rationalisierung der Arbeitsabläufe, Effizienzsteigerung und Nutzung moderner Technologien haben zur Konsequenz, dass immer mehr Verwaltungen dazu übergehen, einen Teil der bislang von ihnen durchgeführten Tätigkeiten nicht mehr selbst vorzunehmen, sondern auf Dritte (andere öffentliche Stellen oder private Anbieter) zu übertragen. Dies wird häufig mit dem etwas schillernden Begriff „Outsourcing“ umschrieben. Vergleichbare Effekte treten ein, wenn mehrere öffentliche Stellen gemeinsam Projekte betreiben, etwa kommunale Servicebüros. Auch eGovernment-Projekte erfordern vielfach entsprechende Aufgabenübertragungen.

Die Handreichung bietet Hilfestellung bei der Frage, wie der damit verbundene Austausch personenbezogener Daten bei verschiedenen Fallkonstellationen rechtlich eingeordnet werden kann.

Im Gegensatz zu früheren Kommentierungen, vertreten die Verfasser des Arbeitspapiers die Auffassung, dass die datenschutzrechtliche Norm des § 11 des Bundesdatenschutzgesetzes (BDSG) bzw. entsprechender landesgesetzlicher Regelungen (vgl. § 6 des Niedersächsischen Datenschutzgesetzes – NDSG) nicht Grundlage für staatsorganisationsrechtliche Entscheidungen sein kann. Soll die inhaltliche Wahrnehmung von Aufgaben vollständig oder in Teilbereichen auf andere Stellen übertragen werden (sog. „Funktionsübertragung“), scheidet die auf die bloße Datenverarbeitung als Hilfsfunktion zur Aufgabenerfüllung gerichtete Vorschrift des § 6 NDSG als Rechtsgrundlage hierfür aus. Voraussetzung ist vielmehr, dass eine solche Aufgabenverlagerung auf anderer rechtlicher Grundlage zulässig oder rechtlich möglich ist. Dies können u. a. gesetzliche Regelungen, Satzungen, Verwaltungsvereinbarungen oder vertragliche Regelungen sein, soweit diese ihrerseits die Grenzen beachten, die sich aus dem Grundgesetz, der Staatsorganisation oder anderen gesetzlichen Vorschriften ergeben.

Die Handreichung können Sie als pdf-Datei auf meiner Homepage unter folgendem Link herunterladen:
http://cdl.niedersachsen.de/blob/images/C51851267_L20.pdf

Im Test:

Die elektronische Gesundheitskarte (eGK)

In meinem XVIII. Tätigkeitsbericht (Seite 28) habe ich über die Hintergründe der elektronischen Gesundheitskarte und den Beginn der Testphase des Karteneinsatzes unter annähernd realen Bedingungen in den Modellregionen berichtet.

Zu den sieben Testregionen in Deutschland gehört das „eHealthProjekt Wolfsburg".
Die ersten Anwendungen der Gesundheitskarte wurden 2008 getestet.
Es beteiligten sich bisher mehr als 8.500 Versicherte, 14 Apotheken und 15 Arztpraxen sowie das Klinikum Wolfsburg.
Zu den getesteten Anwendungen gehörte die Übernahme der Versichertenstammdaten aus der eGK in die Praxisverwaltungssysteme, das Ausstellen des elektronischen Rezeptes und die Führung der Notfalldaten auf der eGK.
Zielsetzung dieser Tests war und ist es, herauszufinden, ob und wie sich die jeweiligen Anwendungen der eGK in den Arbeitsablauf von Arztpraxen, Apotheken und Klinikbetrieben eingliedern lassen und welche Problemsituationen auf Seiten der Versicherten entstehen können.
Die in den vergangenen Monaten gewonnenen Erkenntnisse der Tests werden von allen beteiligten Testregionen der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) zwecks Zusammenführung und Auswertung übersandt.
Folgende Feststellungen konnten getroffen werden:

1. Die Übernahme der Versichertenstammdaten von der eGK in die Praxisverwaltungssysteme erfolgte problemlos.

2. Die Ausstellung der elektronischen Verordnungen funktionierte ohne technische Probleme.

3. Die Führung der Notfalldaten auf der eGK wurde von den Ärzten grundsätzlich begrüßt. Diese wurden jedoch aufgrund eines zur Zeit noch erhöhten Aufwandes nur selten angelegt.

4. Die Anwendungsprozesse sollen in der Anfangsphase teilweise schwer zu handhaben gewesen sein. Hier wurde der Prozessablauf durch Einführung der Mehrfachsignatur in den Praxen verbessert.
   Die Mehrfachsignatur ermöglicht dem Anwender, nicht nur eine, sondern eine endliche Anzahl von Signaturen vorzunehmen. Es gibt hierbei zwei Varianten der Mehrfachsignatur, die Stapel- und die Komfortsignatur.

Die Stapelsignatur ermöglicht es dem Anwender, unmittelbar hintereinander nach dem Anzeigen der zu signierenden Dokumente (Stapel) und der nachfolgenden PIN-Eingabe mehrere Signaturen auszuführen. Nach erfolgter Stapelsignatur wird die PIN-Authentisierung automatisch gelöscht.
Bei der Komfortsignatur kann das Signieren mehrerer Dokumente nach einmaliger PIN-Eingabe über einen längeren Zeitraum (z. B. Arbeitstag) erfolgen. Die PIN-Eingabe erfolgt hierbei vor dem Anzeigen der Dokumente, welche zu diesem Zeitpunkt in der Regel noch gar nicht bekannt sind (z. B. Beginn des Arbeitstages). Der Anwender muss sich, sobald er die Signatur eines Dokuments oder Stapels veranlassen möchte, mittels eines Token oder Biometriemoduls authentisieren.

5. Der Umgang mit der PIN hat sich als umständlich und wenig anwenderfreundlich herausgestellt. Bei Eingabe des PIN wurde das Zeitfenster daher von 10 Sekunden auf 30 Sekunden erweitert. Auch haben sich die Kartenherausgeber inzwischen auf ein einheitliches PIN-Verfahren geeinigt.

Im weiteren Testverlauf wird die Optimierung des Verfahrens weiter vorangetrieben werden.
Ich gehe davon aus, dass der flächendeckende Einsatz der elektronischen Gesundheitskarte frühestens ab Mitte 2010 in Niedersachsen erwartet werden kann.
Auf dem weiteren Weg dorthin werde ich zusammen mit den Datenschützern des Bundes und der Länder die Einführung der elektronischen Gesundheitskarte in Arbeitsgruppen und der Modellregion Wolfsburg begleiten.

ELENA-Verfahren

Das ELENA-Verfahren (Elektronischer Entgeltnachweis) beschäftigt die Datenschutzbeauftragten des Bundes und der Länder bereits seit einigen Jahren. Letzte Informationen hierzu habe ich in meinem XVIII. Tätigkeitsbericht (Seite 29) gegeben.

Beim ELENA-Verfahren handelt es sich um eine Speicherung von Einkommensdaten in einer zentralen Speicherstelle. Diese sollen in erster Linie Sozialleistungsträgern auf Abruf zur Verfügung gestellt werden.
Gegen das Verfahren wird von Datenschutzbeauftragten insbesondere eingewandt, dass der überwiegende Teil der zu speichernden Daten niemals gebraucht werden wird, weil Sozialleistungen gar nicht oder zu einem erheblich späteren Zeitpunkt in Anspruch genommen werden.
Die Datenschutzbeauftragten des Bundes und der Länder haben sich auf ihrer Konferenz am 6. und 7. November 2008 erneut mit dieser Problematik auseinander gesetzt.
Als Ergebnis wurde eine Entschließung zu verfassungsrechtlichen Bedenken hinsichtlich der Verhältnismäßigkeit einer solchen zentralen Datenspeicherung verabschiedet und dem Gesetzgeber zur Kenntnis gebracht.
Am 22. Januar 2009 verabschiedete der Bundestag den Gesetzentwurf zum ELENA-Verfahren. In seiner Sitzung vom 13. Februar 2009 befasste sich der Bundesrat mit dem ELENA-Verfahrensgesetz. Strittig zwischen Bundestag und Bundesrat war, ob die Einkommensdaten zum Wohngeldantrag vom ELENA-Verfahren ausgenommen werden sollten. Im Vermittlungsausschuss wurde die Einigung erzielt, dass auch diese Angaben vorzuhalten sind.
Das Gesetz wurde am 1. April 2009 verkündet. Somit werden voraussichtlich ab dem Jahr 2012 die bisherigen Bescheinigungen des Arbeitgebers bei der Beantragung von Arbeitslosengeld, Bundeserziehungsgeld und Wohngeld durch den elektronischen Entgeltnachweis ersetzt.
Ich gehe davon aus, dass die Vorbereitungen zur Umsetzung des ELENA-Verfahrensgesetzes schnellstmöglich beginnen beziehungsweise weiter vorangetrieben werden.

Den weiteren Verlauf werde ich datenschutzrechtlich begleiten und hierüber berichten.

Der verlorengegangene USB-Stick mit Steuerdaten

Ein aufmerksamer Bürger übersandte mir einen USB-Stick, den er auf der Straße gefunden hatte. Auf diesem Stick hatte ein Mitarbeiter der Steuerfahndung sowohl dienstliche als auch private Daten gespeichert.

Die von mir informierte Oberfinanzdirektion (OFD) Hannover untersagte unverzüglich in einer Rundverfügung die Speicherung unverschlüsselter Daten auf mobilen Datenträgern. Zudem erstellte sie kurzfristig eine Leistungsbeschreibung mit dem Ziel, zu einem landeseinheitlichen Sicherheitsstandard insbesondere bei mobilen Datenträgern zu gelangen. Diese Leistungsbeschreibung soll zudem Grundlage eines Ausschreibungsverfahrens für eine entsprechende Sicherheitslösung sein, die ich datenschutzrechtlich begleiten werde.

2

Datenschutz in der Wirtschaft

Überwachung von Beschäftigten durch beauftragte Sicherheitsunternehmen

Ende März 2008 berichteten Medien bundesweit über die systematische Überwachung von Beschäftigten eines großen Lebensmitteldiscounters durch Detekteien und andere Sicherheitsunternehmen. Nach umfangreichen Ermittlungen haben die Datenschutzaufsichtsbehörden der Länder erhebliche Datenschutzverstöße festgestellt und gegen die rechtlich selbständigen Vertriebsgesellschaften des Unternehmens Bußgelder in einer Gesamthöhe von 1.462.000 Euro verhängt. Wegen der großen Zahl der in Niedersachsen nachgewiesenen Verstöße sind allein gegen die vier hier ansässigen Vertriebsgesellschaften Bußgelder in Höhe von 656.000 Euro festgesetzt worden.

Die vorgelegten Unterlagen aus dem Untersuchungszeitraum Januar 2006 bis März 2008 dokumentierten heimliche Beobachtungen von Beschäftigten durch Sicherheitsunternehmen, die je nach Auftragsziel entweder Sicherheitsmitarbeiter einsetzten (LDK) oder die Observierung (nur) durch eine Videokamera (OBK) durchführten. Rechtfertigungsgründe für die konkreten, in das Persönlichkeitsrecht und Recht auf informationelle Selbstbestimmung der betroffenen Beschäftigten eingreifenden Vorgehensweisen konnten nicht festgestellt werden.

LDK (Ladendetektiv mit Kamera)

Für sog. LDK- Einsätze sind die Sicherheitsunternehmen von den Vertriebsgesellschaften mit der Durchführung kameragestützter Maßnahmen beauftragt worden. Während seines Einsatzes achtete der Sicherheitsmitarbeiter nicht nur auf Kundendiebstähle, sondern – heimlich – auch auf das Verhalten der Filialbeschäftigten. In der Regel erfolgte der Einsatz so, dass ein Mitarbeiter des Sicherheitsunternehmens für eine Woche in eine Filiale kam. Er nutzte in dieser Zeit entweder die im öffentlichen Verkaufsraum bereits vorhandenen Kameras mit Monitor oder installierte eigene, versteckt angebrachte Miniaturkameras für die Verfolgung des Geschehens auf einem im Aufenthaltsraum befindlichen Kontrollmonitor. Die Videobeobachtung spielte jedoch insgesamt nur eine un-

im Lebensmitteldiscounterbereich

tergeordnete Rolle, die Bilddaten wurden auch nicht aufgezeichnet. Im Rahmen seines Beobachtungsauftrags hörte der Sicherheitsmitarbeiter vielmehr die Gespräche der Beschäftigten und (private) Telefonate mit, führte mit ihnen Unterhaltungen über sie und Dritte (Vorgesetzte und Kollegen) und legte die Informationen detailliert in schriftlichen Revisionsberichten nieder. Diese den Vertriebgesellschaften zugesandten Einsatzberichte enthielten regelmäßig u. a. folgende mitarbeiterbezogenen Feststellungen und Bewertungen:

- Einschätzung der Arbeitsleistung, -fähigkeit und -motivation der Mitarbeiter
- Informationen zum Führungsverhalten und zu den Führungsqualitäten der Vorgesetzten in den Filialen
- Informationen über das Pausenverhalten einzelner Mitarbeiter
- Informationen über persönliche Problemlagen einzelner Mitarbeiter
- Informationen über Zwischenmenschliches und daran anknüpfende Beurteilungen
- Informationen zum Gesundheitszustand sowie zu (möglichen) Schwangerschaften
- Informationen über die finanzielle Situation der Mitarbeiter und ihrer Familien
- Informationen über Ereignisse, die aus Sicht des Sicherheitsmitarbeiters einen Verdacht gegen einen oder mehrere Mitarbeiter begründen
- Informationen über die Stimmungslage und Wesensart der Mitarbeiter
- sonstige sehr persönliche Informationen.

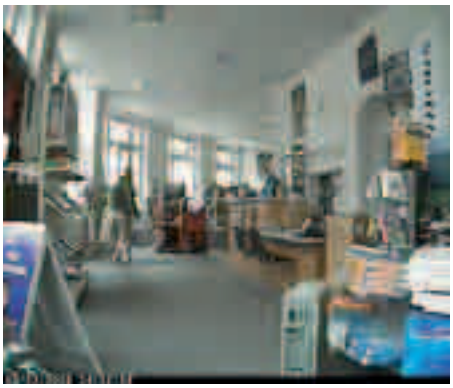
Durch die Beauftragung, die Entgegennahme, das Lesen und Aufbewahren dieser Berichte haben die Vertriebsgesellschaften gegen die Rechtsnorm des § 28 Abs. 1 BDSG verstoßen. Nach dieser Vorschrift ist eine Erhebung und Speicherung personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke nur zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Begründet haben die Vertriebsgesellschaften die Einsätze der Sicherheitsunternehmen mit der Auf-

Weiterführende Informationen:

zum Thema finden sich in der Pressemitteilung des Innenministeriums Baden-Württemberg vom 11.9.2008 (www.innenministerium.baden-württemberg.de)

klärung hoher Inventurverluste, denen mit Mitteln der betriebsinternen Warenkontrolle und Kundenbeobachtung nicht mehr habe begegnet werden können. Zwar kann ein Arbeitgeber grundsätzlich ein berechtigtes Interesse an der Aufklärung von Ladendiebstählen und ihrer künftigen Vermeidung geltend machen. Ein berechtigtes Interesse kann aber nur an für diese Zwecke relevanten Daten bestehen. Mitarbeiterbezogene Feststellungen über deren Privatleben, deren persönliche Angelegenheiten oder sonstige nicht beachtliche Informationen sind jedoch zur Zweckerreichung nicht erforderlich und dürfen nicht erhoben werden. In diesen Fällen überwiegt das schutzwürdige Interesse der Betroffenen am Ausschluss der Verarbeitung offensichtlich.
Von den der niedersächsischen Datenschutzaufsichtsbehörde zur Verfügung gestellten Einsatzberichten enthielten 60 Protokolle schwere mitarbeiterbezogene Datenschutzverstöße. Diese wurden mit einem Bußgeld zwischen 8.000 bis 12.000 Euro je Protokoll geahndet.

OBK (Observation mit Kamera)



Für sog. OBK-Einsätze wurden die Sicherheitsunternehmen beauftragt, in den Unternehmensfilialen verdeckte Observationen mit Kameras durchzuführen. Dazu sind außerhalb der Geschäftszeiten und ohne Kenntnis der Beschäftigen mehrere Minikameras – im Kassen- und Eingangsbereich, im Lager und Pausenraum – so angebracht worden, dass sie nicht entdeckt werden konnten. Die Kameras zeichneten Daten für den Zeitraum eines zumeist einwöchigen Einsatzes auf, ein Sicherheitsmitarbeiter war nicht vor Ort. Nach Einsatzbeendigung wurde das Aufzeichnungsmaterial von den Sicherheitsunternehmen nach Auffälligkeiten, z. B. Straftaten durch Kunden oder Mitarbeiter oder Verstößen gegen betriebliche Vorschriften ausgewertet. Die Observationsberichte und die einschlägigen Videosequenzen wurden im Anschluss daran der auftraggebenden Vertriebsgesellschaft zugeschickt.
Eine Rechtfertigung der mit der Videoüberwachung verbundenen Eingriffe in die Persönlichkeitsrechte der Beschäftigten hätte sich allenfalls aus überwiegenden schutzwürdigen Belangen des Arbeitgebers ergeben können. Das Bundesarbeitsgericht hat für die Videoüberwachung von Arbeitnehmern allgemeine Grundsätze festgelegt und neben dem konkreten Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers verlangt, dass weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft sind, die verdeckte Videoüberwachung praktisch das einzige verbleibende Mittel darstellt und sie insgesamt nicht unverhältnismäßig ist. Die Berücksichtigung dieser Anforderungen konnte in den überprüften Fällen nicht fest-

gestellt werden. Die Vertriebsgesellschaften haben die Aufträge lediglich pauschal mit „hoher Inventurdifferenz und Hinweis auf Mitarbeiterdiebstahl“ begründet. Das Bildmaterial und die Berichte sind daher unter Verletzung datenschutzrechtlicher Vorschriften erstellt worden und hätten nicht entgegengenommen und aufbewahrt werden dürfen.

Nach Auswertung der fünf Filme und jeweiligen Protokolle wurden diese Verstöße mit einem Bußgeld zwischen 8.000 bis 12.000 Euro pro Einsatzfall geahndet.

Darüber hinaus wurde auch die Nichtbeachtung der Verpflichtung aus § 4 f BDSG, die den Vertriebsgesellschaften die Bestellung eigener betrieblicher Datenschutzbeauftragter auferlegt, sanktioniert. Betriebliche Datenschutzbeauftragte haben die Aufgabe, in den Unternehmen auf die Einhaltung des Datenschutzes hinzuwirken. Angesichts des Umfangs und der Art der Erhebung, Verarbeitung und Nutzung personenbezogener Daten in den Vertriebsgesellschaften wäre eine solche Beratungsperson dringend erforderlich gewesen. Durch sie hätten die beanstandeten Datenschutzverstöße möglicherweise vermieden werden können. Die Nichtbestellung betrieblicher Datenschutzbeauftragter ist bei den vier Vertriebsgesellschaften mit einem Bußgeld von jeweils 10.000 Euro geahndet worden.

Google Street View – das Ende der Privatsphäre im häuslichen Umfeld?

Zu recht hat kaum ein anderes Datenerfassungsprojekt der letzten Zeit derartige Aufmerksamkeit erregt wie Google Street View. Das Unternehmen Google plant, die durch Befahren der Straßen der Städte und Gemeinden in Deutschland aufgenommenen Straßenpanoramen für jeden sichtbar ins Internet zu stellen. Dadurch ist die Betroffenheit jedes Einzelnen möglich; sei es, dass er als Fußgänger oder Autofahrer im Straßenbild abgelichtet wird, oder dass sich andere bei Kenntnis der Adresse ein Bild des häuslichen Umfeldes machen können. Spätestens nachdem die Fahrzeuge von Google, die an dem auf dem Fahrzeugdach angebrachten Kameramast im Straßenbild kaum zu übersehen sind, in ersten niedersächsischen Gemeinden im Bremer Umland gesichtet wurden, häuften sich auch bei mir die Anfragen. Besorgte Bürger erkundigten sich nach Maßnahmen, sich gegen eine Veröffentlichung der Bilder wehren zu können, Mitarbeiter von Gemeindeverwaltungen und Kommunalpolitiker wollten sich über Verhinderungsmöglichkeiten des Abfilmens der eigenen Gemeinde informieren.

Beschluss der obersten Aufsichtsbehörden

Der Düsseldorfer Kreis (Gremium der obersten Datenschutzaufsichtsbehörden des Bundes und der Länder für den nichtöffentlichen Bereich) hat am 14. November 2008 zum Thema „Datenschutzrechtliche Bewertung von digitalen Straßenansichten insbesondere im Internet“ folgenden Beschluss gefasst:
„Bei digital erfassten Fotos von Gebäude- und Grundstücksansichten, die über Geokoordinaten eindeutig lokalisiert und damit einer Gebäudeadresse und dem Gebäudeeigentümer sowie den Bewohnern zugeordnet werden können, handelt es sich in der Regel um personenbezogene Daten, deren Erhebung und Verarbeitung nach dem Bundesdatenschutzgesetz zu beurteilen ist. Die Erhebung, Speicherung und Bereitstellung zum Abruf ist nur zulässig, wenn nicht schutzwürdige Interessen der Betroffenen überwiegen.
Bei der Beurteilung schutzwürdiger Interessen ist von Bedeutung, für welche Zwecke die Bilddaten verwendet werden können und an wen diese übermittelt bzw. wie diese veröffentlicht werden. Die obersten Aufsichtsbehörden sind sich einig, dass die Veröffentlichung von georeferenziert und systematisch bereit gestellten Bilddaten unzulässig ist, wenn hierauf Gesichter, Kraftfahrzeugkennzeichen oder Hausnummern erkennbar sind. Den betroffenen Bewohnern und Grundstückeigentümern ist zudem die Möglichkeit einzuräumen, der Veröffentlichung der sie betreffenden Bilder zu widersprechen und dadurch die Bereitstellung der Klarbilder zu unterbinden.
Keine schutzwürdigen Interessen bestehen, wenn die Darstellung der Gebäude und Grundstücke so verschleiert bzw. abstrakt erfolgt, dass keine individuel-

len Eigenschaften mehr erkennbar sind. Um die Möglichkeit zum Widerspruch schon vor der Erhebung zu eröffnen, sollte die geplante Datenerhebung mit einem Hinweis auf die Widerspruchsmöglichkeit rechtzeitig vorher bekannt gegeben werden. Die Widerspruchsmöglichkeit muss selbstverständlich auch noch nach der Veröffentlichung bestehen."

Gegenwärtiger Stand

Vor dem Hintergrund dieses Beschlusses hat der zuständige Hamburgische Beauftragte für Datenschutz und Informationsfreiheit detaillierte Forderungen für eine datenschutzgerechte Gestaltung des Internetdienstes an das Unternehmen Google gerichtet, die letztlich akzeptiert worden sind.
So hat Google u. a. verbindlich zugesichert,

- die geplanten Befahrungen mit einem Hinweis auf die Widerspruchsmöglichkeit rechtzeitig vorher bekanntzugeben,
- eine Technologie zur Verschleierung von Gesichtern und Kfz-Kennzeichen vor der Veröffentlichung derartiger Aufnahmen einzusetzen,
- Widerspruchsmöglichkeiten zur Entfernung bzw. Unkenntlichmachung eines Gebäudes durch einen Bewohner oder Eigentümer vorzuhalten,
- Widersprüche zu Personen, Kennzeichen und Gebäuden bzw. Grundstücken vor Veröffentlichung zu berücksichtigen und die entsprechenden Bilder bereits vor der Veröffentlichung unkenntlich zu machen,
- die Widerspruchsmöglichkeit auch nach der Veröffentlichung vorzuhalten,
- die Löschung oder Unkenntlichmachung der Rohdaten von Personen, Kfz und Gebäudeansichten vorzunehmen, die aufgrund eines Widerspruchs zu entfernen sind.

Widersprüche können eingelegt werden im Internet unter:
http://maps.google.de/intl/de/help/maps/streetview/faq.html#q7 oder
schriftlich bei der Google Germany GmbH, betr.: Street View, ABC-Straße 19, 20354 Hamburg.

Weitere Informationen

zum Thema finden sich u. a. auf den Seiten des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit unter www.hamburg.datenschutz.de

Videoüberwachung– auch bei Kaffee und Kuchen

Der „Fall Lidl" hat im vergangenen Jahr zu einer verstärkten Wahrnehmung der in allen Lebensbereichen präsenten Videoüberwachung geführt. Dabei konnte festgestellt werden, dass sowohl die Bereitschaft zur Installation von Videokameras gewachsen ist, als auch, dass die Einstellung der hiervon betroffenen Bürgerinnen und Bürger kritischer geworden ist.

Videokameras sind inzwischen zu einem günstigen Preis überall erhältlich. Sie werden so zu einem Mitnahmeartikel im Baumarkt, denn „das machen ja alle". Dieses Verhalten führt zu Streitigkeiten unter Nachbarn, in Geschäften und Cafés sowie zwischen Unternehmen und deren Beschäftigten. So werde ich neben meiner rechtlichen Überprüfung auch immer mehr zum Streitschlichter.

Durch einen Zeitungsartikel wurde ich auf eine Videoüberwachung in einem Café der studentischen Szene aufmerksam.

Bei der anschließenden Prüfung vor Ort zeigte sich, dass große Bereiche des Gastraumes mit mehreren gut auflösenden digitalen Dome-Kameras überwacht wurden. Das gesetzlich geforderte Hinweisschild fehlte ebenso wie die vorgeschriebene Verfahrensbeschreibung. Als Ziel für die Videoüberwachung wurde angegeben, dass so Einbrüche außerhalb der Geschäftszeiten aufgeklärt werden könnten. Darüber hinaus nutzte die Betreiberin die Anlage, um von ihrer Wohnung aus einen Blick in das Café werfen zu können. Ein Bewusstsein für die Risiken und Gefahren einer Videoüberwachung war bei ihr nicht vorhanden. Zudem entstand der Eindruck, dass ihr die Anlage von dem verkaufenden Unternehmen aufgedrängt worden war.

Es handelt sich bei dem Gastronomiebetrieb um einen öffentlich zugänglichen Raum mit für Kunden eingerichteten Sitzbereichen, welche einen

längeren Aufenthalt gerade ermöglichen sollen. Die Kommunikation im Freizeitbereich, und damit die private Lebensgestaltung der Kunden, steht hier im Vordergrund. Auch die Mitarbeiter haben einen Anspruch darauf, dass bei Ausübung ihrer beruflichen Tätigkeit keine ständige Arbeits- und Leistungskontrolle seitens des Arbeitgebers möglich ist. Zudem ist zur Erreichung des hier festgelegten Zwecks der Aufklärung von nächtlichen Einbrüchen eine dauerhafte Überwachung des Gastraumes während der Geschäftszeiten nicht erforderlich. Die permanente und flächendeckende Überwachung war daher unzulässig. Die Betreiberin konnte bereits im Gespräch bei der Vor-Ort-Kontrolle von der Unzulässigkeit der Videoüberwachung überzeugt werden. Mittlerweile wurden sämtliche Kameras abgebaut.

Es ist anzumerken, dass bei einer Beschränkung der Videoaufzeichnungen auf die geschäftsfreien Zeiten zur Beweissicherung im Einbruchsfall grundsätzlich keine schutzwürdigen Interessen einer Überwachung entgegen stehen.

Neben der Videoüberwachung in Cafés und Bistros wurden im Berichtszeitraum auch häufig Kameras in Bäckereien gemeldet. Eine präventive dauerhafte Videoüberwachung ist hier zum einen schon deshalb nicht erforderlich, weil der Verkauf der Ware naturgemäß über den Tresen hinweg erfolgt, so dass kein freier Zugang des Kunden zur Ware besteht. Zum anderen ist sie gegenüber den Mitarbeiterinnen und Mitarbeitern, wie bereits dargelegt, auch nicht zulässig.

Darüber hinaus erreichten mich eine Vielzahl von Eingaben aus dem Nachbarschaftsbereich. Hier liegt häufig schon ein länger schwelender Konflikt im zwischenmenschlichen Bereich vor. Bei der Durchführung von Kontrollverfahren ist oft festgestellt worden, dass es sich bei den Geräten um Attrappen handelt. Die betroffenen Nachbarn können diesen Umstand jedoch zumeist nicht erkennen. Für sie besteht daher ein permanenter Überwachungsdruck.

Sofern eine funktionsfähige Videoüberwachungskamera in Betrieb genommen werden soll, ist vorher sicherzustellen, dass ausschließlich ein zulässiger Bereich erfasst wird. Dies betrifft den Kamerastandort, den Kameratyp sowie den gewählten Aufnahmebereich. Hier ist durch einfache bauliche Maßnahmen, wie das Anbringen von Seitenblenden, als auch durch technische Methoden, wie der Verpixelung von Aufnahmebereichen eine datenschutzgerechte Lösung zu erzielen.

Es ist mir in diesem Zusammenhang wichtig darzustellen, dass meine aufsichtsbehördliche Zuständigkeit nicht gegeben ist, wenn sich die Überwachung nur auf das eigene, private Grundstück erstreckt. Nur soweit öffentlich zugängliche Bereiche betroffen sind, kommt das Bundesdatenschutzgesetz zur Anwendung.

Datenhandel – ein Dorn im Auge des Datenschutzes

Datensparsamkeit gegen Datenmissbrauch

Spätestens seit August 2008 ist bekannt, dass Bankkunden in Deutschland um ihre persönlichen Daten bangen müssen. Die Verbraucherzentrale Schleswig-Holstein hatte dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) eine CD aus einem Callcenter übergeben, auf der mehr als 17.000 Datensätze mit Angaben zu Namen, Adresse, Geburtsdatum, Telefonnummer und Kontoverbindung enthalten waren. Die Struktur wies auf eine Herkunft von der Süddeutschen Klassenlotterie hin. Wenige Tage später erhielt das ULD eine weitere CD mit ca. eine Million Datensätzen. Diese für Call-Center bestimmten Daten enthielten wiederum teilweise Angaben zur Kontoverbindung, aber auch E-Mail-Adressen und weitere Verbraucherdaten. Einzelne selektierte Datenbestände bezogen sich gezielt auf ältere Menschen. Danach wurde dem ULD erneut eine CD mit 130.000 Datensätzen zugänglich gemacht; davon ca. 70.000 mit Kontoangaben.

Dem Bundesverband der Verbraucherzentralen in Berlin wurden vier Millionen Datensätze mit Kontonummern angeboten. Die Daten sollen von Klassenlotterien, Gewinnspielunternehmen und Mobilfunkanbietern stammen. Nach Recherchen der NDR/WDR-Sendung „Kriminalreport“ waren auch Kunden der Deutschen Telekom vom verbotenen Datenhandel betroffen. Dem Bericht zufolge hatte sich ein Call-Center in Bremerhaven gesetzwidrig Zugriff auf Datenbanken der Telekom verschafft und diese Daten offenbar an Dritte weiterverkauft. Im Dezember 2008 wurden der „Wirtschaftswoche“ 21 Millionen Datensätze einschließlich der Kontoverbindungen für knapp 12 Millionen Euro zum Kauf angeboten. Auch genaue Angaben zur Vermögenslage waren in manchen Fällen vorhanden.

Es gab Betrugsfälle, in denen Abbuchungen von Konten erfolgten, ohne dass eine Zahlungsverpflichtung bestand. Dubiose, als Lottogesellschaften getarnte Firmen, hatten Tausende Bürger angerufen und ohne Einzugsermächtigung Geld von deren Bankkonten abgebucht.

Die Rechtsverstöße und Skandale haben gezeigt, dass etliche Unternehmen sich ihrer Verantwortung für den Datenschutz ihrer Kunden nicht bewusst sind oder diesen gezielt umgehen. Um am Wirtschaftsleben teilnehmen zu können, müssen Bürger Adress- und Kontodaten bekanntgeben. Deshalb müssen sie darauf vertrauen können, dass diese Daten geschützt und gesichert sind und bleiben. Gesetzgeber, Aufsichtsbehörden und Unternehmen haben den Auftrag, den Datenschutz für die Betroffenen sicherzustellen.

Die Datenschutzbeauftragten des Bundes und der Länder und Verbraucherschützer sahen und sehen einen dringenden Handlungsbedarf. Personenbezogene Daten – insbesondere sensible Daten – haben einen hohen wirtschaftlichen Wert und ein erhebliches Gefährdungspotential für die Betroffenen.

Der Bundestag hat daher eine Novellierung des Bundesdatenschutzgesetzes beschlossen. Dabei sind jedoch durch intensive Lobbyarbeit die Interessen der Werbewirtschaft, des Adresshandels und der Markt- und Meinungsforschung berücksichtigt und damit einige beabsichtigte Einschränkungen abgemildert sowie Übergangsregeln entgegen den Vorschlägen der Datenschutzbeauftragten durchgesetzt worden.

Die Nutzung personenbezogener Daten für Werbung, Markt- und Meinungsforschung wird zwar generell von einer Einwilligung durch den Betroffenen abhängig gemacht. Ausnahmen gelten aber für steuerbegünstigte Spendenwerbung, Werbung an gewerblichen und freiberuflichen Geschäftsadressen und Eigenwerbung der Unternehmen für eigene Kunden. Allerdings gibt es eine Übergangsregelung bis zum Juli 2012, in der die bisher erhobenen Daten noch nach altem Recht verarbeitet werden dürfen.

Verbesserungen ergeben sich durch Informationspflichten der Unternehmen bei schwerwiegenden Datenschutzverstößen oder -pannen. Dabei muss es sich um besonders sensible Daten handeln und dem Betroffenen müssen dadurch schwerwiegende Beeinträchtigungen drohen. Wenn Daten nach § 3 Abs. 9 BDSG, Daten, die einem Berufsgeheimnis unterliegen, Bank- und Kreditkartendaten sowie Daten, die sich auf strafbare Handlungen beziehen, unrechtmäßig zur Kenntnis Dritter gelangen, ist das Unternehmen verpflichtet, die Betroffenen sowie die zuständige Aufsichtsbehörde darüber zu informieren.

Weiterhin wurde die Stellung des betrieblichen Datenschutzbeauftragten gestärkt und der Bußgeldrahmen erweitert.

Zwar verbessern die Gesetzesänderungen den Standard des Datenschutzes, aber die mit den Datenschutzskandalen erkennbaren Missbrauchsfälle und Defizite lassen sich nicht allein mit gesetzgeberischen Möglichkeiten schließen. So war die Datenverarbeitung, die zu den unberechtigten Abbuchungen von Konten und Kreditkarten führte, bereits nach den Regelungen des bisher geltenden Bundesdatenschutzgesetzes unzulässig und illegal. Dies gilt auch für Datenverarbeitungen, in denen Auftragsdatenverarbeiter wie z. B. Call-Center die Daten ihrer Auftraggeber zweckentfremdet haben und weitere Datennutzungen ermöglichten.

Betroffenen kann nur geraten werden, ihre Kontoauszüge regelmäßig zu kontrollieren.

Es ist ratsam, jede Datenerhebung auf ihre Notwendigkeit der Preisgabe zu prüfen. Die Angabe der Telefonnummer ist meist nicht erforderlich. Ebenso gilt dies für Einkommen, Hobbys oder Familienstand. Die E-Mail-Adresse ist bei Online-Anbietern nicht nötig, wenn die Ware per Post kommt. Notfalls sollte eine E-Mail-Zweitadresse angegeben werden. Bei einer Registrierung in Chatrooms oder einem sozialen Netzwerk sollte eine E-Mail-Adresse verwendet werden, die keinen Bezug zum Namen hat. Die persönlichen Angaben sollten unter Pseudonym und ohne vollständige Anschrift und Telefonnummer erfolgen. Auch an Preisausschreiben und Gewinnspielen sollte nicht teilgenommen werden, wenn die Daten nicht in fremde Hände gelangen sollen. Bei Werbeanrufen sollte besser nicht auf die Fragen eingegangen und keine persönlichen Daten preisgegeben oder bestätigt werden.

Versicherungswirtschaft

Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die Versicherungswirtschaft, Einwilligungs- und Schweigepflicht-Entbindungserklärungen

In meinem XVIII. Tätigkeitsbericht (S. 11 ff) hatte ich eine zentrale datenschutzrechtliche Fragestellung im Bereich der Versicherungswirtschaft, die Schweigepflicht-Entbindungserklärung bei privaten Krankenversicherungen, näher beleuchtet. Die von den Versicherungen seit 1989 benutzte pauschale Schweigepflicht-Entbindungserklärung wurde als nicht mehr mit dem Bundesdatenschutzgesetz vereinbar angesehen und sollte – konkretisiert auf den Einzelfall – durch den Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GDV) neu formuliert werden. Inzwischen gibt es hierzu und zu der mittlerweile ebenfalls in Angriff genommenen Neufassung der seit 1994 verwandten allgemeinen Datenweitergabeklausel in Versicherungsverträgen Fortschritte.
Der GDV und die datenschutzaufsichtsbehördlichen Vertreter in der Arbeitsgruppe Versicherungswirtschaft des Düsseldorfer Kreises (Abstimmungsgremium der obersten Datenschutzaufsichtsbehörden des Bundes und der Länder) sind nach Erörterungen über die Neufassung datenschutzkonformer Einwilligungs- und Schweigepflichtentbindungserklärungen im Versicherungsvertragsbereich der Auffassung, dass eine datenschutzrechtliche Einwilligungsklausel möglichst nur noch für die Verarbeitung besonders sensibler personenbezogener Daten – wie Gesundheitsdaten – sowie bei der Verarbeitung personenbezogener Daten für Werbezwecke erforderlich ist.
Die weiteren Verhandlungen gestalteten sich dennoch schwierig. Zwar hat der GDV für die genannten Einwilligungsfälle sowie für die Neuformulierung der Schweigepflicht-Entbindungserklärung Mustererklärungen erarbeitet. Er hat daneben und in Ergänzung zu diesen Klauseln auch einen Entwurf über Verhaltensregeln nach § 38a BDSG zum Umgang mit personenbezogenen Daten durch die Versicherungswirtschaft erstellt. Dieser sogenannte Code of Conduct soll dem Verbraucher einen Überblick verschaffen, wie die Versicherungswirtschaft mit personenbezogenen Daten, die auf der Grundlage des Bundesdatenschutzgesetzes verarbeitet werden, verfährt. Wegen des Umfangs der Richtlinie und des engen Zusammenhangs zu den Klauseln sind die Beratungen über die Inhalte der Entwürfe aber noch nicht abgeschlossen.
Über den Fortgang dieser Angelegenheit werde ich berichten.

3

Schwerpunkt:
Technisch-organisatorischer Datenschutz

Informationstechnik:
Hier Lebensbestandteil und Problemlöserin …

Die Gesellschaft ist globaler geworden. Nicht nur die Wirtschaft in nahezu allen Branchen hat sich auf globale Märkte für Produkte und Dienstleistungen eingestellt. Auch die Informations- und Kommunikationstechnik (IuK-Technik oder IKT) ist durch die Etablierung des weltumspannenden Internet und zahlloser technischer Innovationen zum Treiber und zum Träger für immer größere Datenmengen geworden. Dabei treten die Daten in immer stärker verstreuten Speicherbereichen und mit stetem Anstieg des Komplexitätsgrades für Infrastruktur, Funktionen und Organisation auf. Somit steht auch der Datenschutz vor immer neuen technischen und organisatorischen Herausforderungen.

Kaum noch eine Aktivität – von der Produktion über die privaten und öffentlichen Dienstleistungen, den Handel bis zur Freizeitaktivität – geht ohne die Nutzung der IKT vonstatten. IT-Systeme und insbesondere das Internet haben sich dabei derart rasant und vielschichtig zur Hauptschlagader für Transaktionen, Kommunikationsströme und Informationsressourcen entwickelt, dass für zahlreiche Funktionen des Wirtschaftslebens, der Steuerung und sogar der privaten Bereiche eine Rückgängigmachung dieser Nutzung undenkbar geworden ist.
Diese Abhängigkeit ist so deutlich geworden, dass die Bundesregierung bereits im Jahre 2005 einen „Nationalen Plan zum Schutz der Informationsinfrastrukturen (NPSI)“, dazu im Jahre 2007 einen Umsetzungsplan für die Bundesverwaltung, einen Umsetzungsplan für die Kritischen Infrastrukturen der Bundesrepublik, ein Basisschutzkonzept sowie im Jahre 2008 einen Leitfaden für Risiko- und Krisenmanagement entwickelt hat. Dieser „nationale Plan“ stuft auch die Informationsinfrastrukturen – neben den Straßen, Wasser- und Stromleitungen – als so elementar ein, dass ohne diese das berufliche und private Leben zum Stillstand käme.

www.lfd.niedersachsen.de
Home > Service-Angebote > Technische Hilfen

… dort Werkzeug zur Kompromittierung der Privatsphäre

Obwohl es hierbei vorrangig um die Verfügbarkeit von Infrastrukturen geht, wird bei näherer Betrachtung klar, dass darüber hinaus auch andere Schutzziele betroffen sein können. Bei der Beurteilung des Schutzbedarfes und der Risikobetrachtung von IT-Systemen, Kommunikationswegen sowie der Informationen selbst sind auch die Integrität und die Vertraulichkeit von Daten zu bewerten. Der Umstand, dass IT-Systeme in den allermeisten Fällen auch personenbeziehbare oder -bezogene Daten verarbeiten, ruft schließlich stets die Frage nach der Gewährleistung des Datenschutzes hervor. Eine Entsprechung, etwa ein „Nationaler Plan für die Gewährleistung des Datenschutzes", existiert allerdings nicht. Die technischen und organisatorischen Maßnahmen, die den Datenschutz bei der Entwicklung und dem Betrieb von IT-Verfahren sicherstellen müssen, sind auch in keinem abschließenden Katalog geregelt. Vielmehr haben das Bundesdatenschutzgesetz (BDSG) für den nicht öffentlichen Bereich und das Niedersächsische Datenschutzgesetz (NDSG) für den öffentlichen Bereich im Land und in den Kommunen hierfür Schutzziele und Gestaltungsregelungen vorgeschrieben, weil das Recht auf informationelle Selbstbestimmung und das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme neben dem materiellrechtlichen Schutz der personenbezogenen Daten auch verlangen, dass eine angemessene Datensicherheit gewährleistet ist.

Datenschutz gleich in die Produkte einbauen

Diese Gestaltungsregeln aus dem geltenden Recht fordern angemessene Maßnahmen, die dem Stand der Technik entsprechen sollen. Ziel dieser Regeln sollte es sein, Datenschutz mit der Technik und damit „an der Quelle der Risiken" zu erreichen. Die Technikentwicklung sollte sich also an den Zielsetzungen des Datenschutzes orientieren. Somit gilt diese Anforderung für Hersteller von Hard- und Software ebenso wie für denjenigen, der die IT-Verfahren verantwortlich in Betrieb nimmt.

Hier entsteht in der Praxis oft das Problem, dass durch Zusammenwachsen der Technologien, durch die Nutzung vernetzter und miteinander kombinierter IT-Dienste die Feststellung der Verantwortlichkeit für einzelne Komponenten und Dienste schwieriger wird.

Ein weiterer Entwicklungstrend ist die Konvergenz zwischen den klassischen Telefonnetzen, den Datenleitungen und den Unterhaltungsmedien (so genanntes „Tripple Play"), also das Zusammenwachsen von Fernsehen, Internet und Telefon. Es führt technologisch dazu, dass klassische Telefonnetze zunehmend in integrierten so genannten „Next Generation Networks" bzw. Voice-over-IP-Netzen (IP-Telefonie) aufgehen werden. Damit treten zu den bereits vorhandenen

http://de.wikipedia.org/wiki/IP-Telefonie

Sicherheitsaspekten auch noch die Sicherheitsaspekte hinzu, die von der Internet basierten Technik – zum Beispiel von den Schwächen der dort verwendeten Protokolle – her bekannt sind.
In zahlreichen Kontakten mit Verfahrensbetreibern – insbesondere bei Beratungen – stellte sich heraus, dass das dortige Rollen- und Verantwortungsverständnis für IT-Sicherheit und Datenschutzmaßnahmen keinesfalls immer ausreichend vorhanden ist. Oft wird versucht, Zuständigkeiten zu delegieren – etwa auf den Produkthersteller von Hard- oder Standardsoftware, ein beauftragtes Rechenzentrum oder einen externen Berater. Dabei wird oft übersehen, dass die Verantwortung bei der verantwortlichen Stelle verbleibt und eine datenschutzrechtliche Kontrollpflicht besteht, die die Risiken betrachtet, um die technischen und organisatorischen Datenschutzmaßnahmen erschöpfend zu gestalten und wahrzunehmen.

Strategien für technischen Datenschutz

Besonders bei neuen Technologien oder Strukturveränderungen ergeben sich oft Risiken und Nebenwirkungen für den Datenschutz, die nicht immer gleich offenkundig sind. Sie werden fast immer auch von den innovationsfreudigen Befürwortern bestritten oder verharmlost. Unser Ziel ist es, diese Risiken rechtzeitig zu analysieren, aufzuzeigen und geeignete Strategien und Maßnahmen zu entwickeln oder zu sammeln und in einem Sensibilisierungs- und Diskussionsprozess zu kultivieren. Davon profitieren letztlich auch die Einzelfälle bei Beratungen und Kontrollen, weil standardisierte Lösungen und Maßnahmen die Einzelfallbehandlung beschleunigen.
Wie ich bereits in meinem letzten Bericht hervorhob, ist es aber auch dieselbe innovative Technik, die es als Werkzeug dem Datenschutz erst möglich macht, sich mittels geeigneter Maßnahmen für die informationelle Selbstbestimmung durchzusetzen. Es ist also kreativer Geist gefordert, Datenschutz fördernde Technologien (sogenannte „Privacy Enhancing Technology“) zu entwickeln und durchzusetzen, wie sie auch maßgeblich durch die **Arbeitsteilung und Fachberatung im Verbund, Zusammenarbeit im Arbeitskreis „Technik“** erfolgt.
Die bewährte Zusammenarbeit zwischen den Technikreferenten und Mitarbeitern der Datenschutzbeauftragten von Bund und Ländern ist auch im zurückliegenden Berichtszeitraum für uns von besonderer Bedeutung gewesen. Neben den turnusmäßigen Zusammenkünften des Arbeitskreises Technik wurden auch temporäre Arbeitsgruppen zu technischen Spezialthemen in wechselnden Zusammensetzungen eingerichtet. Fortbildungsmaßnahmen sowie Ergebnisse zu Spezialthemen mit Abstimmungsbedarf zwischen den Ländern wurden in zusätzlichen Workshops organisiert.
Nachfolgend können nur auszugsweise Themenkomplexe aufgezeigt werden.

Identitätsmanagement und was dazu gehört

Wegen der zentralen Bedeutung von Funktionen der Identitäten in IT-Verfahren kommt der datenschutzgerechten Gestaltung in organisatorischer wie technischer Hinsicht besondere Bedeutung zu. Öffentliche Verwaltungen stehen seit Jahren vor der Herausforderung, in ihren Verfahren einerseits straffe und handhabbare Prozesse für die notwendige Authentifizierung und das Identitätsmanagement zu organisieren und andererseits ein hohes Maß an Sicherheit für die Prozesse sowie dem technischen Stand entsprechende, geeignete Maßnahmen des Datenschutzes zu erfüllen.

Klein, smart, sicher: Smartcards

Da Identitäten, anders als in der analogen Welt, in der Regel nicht mit persönlicher Prüfung – zum Beispiel durch Blickkontakt, direkte Gesichtserkennung – erfolgen können, muss in der digitalen Welt mit der Authentifizierung, also dem Vorgang der Verifikation einer behaupteten Identität einer Person eine verlässliche technische Verifikationslösung zum Einsatz kommen. In den meisten Fällen reicht die Einrichtung und Überprüfung mittels Kennung/Benutzername und Passwort/PIN. Wegen der großen und weiter rasant ansteigenden Zahl von Kennungen und Passwörtern für verschiedenste Anwendungen wächst auch der Bedarf an einfacheren und trotzdem verlässlichen manipulationsfesten Lösungen. Inzwischen hat sich hier die Erkenntnis durchgesetzt, dass Smartcards (Chipkarten) mit kryptografischem Schutz nach dem Stand der Technik eine sichere und einfache Lösung darstellt. Sie haben auch den Vorteil, dass theoretisch alle IT-Verfahren diese als zentrales Infrastrukturelement für Authentifikation, Signatur und Verschlüsselung von digitalen Informationen nutzen können.
Smartcards können neben sichtbaren Merkmalen im Plastik (aufgedruckter Name, Funktion, Dienststellenzugehörigkeit) durch technische Merkmale wichtige zentrale Funktionen abbilden. Der eingebaute integrierte Schaltkreis (Chip) enthält mit Hilfe der Hardware-Logik, eines Speicherbausteins und ggf. eines Mikroprozessors (Prozessorchipkarte) u. a. die Möglichkeit, verschlüsselte Daten zur Identität des Besitzers zu speichern und einen Authentifikationsversuch durch Rechenoperationen (Algorithmen) zu überprüfen. Dabei ist es wichtig, gespeicherte Daten vor dem unberechtigten Auslesen zu schützen und das Erzeugen einer funktionstüchtigen Doublette (so genannter Clone) zu verhindern. Der Vorteil einer Smartcard liegt auch darin, dass neben der Authentifikationsfunktion ebenso digitale Signaturen (nach dem Signaturgesetz) aufgebracht werden können. Damit wären auch mittels einer fortgeschrittenen oder einer qualifizierten Signatur verbindliche Rechtsgeschäfte bis hin zum Electronic Government (eGovernment) möglich.
Besondere Herausforderungen an diese Karten werden durch die Schutzanforderungen an die physikalischen und kryptografischen Bedingungen gestellt. **Erfolgreiche Hackingversuche** haben immer wieder gezeigt, dass nur offene

Standards und Chiparchitekturen der Garant dafür sind, dass Sicherheitslücken öffentlich bekannt werden und dadurch der Druck auf die Anbieter und Entwickler zunimmt, diese schnellstmöglich zu schließen.

Verzeichnisdienst für einheitliche Basisinformation und Zertifikate

Um für Bürger, Unternehmen und Behörden einen einheitlichen Zugriff auf Authentifizierungsdaten zu bekommen, ohne auf zahllose verteilte Quellen zurückgreifen zu müssen, ist das Land bemüht, einen virtuellen zentralen Verzeichnisdienst in Form eines Metadirectorys bereitzustellen. Bisher liegen diese Informationen verteilt in verschiedenen Zuständigkeitsbereichen. Über ein Metaverzeichnis, also verbindende Übersetzungs- und Vermittlungsebenen, werden bereits einfache Verzeichnisinformationen wie Namen, E-Mail-Adressen und Erreichbarkeiten, Behörden übergreifend bereitgestellt. Für das Funktionieren von Signaturkarten bedarf es aber zusätzlicher Daten wie Zertifikate sowie Funktionen.
Gefragt sind schon heute in zahllosen IT-Anwendungen Statusinformationen über vorhandene Zertifikate. Ausgeblendet sind dabei die gesperrten Zertifikate. Die zentrale Anforderung ist hier zunächst der Schutz vor unberechtigtem Zugriff auf unverschlüsselte Personendaten sowie die Integrität der Verzeichnisdaten. Funktional soll zudem ein einfacherer Zugang zu Diensten über ein einmaliges Logon mittels eines so genannten „Single Sign On“ (SSO) ermöglicht werden. Der Benutzer kann durch eine einzige Authentifikation seine für ihn hinterlegte Autorisierung für bestimmte Informationen, Datenbanken und Abläufe vollziehen, ohne bei jedem Verfahren dies wiederholen zu müssen.

Verzeichnisdienst des LSKN (IZN) für die Landesverwaltung

Ziel der Landesverwaltung ist ein einheitlicher Verzeichnisdienst mit Single Sign On und einheitlichem Identitätsmanagement. Begonnen wurde mit einem virtuellen Verzeichnisdienst in einem Pilotbetrieb. Zertifikate anderer Bundesländer sollen über die European Bridge CA geprüft werden können. Dies gilt jedoch nur für Zertifikate für fortgeschrittene Signaturen, weil die European Bridge CA nicht zur Prüfung höherwertiger Zertifikate eingesetzt werden darf.
Als Einschränkungen im Sinne des Datenschutzes sind u. a. folgende Merkmale vorgesehen:

- Abfragen im Verzeichnisdienst zu Daten über Zertifikate oder deren Inhaber sollen in unterschiedlichem Detaillierungsgrad erfolgen können.
- Auch eine Beschränkung auf die Angabe nur der Behörde/Dienststelle soll ermöglicht werden, soweit nicht die Verifikation der Gültigkeit von Zertifikaten ansteht, die der Inhaber mit einer signierten Nachricht zusammen versendet.
- Suchanfragen mit Jokerzeichen sollen unterdrückt werden.

Sicherheit und Datenschutz haben ihren Preis: „PKI“ wird benötigt

Gute (also funktionssichere und ungebrochene) Verschlüsselung (Kryptografie) bedarf einer ganzheitlichen Infrastruktur mit organisatorischen Trennungen (Zertifizierungsinstanzen), Prüffunktionen und technischen Komponenten: die so genannte „Public Key Infrastructure“ (PKI).
Das LSKN (vormals izn) hat hier für die Landesverwaltung mit der Einführung der digitalen Signaturkarte grundlegende Arbeit geleistet. Insbesondere durch anwendungskritische Verfahren wie das Haushaltsmanagementsystem u. a. sind 16.000 SignaturCards Niedersachsen vom LSKN (izn) ausgegeben worden, für die eine PKI notwendig geworden war.

eSignatur und Verwaltungs-PKI

Um die Notwendigkeit des beschriebenen Aufwandes zu verdeutlichen, sei vergleichend auf die „analoge“ Welt verwiesen, die mit einer eigenhändigen Unterschrift auf einem Schriftstück die Echtheit und Integrität des Dokumentes und die Authentizität des Zeichnenden – zumindest teilweise – besiegeln soll. Um die Integrität mindestens in vergleichbarer Weise zu erreichen, wenn es um elektronische Dokumente geht, muss eine digitale Signatur folglich die leichtere Kopierbarkeit und Fälschbarkeit eines digitalen Dokuments kompensieren. Unter einer elektronischen Signatur versteht man Daten, die mit elektronischen Informationen verbunden sind, und mit denen man den Unterzeichner bzw. Signaturersteller identifizieren und die Echtheit und ggf. die Integrität der signierten elektronischen Informationen überprüfen kann.
Seit 2004 existiert im LSKN eine so genannte „Master-Registration Authority (Master-RA)“, also eine Registrierungsstelle für digitale Zertifikate mit zwei Sub-RA's (Unter- Registrierungsstellen). Mit deren Einrichtung können die Zertifikate der Verwaltungs-PKI für die niedersächsische Landesverwaltung ausgestellt werden. Zertifikate sind in diesem Zusammenhang als digitale Beglaubigungen zu interpretieren. Sie bestätigen die Authentizität eines öffentlichen Schlüssels und seinen zulässigen Anwendungs- und Geltungsbereich.
Grundlage für die PKI in der Landesverwaltung Niedersachsen war ein Beschluss des KoopA-ADV[1] bereits im Jahre 2001 sowie der beim Bundesamt für Sicherheit in der Informationstechnik (BSI) betriebenen „Root Certification Authority“ (CA, Zertifizierungsstelle), die sich auf der höchsten Hierarchiestufe befindet.
Die Zertifikate der Verwaltungs-PKI sind insbesondere für die Transportsicherung (Verschlüsselung und Signatur) und personenbezogene Authentisierung vorgesehen.
Die Zertifikate der Verwaltungs-PKI unterscheiden sich von den qualifizierten PKS-Zertifikaten auf der über 16.000-mal eingesetzten SignaturCard Nieder-

1 Kooperationsausschuss Automatisierte Datenverarbeitung Bund/Länder/Kommunaler Bereich (www.koopa.de).

sachsen dadurch, dass die Verwaltungs-PKI die Signaturstufe „fortgeschrittene Signatur“ (§ 2 Nr. 2 Signaturgesetz) aufweist, was eine einfachere Antragstellung und niedrigere Kosten mit sich bringt. Durch die Möglichkeit, Software-Zertifikate, Gruppen-Zertifikate und Funktions-Zertifikate zu nutzen, lässt sich eine größere Flexibilität erreichen.

Eine „qualifizierte Signatur“ (§ 2 Nr. 3 Signaturgesetz) weist demgegenüber zusätzliche Sicherheitsvorteile auf. Sie beruhen auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat und müssen mit einer „sicheren Signaturerstellungseinheit (SSEE)“ erzeugt werden. Die Definition einer SSEE richtet sich nach der Richtlinie 1999/93/EG. Zusätzlich wird eine geeignete Sicherheitsevaluierung dafür durch Schutzprofile nach Common Criteria mithilfe der CEN-Spezifikation CWA 14169 (Europäisches Komitee für Normung) erforderlich sein. Durch eine Entscheidung der Europäischen Kommission vom 14. Juli 2003 wurde diese CEN-Spezifikation als dafür geeignete Norm ausgewiesen.

Bedauerlicherweise ist in den vergangenen Jahren der qualifizierten Signatur am IT-Markt allgemein nicht zum Durchbruch verholfen worden, obwohl dies einen erheblichen Fortschritt für die IT-Sicherheit und den Datenschutz erzielen könnte.

Gerade für den Bereich von eGovernment-Verfahren wäre es wünschenswert gewesen, wenn Bundes- und Landesverwaltung die Entwicklung und den Aufbau einer flächendeckenden Infrastruktur auf hohem allgemeinen Sicherheitsniveau durchgesetzt hätten. Insbesondere für die Steuerverwaltung wäre es von Vorteil gewesen, alle Steuerbürger mit einer entsprechenden Karte auszustatten. Statt dessen wurden in den Rechtsvorschriften – zum Beispiel zur Steuerdatenübermittlungsverordnung, im Verfahren ELSTER – einige Lockerungen vorgenommen, mit denen weniger sichere Verfahren als ausreichend definiert worden sind, obwohl dies sachlich-logisch nicht zutrifft.

Auch die gewerbliche Wirtschaft vermochte es bislang nicht, bis auf vereinzelte Anwendungen, Signaturkarten in nennenswerten Zahlen in Umlauf zu bringen.

Auch das LSKN (izn) stellte bereits seit geraumer Zeit fest, dass Zertifikate der Verwaltungs-PKI auf Dauer in größeren Stückzahlen für die eGovernment-Lösungen des Landes Niedersachsen benötigt und sowohl in neuen als auch in bestehenden Anwendungen zum Einsatz kommen werden. Als Beispiel sei die Authentisierung an Netzen zu nennen. Die Sicherheit für Zugänge aus dem Internet in das niedersächsische Landesnetz für Telearbeiter, Außendienstmitarbeiter und andere nicht stationäre Arbeitsplätze über ein Virtual Private Network (VPN) kann nur sinnvoll erreicht werden, indem sich die Nutzer persönlich mit einem Token authentisieren müssen. Diese Aufgabe übernehmen das Zertifikat der Verwaltungs-PKI und der dazugehörige Schlüssel auf der SignaturCard Niedersachsen.

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ (AK Technik) hat in seiner Sitzung im Februar 2007 festgelegt, einen einheitlichen Forderungskatalog für PKI’en und die dazugehörigen Ver-

zeichnisdienste zu entwickeln. Grundlage wurde ein Fragenkatalog, der vom Hessischen Datenschutzbeauftragten und durch Zuarbeit der Technikreferenten der übrigen Datenschutzbeauftragten der Länder entworfen wurde.
In einer Unterarbeitsgruppe des AK Technik wurden aus der Sicht des Datenschutzes 2007/2008 Anforderungen an die PKI'en und Verzeichnisdienste erarbeitet. Dies geschieht auch noch weiterhin und in Zusammenarbeit mit Vertretern des Bundesamtes für Sicherheit in der Informationstechnik (BSI).
Eine besondere und noch offenen Problematik stellt der Umgang mit „Key-Recovery" von Signaturschlüsseln dar, also deren Rekonstruktionsmöglichkeit.

Ein neues Grundrecht ...

Mit einem erneut bemerkenswerten Urteil hat das Bundesverfassungsgericht (BVerfG) am 27. Februar 2008 erstmals ein „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme"[2] definiert. Es leitet sich – wie auch das Recht auf informationelle Selbstbestimmung – aus den Persönlichkeitsrechten der Artikel 1 und 2 des Grundgesetzes ab. Neu ist allerdings dabei, dass sich der Schutzbereich für den Menschen auch auf dessen dingliche Umgebungen – namentlich seiner informationstechnischen Systeme – ausdehnt. Dies wurde in den rechtlichen Bewertungen vor dem Urteil vielerorts bezweifelt.
Der Datenschutz erfuhr mit diesem Urteil – 25 Jahre nach dem Volkszählungsurteil – verfassungsrechtlich eine weitere Stärkung und wurde damit den Herausforderungen des elektronischen Zeitalters angepasst. Es ging um die verfassungsrechtliche Zulässigkeit, ob IT-Systeme durch Polizei oder Verfassungsschutz unter Ausnutzung von Sicherheitslücken in der Hard- oder Software verdeckt ausgespäht und deren Informationen kopiert und genutzt werden dürfen. Anlass für die Entscheidung des BVerfG war das Verfassungsschutzgesetz des Landes Nordrhein-Westfalen. Dort, wie auch im Änderungsentwurf für das BKA-Gesetz, sollten mit dieser Technik die neuen Instrumente der Online-Durchsuchung (Online-Durchsicht und Online-Überwachung) gesetzlich verankert werden.
Der AK Technik hatte sich bereits im Vorfeld des Urteils intensiv mit den Fragen befasst, die der Klage zugrunde lagen, denn vor der verfassungsrechtlichen Bewertung steht zunächst die Würdigung und Einordnung der Erkenntnisse der Informatik und Informationstechnik. In Fachkreisen und in der Fachpresse wurden insbesondere im Jahre 2007 diese Fragen aus juristischer Sicht und aus Sicht der Fachinformatik ausgiebig diskutiert.[3] Der AK Technik wurde von der Daten-

2 Urteil des BVerfG zum „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme"; BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1–333), http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html.
3 Prof. Dr. Hartmut Pohl, FH Bonn-Rhein-Sieg in DuD, 9/2007; mit dem Autor hatte das Technikteam meiner Dienststelle ebenso fachlich konferiert, wie mit zahlreichen anderen Organisationen und Fachleuten.

schutzkonferenz beauftragt, die technischen Hintergründe der Online-Durchsuchung zu untersuchen und zu beschreiben. In seinem **Grundsatzpapier „Technische Aspekte der Online-Durchsuchung"** vom 21. September 2007 hatte der Arbeitskreis Technik (federführend MV) schließlich für die Konferenz auf der Grundlage der damaligen Aussagen des Bundesinnenministeriums die Risiken der Onlinedurchsuchung aus technischer Sicht analysiert und bewertet und eine Systematisierung der Probleme und Konsequenzen aufgezeigt.

Diese Gesamtbetrachtung floss in die **Entschließung** der Konferenz der Datenschutzbeauftragten am **25./26. Oktober 2007** ein. Im Ergebnis plädierte diese für ein „Nein zur Online-Durchsuchung". Als Gründe sind ebenso naheliegende wie schwerwiegende Aspekte zu nennen:

Eine heimliche Online-Durchsuchung führt zu erheblichen Eingriffen in die Grundrechte. Betroffen sind das informationelle Selbstbestimmungsrecht, die Unverletzlichkeit der Wohnung und das Fernmeldegeheimnis (Telekommunikationsgeheimnis). Der Computer hat inzwischen im Alltag der meisten – und künftig wohl fast aller – Menschen eine zentrale Bedeutung für die Generierung, Gestaltung und Aufbewahrung privatester Informationen: Angefangen bei Fotografien und Reiseberichten und grenzenlos fortsetzbar bis in die Tiefen der persönlichsten Privatsphäre in Form von Tagebuchaufzeichnungen, persönlichen Briefen, Gedanken, Bewertungen sowie politischen und religiösen Überzeugungen und Gefühlen.

Sofern also die rechtliche Erlaubnis der Installation von Überwachungssoftware, etwa mit Hilfe des Internets oder durch die Versendung von E-Mails unter dem Namen einer anderen Behörde, erwogen wird, stellt dies einen tatsächlichen, bis zur Kenntnisnahme und Auswertung aber mindestens latenten, in jedem Fall aber schwerwiegenden Informationszugriff auf restlos alle genannten Ressourcen auf dem angegriffenen IT-System dar. Sofern zudem das unbemerkte Eindringen in Wohnungen zu diesem Zweck nicht ausgeschlossen wird, kommt der Schutzbereich der Unverletzlichkeit der Wohnung hinzu.

Eine weitere Verstärkung der Eingriffsintensität tritt durch die technischen Möglichkeiten auf, Art und Dauer zu verlängern. Denn bei dem heimlichen Zugriff auf informationstechnische Systeme ging und geht es nicht nur um die „Online-Durchsicht" als einmalige Durchsuchung und die damit verbundene Übertragung von Festplatteninhalten an die Strafverfolgungs- oder Sicherheitsbehörden. Vielmehr stand und steht auch die anhaltende Überwachung, das Ausspähen von Passworten und die Protokollierung aller elektronischen Aktivitäten zur Debatte.

Unter informationstechnischen Systemen sind nicht nur klassische Computer wie PC und Laptop zu verstehen. Betroffen sind alle informationsverarbeitenden Systeme, die relevante Daten verarbeiten. Dazu gehören beispielhaft auch Computernetze und ihre Komponenten, Mobiltelefone, PDA, Netbooks, Server u. v. m., die in die heimliche Durchsuchung einbezogen werden können. Dabei ist die Feststellung des Computers einer Zielperson technisch ohne Zusatzinformationen nicht ohne weiteres möglich. Die Gefahr ist daher sehr groß, dass von einer solchen Maßnahme eine Vielzahl von – auch unverdächtigen – Nutzern betroffen sein werden.

Fest steht, dass sich der unantastbare Kernbereich privater Lebensgestaltung bei Online-Durchsuchungen bei der Datenerhebung nicht durch technische Mittel schützen lässt. Ein automatisiert erzwungener Kernbereichsschutz ist somit nicht realisierbar. Der Schutz kann somit nur durch organisatorische Maßnahmen sichergestellt werden.
Darüber hinaus wird eingeräumt, dass sich mit Hilfe der entsprechenden Software die auf den Festplatten gespeicherten Inhalte manipulieren ließen, was die Beweiseignung der gewonnenen Erkenntnisse und damit – jedenfalls bei der Verfolgung von Straftaten – die Geeignetheit der Online-Durchsuchung in Frage stellt.
Es bleibt auch die aus datenschutzpolitischer Sicht grundsätzliche Befürchtung, dass Online-Durchsuchungen entsprechend dem technischen Fortschritt als Standardmaßnahme künftig auch bei Gefahren und Straftaten von geringerer Bedeutung gesetzlich gefordert, durchgesetzt und angewandt werden könnten.
Eine weitere offene Frage ist die praktische Wirksamkeit der Maßnahme gerade bei der Zielgruppe. Es ist davon auszugehen, dass Terrorverdächtige Mittel und Wege finden werden, durch geeignete Gegenmaßnahmen eine erfolgreiche Online-Durchsuchung zu verhindern. Die heimliche Online-Durchsuchung führt deshalb voraussichtlich nicht zu mehr Sicherheit, aber sicher zu mehr Einschränkungen der Freiheit.

… und die Notwendigkeit, Gesetze nachzubessern

Die DSB-K appellierte mit der Entschließung vom 25./26. Oktober 2007 aus den genannten Gründen an die Bundesregierung, die Landesregierungen und die Parlamente, auf die Einführung der repressiven und präventiven Online-Durchsuchung zu verzichten und das Urteil des Bundesverfassungsgerichts in dem Verfahren gegen die Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalens abzuwarten.
Nach dem Urteil vom 27. Februar 2008 begann die Zeit der Interpretationen. Mit einer erneuten Entschließung hatte daher die 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008 in Berlin bekräftigt[4], dass bei Gesetzgebungsvorhaben die Vorgaben des Bundesverfassungsgerichts bei der Online-Durchsuchung beachtet werden sollen.
Die DSB-K begrüßte, dass das Bundesverfassungsgericht die Regelung zur Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalen für nichtig erklärt hatte. Durch das aus Art. 1 und 2 GG abgeleitete „neue“ Grundrecht ist auch der Staat in der Verantwortung, sich aktiv für die Vertraulichkeit und Integrität informationstechnischer Systeme einzusetzen. Das Bundesverfassungsgericht verpflichtet den Staat, im Zeitalter der elektronischen Kommunikation

4 Die Entschließung ist von einer adhoc-Arbeitsgruppe der Datenschutzbeauftragten des Bundes und der Länder in Berlin vorbereitet worden, bei der aus meiner Geschäftsstelle die juristischen wie auch die technisch-organisatorischen Mitarbeiter mitgewirkt haben. Die Arbeitsgruppe hat am 11. März 2008 über die Folgen des Urteils des Bundesverfassungsgerichts vom 27. Februar 2008 beraten.

Vertraulichkeit zu gewährleisten. Die Gesetzgeber in Bund und Ländern sind gehalten, diesen Auftrag konsequent umzusetzen.

Erforderlich sind Verbesserungen der gesetzlichen Regelungen, die die Bürgerinnen und Bürger vor einer „elektronischen Ausforschung" schützen sollen. Diese Weiterentwicklung des Rechtes muss den Vorgaben des Gerichts, insbesondere im Hinblick auf technische Entwicklungen, Rechnung tragen. Gerade vor dem Hintergrund, dass Bund, Länder und Kommunen verstärkt auf automatisierte und Internet gestützte Dienstleistungen (eGovernment) setzen, stellt die Akteure vor die Aufgabe, einen wesentlichen Beitrag zu leisten, Vertrauen in die Sicherheit von eGovernment herzustellen.

Hervorzuheben sind auch die Ausführungen des Bundesverfassungsgerichts zum technischen Selbstschutz der Betroffenen. Unter dem Begriff Selbstdatenschutz habe ich an anderer Stelle dieses Berichtes die Bedeutung und unsere präventiven Aufklärungsaktivitäten dazu hervorgehoben. Die Möglichkeiten jedes IT-Nutzers, sich gegen einen unzulässigen Datenzugriff zu schützen, etwa durch den Einsatz von sicheren Verschlüsselungsverfahren zur kryptierten E-Mail-Kommunikation und Datenspeicherung, durch den Einsatz manipulationsgesicherter Betriebssystemumgebungen oder durch anonymisiertes Surfen im Internet, dürfen nicht rechtlich unterlaufen oder eingeschränkt werden.

Besonders zu begrüßen ist auch, dass das Bundesverfassungsgericht das neue Datenschutzgrundrecht mit besonders hohen verfassungsrechtlichen Hürden vor staatlichen Eingriffen schützt. Es obliegt nun den Gesetzgebern in Bund und Ländern, diese Eingriffsvoraussetzungen zu respektieren. Deshalb hat sich die DSB-Konferenz in diesem Zusammenhang gegen Online-Durchsuchungen durch die Nachrichtendienste ausgesprochen.

Herausragende Bedeutung kommt durch das Urteil auch erneut der Definition des unantastbaren Kernbereiches privater Lebensgestaltung zu. Denn diesen zu gewährleisten, erstreckt sich auch auf Eingriffe in informationstechnische Systeme. So kommt es darauf an, Inhalte, die diesen Kernbereich betreffen und deren Erhebung bei verdeckten Online-Ermittlungen in der praktischen Anwendung tatsächlich unvermeidbar sind, unverzüglich zu löschen. Im Gesetz und in der tatsächlichen organisatorischen Verfahrensgestaltung halte ich es für unabdingbar, eine Weitergabe oder Verwertung dieser Inhalte absolut auszuschließen.

Da die „Quellen-Telekommunikationsüberwachung" eine andere verfassungsrechtliche Einordnung in Artikel 10 des Grundgesetzes besitzt als die Online-Durchsuchung, ist deren Durchführung auch in einer eigenen Rechtsgrundlage geregelt. Da diese jedoch vergleichbare schwerwiegende Eingriffe in die Grundrechte darstellt und die Quellen-Telekommunikationsüberwachung mit der Infiltration von IT-Systemen einhergeht, halte ich es für dringend geboten, die gleichen Schutzvorkehrungen zu treffen, wie für die Online-Durchsuchung selbst.

Zu überdenken: Schutzziele und technisch-organisatorischer Datenschutz

Bedingt durch die Neubestimmung des „Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" ist m. E. endgültig deutlich geworden, dass eine Neuorientierung zu der Systematik der Sicherungs- und Schutzziele bei den Regelungen des technischen und organisatorischen Datenschutzes erforderlich ist. Wir sprechen hier auch von dem Stand der Technik entsprechenden Gestaltungsregeln, die zur Gewährleistung einer angemessenen Datensicherheit benötigt werden. Bereits 1999 stand zur Diskussion, ob bei der Novellierung des NDSG die so genannten „10 Gebote" des § 7 NDSG nicht einer modernisierten Neufassung weichen sollten. Damals ließ sich dieser Vorschlag nicht durchsetzen.
Heutige, allgemein anerkannte Gestaltungsziele der informationstechnischen Sicherheit sind

- Vertraulichkeit
- Integrität
- Verfügbarkeit und
- Authentizität.

Sie werden in neueren Datenschutzgesetzen ergänzt um die Gebote zur

- datensparsamen Verfahrensgestaltung sowie
- zur Transparenz und
- Revisionsfähigkeit

der Verfahren. Diese modernen Sicherungsziele sind technologieunabhängig; sie stellen einen allgemein gültigen Sicherheitsrahmen dar, der auch bei neuen Formen der Datenverarbeitung Bestand haben wird.
Bereits 1999 hatte der AK Technik entsprechende Vorschläge erarbeitet[5], die in der letzten Novellierungsrunde und anlässlich der EU-Datenschutz-Richtlinie unterbreitet worden waren. Unter dem Blickwinkel des Urteils des BVerfG kommen den Begriffen der Datensicherheit und des technischen Datenschutzes und insbesondere der ausdrücklich übernommenen Terminologie „Vertraulichkeit" und „Integrität" eine nicht zu unterschätzende Bedeutung zu.
Um aktuell erneut zu klären, ob die technisch-organisatorischen Regelungen ebenfalls einer Anpassung bedürfen, hat der AK Technik im Oktober 2008 eine länderübergreifende Arbeitsgruppe[6] eingerichtet, die diesen Fragen – auch im Dialog mit Forschung und Lehre – nachgeht. Die ersten Arbeitssitzungen, an dem der Technikbereich meiner Geschäftsstelle beteiligt ist, fanden bereits statt.

5 Arbeitskreis „Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder: „Empfehlungen für die Vereinheitlichung der Regelungen zum technischen und organisatorischen Datenschutz", Düsseldorf, 18. Februar 1999.

6 Arbeitsgruppe „Novellierungsbedarf der datenschutzrechtlichen Technikregelungen" des AK Technik unter Federführung des Bundesbeauftragten für Datenschutz und Informationsfreiheit unter Mitwirkung der Landesbeauftragten für den Datenschutz aus Berlin, Hessen, Niedersachsen, Rheinland-Pfalz, Sachsen-Anhalt, Schleswig-Holstein und Thüringen.

Weitere Fragen stellen sich m. E. zu

- dem Bedarf an verfahrensrechtlichen Regelungen,
- gesetzlich geforderten Sicherheitskonzepten für IT-Verfahren aufgrund einer Risikoanalyse (wie z. B. im Berliner Datenschutzgesetz realisiert) sowie
- einer Pflicht zu einem geeigneten Prozessmanagement.

Über die Abwehrfunktion hinaus muss der technische Datenschutz auch zu einer System gestaltenden Funktion weiterentwickelt werden. Das Ziel einheitlicher Technikregelungen in den Gesetzen von Bund und Ländern wäre zudem im Interesse von Datensicherheit (IT-Sicherheit) und informationeller Selbstbestimmung sowie dem neuen „IT-Grundrecht" sehr zu begrüßen.
Neue Technikregelungen könnten dazu beitragen, dass auch Synergieeffekte zwischen dem Aufwand für IT-Sicherheit einerseits und für den technischen Datenschutz und Vorabkontrollen andererseits nutzbar gemacht werden.

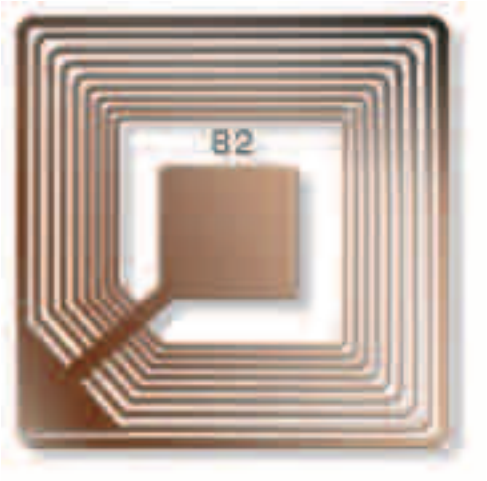
RFID-Chips: Regelungsbedarf wird von Industrie und Handel abgelehnt

RFID (Radio Frequency Identification) ist eine Technologie, mit der miniaturisierte IT-Systeme (RFID-Chips, RFID-Tags) über Funksignale mit Lesegeräten Daten austauschen. Bei den passiven Chips wird die dazu erforderliche elektrische Energie über das Funksignal des Lesegerätes bereitgestellt, so dass sie selbst ohne eigene Stromversorgung auskommen und sehr stark miniaturisiert werden können. Dabei ist je nach angewandter Technik eine Übertragungsreichweite von wenigen Zentimetern bis zu mehreren Metern möglich.
Von der Aussendung eines einfachen Bestätigungssignals bis zur Übertragung komplexerer Datenstrukturen ergeben sich unterschiedlichste Einsatzgebiete. Weit fortgeschritten ist der RFID-Einsatz in den Bereichen Warenlogistik, Produktionsautomation und Diebstahlsicherung. Auch bei Zutrittsberechtigungssystemen, Ausweisdokumenten, Eintrittskarten für Großveranstaltungen und der Tierkennzeichnung findet die zunehmend preiswerter werdende Technologie immer häufiger Anwendung.

Die Industrie preist insbesondere die Kostenvorteile bei Einführung der RFID-Chips. „Die Radiofrequenz-Identifikation (RFID) hat in den vergangenen Jahren Einzug in Wirtschaft, Wissenschaft und Alltag gehalten. Die Möglichkeit, Objekte berührungslos per Funk zu identifizieren, erhöht die Effizienz von Prozessen in den unterschiedlichsten Branchen und nützt Verbrauchern im Alltag", so die Interessenvertretung der Branche[7]. Neben manchen unbestreitbaren Vorteilen sind jedoch auch eine Reihe möglicher Gefahren für das Recht auf informationelle Selbstbestimmung mit dieser Technik verbunden.
Deshalb hatte sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits durch **Entschließungen** im März 2004 und im Oktober 2006 kritisch geäußert und vor unbemerkter und nicht kontrollierbarer Verarbeitung personenbezogener oder -beziehbarer Daten gewarnt. Hersteller und Betreiber wurden zu einem verantwortungsvollen, für die Bürgerinnen und Bürger transparenten und datenschutzgerechten Einsatz der RFID-Technologie aufgerufen.
Für die detailliertere Befassung hat darüber hinaus der Arbeitskreis Technik der DSB-Konferenz die **Orientierungshilfe „Datenschutzgerechter Einsatz von RFID"[8]** herausgegeben, die aus unserer Sicht noch immer Geltung besitzt. Sie wendet sich sowohl an die Anwender als auch die Hersteller von RFID-Systemen, um zur Beachtung datenschutzrechtlicher Grundsätze bei Einsatz und Weiterentwicklung entsprechender Produkte zu motivieren. Der Leitfaden ist allerdings

7 Das Informationsforum RFID e. V. in Berlin vertritt Unternehmen aus den Bereichen Handel, Konsumgüterindustrie, Automobilbranche, IT und Dienstleistung mit dem Zweck, den weiteren Einsatz der Radiofrequenz-Identifikation zu fördern; www.info-rfid.de.

8 Orientierungshilfe „Datenschutzgerechter Einsatz von RFID", herausgegeben vom Arbeitskreis „Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Stand 14. Dezember 2006, www.datenschutz-mv.de/dschutz/informat/rfid/ohrfid.pdf; die OH wurde von der Datenschutzkonferenz im Januar 2007 zustimmend zur Kenntnis genommen.



ebenso geeignet, Kunden und Verbraucher für die möglichen Risiken zu sensibilisieren und ihnen einen kritischen Umgang mit dieser Technik zu ermöglichen.
Das **Informationsforum RFID e. V.** hatte zusammen mit BITKOM, BDI, GS1 Germany und HDE eine gemeinsame Stellungnahme mit Schreiben vom 15. Dezember 2006 als Reaktion auf die Entschließung der DSB-Konferenz verfasst, mit der im Kern ein Regulierungsbedarf für RFID-Technik verneint wird.
Der Thüringer Landesbeauftragte für den Datenschutz hat den Verbänden – nach Befassung im AK Technik und in der DSB-Konferenz im April 2007 – namens der Kollegen das abgestimmte Ergebnis mitgeteilt[9]. Danach begrüßt die Konferenz ausdrücklich, dass die gemeinsame Stellungnahme dem Schutz personenbezogener Daten im Rahmen des breiten Einsatzes der RFID-Technologie einen hohen Stellenwert beimisst. Sie versteht die Stellungnahme daher als Angebot, die Diskussion um eine datenschutzgerechte Ausgestaltung von RFID-Anwendungen gemeinsam konstruktiv fortzuführen.
Entgegen der Kritik haben die Datenschutzbeauftragten „bisher keinesfalls pauschal neue, gesetzliche Regelungen gefordert, sondern vielmehr darauf aufmerksam gemacht, dass die technische Entwicklung zunächst aufmerksam zu beobachten ist. Nur für den Fall, dass die angekündigten bzw. schon abgegebenen Selbstverpflichtungserklärungen der Hersteller und Anwender von RFID-Technik nicht in angemessener Weise zum Schutz der Persönlichkeitsrechte Betroffener beitragen oder vorhandene rechtliche Regelungen Defizite aufweisen, wird eine ergänzende Rechtsetzung erforderlich", so die Stellungnahme weiter.
Die genannte Orientierungshilfe der Datenschutzbeauftragten fordert eine differenzierte Betrachtungsweise und beschreibt detailliert die Risiken beim Einsatz von RFID-Systemen. Anhand unterschiedlicher Einsatz-Szenarien werden die Datenschutzrisiken bewertet. Ausdrücklich berücksichtigt wird dabei die Tatsache, dass der Personenbezug außerhalb des RFID-Tags oder auch durch Verkettung mehrerer zunächst nicht personenbezogener Transaktionsdaten hergestellt werden kann.

„Internet der Dinge"
Es sei hier auch auf die vom Bundesministerium für Bildung und Forschung in Auftrag gegebene „TAUCIS-Studie" hingewiesen. Sie wurde vom „Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein" und dem „Institut für Wirtschaftsinformatik der Humboldt-Universität Berlin" erstellt und setzt sich mit der zunehmenden Allgegenwart der Informationstechnologie in allen Lebensbereichen („Ubiquitäres Computing") und deren Auswirkung auf die informationelle Selbstbestimmung auseinander.

www.lfd.niedersachsen.de
Pfad > Home > Technik und Organisation > Technische Hilfen > RFID

9 Der Thüringer Landesbeauftragte für den Datenschutz hat den Verbänden – nach Befassung im AK Technik und in der DSB-Konferenz – mit Schreiben vom 5. April 2007 als Vorsitzender im Auftrag der 73. DSB-Konferenz das so abgestimmte Ergebnis mitgeteilt.

In der Bewertung der daraus resultierenden Risiken gehen die Auffassungen noch auseinander. Den Risiken für das Recht auf informationelle Selbstbestimmung muss nach Auffassung der Datenschutzkonferenz durch eine datenschutzfreundliche Technikgestaltung und durch eine offensive Informationspolitik auch dann schon Rechnung getragen werden, wenn eine Bedrohung erst durch nachträgliche Herstellung des Personenbezugs etwa über Kundenkarten oder elektronische Bezahlsysteme entstehen kann.
Aus Sicht der Datenschutzbeauftragten werden in der Orientierungshilfe ganz bewusst auch Szenarien betrachtet, deren Realisierung noch nicht erfolgt, in naher Zukunft aber zu erwarten ist. Tatsächlich sind noch längst nicht alle Produkte des Einzelhandels mit individuellen RFID-Tags gekennzeichnet. Der flächendeckende Einsatz dieser Technologie ist aber gerade erklärtes Ziel der Hersteller und der künftigen Anwender etwa im Einzelhandel.
Es ist deshalb ein vordringliches Anliegen der Datenschutzbeauftragten, frühzeitig zu sensibilisieren und eine umfassende Technikfolgenabschätzung einzufordern, um entwicklungsbegleitend alle Möglichkeiten der datenschutzfreundlichen Technikgestaltung nutzen zu können.
Viele technische Detailfragen können abschließend jedoch nur bei der datenschutzrechtlichen Begleitung einzelner Projekte geklärt werden. Das betrifft beispielsweise den jeweiligen Zeitpunkt der möglichen Herstellung des Personenbezugs, aber auch Fragen der Verschlüsselung, der Kennzeichnung einzelner Kommunikationsvorgänge oder der Art und Weise der Deaktivierung von RFID-Tags.

Wir werden insbesondere vor dem Hintergrund, dass die RFID-Technologie auch eine Schlüsselrolle im „Internet der Dinge" (zunehmend verselbstständigte Informations- und Kommunikationsprozesse von Gegenstand zu Gegenstand) zukommt, weiterhin besonderes Augenmerk auf die Entwicklung und die Anwendungen werfen.

Weitere Ausführungen

finden sich in meinem XVIII. Tätigkeitsbericht 2005 / 2006 in den Kapiteln **„Allgegenwärtigkeit von Computern bergen Risiken für die informationelle Selbstbestimmung"** unter
www.lfd.niedersachsen.de
Pfad > Home > Allgemein > Tätigkeitsberichte > 2005–2006

Mobil geortet – mal freiwillig, mal nicht?

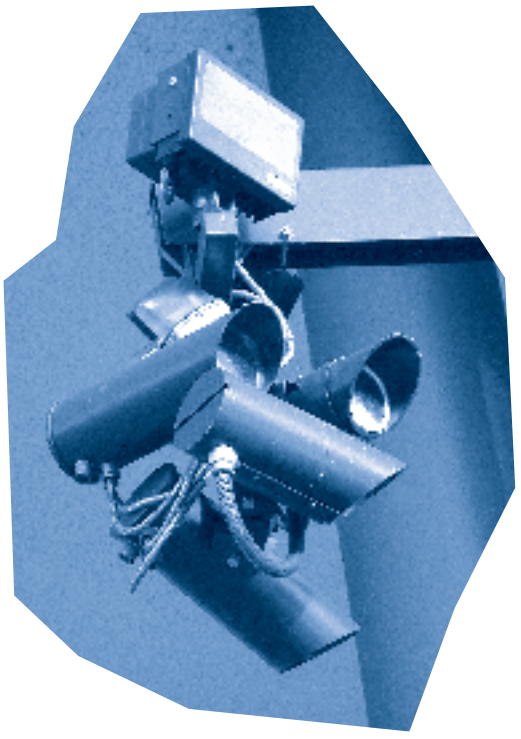
Die Bereiche, in denen der Mensch unbeobachtet bleibt, werden immer weniger. Obwohl das Grundgesetz das Freiheitsrecht aus Artikel 1 (Menschenwürde) und aus Artikel 2 (allgemeines Persönlichkeitsrecht) und das daraus abgeleitete Recht auf informationelle Selbstbestimmung als eines der wichtigsten Menschenrechte der Informationsgesellschaft garantiert, werden staatliche Eingriffsnormen tendenziell immer zahlreicher und intensiver, und sie werden aus technischer Sicht immer vielfältiger und komplexer. Es bedurfte erneut einer ausführlichen Grundsatzentscheidung des Bundesverfassungsgerichtes, um hier Grenzbereiche zu klären, die das Grundgesetz vorgibt. Das höchste deutsche Gericht hat das Recht auf den absoluten Schutz des Kernbereichs privater Lebensgestaltung vor staatlichen Eingriffen zuletzt in seinem Urteil 2007 beschrieben. Dies war einmal mehr nötig, weil die Gesetzgeber in Bund und Ländern immer wieder die verfassungsmäßigen Grenzen der Eingriffsrechte überschritten hatten.

1 BvR 370/07 vom 27.2.2008, http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html

Die faktischen Überwachungen im nicht-öffentlichen Bereich treten jedoch ebenso zahl- und facettenreich zutage und lassen immer weniger Raum für ein unbeobachtetes Leben der Menschen.

www.lfd.niedersachsen.de
> Home > Service-Angebote > Technische Hilfen

Videoüberwachung und Abhörtechnik ist das eine …



Inzwischen verdichtet sich zum Beispiel das Videoüberwachungsnetz in Ballungsräumen, auf öffentlichen Straßen und Plätzen sowie an Verkehrsknoten im öffentlichen Raum.
Und der Überwachungsdrang setzt sich im privatrechtlichen Umfeld, welches für die Öffentlichkeit zugänglich gehalten wird, vehement fort. Preiswerte Videotechnik findet sich in immer mehr Geschäften als Maßnahme zum Diebstahlschutz.

… Tracking ist das andere

Auch andere Mittel und Wege der Überwachung und der Spurverfolgung – des so genannten Tracking – setzen sich inzwischen im Privatumfeld durch. Da inzwischen fast jede Person ein Mobiltelefon bei sich trägt, hält jeder darin auch stets eine potentielle Ortungstechnik für den minütlichen Aufenthaltsort bereit. Die Feststellung, wer sich wann, wo und wie lange aufgehalten hat, ist durch den Funkkontakt zwischen dem Handy und der GSM-Funkzelle des Netzbetreibers, also der Basisstation, bei der es eingebucht ist, faktisch nahezu lückenlos registriert.
Zusätzlich zur Identität der Funkzelle können auch andere Messungen, wie die Signalstärke und die Signallaufzeit verwendet werden, um die rechnerische Genauigkeit der geografischen Position des Handybesitzers zu erhöhen. Die Her-

steller von Mobilfunkgeräten gehen auch zunehmend dazu über, so genannte Assisted Global Positioning Systems (A-GPS) einzusetzen, denn Handys beherrschen oftmals auch die mobile Navigation mittels GPS. Damit gelingt durch Übermittlung von Hilfsdaten in der Kombination von GPS-Daten mit denen des GSM-Funknetzes eine schnellere GPS-Positionsbestimmung.

Ortungsdienste (so genannte Location Based Services) machen sich die Möglichkeit der geografischen Positionsbestimmung zunutze, um entsprechende Dienstleistungen anzubieten. Sofern dies freiwillig geschieht, soweit also der Gerätebesitzer diese Ortungstechnik selbst in Auftrag gibt, entspricht dies prinzipiell seinem Selbstbestimmungsrecht zur Verwendung der ihn betreffenden personenbezogenen Daten. Das setzt allerdings voraus, dass dies auch bewusst und gewollt geschieht. Ein beiläufiges rechtliches „Inkaufnehmen" von Speicherungen und Weiterverarbeitungen von Ortungsdaten durch die Unterschrift des Kunden ohne wirkliche Kenntnis des Inhaltes von „Kleingedrucktem" ist jedoch die häufigste Art, auf die selbstbestimmte Informationssteuerung über seine eigenen Daten zu verzichten. Über die Gefahren klären die Anbieter im Vorfeld auch zu wenig auf.

Sinnvoll kann die Inanspruchnahme von Ortungsdiensten vielleicht sein, um für einen Notfall die schnelle Ortung für schnelle Rettungseinsätze – etwa für chronisch herzkranke Menschen – zu ermöglichen. Auch bei dem Abonnement einer Suchfunktion, mit dem der Aufenthaltsort des Kindes überwacht werden kann, ist zunächst der Schutz des Kindes das positive Ziel. Die Persönlichkeitsrechte eines Kindes werden andererseits damit aber erheblich eingeschränkt. Die erforderliche Abwägung zwischen Sicherheitsaspekten und den rechtlichen und auch pädagogisch sinnvollen Freiräumen von Kindern oder Jugendlichen bleibt eine wichtige Herausforderung.

Es traten in den letzten Jahren zunehmend auch „Dienstleistungs"-Angebote in Erscheinung, die der heimlichen Überwachung anderer Personen dienen. Damit wurde auch die Kenntnis des Standortes z. B. der Partnerin oder des Partners möglich, ohne dass diese Kenntnis von der Überwachung hatten. Das Handy mutiert damit faktisch zu einem „Bewegungsmelder", der die Position auf einer Internetplattform zur Verfügung stellt. Mit dieser Technik wird beispielsweise auch der Aufenthaltsort und das Bewegungsprofil mobil eingesetzter Mitarbeiter erkennbar. Im Berichtszeitraum erhielt ich immer häufiger Anfragen von Rat suchenden Bürgerinnen und Bürgern, wie die Ortungstechnik und die genannten Dienste funktionieren und ob sie zulässig seien.

Der Bundestag hat inzwischen am 26. März 2009 eine Änderung des Telekommunikationsgesetzes (TKG) verabschiedet, mit der die Eindämmung der heimlichen Ortung von Handynutzern geregelt werden soll. Ziel ist es, die Möglichkeit zum Aufspüren von Handys durch die Übermittlung der Standortdaten genauer zu beschreiben. Damit soll die Missbrauchsgefahr von Tracking-Diensten sowie sogenannten Freundesuchservices über Location Based Services entgegengewirkt werden. Künftig muss die erforderliche Einwilligung in die Feststellung des Standortes eines Mobilfunkendgerätes zum Zweck der Übermittlung an einen anderen Teilnehmer oder Dritte, die nicht Anbieter des Dienstes sind, „ausdrücklich, gesondert und schriftlich erteilt" werden.

Eine – wenn auch eingeschränkte – Kontrollfunktion wurde festgeschrieben: In den Fällen, in denen der Standort eines Mobilfunkgerätes an einen anderen Teilnehmer oder Dritte außerhalb des Diensteanbieters übermittelt wird, hat dieser Diensteanbieter den Teilnehmer nach höchstens fünfmaliger Feststellung des Standortes über die Anzahl der erfolgten Standortfeststellungen mit einer Textmitteilung zu informieren.

Die neue Regelung ist in § 98 Abs. 1 Sätze 2 und 3 Telekommunikationsgesetz (TKG) enthalten

Damit wird zwar nicht absolut verhindert, dass zum Beispiel ein Partner mit dem verschenkten Handy den anderen Partner ohne dessen Kenntnis wiederholt ortet. Aber dies wird zumindest deutlich erschwert.

Informationsgesellschaft: Dem „stets erreichbar" folgt das „stets sichtbar"

Was trotz der einschränkenden Regelungen des Telekommunikationsgesetzes an Risiken für die Freiheitsrechte bleibt, ist der Entwicklungsprozess in der Informationsgesellschaft, der sich in der Online-Community widerspiegelt. Selbst bei der Freiwilligkeit bleiben Risiken für das Selbstbestimmungsrecht, die man sich oft erst zu spät bewusst macht. Das – wenn auch freiwillige – Registrieren in Ortungsdiensten, um in einem Freundeskreis, einen bestimmten oder sogar für einen nur bestimmbaren, aber im Prinzip unbekannten Personenkreis ortbar zu sein, birgt das Risiko, sich einem nicht überschaubaren Ausmaß von Transparenz auszusetzen, dessen Tragweite nicht immer gleich erkennbar ist. Und selbst wenn die Freischaltung durch das Abonnement vielleicht irgendwann vergessen wird, wird der Ortungsauftrag und damit die „gläserne Situation" bestehen bleiben.

Es bleibt eine allgemeingültige Erkenntnis, dass die Medienkompetenz nicht nur des mündigen Bürgers, sondern vor allem der Heranwachsenden gestärkt werden muss. Hierbei reicht es eben nicht aus, nur die Handhabung von Internet, Anwendungssoftware und Handy zu erlernen. Es gehört ebenso das Schärfen des Risikobewusstseins gegenüber sozialer Kontrolle in der Onlinewelt dazu.

Medienkompetenz schließt auch ein, die Maßnahmen zu kennen und zu beherrschen, die zur Durchsetzung rechtlicher und vor allem auch tatsächlicher (technischer und organisatorischer) Selbstbestimmtheit führen. In manchen Fällen kann die Lösung auch im Verzicht auf bestimmte vermeintliche Innovationen liegen.

Mobiler offener Informationstresor: Das Handy

Das Handy ist in den letzten Jahren zum persönlichen Assistenten geworden: zum Kurznachrichtensender (SMS) und elektronischen Notizzettel, zum Adressbuch und zum Navigationsgerät mittels Global Positioning System (GPS), zum MP3-Player und zum Radio, zur Digitalkamera und nicht zuletzt natürlich zum Telefon für die Tasche. Die unaufhaltsam weiterentwickelten Smartphones und Personal Digital Assistants (PDA) bieten fast alle Leistungsmerkmale, die man von „erwachsenen" Computern kennt. Weder auf das Lesen und Schreiben von E-Mails, noch auf Tabellenkalkulation oder den Zugriff via Funknetz (WLAN), Hotspot und Breitbandmobilfunknetz auf die Geschäftsdaten im Büro muss der Besitzer verzichten.

Aber ob Handy, Smartphone oder PDA, das kleine Gerät repräsentiert noch mehr: Es wird inzwischen oftmals als Identifikationsmerkmal des Einzelnen verstanden, ein Gegenstand, dessen Abwesenheit ähnlich verlustreich wäre, wie die des Portemonnaies, des Schlüsselbundes oder des Personalausweises. In einer Studie haben 43,2 % der 18- bis 35-jährigen geäußert, sich kein Leben ohne Mobiltelefon vorstellen zu können. 10,6 % gaben an, alle wichtigen persönlichen Daten darauf zu speichern.

In der Studie „Online Survey 2008" von BITKOM/ Goldmedia haben 43.2 % der 18 bis 35-jährigen geäußert, sich kein Leben ohne Mobiltelefon vorstellen zu können. 10,6 % gaben an, alle wichtigen persönlichen Daten darauf zu speichern. Quelle: http://www.bitkom.de/files/documents/081009_BITKOM_Goldmedia_Mobile_Life_2012(1).pdf

Schillernde Funktionen – wenig Sicherheitsbewusstsein

Wenn man berücksichtigt, dass dem Handy die herausragende Stellung eines persönlichen Begleiters zukommt, wird deutlich, wie sensibel die darauf gespeicherten Daten sein können. Es liegen sämtliche Kontaktdaten mit Anschrift, Telefonnummer, E-Mail-Adresse, teils mit wertenden oder mindestens ergänzenden Informationen der vielleicht gesamten Geschäftspartner-, Bekannten-, Kollegen- und Freundeskreise in Datenstrukturen vor. Angereichert wird dies mitunter durch zahllose Text- und Tabellendateien. Aber auch vor der bequemen, bei fehlender Verschlüsselung aber oft ungesicherten Speicherung von Passwörtern und PINs schrecken manche nicht zurück.

Warum birgt dies Gefahren für personenbezogene Daten?

Zum einen droht der Verlust und der Missbrauch des Gerätes und damit aller darauf liegenden Daten, sofern sie unverschlüsselt gespeichert sind.

Außerdem kann in einem unbeaufsichtigten Augenblick die Speicherkarte mit einem Handgriff herausgezogen und entwendet oder auch nur kopiert werden. Ein Fall, der in der Gastronomie oder in Fernreisezügen leicht vorstellbar ist.

Zum anderen verfügen die Geräte über verschiedene drahtlose Verbindungen wie Wireless Local Area Network (WLAN), Bluetooth oder Infrarot. So-

Speicherkarten (auch Flash Card, Memory Card) gibt es in verschiedenen Typen/Bauarten, z. B.:

- Memory Stick (MS)
- Secure Digital Memory Card (SD)
- Mini-SD
- Micro-SD
- Multimedia Card (MMC)
- Compact Flash Cards (CF-Card)
- Smart Media Card (SMD)
- xD-Picture Card

Sie weisen verschiedene, immer höhere Speicherkapazitäten von bis zu 32 GB auf. Damit steigt auch die theoretische Menge gespeicherter sensibler personenbezogener Daten.

als sensibles Multitalent

fern diese aktiviert und unverschlüsselt verfügbar sind, sind auch die auf dem Gerät gespeicherten Daten ungeschützt und können unter Umständen über drahtlosen Kontakt von Unbefugten ausgelesen und kopiert – also gestohlen – werden.
Leider sind die Sicherheitsstandards, die sich für den PC und das Notebook als fast selbstverständlich etabliert haben, für Mobilgeräte nicht serienmäßig installiert. Selbst der Wunsch der Nachrüstung lässt sich nicht immer verwirklichen. Manche Betriebssysteme – vor allem die älteren Versionen – lassen dies nicht zu. Die meisten Geräte kennen noch nicht einmal Antivirus-Software und eine Software-Firewall, um den elementaren technischen Schutz zu gewährleisten. Auch für die Verschlüsselung von Daten auf den Speichermedien sind Lösungen nur durch fachkundige Suche und Beratung zu bekommen. Im Interesse des Selbstdatenschutzes, aber auch des Schutzes für die Kontaktdaten der Gesprächspartner sollte beim Kauf des Gerätes auf diese wichtigen Schutzmaßnahmen nicht verzichtet werden.

Datendiebe ärgern –
Sicherheitstipps zum Diebstahlschutz:

Vorbeugende Maßnahmen:

- Stets die PIN für die SIM-Karte verwenden
- Wenn möglich, Sicherheitscode für das Gerät aktivieren
- die IMEI-Nummer (International Mobile Equipment Identity = 15stellige eindeutige internationale Mobilgerätekennung) merken und an sicherem Ort verwahren
- Gürteltasche nutzen und verdeckte Trageweise statt loser Aufbewahrung
- Auf Softwareausstattung für Sicherheit achten: Personal Firewall, Antivirus-Software, Verschlüsselung für internen Speicher und für Dateien auf Speicherkarten (Flash Cards)
- WLAN nicht unverschlüsselt aktivieren, Benutzerauthentisierung nutzen
- restriktive Datei- und Ressourcenfreigabe auf Betriebssystemebene
- Bluetooth für den Datenaustausch im Nahbereich möglichst meiden oder nur bei Bedarf und im unsichtbaren Modus aktivieren (Grund: Sicherheitsschwächen der verwendeten Protokolle, unkontrollierte Ausbreitung der Funkwellen)
- Infrarot-Verbindungen meiden (Grund: da das Protokoll keine Authentisierung vorsieht, kann ein Angreifer Schadcode/Daten über die IrDA-Schnittstelle an einen PDA senden); diese Technik verliert allerdings an faktischer Bedeutung
- Firmware des Gerätes, Betriebssystem und Anwendungsprogramme regelmäßig und rechtzeitig aktualisieren (Sicherheitspatches, Updates)

Besonders attraktiv – leider auch für den Dieb – sind teure Geräte ohne SIM-Lock, also ohne Begrenzung auf einen bestimmten Netzanbieter. Hier reicht eine neu eingelegte SIM-Karte, um das Gerät unberechtigt weiternutzen oder auf dem Schwarzmarkt als vollwertig anbieten zu können. Als Gegenmaßnahme sollte das Gerät mit einem Sperrcode (Sicherheitscode) versehen werden. Je nach Einstellung wird das Gerät so nach einer vorbestimmten Zeit ohne Aktivität bzw. nach dem Ausschalten vollständig deaktiviert. Ohne den Code ist das Gerät grundsätzlich nicht zu reaktivieren. Dies stellt jedoch nur eine relative Sicherheit dar, weil durch Generieren eines Sicherheits-Mastercodes der Code umgehbar ist.

Bestimmte Hersteller bieten inzwischen verbesserte Verfahren an. Bei unberechtigtem Besitz und nach dem Einlegen einer anderen SIM-Karte sendet das Gerät eigenständig eine SMS mit der Nummer dieser anderen SIM-Karte an eine vorher festgelegte Teilnehmernummer. Bei strafrechtlicher Verfolgung könnte die Polizei somit eine Nummernidentifikation und eine Ortung durchführen.

Repressive Maßnahmen bei Verlust:

- Antrag zur Sperrung der Teilnehmernummer, soweit möglich unter Angabe der eigenen Nummer und eines vereinbarten Passwortes
- Antrag zur Sperrung des Gerätes durch Angabe der geräteabhängigen IMEI-Nummer. (vorher notieren; Anzeige durch Eingabe von *#06#).

Auch Diebstahlschutz ist Datenschutz

Jedes Jahr werden tausende Mobilfunkgeräte gestohlen. Jeder dieser Fälle ist auch ein Datenverlust und eine potentielle Verletzung der Vertraulichkeit von personenbezogenen Daten.

Bürger suchen Rat

Wir erhalten häufig Anfragen zu Datenschutzaspekten, die im Mobilfunk eher das Telekommunikationsrecht betreffen, etwa zur Zulässigkeit und Handhabung der Vorratsdatenspeicherung oder der Mobilfunkortung. An der Tatsache, dass uns viel seltener Fragen erreichen, die sich auf die eigenen Handhabung der Datenschutzmaßnahmen (Selbstdatenschutz) oder auf die Anforderungen an die Technik beim Kauf beziehen, wird erkennbar, wie lückenhaft das Sicherheitsbewusstsein im Allgemeinen ausgeprägt ist.

Landesverwaltung vorbildlich: Schritt eins ist getan

Angesichts der vorgenannten Risiken habe ich auch die Standards bei den Geräten der Landesverwaltung in Augenschein genommen. Der Landesbetrieb für Statistik und Kommunikationstechnologie Niedersachsen (LSKN) als IT-Dienstleister für die Landesbehörden hat in dem Projekt „Sicherer PDA“ inzwischen eine Standardlösung für den Warenkorb entwickelt, die einen hohen Sicherheitsstandard für PDA erfüllt und damit auch dem Datenschutz zugute kommt. Das Produkt wird nur mit einer zertifikatsbasierten Authentisierung (Maschinenzertifikat) am Gateway (der Vermittlungsstelle als Übergang zum Netz) in Betrieb genommen. Es besteht ein sicherer VPN-Zugang (ein sicherer Tunnel mittels Virtual Private Network) auf dem Gerät für Dokumente und E-Mails (Internet und Intranet). Der gesamte Datenverkehr zwischen Server und Gerät ist mit dem Sicherheitsprotokoll IPSec verschlüsselt. Auf dem PDA wird die Datenhaltung verschlüsselt. Eine Virenschutz-Software stellt den Schutz vor Schadsoftware sicher. Einige Fragen bleiben hier jedoch noch für den Datenschutz offen.

Datenschutzempfehlungen

Um speziell für die inzwischen überbordenden Funktionen Handlungsempfehlungen für den Datenschutz geben zu können, habe ich derzeit ein Projekt gestartet, mit dem für Smartphones und PDA aktuelle Maßnahmen zum Datenschutz in einem Leitfaden definiert werden sollen. Zielgruppe sind sowohl Privatpersonen als auch behördliche und geschäftliche Anforderungen. Dabei werden auch die vom LSKN gesammelten Erkenntnisse aus Sicht der IT-Sicherheit Berücksichtigung finden.

www.lfd.niedersachsen.de
Home > Service-Angebote > Technische Hilfen
Orientierungshilfe „Datenschutz in drahtlosen Netzen“
http://www.lfd.m-v.de/dschutz/informat/wlan/oh_wlan.pdf


daten
schutz

Mehr denn je nötig: Aktiver Selbstdatenschutz

Um Datenschutz wirksam werden zu lassen, bedarf es zunächst materiellrechtlicher Regelungen mit realitätsnahen und wirksamen Festlegungen zu Rechten und Pflichten, also Vorschriften, die den Schutz der Persönlichkeitsrechte durchsetzen können. Zusätzlich sind organisatorische Pflichten von Unternehmen, Behörden und Institutionen zu regeln, um Datenschutz systematisch umzusetzen. Und drittens ist es erforderlich, bei der Entwicklung und dem Betrieb von Technik und von Software technische Maßnahmen zu ergreifen, die angemessen und wirksam sind, um diese Ziele auch tatsächlich zu erreichen.

Wer den Schutz seiner personenbezogenen Daten jedoch nicht ausschließlich gesetzlichen Regelungen und der verantwortungsvollen Umsetzung Anderer anvertrauen will und wer auch nicht daran glaubt, dass dieser Schutz von allen Softwareherstellern, Technikanbietern und Webdiensten immer technisch einwandfrei umgesetzt wird, der legt eine berechtigte Skepsis an den Tag. Denn es muss mehr geschehen, um dem Datenschutz Geltung zu verschaffen. Durch aktiven Selbstdatenschutz kann jede Person vielen Fehlentwicklungen vorbeugen. Mein dringender Rat dazu lautet, das allgemeine Sicherheitsbewusstsein zu schärfen und sich stets zu überlegen, wie man zur Selbsthilfe greifen kann.

Hilfen zur Selbsthilfe

Besonders im technischen Bereich droht eine Unzahl von Fallen und versteckten Gefahren. Ich habe deshalb durch die Aktionsreihe Selbstdatenschutz bereits vor einigen Jahren Hilfen zur Selbsthilfe entwickelt, mit denen die wichtigsten Schutzmaßnahmen direkt erkannt und umgesetzt werden können:

1. **Der 24-Stunden-Grundkurs „Datensicherheit“**
   für private Anwender sowie kleine Gewerbebetriebe wurde in Zusammenarbeit mit dem Landesverband der Volkshochschulen Niedersachsen e. V. entwickelt und zielt auf Grundlagenkenntnisse in Datensicherheit und Datenschutz von der Absicherung des Betriebssystems, über Schutzmaßnahmen im Internet und beim E-Mail-Verkehr bis zur Datenverschlüsselung. Der Kurs steht bundesweit allen Volkshochschulen zur Aufnahme in ihr Programmangebot zur Verfügung.
2. **Kooperation mit privaten Initiativen**
   Meine Publikation *„Sicherheit in Funknetzwerken“* in der Reihe „System- und Datensicherheit für Jedermann“ wurde mit Hilfe der Initiative „hi-senior“ (ein Zusammenschluss interessierter und versierter PC- und Internetnut-

Grundschutz ist das Mindeste

Grundsätzlich gilt, den Rechner nicht direkt mit dem Internet zu verbinden sondern eine Firewall zwischenzuschalten. In Firmennetzwerken sind dies mehrfache Hardware-Firewalls, im privaten Nutzungsbereich meist eine Personal Firewall (Softwarelösung).

Die zweite der wichtigsten Schutzmaßnahmen sind Scanner gegen Malware (Viren, Spyware, Rootkits).

Angriffe erfolgen auf bestimmte Anwendungsprogramme. Dies wird z. B. möglich durch Sicherheitslücken in Browsern oder über modifizierte PDF-Dateien. Dieser Grundschutz ist in der Lage, die wichtigsten Angriffe abzuwehren.

Add-ons – leider auch mit Risikozuschlag

Viele Webseiten kommen inzwischen nicht mehr ohne JavaScript und Adobe Flash Player aus. Will man nicht auf deren Funktionalität verzichten, kommt man nicht um deren Aktivierung herum und schaltet damit auch die Risiken mit ein.

„Cookies Plus“:
Hochverrat beim Filmchen-Gucken

Neue Sicherheits-Herausforderungen stellen die Flash-Cookies des Macromedia Flash Players des Herstellers Adobe (auch Local Shared Objects – LSO – genannt) dar, da diese nicht im Browser deaktivierbar sind.

Das Löschen der „verräterischen“ Cookies muss manuell oder per Software (z. B. Flash-Cookie-Killer, Flash-Cookie-Manager oder mittels Erweiterungen beim Firefox-Browser) erfolgen.

Hilfe zum Einstellen bietet der Hersteller Adobe unter http://www.macromedia.com/support/documentation/de/flashplayer/help/settings_manager03.html.

zer der „50plus-Generation“ aus Hildesheim (www.hi-senior.de) auf seine Anwendbarkeit getestet. In einer aktualisierten Version steht die Schrift unter www.lfd.niedersachsen.de > Service-Angebote > Selbstdatenschutz als PDF zum Download bereit und ist nach „PC-Sicherheit für Einsteiger“ das zweite Werk in dieser Reihe.

3. **Testangebote: „Netzwerkcheck“ in Kooperation mit Heise Security**
   Als interaktives Angebot für einen PC-Selbsttest wurde bereits vor dem Berichtszeitraum gemeinsam mit dem Heise Zeitschriften Verlag (c't / Heise Security) ein **Netzwerkcheck** entwickelt, der kostenlos online zur Verfügung steht. Dabei werden über eine Netzwerkverbindung zum aufrufenden Rechner dessen für den Internet-Verkehr möglicherweise geöffneten Anschlüsse geprüft (Port-Scan). Das Scan-Ergebnis wird aufgelistet, bewertet und zur Verfügung gestellt. Im Normalfall sollten die meisten Ports geschlossen sein. Werden verdächtige offene Anschlüsse erkannt, ergeben sich klare Handlungsempfehlungen zur Absicherung des getesteten Systems. Da der Anwender mit Bordmitteln nicht in der Lage ist, die Existenz derartiger Schlupflöcher aufzuspüren, stellt der auf unserer Webseite unter www.lfd.niedersachsen.de > Service-Angebote > Selbstdatenschutz > Testangebote aufrufbare Service ein hilfreiches und häufig frequentiertes Mittel zur Abwehr möglicher Angriffsszenarien dar.

Der Bedarf steigt

Auch im Berichtszeitraum wurden zahllose schriftliche und telefonische Anfragen an meine Geschäftsstelle herangetragen, denen die Sorge um die persönlichen Daten durch die zunehmende Durchdringung des Alltages mit Informationstechnik und vor allem mit Internet basierten Diensten zugrunde liegen. Spätestens durch die Vorfälle mit Datenschutzverstößen, die die Öffentlichkeit ab Frühjahr 2008 massiv wahrgenommen hat, stellte sich ein spürbarer Anstieg des Interesses und damit der Beratungsanfragen zum Selbstdatenschutz ein.

Beratung mit hoher Akzeptanz

Auch wenn der Begriff „Selbstdatenschutz“ nicht genannt wird, ist das Bewusstsein des Einzelnen gestiegen, zum Schutz seines Rechts auf informationelle Selbstbestimmung technische, organisatorische und rechtliche Maßnahmen selbst zu ergreifen. Nur für die Umsetzung fehlen oftmals die erforderlichen Kenntnisse des Einzelnen. Mein erster Beratungsansatz ist stets ein präventives Verhalten, namentlich möglichst wenig Anlass zu bieten, dass Daten überhaupt erhoben werden (Datenvermeidung, Datensparsamkeit). Der weitere Beratungsansatz zielt dann darauf ab, Gefahren für den Datenschutz und die Datensicherheit kennenzulernen und selbst aktiv Gegenmaßnahmen zu ergreifen. Dabei wird von unserer Seite stets auf die bereits genannten Publikationen verwiesen.

Während bisherige Cookies max. 4 Kilobyte Größe erreichen, können „DOM Storage“-Objekte bis zu 5 Megabyte groß sein. Das Löschen von Cookies wird ohnehin bisher oft vergessen. Umso wesentlicher also für den Selbstschutz vor ungewolltem Aushorchen und vor Profilbildung ist es, diese neuen „Maxi-Cookies“ regelmäßig zu löschen.

Immer mehr Angriffs-Szenarien
Eine zusätzliche Erhöhung der Angriffswahrscheinlichkeit auf personenbezogene Daten besteht in der Tatsache, dass Rechner wegen der häufig bestehenden Flatrate ohne Unterbrechung online sind. Das gibt den Anwendungen Gelegenheit, die offene Internetverbindung zu nutzen und fortwährend Datenverkehr zu erzeugen. Nicht jeder Datenverkehr wird dabei kontrollierbar. Manche unberechtigten Datenkommunikationen sind nur mit speziellen Tools überwachbar. Besonders kritisch ist dies anzunehmen bei Voice over IP, Instant Messaging und zeitgesteuerten automatischen Downloads von Podcast-Abonnements (insbesondere Video- und Audio-Streaming).
Ein großes Problem besteht in der Tatsache, dass die Komplexität der Software allgemein ständig ansteigt, womit die Anfälligkeit für Sicherheitslücken und damit die Angreifbarkeit steigt.

www.lfd.niedersachsen.de
Pfad > Home > > Service-Angebote > Selbstdatenschutz
www.datenschutz.de
> Schlagwortsystem > Technik > Selbstdatenschutz (Virtuelles Datenschutzbüro)
www.bsi-fuer-Buerger.de
(Bundesanstalt für Sicherheit in der Informationstechnik)
www.buerger-cert.de
(bietet kostenfreie aktuelle Warnmeldungen und Sicherheitshinweise per E-Mail)

Die Akzeptanz gegenüber diesen auch checklistenartigen und interaktiven Präventionsangeboten ist nach wie vor sehr hoch, wie den Äußerungen unserer Kunden häufig zu entnehmen ist.

Schillernde Dienste im Internet …

Die Nutzung des Internet ist inzwischen zur Alltagsnormalität der meisten Menschen geworden. Immer mehr Dienste, die bisher von Menschen unmittelbar erbracht worden sind, werden auf Onlineplattformen in das Internet verlagert. Während früher die Hotelbuchung bei Geschäfts- und Dienstreisen meist über Prospekte, Empfehlungen oder Vorortkenntnisse und dann per Fax oder Telefon erfolgte, geschieht dies heute überwiegend über Hotelportaldienste. Neben der Datenbanksuche über Vergleichskriterien, schnellem Preisvergleich und Umgebungsinformationen bieten diese Portale auch gleich Geodaten, Routenplaner, Reservierungs- und Bezahldienste u. v. m. an. Auch Urlaubsbuchungen verlagern sich immer häufiger auf Webdienste – zu Lasten der Reisebüros. Wer eine Anschaffung tätigen will, kann sich heute zahllose Verbrauchertipps, Produkt- und Vergleichstests und anschließend auf Preisportalen die aktuell generierten Preis-Rangfolgen aufrufen.
Zu den elementaren Abwicklungsprozeduren bei Zahlungsgeschäften zählte früher der Gang zur Bank oder Sparkasse; heute verdrängen Telefon- und Homebanking immer mehr die persönlich erbrachten Dienstleistungen, weil inzwischen kaum ein Haushalt computer- und internetfrei ist.
Die Beispielliste ließe sich endlos fortsetzen. Geheimnis des Erfolges von Internet basierten Diensten ist die Bequemlichkeit, die vermeintlich schnelle Recherche und das Gefühl, weltweite Übersicht mit wenigen Mausklicks zu erlangen. Zudem winken niedrigere Preise.

… und ihre Begleiterscheinungen

Während immer mehr private Lebensbereiche von der Technisierung betroffen sind, wächst auch die Zahl der Szenarien, die die Sicherheit der personenbezogenen Daten mit teils erheblichem Schutzbedarf erschweren oder sogar gefährden.
Zunächst steigt das Datenvolumen, das auf den über das Internet verbundenen Rechnerplattformen teils redundant gespeichert und übermittelt wird. Jede Transaktion zieht eine Datenspur nach sich, die sich auf dem heimischen Rechner, in Zwischenspeichern wie Browsercaches, auf Netzknoten und Proxy-Rechnern sowie in den Datenbanken und Storagebereichen von Rechenzentren findet. Die Kontrolle darüber, ob, wie lange, in welcher Tiefe und mit welcher Kombinierbarkeit und Aussagekraft diese Daten gespeichert und weiterverarbeitet werden, ist rechtlich zwar weitgehend geregelt, lässt sich jedoch in der Praxis nur durch hohen fachkundigen Aufwand realisieren. Tatsächlich wissen

die meisten Beteiligten von genau diesen Umständen nichts oder nur unvollständig etwas.
Das zunehmende Maß an interaktiven Prozessen – etwa vom unverbindlichen Anfragen in einer Onlinedatenbank über das plötzliche Wechseln in verbindliches Buchen oder auch das versehentliche und irrtümliche „OK" an der falschen Stelle – lässt oftmals den Überblick darüber schwinden, an welchen Stellen rechtswirksame Aktionen erfolgen und Willenserklärungen abgegeben worden sind. Die Gefahren, die durch unbeabsichtigtes oder fehlerhaftes Preisgeben persönlicher Angaben oder durch das Ausspähen oder Erschleichen von Daten ausgehen, sind in noch zu hohem Ausmaß nicht oder nur unzureichend bekannt.

Datenspuren – „Darf es etwas weniger sein?"

Eine der meist gestellten Fragen zu „Datenspuren" dreht sich um die Anonymität im Internet. Die eigentliche Angebotspflicht zur Anonymisierung oder Pseudonymisierung, die sich bei der Telekommunikation und der Nutzung von Telemedien aus der Konsequenz des Fernmeldegeheimnisses ergibt (Artikel 10 des Grundgesetzes), spiegelt sich zum Beispiel in der Anonymisierungsregelung für Telekommunikations-Verkehrsdaten (nach § 96 Telekommunikationsgesetz – TKG), der Telekommunikations-Standortdaten (nach § 98 TKG), bei der Nutzung von Telemedien und ihrer Bezahlung (§ 13 Abs. 6 Telemediengesetz – TMG) oder in der Anonymisierungspflicht von Nutzungsdaten zum Zwecke der Marktforschung (§ 15 Abs. 5 TMG) wider. In der praktischen Umsetzung ergeben sich freilich eine Reihe von Ausnahmen.
In der Praxis hat sich auch gezeigt, dass im Zusammenhang mit den Nutzerregistrierungen auf zahllosen Internetplattformen, Onlineforen und Datenbanken sowie mit den Bezahlvorgängen, die zunehmend über den Internetbrowser abgewickelt werden, das anonymisierte Kommunizieren häufig Grenzen findet. In der Regel gibt der Nutzer mehr oder weniger freiwillig seine persönlichen Daten preis. Art und Umfang entsprechen dabei nicht immer auch der Notwendigkeit. Bei der Vielzahl von Registrierungen geht insbesondere mit der Zeit der Überblick darüber, wer welche Daten über den Nutzer tatsächlich kennt oder vorhält, praktisch verloren. Allein diese Unkenntnis oder Fehleinschätzung ist eine Bedrohung für die Fähigkeit des Einzelnen, die Kontrolle über den Datenfluss zu seinen persönlichen Lebensverhältnissen zu behalten, geschweige denn strikt geheim zu halten.
In der Praxis kommen zwei Problemfelder hinzu. Zum einen ist festzustellen, dass die Betreiber der technischen Plattformen nicht immer „Herr der Sicherheitslage" sind, weil Sicherheitslücken in der Standardsoftware – wie Datenbanken, Webserver, Programmiersprachen, Content-Management-Systemen – nicht geschlossen werden, sei es aus Unwissenheit oder aus Mangel an Sorgfalt oder an Personalressourcen. Zum anderen offenbart sich dem einzelnen Nutzer nicht immer, ob sich ein Webseitenanbieter hinsichtlich des materiellen Daten-

schutzes tatsächlich rechtstreu verhalten hat und verhalten will. Wie die bekannt gewordenen und in der Öffentlichkeit wahrgenommenen Datenschutzvorfälle gezeigt haben, sind nicht einmal bislang als renommiert geltende Unternehmen vor rechtlichen Fehleinschätzungen und Fehlverhalten gefeit. Erst recht gilt dies für international agierende Scheinfirmen, denen daran liegt, Nutzerdaten in möglichst großen Mengen zu sammeln und diese missbräuchlich und rechtswidrig gewinnträchtig zu nutzen. Eine erhebliche Dunkelziffer liegt in einer Grauzone der Anbieter, die – in „bewusster" Unkenntnis des Grundsatzes der Datensparsamkeit – Daten durch Protokollierung oder Zukauf von Adresshändlern sammeln und z. B. für exzessive Werbung nutzen.

Es geht also nicht immer nur – aber auch – um die für die Strafverfolgung gesetzlich verankerte Pflicht zur verdachtsunabhängigen Speicherung der Verkehrsdaten für sechs Monate nach § 113a TKG, die so genannte „Vorratsdatenspeicherung". Viel häufiger noch ergeben sich Unklarheiten darüber, welche Datenprotokollierung durch Anbieter und Betreiber von Webseiten, Webshops und Portalen sowie Foren, Weblogs und anderen Diensten nach dem Telemediengesetz erlaubt sind.

Als erste Maßnahmen des Selbstdatenschutzes gilt noch immer der Grundsatz der Datenvermeidung, denn die Daten, die gar nicht erst erhoben werden, können auch nicht missbraucht werden.

Für die Fälle, in denen die Preisgabe von persönlichen Angaben nicht zu vermeiden ist, lautet die Grundforderung, nur die Daten zu erheben, deren Verarbeitung im Rahmen des Rechtsverhältnisses unabdingbar ist. Der Nutzer muss hier aber selbst steuernd eingreifen, weil mit einer relativ umfassenden Einverständniserklärung die Zustimmung zur Verarbeitung oft leichtfertig gegeben wird. Dies ist meistens der Eile geschuldet, um keine Verzögerungen in Kauf nehmen zu müssen, die einer schnellen Information oder einem anderen lockenden Vorteil im Wege stehen würde. Hier ist eine kritische und eher zurückhaltende Verfahrensweise Voraussetzung dafür, dass Datenbestände nicht unnötig entstehen.

Nutzerverfolgung ist allgegenwärtig

Sie heißen Google Analytics, etracker (etracker GmbH, Hamburg), Omniture.com, TRACKINGCENTER (TANDEM Kommunikation GmbH & Co. KG, Offenburg), um nur einige zu nennen.

Sie werben mit unbegrenzten Echtzeit-Webanalysen, individuellen Analysen, Live-Besucherverfolgung und Webcontrolling. Zur Klarstellung: Webseiten, die anonym Zugriffe zählen oder der Abwehr von Hacking-/Cracking-Attacken dienen, sind zunächst unproblematisch, wenn dies mit Einverständnis des Nutzers geschieht. Sobald aber IP-Adressen gespeichert werden, sind weitergehende Analysen bis hin zum Data-Mining des Nutzerverhaltens realisierbar, die nicht mehr als datenschutzkonform gelten können.

Nach der Übernahme des Werbevermarkters DoubleClick im Jahre 2007 ist die Informationsvorherrschaft von Google erneut erheblich gestiegen. Google stehen nunmehr die Bewegungsprofile einer Mehrheit der weltweiten Internetnutzer zur Verfügung. Nach § 12 Abs. 1 TMG ist eine Verarbeitung von personenbezogenen Daten nur zulässig, wenn der Besucher der Seite vorher zugestimmt hat oder eine gesetzliche Ermächtigung vorliegt. Bei dem Einsatz von Webtracking-Diensten durch den Webseitenbetreiber findet die Analyse im Wirkungsbereich eines Dritten statt. Durch die Erhebung der Daten mittels Google Analytics wird u. U. die vollständige IP-Adresse des Besuchers der Webseite an einen Dritten, nämlich Google Inc. übermittelt. Zudem erfolgt die Übermittlung ins Ausland, vorrangig in die USA. Die Durchsetzung des Schutzes der informationellen Selbstbestimmung ist damit in Frage gestellt.

Der größte Irrtum: „Ich habe im Prinzip ja nichts zu verbergen!“

Sogar kritischen Geistern entgleitet dieser Satz bisweilen, den unkritischen ohnehin. In Wahrheit deutet der Satz darauf hin, dass man sich ja nichts hat zu Schulden kommen lassen. „Niemand kann mir mit meinen eigenen Daten einen Fallstrick legen.“ Dass es sich hier aber um einen fatalen Irrtum handelt, ergibt sich bereits beim Vergleich der virtuellen mit der realen Welt. Niemand, der eine Zeitung am Kiosk kauft, käme auf die Idee, dem freundlichen Verkäufer seine Anschrift, seine Kontoverbindung, seinen Lebenslauf oder auch nur seinen Personalausweis zu offenbaren. Selbst im Kollegenkreis oder auch im Verein sortiert jeder, was genau er von sich preisgibt. Das hängt damit zusammen, dass in jeder realen Lebenssituation automatisch geprüft wird, wie tief die Kenntniss über die eigene Person sein darf oder soll. Auf diese unumstrittene Schutzstrategie der Privatsphäre durch eine Art Zwiebelschalenprinzip wird niemand mit dem Hinweis verzichten, nichts zu verbergen zu haben.
In der digitalen Welt hat sich diese Selbstverständlichkeit noch nicht überall durchgesetzt. Der erste Fall des Missbrauchs von Daten führt jedoch spätestens zu der Erkenntnis, dass auch und besonders im Internet sehr viel mehr Vorsicht und Verzicht auf Datenpreisgabe zu üben ist.
Gegenstand unserer Schriften (Flyer, Orientierungshilfen und Checklisten) beinhalten die wichtigsten Maßnahmen zum Selbstdatenschutz. Die allerhäufigsten Angriffsflächen kann man mit relativ einfachen Mitteln in den Griff bekommen:

Anonym surfen

Will man im absolut verstandenen Sinne des Wortes anonym im Internet surfen, benötigt man dazu einen Zugang zum Internet, bei dem die Identifizierung der IP-Adresse nicht dokumentiert wird. Hierzu gibt es Dienste, die mit speziellen mehrfach kaskadierten Zwischenstationen – so genannten Mixen – arbeiten.

Beispielhaft sei hier besonders AN.ON und der „Java Anon Proxy (JAP)“ zu nennen (http://anon.inf.tu-dresden.de). Es fußt auf dem Forschungsprojekt „Starke Anonymität und Unbeobachtbarkeit im Internet“ (AN.ON), das vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) initiiert, vom Bundesministerium für Wirtschaft und Technologie (BMWi) gefördert und in Kooperation mit der Technische Universität Dresden und der Universität Regensburg sowie mit forschender Begleitung der Freien Universität Berlin realisiert worden war. Nach der Beendigung des Projektes (Abschlusspräsentation 24. November 2006, BMWi, Berlin) steht es als Open Source Lizenz AN.ON weiter bei der TU Dresden zur Verfügung und wird als kommerzieller Dienst „JonDonym“ weiterentwickelt (https://www.jondos.de/de).
Die Grenzen liegen hier allerdings bei der verpflichtenden Protokollierung gewisser Verkehrsdaten nach § 113a TKG. Demnach speichert zum Beispiel der erste Mix die IP-Adresse, das Datum und die Uhrzeit der eingehenden Verbindung.
Für nichtstaatliche Zugriffe gibt es allerdings prinzipbedingt keine Möglichkeiten, die Anonymität aufzudecken.

Weiterführende Informationen und Links dazu:

https://www.datenschutzzentrum.de/projekte/anon/

Sweet Home mit offenen Scheunentoren

Der Webbrowser ist inzwischen eine hochfunktionale Kommandozentrale geworden. Mit vielen Zusatzprogrammen (so genannten Plug-ins oder Erweiterungen) lassen sich hilfreiche Mehrwertdienste installieren. Je komplexer aber dieser Browser damit wird, desto mehr potentielle Sicherheitslücken entstehen auch. Umso wichtiger ist es, die Einstellungen kritisch zu überprüfen und im Zweifel zu Gunsten der Sicherheit zu justieren. Bei der Nutzung des Rechners durch mehrere Personen gehört auch das Leeren des Zwischenspeichers (so genannter Cache), das Löschen von Cookies und der Verlaufsliste (auch History) aufgerufener Seiten dazu. Auch der Speicher der Adresszeilenaufrufe (URL), der sich einmal eingetippte Eingaben merkt, ist eine aufschlussreiche Informationsquelle für das Surfverhalten und die „Lieblingsseiten“.
Mehr Abwägung und fachlicher Beurteilung bedarf es bei der Frage, welche programmtechnische Aufrüstung nötig und unter Aspekten der IT-Sicherheit vertretbar ist. Die Ausführung gefährlicher aktiver Inhalte, die durch

- Java-Applets
- JavaScript / JScript
- ActiveX-Steuerelemente
- Visual Basic Script (VBS)

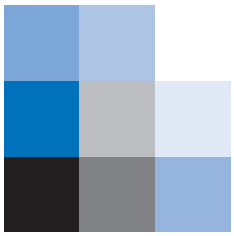
realisiert sein können, generell zu sperren, ist die sichere Seite, führt aber auch zum Verlust bestimmter Darstellungen oder Dienste.

Bei den aktuellen Browserversionen bieten die Hersteller - allerdings noch immer in unterschiedlicher Qualität – gebündelte Funktionen unter „Sicherheitseinstellungen“, unter „Privacy“ oder „Datenschutz“ an.

Der Webbrowser weist aber auch bereits in seinem Urzustand eine ganze Reihe von Sicherheitsschwachstellen und -lücken auf. Nicht immer werden sie zeitnah erkannt und nicht einmal alle werden tatsächlich durch so genannte Bugfixes oder Patches vom Hersteller geschlossen. Und selbst wenn sie durch verfügbare Updates schließbar sind, versäumen zu viele Benutzer – vor allem im Bereich der Privatnutzung – diese wichtigen Updates zu installieren. Jede Sicherheitslücke ist aber ein potentielles Einfallstor für Schadsoftware (Malware) – allen voran Viren, Trojaner, Botnetz-Loader und anderes „Getier".
Ähnlich verhält es sich mit versäumten tagesaktuellen Updates von Virenschutzsoftware. Neuere Varianten von Schadsoftware, die von Angreifern immer leichter auch ohne Programmierkenntnisse entwickelt und versandt werden können, werden somit nicht erkannt. Der eigene Rechner ist schnell unbemerkt befallen und kann selbst zur Malware-Schleuder oder zum ferngesteuerten „Botnetz-Zombie" werden.

Software mit Heimweh: Spyware

Eine ganze Reihe von Software-Herstellern baut in ihre Software Komponenten ein, die oft ohne Kenntnis des Nutzers eine offene Internetverbindung ungefragt nutzen, um Informationen über die Rechnerkonfiguration, die installierten Programme oder über andere Datenspuren einzusammeln und an den Firmenserver zu übertragen. Häufig versäumen Nutzer die Installation eines Antispyware-Programms zum Aufspüren und Beseitigen solcher Komponenten oder wenigstens einer Firewall, um die so genannten Ports des Systems und die darüber laufenden Prozesse zu beaufsichtigen und diesen ggf. Einhalt zu gebieten.



Beteiligung bei IT-Verfahren des Landes und der Kommunen

Der Landesbeauftragte für den Datenschutz ist rechtzeitig über Planungen des Landes und der kommunalen Gebietskörperschaften zum Aufbau automatisierter Informationssysteme zu unterrichten.
Darunter fallen also auch neue Projekte für IT-Verfahren und wesentliche Änderungen bestehender IT-Verfahren. Dieser Unterrichtungspflicht des § 22 Abs. 2 NDSG wird nicht immer konsequent, oftmals nicht rechtzeitig vor Projektstart und bisweilen nicht rechtzeitig vor Betriebsfreigabe nachgekommen. In der Folge sind Beratungsansätze oder Kurskorrekturen in materiellrechtlicher Hinsicht oder im Bereich der technisch-organisatorischen Maßnahmen mindestens erschwert, unter Umständen auch nicht mehr möglich.
Bei Nachfragen unsererseits ist bisher jedoch stets umgehend und umfassend die Offenlegung und Beteiligung nachgeholt worden.
Die bis 2006 durchgeführten regelmäßigen Gesprächsrunden mit dem Informatikzentrum Niedersachsen (izn), die dieses Problem spürbar reduziert hatten, sind in den Jahren 2007 und 2008 leider in der regelmäßigen Form ausgeblieben. Der IT-Dienstleister der Landesverwaltung ist inzwischen der Landesbetrieb für Statistik und Kommunikationstechnologien Niedersachsen (LSKN) als Rechtsnachfolger des Informatikzentrum Niedersachsen. Eine Wiederaufnahme dieser „Jours fixes" könnte dazu beitragen, diese Defizite zeitnah auszuräumen. Ergänzend halte ich diese Form des Austausches mit dem CIO und dem CISO für hilfreich, weil hier die strategischen Entscheidungen fallen.
Im Zuge meiner Gesprächskreise mit IT-Dienstleistern und Rechenzentren der Universitäten, Fachhochschulen sowie mit kommunalen Datenzentralen, den kommunalen Spitzenverbänden in Niedersachsen und dem LSKN wurde dieser Austausch allerdings weiterhin realisiert (siehe eigens Kapitel in diesem Bericht).

1. Mitwirkung im Koordinierungsausschuss IT

Der Koordinierungsausschuss IT (KA-IT) dient der ressortübergreifenden Koordination und Abstimmung für Angelegenheiten der Informationstechnik. Unter anderem berät er über alle Fragen von grundsätzlicher Bedeutung für den IT-Einsatz in der Landesverwaltung und wirkt bei den strategischen Vorgaben mit. Vor allem beim IT-Landeskonzept, beim IT-Gesamtplan und den Grundsätzen der Durchführung des landeszentralen IT-Controlling ist der KA-IT zu beteiligen.[1] Zwangsläufig sind in den dort zu beratenden Vorhaben Fragen berührt, die die informationelle Selbstbestimmung, etwa bei Personaldaten oder Bürgerdaten, betreffen. Damit sind technische und organisatorische Maßnahmen für Daten-

1 Abschnitt 6 der Grundsätze zur Steuerung und Koordinierung des Einsatzes der Informations- und Kommunikationstechnik in der Landesverwaltung (SK-IT), Gem. RdErl. d. MI, d. StK u. d. übr. Min. v. 7.9.2004 – VM 501-02828/3-2 – vom 07.09.2004 (Nds. MBl. S. 563).

sicherheit und Datenschutz auf abstraktem, aber auch auf ganz konkretem Niveau zu bestimmen.
Da ein Vertreter des Landesbeauftragten für den Datenschutz aus dem Bereich technischer und organisatorischer Datenschutz als beratendes Mitglied an den Quartalsberatungen teilnimmt, besteht hier stets die direkte Möglichkeit, im frühzeitigen Dialog etwaige Fragen zu klären und beratend einwirken zu können. Insbesondere bei eGovernment-Vorhaben oder Planungen zur Konsolidierung von Technologien wurden technische und organisatorische Rahmenbedingungen diskutiert und einzelne Fragen einer anschließenden materiellrechtlichen Prüfung unterzogen.

2. Informationssicherheit und technischer Datenschutz

In meinem XVIII. Tätigkeitsbericht (2005–2006) hatte ich über die Informationssicherheit in der Landesverwaltung berichtet.
Informationssicherheit ist nach allgemein anerkanntem Verständnis der relative Zustand, der durch die Summe aller organisatorischen und technischen Aspekte im Informationsmanagement erreicht wird. Dies schließt die IT-Sicherheit im enger gefassten technischen Sinne ein. Der Begriff Datensicherheit – wie im Datenschutzrecht verankert – findet sich also inhaltlich in dieser Definition wieder. Datensicherheitsmaßnahmen im betrieblichen Sinne lassen sich zu großen Teilen mit den Datensicherheitsmaßnahmen des technischen und organisatorischen Datenschutzes zur Deckung bringen. Im Zweifel haben jedoch gesetzliche Regelungen des Datenschutzes Vorrang vor untergesetzlichen Sicherheitsregelungen, zumal erstere Verfassungsrang beanspruchen.
In Einzelfällen und Zweifelsfragen haben wir immer Beratung angeboten und durchgeführt. Das galt und gilt für die Landesverwaltung ebenso wie für Kommunen und andere Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts.

IT-Sicherheit als Herausforderung der Niedersächsischen Landesverwaltung

Seit Oktober 2008 ist im Niedersächsischen Ministerium für Inneres, Sport und Integration die Funktion eines IT-Sicherheitsmanagers (eines so genannten Chief Information Security Officers – kurz CISO) der Niedersächsischen Landesverwaltung eingerichtet und personell besetzt worden. Mit dieser Maßnahme bleibt die Hoffnung verbunden, dass die ins zeitliche Abseits geratene Absicht wiederbelebt wird, das IT-Sicherheitsmanagement der Landesverwaltung zu systematisieren und zu professionalisieren. Ausdrücklich sei an dieser Stelle die operative und konzeptionelle Arbeit der Kompetenzstelle IT-Sicherheit beim LSKN (KITS) lobend erwähnt. Sie kann jedoch nur so sorgfältig und wirksam das Informationssicherheitsniveau und damit auch den technischen Datenschutz der Landes-IT entwickeln und betreiben, wie es vom Informationssicherheitsmanagement strategisch vorbereitet, gestützt und gesteuert wird.
Bedauerlicherweise ist es offenbar im Rahmen der Ressortabstimmung unter Federführung des CIO bis 2008 nicht gelungen, die Informationssicherheits-Leitlinie und die darunter positionierten Richtlinien zu verabschieden. Damit besteht weiterhin ein gravierendes Regelungsvakuum. Im Rahmen der KA-IT-Beratungen hatte ich mit meiner Dienststelle an den Papieren vor einigen Jahren mitgewirkt und seit 2005 wiederholt darauf hingewiesen, dass diese Regelungslücke grundlegende Probleme für die Umsetzung in allen IT-Verfahren bereitet.
Es fehlt also weiterhin an einer

- Leitlinie zur IT-Sicherheit
  (Ressort übergreifend und strategisch) und an
- Richtlinien zur IT-Sicherheit
  (Ressort übergreifend und taktisch, für technische Standards, Definitionen, Maßnahmen)

Einzig vorhanden sind bisher, dank dauerhafter operativer Arbeit des LSKN,

- IT-Sicherheitskonzepte (sach- und zielgruppenspezifisch detailliert, operativ, für konkrete Produkteinstellungen und zu verwendende Mechanismen)
- lokale Arbeitsanweisungen
  (IT-Sicherheitsvorgaben für die Mitarbeiter, eigenverantwortlich umsetzbar am jeweiligen Arbeitsplatz)

Aus Sicht des LfD besteht weiterhin das Angebot der grundlegenden Zusammenarbeit mit dem CISO und dem LSKN, um den technischen Datenschutz mit einem systematischen Informationssicherheitsmanagement zu koordinieren.

Storage Management / Managed Storage

Seit etwa Herbst 2007 wird im LSKN das Projekt „Managed Storage“ in den Phasen Planung und Pilotierung betrieben. Die damit einhergehende Planung, externe Dienstleister dabei in Anspruch zu nehmen, veranlasste mich im Jahre 2008 bei verschiedenen Gelegenheiten, auf die Notwendigkeit hinzuweisen, eine datenschutzrechtliche Vorabkontrolle (nach § 7 Abs. 3 NDSG) durchzuführen.

Eine gezielte informelle oder offizielle Beteiligung des LfD ist bis zum Mai 2009 sowohl durch den Bereich CIO, als auch seitens der Projektleitung des LSKN unterblieben.

Den mir bisher vorliegenden Informationen nach zu urteilen, ist bereits eine vorläufige Betriebsfreigabe erfolgt, die die Mitwirkung externer Firmenmitarbeiter im operativen Betrieb in den Räumlichkeiten des LSKN einschließt. Ob ein hinreichendes IT-Sicherheits-Konzept und ein Datenschutzkonzept vorliegen, ist bislang noch nicht vollständig geklärt.

Die besondere Risikolage ergibt sich bei diesem Vorhaben aus der Tatsache, dass der Storagebereich in Zukunft alle Verwaltungsbereiche der Nds. Landesverwaltung betreffen wird. Eine Vergabe an externe Firmen/Personen unterfällt zusätzlichen Sicherheits- und Datenschutzrisiken und notwendigen Schutzmaßnahmen. Insbesondere wenn Daten unverschlüsselt im Storage abgelegt sind, dürften die Schutzziele der Vertraulichkeit und Integrität von Echtdaten in einem fast unbegrenzten Ausmaß für prinzipiell alle Querschnitts- und Fachverfahren sowie Kommunikationsdaten betroffen sein.

Ich habe daher eine detaillierte Prüfung dieser Sachverhalte und des IT-Projektes angeordnet.

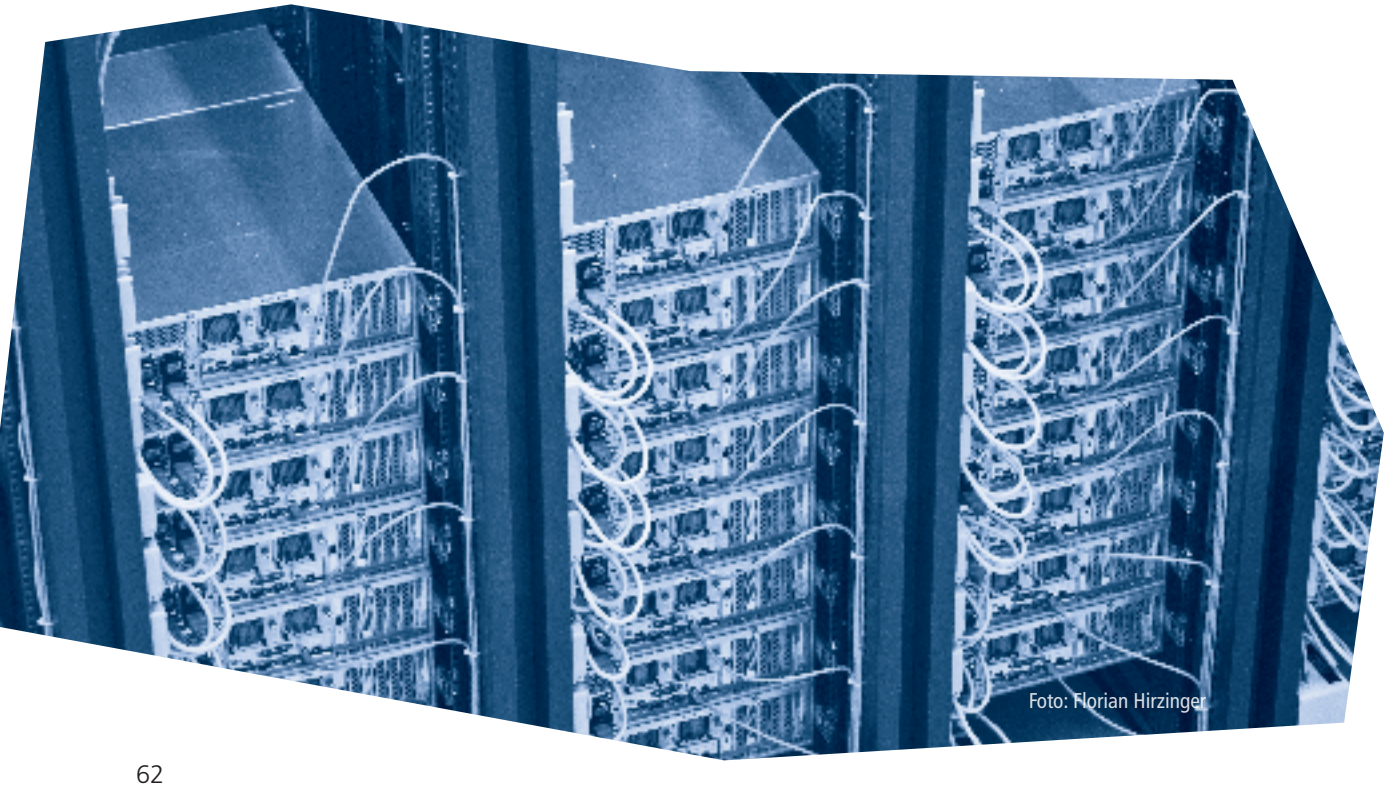


Foto: Florian Hirzinger

Gesprächskreis mit Leitern der Rechenzentren und anderen IT-Führungskräften

In meinem XVIII. Tätigkeitsbericht hatte ich über die Initiierung eines Gesprächskreises berichtet, der jeweils mit den Leitern, sonstigen Führungskräften und Datenschutzbeauftragten von IT-Betrieben und Rechenzentren durchgeführt wurde. Die Veranstaltungsreihe ist weiterhin eingebettet in die Angebote meines Datenschutzinstituts. Zur Zielgruppe gehören die großen Organisationsbereiche und externen IT-Dienstleister (Datenzentralen), die IT-Dienstleistungen für Hochschulen, Fachhochschulen, Kommunen und die Landesverwaltung erbringen.

Informationen zu den Terminen
und den Inhalten finden Sie auf unserer Website unter
www.lfd.niedersachsen.de
Pfad > Home > Aktuelles > Datenschutzinstitut Niedersachsen

Die Motivation

Rechenzentren müssen heute nicht nur einen leistungsfähigen und effizienten Betrieb, sondern auch sichere und datenschutzgerechte Technik und Prozesse aufweisen. Dies gilt ebenso für die Auftragsdatenverarbeitung. Hier sind Experten gefragt, die die jeweiligen Spezialgebiete abdecken.
Bei Verfahren der Informations- und Kommunikationstechnik (IT-Verfahren) sind Art, Umfang und Ausgestaltung von technischen und organisatorischen Maßnahmen des Datenschutzes einerseits immer individuell auf den jeweiligen Anwendungsbereich festzulegen und umzusetzen. Andererseits lassen sich sach- und fachgerechte sowie gleichzeitig datenschutzgerechte, angemessene Lösungen nur vergleichbar machen, beurteilen und überprüfen, wenn diese weitestgehend standardisiert werden. Außerdem sollten erfolgreiche Modelle möglichst breit bekannt gemacht, übernommen und umgesetzt werden, die sich nach dem „best practices“ Prinzip, also nach den aus der praktischen Erfahrung heraus als bewährt geltenden Modellen, herausgebildet haben.
Ich verfolge auch weiterhin den präventiven Weg und vertrete die Auffassung, dass es nicht ausreichen würde, wenn ich nur datenschutzrechtliche Beratungen, Kontrollen oder Stellungnahmen in zahlreichen Einzelfällen abgeben und deren Umsetzung im Übrigen häufig dem Zufall überlassen müsste. Es gilt, die ständig wiederholbaren Fehler zu identifizieren und mit Standardlösungen zu mehr Effizienz zu gelangen.
Deshalb kommt es darauf an, präventive Maßnahmen systematisch thematisch aufzubereiten, gemeinsam zwischen Datenschutz und IT zu erörtern und den Verantwortlichen an zentralen Stellen die Möglichkeit zu geben, sich rechtzeitig planerisch mit den datenschutzrechtlichen Notwendigkeiten auseinanderzusetzen. Mit diesem Gesprächskreis wurde dieses Ziel konsequent verfolgt.

Technische Innovationen im Blickfeld: Der Start

Der konstituierenden Veranstaltung mit der Themenfindung folgten drei weitere Veranstaltungen bis Januar 2007 mit den Themen

2. Gesprächskreis: „Portale für Internet und Intranet – Datenschutzgerechte Ansätze bei Planung, Entwicklung und Betrieb von Plattformen als Bestandteil einer eGovernment-Umgebung“
3. Gesprächskreis: „Identitäts-Management-Systeme“
4. Gesprächskreis: „Datenschutz in Service Level Agreements (SLA): Auftragsdatenverarbeitung, Dienstleister-Kunden-Beziehung und ITIL-Prozesse datenschutzgerecht gestalten“

Über deren Inhalte hatte ich bereits im XVIII. Tätigkeitsbericht berichtet.

Augen nicht vor Herausforderungen der Technik verschließen: Neue Themen 2007/2008

Im zurückliegenden Berichtszeitraum wurden in der Fortsetzung der Reihe bis Dezember 2008 fünf weitere Veranstaltungen durchgeführt. Sie widmeten sich jeweils einem eigenständigen Thema. Die Themen werden im Folgenden erläutert.

„Fernwartung, Remotezugänge, ausländische IT-Dienstleister, mobiles Administrieren: datenschutzrechtliche Leitplanken“ (5. Gesprächskreis)

Personalaufwand ist teuer, daher gilt es im IT-Service, mit systematischen Methoden manuellen Aufwand durch standardisierte und hochautomatisierte Prozesse zu ersetzen. Ähnlich einer industriellen Produktion sollen IT-Services durch eine prozessoptimierte „IT-Fabrik“ geleistet werden. Die „Turnschuhadministration“ hat ausgedient.

Was aber, wenn manuelle Eingriffe bei der Wartung oder im Incidentmanagement sowie beim Notfall unabdingbar sind? Um in diesen noch immer häufigen Szenarien dennoch flexibel reagieren zu können, sind Remotezugänge für Fernwartung und -steuerung unverzichtbar geworden. Der IT-Service (IT-Service-Management) eines Rechenzentrums-Betriebs auf der Grundlage einer Dienstleister-Kunden-Beziehung verantwortet die betriebliche Umsetzung der Systemadministration und deren datenschutzrechtskonforme Ausgestaltung. Die organisatorischen und technischen Vorgaben dafür werden heutzutage allerdings über Service Level Agreements (SLA), also Dientleistungsgütebeschreibungen auf vertraglicher Grundlage, vom Auftraggeber entwickelt und mit dem Dienstleister ausgehandelt. So sind die Festlegungen zu technischen und organisatorischen Maßnahmen für die Informationssicherheit und den Datenschutz über einen Prozess zu steuern. Es reicht dabei keineswegs aus, sich auf angebotene Standardmaßnahmen des Dienstleisters zu beschränken. Diese können

und sollten durchaus eine Grundlage für den Grundschutz sein. Sie müssen aber stets durch individuelle Maßnahmen nach dem jeweiligen Schutzbedarf und der Risikobewertung angepasst werden (so genanntes Customizing).
Das häufigste Szenario für die Fernwartung ergibt sich bei der Unterstützungsleistung für den Endbenutzer bei seinen Anwendungen. Dieser Vorgang erfolgt durch zunehmend zentralisierten Support, den so genannten User Help Desk oder First Level Support. In schwierigeren Fällen, oder wenn systematische Fehler auftreten, treten auch die spezialisierten Kompetenz-Centers als so genannter Second Level Support in Erscheinung. In beiden Fällen ist schnelle Hilfe nur durch Fernwartung möglich.
Ein weiteres Szenario ist bei der hochspezialisierten Administration in Rechenzentren zu beachten. Auch ein Rechenzentrum kann nicht alle Aufgaben vollständig autark lösen. Die Komplexität heutiger Systemumgebungen, IT-Anwendungen und Komponenten fordern eine starke Ausprägung der Arbeitsteilung. Die Rechenzentren sind zunehmend auf ergänzendes externes Spezialwissen angewiesen, das nur durch entsprechende Hardwarehersteller, Lösungsanbieter und Softwarehersteller geleistet werden kann. Nicht selten hält sich ein Spezialist jedoch nicht in lokaler, manchmal nicht einmal in nationaler Reichweite auf, so dass für schnelles Eingreifen nur eine Fernwartung in Frage kommt.
Remotezugriffe werfen in der Praxis jedoch eine Reihe von Fragen auf. Informationssicherheit und Datenschutz fordern Begrenzungen für Zugriffe und Transparenz des Geschehens. Der Gesprächskreis hat sich daher intensiv den Fragen gestellt:

- Wie sicher lassen sich datenschutzrechtliche Grundziele wie Zweckbindungsgebot und Datenvermeidung/Datensparsamkeit sowie die Gestaltungsziele Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität beim Betrieb durch Externe (Subunternehmer) erreichen?
- Welche Remoteadministrationen sind unkritisch, welche eher bedenklich, welche Grenzen sind zu beachten?
- Welche Konsequenzen gibt es und wie müssen die organisatorischen Festlegungen und technischen Vorkehrungen gegen Missbrauch und für datenschutzgerechte Modelle aussehen?
- Was müssen Informations-Sicherheitspolicies, IT-Sicherheitskonzepte und Datenschutzrichtlinien dafür beinhalten?
- Wie sind die Regelungen für Remotezugriffe in einem SLA abzubilden?
- Was kann durch Zustimmungserklärungen oder Dienstvereinbarungen geregelt werden?
- Welche Maßnahmen sind bei Internet basierten Zugriffen durchzuführen?
- Was ergeben sich für datenschutzrechtliche Konsequenzen bei international agierenden Dienstleistern?

Die Ergebnisse der fachlichen Lösungsansätze wurden in einer Dokumentation zusammengefasst.

„Logging und Protokolldateien: Datenschutz und IT-Sicherheit im Abwägungsprozess“ (6. Gesprächskreis)

Der Alltag in Verwaltungen, Hochschulen und Betrieben ist immer enger durchzogen von IT-Verfahren. Ihre Zahl und die Komplexität des Zusammenspiels steigt rasant. Die Administration durch IT-Verantwortliche, IT-Dienstleister und Rechenzentren erfordert den Ausbau automatisierter Prozesse, um diese Entwicklung wirksam zu beherrschen. Das trifft sowohl auf die IT-Fachverfahren zu, als auch auf die Betriebsysteme, das Datenbankmanagement, die Netze und die IT-Dienstekomponenten.

Manuelle Verfahren überfordern zunehmend die Personalressourcen, daher sind Überwachungstools und Protokollfunktionen unverzichtbar, um diese Aufgabe zu bewältigen.

Protokollinformationen über die Betriebszustände, die Einlogg-Vorgänge und die Zugriffe auf die Systeme und die Daten sind aber nur auswertbar, wenn Such- und Filterfunktionen sowie Regelwerke zur Verfügung stehen, die den Alarmfall vom unkritischen Standardfall unterscheiden helfen. Nur so sind Administratoren, Datenschutzbeauftragte oder Revisionsverantwortliche in der Lage, eine für ihre Aufgaben nachvollziehbare Dokumentation für zeitnahe Reaktionen zu erhalten.

Viele eingesetzte Produkte (DBMS, Netzüberwachungs-Tools, standardisierte und vorkonfektionierte Fachanwendungen) bieten bereits vorkonfigurierte Protokollfunktionen, um den Einstieg und den Start des Betriebs zu erleichtern. Nicht immer sind diese „Default“-Zustände datenschutzkonform – tatsächlich in den seltensten Fällen. Die Pflicht zur Prüfung individueller Festlegungen in jeder Umgebung und jedem Betriebsumfeld ist damit also nicht aufgehoben. IT-Sicherheits-Konzepte und Datenschutzkonzepte müssen zudem die erforderlichen Einstellungen über die individuelle Protokollierung verbindlich festlegen.

Worauf ist hier zu achten?

Eine Protokollierung ist also einerseits als technische Datenschutzmaßnahme sowie andererseits zur IT-Sicherheit erforderlich, um die genannten Aufgaben zu erfüllen. Andererseits gilt der datenschutzrechtliche Grundsatz der Datensparsamkeit.

Welche Dosis ist also bezüglich der Speicherdauer und des Datenumfangs erforderlich und welche ist datenschutzrechtlich zulässig? (datenschutzrechtliches Grundziel Datenvermeidung/Datensparsamkeit).

Durch Referate und Fachdiskussionen wurden folgende Aspekte für die IT-Praxis beleuchtet:

- Die Möglichkeit, Nutzerprofile aus Logfiles abzuleiten oder Listen über Auffälligkeiten zu erstellen, muss unter rechtlichen Gesichtspunkten kritisch geprüft werden.
- Das datenschutzrechtliche Zweckbindungsgebot erfordert Maßnahmen zur Trennung von Protokollinformationen.

- Die Gestaltungsziele Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität beim Betrieb von Protokollmanagements erfordern geeignete, wirksame Maßnahmen im technischen und organisatorischen Umfeld.
- Wie müssen die organisatorischen Festlegungen und technischen Vorkehrungen gegen Missbrauch aussehen?
- Was müssen Informations-Sicherheitspolicies, IT-Sicherheitskonzepte und Datenschutzrichtlinien dafür beinhalten?

Die Vorträge und die Dokumentation der Veranstaltung sind auf meiner Internetseite verfügbar.

„Vorabkontrolle – Schutzstufenkonzept – Informationssicherheit: Datenschutzkonformität und praxisnahe Handhabung“ (7. Gesprächskreis)

Das Niedersächsische Datenschutzgesetz (NDSG) fordert Verfahrensbeschreibungen (§ 8) und zusätzlich die schriftliche Dokumentation des Prüfergebnisses der Beherrschbarkeit von automatisierten Verfahren, die so genannte Vorabkontrolle (§ 7 Abs. 3). Ein automatisiertes Verfahren darf demnach nur dann eingesetzt oder wesentlich geändert werden, soweit Gefahren für die Rechte Betroffener, die wegen der Art der zu verarbeitenden Daten oder der Verwendung neuer Technologien entstehen können, durch Maßnahmen nach Absatz 1 wirksam beherrscht werden können.

Die Praxis von IT-Anwendungen sieht oft so aus, dass Verfahrensbeschreibungen fehlen und nicht fortgeschrieben werden. Die Prüfung der Beherrschbarkeit bleibt noch öfter aus. Die Konsequenz ist, dass ein „Blindflug“ absolviert wird, das bedeutet, dass zwangsläufig keine Kenntnis darüber besteht, ob Datenschutz beachtet wird bzw. welche erforderlichen Maßnahmen umgesetzt werden müssten. Die Zeit drückt, der Auftrag, ein Verfahren einzuführen, steht aus vielen Gründen oft im Vordergrund. Damit wird jedoch das Risiko eingegangen, dass die Inbetriebnahme rechtswidrige Zustände nach sich zieht. „Prüfungen und Dokumentation werden sicher noch warten können“, denkt der getriebene Projektleiter. Auf „die lange Bank schieben“ wird erfahrungsgemäß jedoch selten dazu führen, dass die Heilung solcher Fehler ohne erheblich größeren Aufwand von statten geht.

Datenschutzrechtlich ist diese Verfahrensweise durchaus problematisch: Ein IT-Verfahren darf nicht in Betrieb gehen, wenn die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten und der informationellen Selbstbestimmung nicht durch Konzept und Realität wirksam zum Tragen kommen.

Ob IT-Fachverfahren, Betriebsysteme, Datenbankmanagement, Netze oder IT-Dienstekomponenten: Das Problem, dass die Planung und Umsetzung von Datenschutzkonzepten oder sogar die gesetzlich geforderte Verfahrensbeschreibung und Vorabkontrolle ausbleiben, trifft primär den verfahrensverantwortlichen Auftraggeber, aber auch den betriebsverantwortlichen Auftragneh-

mer. Deshalb lassen sich die Anforderungen nur durch einen systematischen und prozesshaften Weg sachgerecht und transparent erfüllen.
Die Best Practice-Ansätze nach ITIL (IT Infrastructure Library) sowie die nach IT-Grundschutz des BSI und ISO Standard-Reihe 2700x etablierten Standards sehen für Informationssicherheit Prozesse vor, die sich mit dem technischen und organisatorischen Datenschutz verzahnen lassen. Im Rahmen des Service Managements können Datenschutzanforderungen direkt implementiert werden.
So lassen sich

- die Gestaltungsziele Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität für die Einführung und den Betrieb von IT-Verfahren zeitnah entwickeln und direkt umsetzen,
- die integrierte oder rekursive Analyse von Anforderungen aus dem Datenschutzrecht, der Informationssicherheit, des Geheimschutzes usw. durchführen und zu Informations-Sicherheitspolicies, IT-Sicherheitskonzepten und Datenschutzrichtlinien weiterentwickeln,
- die verbindliche Integration dieser gewonnenen Festlegungen und Implementierungen sogar in Service Level Agreements (SLA) verankern.

Die Vorträge und die Dokumentation der Veranstaltung sind auf meiner Internetseite verfügbar.

„SOA: IT-Architektur und Datenschutz – Balance zwischen generischem und spezifischem Datenschutzniveau (8. Gesprächskreis)

Der Einsatz serviceorientierter Architekturen (Service Oriented Architecture = SOA) ist in aller Munde. SOA ist eine Architektur unter Berücksichtigung der Prozessorientierung und setzt darauf abgestimmte technische und organisatorische Abläufe voraus. Prozesse sind ebenso datenschutzgerecht zu gestalten wie die Datenhaltung und ihre Verarbeitung.
Vor allem die Erhöhung der Flexibilität von Softwarekomponenten und -diensten in IT-Anwendungen sowie der Kostendruck sind Treiber für SOA. Dies wirft die altbekannten Fragen der IT-Architektur und Softwareentwicklung nach Modularisierung, Standardisierung und Wiederverwendbarkeit auf. Vor dem Hintergrund webbasierter Anwendungen sind gegenüber monolithischen Lösungen zudem die zusätzlichen Risiken aus der Internettechnologie zu betrachten. Diese fordern eine entsprechende Analyse des Schutzbedarfes und der daraus abzuleitenden Anforderungen an die IT-Sicherheit und den Datenschutz.
Andererseits bietet SOA auch Chancen für besser handhabbare Datenschutzmaßnahmen durch Kapselung. Interessant aus betriebswirtschaftlicher wie aus datenschutzrechtliche Sicht ist zudem, ob durch den Grundsatz der Datensparsamkeit der Schutzbedarf einer Komponente und damit der Aufwand für Maßnahmen des technischen Datenschutzes und für Informationssicherheit verringert werden kann.

In einer serviceorientierten Architektur ist umso mehr ein ganzheitlicher Ansatz vonnöten, denn die Betrachtung der einzelnen Fachanwendungen reicht aufgrund der Wechselwirkungen in einem Systemverbund für einen systematischen Schutz nicht aus.
Worauf ist also in der Softwareentwicklung und im Betrieb der unter SOA laufenden Anwendungen zu achten? Neben den Nutzenaspekten gesellt sich auch das Erfordernis, zusätzliche Risiken zu identifizieren, die sich möglicherweise aus dem Verbund an Funktionen in SOA-Umgebungen ergeben können. Anschließend gilt es, geeignete Maßnahmen für den Schutz der informationellen Selbstbestimmung und die Gestaltungsziele Vertraulichkeit, Verfügbarkeit,
Integrität und Authentizität der IT-Verfahren und der Daten zu definieren und umzusetzen.
Aus der Sicht des LfD wurden rechtliche, technische und organisatorische Anforderungen speziell für SOA aufgezeigt.
Es sollte jedoch auch die Praxis betrachtet werden. Das Fraunhofer-Institut für Software- und Systemtechnik (ISST) berichtete in dieser Veranstaltung von Lösungen und Erfahrungen bei der Planung und Einführung des umfangreichen SOA-Projektes „Integrierte Software Berliner Jugendhilfe“ (ISBJ) für den Senat des Landes Berlin bis 2007.
Anhand dieses Projektes zur eGovernment-Infrastruktur konnten durch Erfahrungsaustausch und Diskussion von Datenschutzanforderungen Praxis und theoretische Ansätze abgeglichen werden.

„Virtualisierung – Effizienztreiber oder Datenschutzfalle?“
(9. Gesprächskreis)

Rechenzentren und Serverumgebungen, die ökonomisch weiterhin tragfähig sein sollen, müssen sich mehr und mehr konzeptionellen Änderungen unterwerfen, die Lösungen für die gestiegenen Anforderungen an Flexibilität, Skalierbarkeit und Kosteneffizienz bieten. Die Prozesse eines dienstleistungsorientierten Rechenzentrums müssen sich daher, ebenso wie Hard- und Software, möglichst problemlos und flexibel den jeweiligen Fachanwendungen, Dienstezuschnitten und speziellen Kundenanforderungen anpassen können.
Dies gelingt nur durch eine modulare Architektur, durch Standardisierung der verwendeten Hard- und Software-Produkte, Werkzeuge und Methoden sowie durch die grundsätzliche Überlegung, alle Komponenten nicht mehr einer dedizierten physischen Hardwarekonfiguration fest zuzuordnen, sondern alle logischen Schichten zu entkoppeln. Es entsteht somit eine IT-Fabrik, die nach den Prinzipien der industriellen Produktion funktioniert.
Ein Teil der Lösung heißt Virtualisierung. Hierunter versteht man eine abstrakte Ebene, die die physikalische Hardware vom Betriebssystem entkoppelt und somit eine größere Auslastung der IT-Ressourcen und eine höhere Flexibilität ermöglicht. Virtualisierung umfasst beispielsweise folgende Ausprägungen:

- Block-Virtualisierung und Thin Provisioning
- CPU- und Speicher Ressource Pool
- virtuelle Netzwerke für virtuelle Umgebungen
- virtueller Storage/virtuelle SAN- und NAS-Umgebungen (Storage Area Network; Network Attached Storage
- Virtualisierungsprogramme: Sie simulieren/emulieren Hardware (z. B. Festplatten, Grafikkarten). Sie ergeben eine virtuelle technische Umgebung, in der verschiedene Betriebssysteme installiert und konfiguriert werden können. Damit können auf einer einzelnen physikalischen Hardware eine Vielzahl von virtuellen Computern arbeiten.

Bedeutende Änderungen ergeben sich auch, weil erhöhte Anforderungen an die Systemmanagementtools zu stellen sind, um eine umfassende Sicht auf die komplette virtualisierte Infrastruktur und ihre Abhängigkeiten von der physikalischen Umgebung zu erhalten.
Fraglich wird damit aber aus datenschutzrechtlicher Sicht, ob durch Virtualisierung

- der Schutzbedarf der Daten und damit die erforderlichen technischen und organisatorischen Maßnahmen für alle Komponenten auf ein einheitliches Niveau gehoben werden müssen oder
- ob Virtualisierung auch eine spezifisch zugeschnittene Skalierung des Aufwandes ermöglicht,
- zusätzliche architekturbedingte Sicherheitslücken, Angriffsflächen bzw. Angreifbarkeit und damit IT-Sicherheitsprobleme entstehen, die neue technische und organisatorische Maßnahmen erfordern,
- eine Arbeitsteilung von Maschinen und eine Verteilung von Daten auf andere Plattformen erfolgt, die die Transparenz erschwert oder sogar die Grundsätze der Vertraulichkeit und Integrität in Frage stellen könnten. (Dabei ist es immer schwerer zu erkennen, ob Daten „auf dem eigenen Rechner verarbeitet werden oder in Schanghai“ – Zitat BfDI Schaar)
- In Rechenzentren und Serverumgebungen müssen speziell auch die Systemübergänge mit den Fragen der Einhaltbarkeit des Zweckbindungsprinzips bei der Schaffung der Durchlässigkeit dieser Systemgrenzen geprüft werden. Auch die Mandantenfähigkeit muss in diesem Zusammenhang neu bewertet werden.

Damit wird auch die Frage nach dem Kostenaufwand für derlei Analysen und Maßnahmen zu beurteilen sein.
Neben den zu modifizierenden Bewertungen der datenschutzrechtlichen Risiken bieten „virtuelle Sandkästen“ aber auch klare Vorteile für die IT-Sicherheit. Hier können gefahrlos neue Programmversionen getestet oder die Auswirkungen von Patches und Updates überprüft werden.
Wie auch bei serviceorientierten Architekturen (SOA) ist umso mehr ein ganzheitlicher Ansatz erforderlich, denn die Betrachtung der einzelnen Fachanwen-

dungen reicht aufgrund der Wechselwirkungen in einem virtuellen Umfeld und einem Systemverbund für einen systematischen Schutz nicht aus.
Worauf ist also in der Entwicklung und im Betrieb virtueller Maschinen und Systeme zu achten? Neben den Nutzenaspekten gesellt sich auch das Erfordernis, zusätzliche Risiken zu identifizieren, die sich möglicherweise aus der Virtualisierung ergeben können. Anschließend gilt es auch hier, geeignete Maßnahmen für den Schutz der informationellen Selbstbestimmung und die Gestaltungsziele Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität für IT-Verfahren und der zu verarbeitenden Daten zu definieren und umzusetzen.
Nach dem üblichen Initialreferat meiner Geschäftsstelle zu „Virtualisierung und Datenschutz“ stellte Prof. Dr. Günther Hellberg, Fachhochschule für die Wirtschaft Hannover aus wissenschaftlicher und praktischer Sicht mit dem Titel „Virtualisierung in Theorie und Praxis - aktuelle Ansätze und Konzepte mit IT-sicherheitstechnischer Betrachtung“ dar.
Auch hier bewährte sich die offene Gesprächskreiskultur, weil alle Beteiligten in der Diskussion Gelegenheit hatten, theoretische wie praktische Anforderungen im Licht der datenschutzrechtlichen Notwendigkeiten zu bewerten.

Zwischenbilanz

Das von Beginn an gesetzte Ziel war es, diesen Gesprächskreis als festen Bestandteil eines Netzwerkes für das Land Niedersachsen zu etablieren und, in Abstimmung mit den Teilnehmenden, in einem sachgerechten zeitlichen Rhythmus die fachlichen Kontakte zu pflegen, um einen höchstmöglichen Nutzwert aus diesem Netzwerk ziehen zu können. Die kontinuierliche Fortsetzung und die engagierte Teilnahme der Fachleute sowie das Podium mit Referenten unterschiedlicher Forschungseinrichtungen und IT-Firmen hat bereits zu einer Etablierung im Datenschutzinstitut für die Fragen des technischen Datenschutzes und des Telemedienrechtes geführt.
In der Fortsetzung der Reihe sind für 2009/2010 folgende Themenschwerpunkte bereits geplant:

10. Gesprächskreis: Protokollierung II (Datenschutz & IT-Sicherheit)
- Loggdaten in Applikationen und Systemen
- Protokollierung beim Accessmanagement

11. Gesprächskreis: Protokollierung III (Datenschutz & IT-Sicherheit)
- Datenarten nach TKG, TMG
- Vorratsdaten

12. Gesprächskreis: Computerstrafrecht und Datenschutz
- Integrität von IT-Systemen
- „Hackerparagraf und andere Admin-Sorgen“

13. Gesprächskreis: Backup/Archivierung datenschutzkonform

- Speziell E-Mail-Archivierung
- Signatur-/Schlüssel-Backup (Key-Recovery)
- Langzeitarchivierung

Aufwand und Nutzen

Auch wenn der fachliche Aufwand für die Vorbereitungen der bei jeder Sitzung wechselnden Themen und deren unterschiedlichen technischen, organisatorischen und rechtlichen Problemstellungen deutlich höher ist als bei Standardschulungen, ist aufgrund des Nutzwertes von einer sehr lohnenden Investition auszugehen. Durch die Möglichkeit des Erfahrungsaustausches und der oft neuartigen Befassung mit Innovations- und Zukunftsthemen der Informationstechnik wird eine präventive und multiplikative Wirkung für die Weiterentwicklung des technischen und organisatorischen Datenschutzes erzielt.

Auch für die Zukunft gewappnet?

Die quantitative Arbeitsbelastung für diese Gesprächskreise ist aufgrund der geringen Personaldecke für den technischen Datenschutz besonders hoch. Dabei entfallen 43 % aller Personentage (bezogen auf Nettoschulungstage) des Datenschutzinstituts auf die drei Angehörigen des Technikteams. Der wachsenden Bedeutung der schnelllebigen Entwicklung neuer Technologien entsprechend sollte unter anderem auch deshalb zeitnah eine Verstärkung des Personals erreicht werden. Dies käme sowohl dem öffentlichen als auch dem nicht-öffentlichen Bereich der Datenschutzaufsicht zugute, weil das Team 3 querschnittliche Dienstleistung erbringt.

Gruppenprüfung bei Kommunen – eine Nachschau

Bereits in meinem XVIII. TB hatte ich über eine aktuelle Gruppenprüfung zum Schwerpunktthema „Protokollierung“ in vier Landkreisen, vier Städten und zehn Samtgemeinden und Gemeinden durch mein Technikteam berichtet. Wie angekündigt, konnten die wesentlichen Arbeiten noch 2007 abgeschlossen und die Ergebnisse in einer Orientierungshilfe zum Thema datenschutzgerechte Protokollierung aufbereitet werden. Diese steht seit Ende 2007 auf meiner Website zum Download bereit.

www.lfd.niedersachsen.de
> Service-Angebote > Checklisten > Protokollierung

Neben den Ergebnissen zum Schwerpunktthema haben insbesondere die bei den Prüfungsteilnehmern allgemein angetroffenen technisch-organisatorischen Rahmenbedingungen weiteren Anlass zu kritischen Hinweisen gegeben. Die Defizite reichten von ungenügender Ausstattung und Absicherung der Systembetriebsräume bis hin zum völligen Fehlen jeglicher schriftlicher Regelungen zum Thema Datenschutz.

Als weitere Beispiele mit besonderer Bedeutung seien genannt:

- die aufgrund von Interessenkonflikten mit anderen dienstlichen Aufgaben nicht ordnungsgemäße Bestellung einiger behördlicher Datenschutzbeauftragter (§ 8a Abs. 2 NDSG)
- die teilweise unzulänglich formulierten und/oder technisch nicht realisierten Anforderungen an Qualität, Änderungshistorie und Wechselhäufigkeit von Passworten
- die sehr häufig mangelnde Rechtskonformität der Spam-Filterung
- der überwiegend anzutreffende ungehinderte Zugriff aller Bediensteten auf Laufwerke und USB-Ports
- das mit wenigen Ausnahmen fast durchgehende Fehlen von Vorabkontrollen (§ 7 Abs. 3 NDSG)

In den Diskussionen mit den jeweiligen Prüfungsteilnehmern wurden hierfür überwiegend nachvollziehbare Begründungen angeführt; angefangen von akuter Finanznot über Personalknappheit bis hin zu der vertretenen Auffassung, aufgrund der hervorragenden persönlichen Zusammenarbeit in der Verwaltung bedürfe es keiner formalen Regelungen.

Dennoch ist es in den erfreulich offen und konstruktiv geführten Gesprächen stets gelungen, den Verantwortlichen die sich aus den festgestellten Mängeln ergebenden Konsequenzen deutlich werden zu lassen; im Ergebnis haben alle Prüfungsteilnehmer die geforderten Maßnahmen zur Verbesserung der Situation des Datenschutzes in den wichtigsten Punkten umgesetzt.

Die Erfahrungen, die ich im Verlauf der Prüfung bei den Kreisverwaltungen gemacht habe, sind durch die Ergebnisse aus dem Bereich von Städten und (Samt-)Gemeinden komplettiert worden. Neben der Bestätigung der bisherigen Erkenntnisse traten zwei weitere Aspekte deutlich in den Vordergrund:

So zeigt sich zum einen ein deutlicher Qualitätsunterschied zwischen den Kreis- und Gemeindeverwaltungen insgesamt, der sich ganz wesentlich aus einer unterschiedlichen Finanzlage und einer deutlich knapperen Personaldecke bei den Gemeinden erklärt. Darüber hinaus sind aus Datenschutzsicht erforderliche, klare Organisationsstrukturen in kleineren Gemeindeverwaltungen deutlich schwieriger in die tägliche Praxis umzusetzen. Die Forderung nach klar trennbaren Funktionen lässt sich allgemein in größeren Organisationen leichter umsetzen als in sehr kleinen, bei denen naturgemäß eine Mitarbeiterin oder ein Mitarbeiter oft mehrere Aufgaben auf sich vereinen.

Während ich die Kreisverwaltungen nach Auswertung der jeweiligen vor-Ort-Prüfungen gebeten hatte, über vorgenommene Veränderungen zu berichten, wurde den Gemeinden zur Nachschau lediglich ein weiterer Besuch nach Ablauf eines Jahres angekündigt. Diese Besuche bei ausgewählten Verwaltungen habe ich im Herbst des Jahres 2008 durchgeführt.
Erfreulich ist, dass alle nochmals befragten Prüfungsteilnehmer nicht nur die im Prüfbericht des Erstbesuchs als „zwingend erforderlich“ gekennzeichneten Maßnahmen umgesetzt haben, sondern sich im Rahmen der Möglichkeiten auch um die Umsetzung der lediglich „empfohlenen“ Verbesserungsvorschläge bemüht hatten; sei es durch Trennung unvereinbarer Funktionen oder Verbesserungen in technischer und/oder organisatorischer Hinsicht.

Insgesamt hat die abgeschlossene Gruppenprüfung klar aufgezeigt, dass der eingeschlagene Weg einer Prüfung und Beratung vor Ort richtig und für beide Seiten unverzichtbar ist. Der mir entstandene erhöhte Personal- und Sachaufwand ist auch durch die Übertragbarkeit der Schwerpunkt-Ergebnisse auf andere Daten verabeitende Stellen und den Zugewinn an eigenen praktischen Erfahrungen, die sich positiv auf die übrige Beratungs- und Schulungstätigkeit auswirken, gerechtfertigt.

CHARTA DER GRUNDRECHTE DER EUROPÄISCHEN UNION
proklamiert in Nizza am 07. Dezember 2000 (2000/C 364/01)

Artikel 8
Schutz personenbezogener Daten

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Niedersächsische Verfassung

Artikel 62
Landesbeauftragte oder Landesbeauftragter für den Datenschutz

(1) Die Landesbeauftragte oder der Landesbeauftragte für den Datenschutz kontrolliert, dass die öffentliche Verwaltung bei dem Umgang mit personenbezogenen Daten Gesetz und Recht einhält. Sie oder er berichtet über ihre oder seine Tätigkeit und deren Ergebnisse dem Landtag.
(2) Der Landtag wählt auf Vorschlag der Landesregierung die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz mit einer Mehrheit von zwei Dritteln der anwesenden Mitglieder des Landtages, mindestens jedoch der Mehrheit seiner Mitglieder.
(3) Die Landesbeauftragte oder der Landesbeauftragte für den Datenschutz ist unabhängig und nur an Gesetz und Recht gebunden.
(4) Das Nähere bestimmt ein Gesetz. Dieses Gesetz kann personalrechtliche Entscheidungen, welche die der Landesbeauftragten oder dem Landesbeauftragten für den Datenschutz zugeordneten Bediensteten betreffen, von deren oder dessen Mitwirkung abhängig machen. Das Gesetz kann weitere Aufgaben der Landesbeauftragten oder des Landesbeauftragten für den Datenschutz vorsehen.

Der Landesbeauftragte für den Datenschutz Niedersachsen