Internet

Weiterhin im Mittelpunkt der schnellen technischen Entwicklungen und Anwendungen steht das Internet; Angebote wie Telefonie, Rundfunk und Video werden schon heute zunehmend über das Internet-Protokoll TCP/IP übertragen. Das Internet ist zu einem Kommunikationsmedium für jedermann geworden; eCommerce, eBusiness und eGovernment beherrschen die Szene, eCrime sowie Cyber-Terrorismus sind gefährliche, ungewollte Nebenerscheinungen. Das Internet ging in seinen Anfängen vom Prinzip der Kontrollfreiheit aus. Anonymität, für die heute Datenschützer und Cyberrechtler kämpfen, war selbstverständlich. Jeder Versuch einer korrigierenden oder steuernden Funktion wurde entschieden zurückgewiesen und leidenschaftlich bekämpft. Das Prinzip des freien Flusses der Information (free flow of information) war fast noch mehr verwurzelt als das Prinzip der Informationsfreiheit (freedom of information).

Die vielfachen Nutzungsmöglichkeiten des Internets sind inzwischen Bestandteil unseres Alltags geworden, sowohl am Arbeitsplatz als auch Zuhause. Das Internet wird nicht nur zur Abfrage von Informationen genutzt, sondern zunehmend auch zur Abwicklung von Rechtsgeschäften und zur interaktiven Beantragung und Bearbeitung von Verwaltungsentscheidungen. Das öffentliche Kommunikationsnetz Internet offenbart dabei systembedingt viele Informationen über seine Nutzer. So werden Name und Adresse beim Absenden der E-Mail beigestellt. Beginn, Ende und Dauer einer Verbindung, Datenmenge, das verwendete Protokoll sowie die eingesetzte Software sind erkennbar. Das alles sind personenbeziehbare Informationen, die viel über die handelnden Personen aussagen. An den Kommunikationsschnittstellen zwischen Netzen und Nutzern (Knotenpunkte im Internet, Internet-Portal und virtuelle Poststelle) laufen alle Kommunikationsvorgänge zusammen. Dabei entstehen umfangreiche Datensammlungen und damit neuartige Bedrohungen für die Privatsphäre der Bürger. Einige dieser Überwachungsmöglichkeiten sollen hier aufgezeigt werden:

- Auf die Terroranschläge vom 11. September 2001 haben die USA unter anderem mit weitgehenden Überwachungsmaßnahmen und Eingriffen im Internet reagiert (Patriot Act). Wer durch Selbstschutz sein Recht auf unbeobachtete Kommunikation wahrnehmen will und Spuren zu verwischen sucht, wird als Eindringling eingestuft, der keinen Anspruch auf Achtung seines „right to privacy“ hat.
- Das deutsche Terrorismusbekämpfungsgesetz vom 14. Dezember 2001 enthält weitgehende Befugnisse zur Überwachung der Konten und Geldbewegungen bei Kreditinstituten, der Postbewegungen bei allen Postdienstleistern, der Transport- und Reisebewegungen bei Lufttransporteuren und der Telekommunikationsdienstleistungen bei entsprechenden Anbietern. Eine zentrale Rolle bei der Bekämpfung des internationalen Terrorismus wird dem Bundesverfassungsschutz zugewiesen. Diese Befugnisse ermöglichen es, umfassende Verhaltens- und Bewegungsprofile zu erstellen. Im Einzelnen wird dazu auf die Darstellung in Kapitel 10.1.1 verwiesen.

- Auf Initiative des Bundesrates sollen durch Änderung der StPO alle Telekommunikationsunternehmen und sämtliche Internetprovider verpflichtet werden, alle Daten über Kunden und ihre Nutzungen ausnahmslos zu speichern und für Polizei- und Sicherheitsbehörden bereithalten. Dies stellt eine Vorratsspeicherung dar, die das Bundesverfassungsgericht im Volkszählungsurteil als unzulässig angesehen hat.
- Suchmaschinen liefern Infopartikel und Fakten über ihre Nutzer. So kann der Betreiber der Suchmaschine rückverfolgen, welche Seiten mit welchen Suchbegriffen von einem Nutzer gefunden und in welcher Reihenfolge abgerufen worden sind. Auch die Verweildauer ist erkennbar.
- Cookies werden auf fremden Rechnern gespeichert. Sie machen Nutzer beim nächsten Besuch erkennbar; Online-Händler identifizieren über Sammelfilter ihre Kunden.
- Customer Relation Management (CRM) hat Konjunktur. Durch Verknüpfung (Data Warehouse) und Auswertung (Data Mining) systematisch zusammengeführter Kundendaten versuchen Handelsunternehmen personenbezogene Erkenntnisse für erfolgreiches Direktmarketing oder kommerziellen Datenhandel zu gewinnen. Die betroffenen Kunden sind vielfach weder unterrichtet noch um Einwilligung gebeten worden (vgl. Kapitel 20).
- Arbeitgeber haben zwar das Recht, die Erfüllung dienstlicher Aufgaben auch bei der Internetnutzung angemessen zu kontrollieren, unzulässig dagegen ist eine Totalüberwachung der Mitarbeiter (vgl. dazu Kapitel 8.3). Das Überwachungsprogramm mit dem sinnigen Namen „Little Brother“ bietet dazu die Möglichkeit; Verhalten und Leistung der Mitarbeiter können so detailliert offengelegt werden. So kann die dringend benötigte Kommunikationskultur in Unternehmen und Behörden zerstört werden. Damit wird mehr Schaden angerichtet als dies je nützen könnte.

Diese mächtigen Überwachungsmöglichkeiten drohen das zarte Pflänzchen der beginnenden Informationsgesellschaft zu ersticken. Besonders seit dem 11. September 2001 verschiebt sich die Balance zwischen Schutz der Privatsphäre einerseits und sicherheitstechnischen und kommerziellen Interessen andererseits. Zum wiederholten Mal wurde der Versuch gestartet, den Datenschutz bei der Nutzung von Internet und Telekommunikation auszuhebeln. Internet- und Telekommunikations-Provider sollten zur zwangsweisen Vorratsspeicherung sämtlicher Daten ihrer Kunden zu verpflichten werden (vgl. Kapitel 8.6.3). Eine entsprechende Initiative des Bundesrates ist zwar durch den Ablauf der Legislaturperiode des Bundestages vorerst gegenstandslos geworden. Es ist aber sicher davon auszugehen, dass es neue Vorstöße in dieser Richtung geben wird, zumal auch die dänische Ratspräsidentschaft auf europäischer Ebene entsprechende Initiativen eingeleitet hat. Dies darf nicht geschehen!

Selbstdatenschutz

Da Staat und Recht in globalen Netzen und einer Welt allgegenwärtiger Datenverarbeitung nur begrenzt in der Lage sind, die informationelle Selbstbestimmung ihrer Bürger zu schützen, ist es erforderlich, dass nach Ausschöpfen aller bereits genannten Möglichkeiten zum Schutz der Selbstbestimmung den Bürgern ermöglicht wird, Mittel zu ergreifen, um ihre informationelle Selbstbestimmung selbst zu schützen.

Für einen umfassenden Persönlichkeitsschutz sollten dem Nutzer die technischen Instrumente sowie notwendige Infrastrukturleistungen zur Verfügung gestellt werden. Ein wichtiges Mittel des Selbstdatenschutzes ist die selbstbestimmte Wahl von anonymen Nutzungen, von Pseudonymen oder von Verschlüsselungstechniken. Ein weiteres Instrument des Selbstdatenschutzes ist die Möglichkeit, sich durch Zugriff auf die Datenschutzerklärung der Daten verarbeitenden Stelle jederzeit ausreichende Gewissheit über die Bedingungen der Datenverarbeitung zu verschaffen. Durch Offenlegen der Datenverarbeitungspraxis kann dem Nutzer ein Teil seiner Besorgnis genommen werden.

Schutz und Hilfestellung gegen Bedrohungen bei der Nutzung von E-Mail und Internet werden in vielfacher Hinsicht geboten. Die Möglichkeiten reichen von umfassenden Informationen zur datenschutzgerechten Auswahl und Konfiguration des Web-Browsers oder des Mail-Clients bis hin zum Einsatz von Hard- und Softwareprodukten, die es dem Nutzer erlauben, die Verbindungen seines Rechnersystems zum Netz wirksam zu kontrollieren. Eine zentrale Rolle bei allen Bemühungen muss aber stets der Benutzer einnehmen; er muss sich über mögliche Gefahren informieren und Abwehrstrategien entwickeln. Geeignete Hilfsmittel zur Entwicklung und Umsetzung solcher Strategien sind teils kostenlos, teil zu durchaus erschwinglichen Preisen am Markt verfügbar. Entsprechende Informationen finden sich unter anderem auf unserer Homepage http://www.lfd.niedersachsen.de, unter http://www.datenschutz.de oder in den einschlägigen Veröffentlichungen der Fachpresse.

PC-Selbsttest

Über unsere Homepage www.lfd.niedersachsen.de stellen wir einen Selbsttest zur Verfügung. Der Test ist für Privatanwender gedacht und soll helfen, unsichere Systemkonfigurationen aufzudecken. Nur wenn bekannt ist, welche Lücken ein System aufweist, kann qualifiziert Abhilfe geschaffen werden. Daher überprüft der Test in einem mehrstufigen Verfahren nicht nur die Einstellungen des Browsers, sondern führt auf Wunsch des Nutzers auch einen sog. Port-Scann durch. Die Ergebnisse werden dem Tester vertraulich zur Verfügung gestellt und ermöglichen, die notwendigen Maßnahmen zur Absicherung des Systems zu treffen.

Internet am Arbeitsplatz

Neben den gängigen Kommunikationsverbindungen Telefon und Fax gehört ein eigener Internetanschluss mittlerweile in der privaten Wirtschaft und in der öffentlichen Verwaltung zur unverzichtbaren und fast schon selbstverständlichen Mindestausstattung eines Arbeitsplatzes. So verfügen in Niedersachsen über das iznNet mehr als 50 000 Bedienstete der unmittelbaren Landesverwaltung über einen eigenen Zugang zum Internet nebst persönlicher E-Mail-Adresse. Den Beschäftigten wird die Nutzung des Internet vielfach ausschließlich zu dienstlichen oder betrieblichen Zwecken, teils aber ausdrücklich oder im Rahmen einer so genannten „betrieblichen Übung“ auch zu privaten Zwecken gestattet.

Nach einer Umfrage der Zeitschrift Capital aus dem September 2001 war es den Beschäftigten großer Firmen, so etwa Siemens, Deutsche Post World Net oder Bertelsmann, untersagt, das Internet zu privaten Zwecken zu nutzen. Ausgehende E-Mails wurden grundsätzlich nur von 13 % der befragten Unternehmen kontrolliert. Veröffentlichungen in den Medien und die in meiner Geschäftsstelle aus dem Kreis der betroffenen Beschäftigten und Mitarbeitervertretungen eingehenden Anfragen lassen jedoch vermuten, dass die Betriebe und Dienststellen vermehrt dazu übergehen, die Surfgewohnheiten der Beschäftigten zu kontrollieren.

Die Motive der Arbeitgeber und Dienststellen für eine Überprüfung sind vielfältig. Sie erfolgen teils gezielt auf entsprechende Hinweise der Systemadministration, aus Anlass von Beschwerden einzelner Beschäftigter über die Zusendung „unerwünschter" E-Mails oder flächendeckend allein aus dem Interesse, Erkenntnisse über die Art und Weise sowie den Umfang der Internutzung zu gewinnen und unnötige Kosten zu sparen. Auf die in der Öffentlichkeit und im politischen Raum kontrovers erörterten Ergebnisse der Prüfung des Niedersächsischen Landesrechnungshofs, der auf der Grundlage einer Auswertung der beim Informatikzentrum Niedersachsen gespeicherten Protokolldaten davon ausgeht, dass der Umfang der privaten Internetrecherchen der Bediensteten erheblich ist, weise ich in diesem Zusammenhang hin.

Die bei mir eingehenden Anfragen zeigen auch, dass vielfach große Unsicherheit bestehen, welche Daten bei der Nutzung von Internet und E-Mail überhaupt protokolliert werden dürfen und unter welchen Voraussetzungen es zulässig ist, Protokolldaten zum Zwecke der Überwachung des Nutzerverhaltens auszuwerten. Viele meinen, es sei schon aufgrund der gesetzlichen Zweckbindung verboten, personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, für andere Zwecke, etwa zur Verhaltens- und Leistungskontrolle der Beschäftigten, zu verwenden (vgl. § 31 BDSG, § 10 Abs. 4 NDSG, § 101 Abs. 6 NBG). Es sei daher nicht zulässig, Abmahnungen, Kündigungen oder sonstige dienst- und arbeitsrechtliche Maßnahmen wegen unerlaubter Internetnutzungen auf die einem Verwertungsverbot unterliegenden Protokolldaten zu stützen. Außerdem stehe auch das Fernmeldegeheimnis aus Art. 10 GG einer Kontrolle der Internutzung entgegen. Die derzeitige Rechtslage ist sehr kompliziert, sodass schon von daher Anlass besteht, eindeutige gesetzliche Regelungen in einem von mir und anderen Datenschützern seit längerem eingeforderten Arbeitnehmerdatenschutzgesetz zu schaffen.

Vielfach ist den Beschäftigten und den Mitarbeitervertretungen nicht bekannt, welche Protokolldaten überhaupt durch die zuständige Systemadministration zum Zwecke der Datensicherung und des ordnungsgemäßen Betriebs der Datenverarbeitungsanlage erhoben und gespeichert werden und auf welche Weise Rückschlüsse auf das Nutzerverhalten gezogen werden können.

Viele Unternehmen oder Behörden betreiben Proxyserver oder Firewall-Systeme, um ihre internen Netzwerke gegen Angriffe von außen zu schützen. Die eingesetzten Firewall- und Proxyserver sind in der Lage, verschiedene Arten von Daten zu erfassen und zu speichern. Zu unterscheiden sind dabei Bestands-, Verbindungs-, Nutzungs- und Inhaltsdaten, die durch das Surfen entstehen. Eine Protokollierung ist

grundsätzlich auf allen Firewall- und Proxyservern möglich. Die Protokolldateien enthalten alle Anfragen an den zentralen Proxyserver mit Datum, Uhrzeit, aufgerufener Internetadresse (URL), Größe des angefragten Objekts, Zeit für die Beantwortung der Anfrage, Informationen zu Übertragungsmethoden und Zugriffswege sowie die IP-Adresse des Netzes oder des Rechner aus der die Anfrage kam. Da die IP-Adresse oftmals einem bestimmten Arbeitsplatz-PC zugeordnet werden kann und am Arbeitsplatz-PC ermittelt werden kann, wer zur fraglichen Zeit angemeldet war, kann ein Personenbezug hergestellt werden.

Bei der Beantwortung der Frage, ob und unter welchen Voraussetzungen der Arbeitgeber berechtigt ist, Kontrollen der Internetnutzung durchzuführen, ist von entscheidender Bedeutung, ob das Internet durch die Beschäftigten ausschließlich zu dienstlichen oder betrieblichen Zwecken oder darüber hinaus auch zum privaten Gebrauch genutzt werden darf. Abhängig von den jeweiligen Gegebenheiten und Nutzungsbedingungen vor Ort sind bei der Bewertung der Rechtslage die unterschiedlichsten Rechtsvorschriften aus dem Bereich des Tele- und Mediendiensterechts, des allgemeinen Datenschutzrechts oder des Dienst- und Arbeitsrechts zu berücksichtigen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung die an eine datenschutzgerechte Internet-Nutzung zu stellenden Anforderungen beschrieben. Darüber hinaus hat der Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer „Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internet-Diensten am Arbeitsplatz“ zu diesem Thema detaillierte Hinweise veröffentlicht. Die Orientierungshilfe kann unter „Home/Service/Empfehlungen Recht/Internutzung“ aus meinen Internetangebot herunter geladen oder dort eingesehen werden (siehe auch Anlage 21). Ich empfehle, die folgenden Leitplanken einzuhalten:

1. Die Arbeitsplätze mit Internet-Zugang sind so zu gestalten, dass keine oder möglichst wenige personenbezogene Daten erhoben werden. Die Nutzung des Internet am Arbeitsplatz darf nicht zu einer vollständigen Kontrolle der Bediensteten führen. Präventive Maßnahmen gegen eine unbefugte Nutzung sind nachträglichen Kontrollen vorzuziehen.

2. Die Beschäftigten sind umfassend darüber zu informieren, für welche Zwecke sie einen Internet-Zugang am Arbeitsplatz nutzen dürfen und auf welche Weise der Arbeitgeber die Einhaltung der Nutzungsbedingungen kontrolliert.

3. Fragen der Protokollierung und einzelfallbezogenen Überprüfung bei Missbrauchsverdacht sind durch Dienstvereinbarungen zu regeln. Die Kommunikation von schweigepflichtigen Personen und Personalvertretungen muss vor einer Überwachung grundsätzlich geschützt bleiben.

4. Soweit die Protokollierung der Internet-Nutzung aus Gründen des Datenschutzes, der Datensicherheit oder des ordnungsgemäßen Betriebs der Verfahren notwendig ist, dürfen die dabei anfallenden Daten nicht zur Leistungs- und Verhaltenskontrolle verwendet werden.

5. Wird den Beschäftigten die private E-Mail-Nutzung gestattet, so ist diese elektronische Post vom Telekommunikationsgeheimnis geschützt. Der

Arbeitgeber darf ihren Inhalt grundsätzlich nicht zur Kenntnis nehmen und hat dazu die erforderlichen technischen und organisatorischen Vorkehrungen zu treffen.

6. Der Arbeitgeber ist nicht verpflichtet, die private Nutzung des Internet am Arbeitsplatz zu gestatten. Wenn er dies gleichwohl tut, kann er die Gestattung unter Beachtung der hier genannten Grundsätze davon abhängig machen, dass die Beschäftigten einer Protokollierung zur Durchführung einer angemessenen Kontrolle der Netzaktivitäten zustimmen.

7. Die gleichen Bedingungen wie bei der Nutzung des Internet müssen prinzipiell bei der Nutzung von Intranets gelten.

Arbeitgeber sind befugt, bei ausschließlich dienstlicher oder betrieblicher Nutzung die Protokolldaten stichprobenartig oder bei Verdacht auf Missbrauch auszuwerten. Die besondere Zweckbindung der Protokolldaten steht in diesen Fällen einer Nutzung zu Kontrollzwecken nicht entgegen. Ich empfehle, eine Dienst- oder Betriebsvereinbarung über die Nutzung von Internet und E-Mail abzuschließen, in der die Nutzungsbedingungen und insbesondere auch die Protokollierung und Auswertung zu Kontrollzwecken eindeutig und zweifelsfrei geregelt sind.

Sichere E-Mail

Der E-Mail-Dienst hat in den letzten Jahren immens an Bedeutung gewonnen. Mit dem umfassenden Einsatz von vernetzten Rechnersystemen in Verwaltung und Wirtschaft hat sich dieses Kommunikationsmedium in der modernen Arbeitswelt etabliert. Aber auch im Privatbereich ist die E-Mail heute überaus beliebt. Eine Vielzahl von Providern bieten kostenlose E-Mail-Postfächer für Privatkunden an. Die schnelle und preiswerte Kommunikation ist der große Vorteil, der zu dieser starken Verbreitung geführt hat.

Mit dem Einsatz von E-Mail treten aber auch eine Reihe neuer Gefahren auf. Ungesichert übertragene E-Mails können abgefangen, gelesen und verfälscht werden. Zudem ist nicht sichergestellt, dass die E-Mail wirklich den Empfänger erreicht. E-Mails können Viren oder andere Schadprogramme enthalten, die Datenbestände auf Arbeitsplatz-PCs und in Netzwerken gefährden. Verbreitungsszenarien wie beim „Loveletter“-Mailvirus haben dies deutlich gezeigt. Während jedoch Virenscanner in großen Teilen von Verwaltung und Wirtschaft heute obligatorisch sind und so auch die Mailserver und Mailclients sichern, gilt dies nicht für Lösungen, die die Inhalte der Mailkommunikation sichern sollen.

Die Niedersächsische Landesverwaltung hat im Jahr 1996 mit der Einführung von Electronic Mail begonnen. Seit diesem Zeitpunkt wurden etwa 50 000 Mitarbeiter der Landesverwaltung an den Telekommunikationsdienst Electronic Mail angeschlossen, weitere Anschlüsse und der Verbund mit der niedersächsischen Kommunalverwaltung sind geplant. Der E-Mail-Dienst ist zu einem wichtigen und unverzichtbaren Arbeitsmittel in der öffentlichen Verwaltung geworden. Er bildet darüber hinaus die Basis für die Realisierung verschiedener eGovernment-Projekte.

Der sich über einen längeren Zeitraum hinziehende Anschluss der Dienststellen an den landesweiten Mailverbund hatte zur Folge, dass einheitliche Festlegungen zur technischen Ausgestaltung und zur Nutzung des komplexen Dienstes fehlten. Leider erst nach fast abgeschlossener Einführung erarbeitet eine Arbeitsgruppe des IMA-IuK eine Rahmendienstanweisung zur Nutzung des E-Mail-Dienstes sowie eine Dienstanweisung für Administratoren. An den Entwurfsarbeiten habe ich mich aktiv beteiligt. Kernpunkte der Dienstanweisung sind:

- Personenbezogenen Daten und Informationen, die besonders schutzbedürftig sind, dürfen nicht ohne zusätzliche Sicherungen (elektronische Signatur, Verschlüsselung) versandt werden.
- Bei Einsatz der Verschlüsselung ist die elektronische Signatur obligatorisch.
- Der E-Mail-Dienst ist nur für den dienstlichen Gebrauch zugelassen.
- Eine Kontrolle der Nutzung des E-Mail-Dienstes erfolgt nur im erforderlichen Umfang (gelegentliche Stichproben und Anlasskontrollen).
- Die auf Grund der elektronischen Verarbeitung entstehenden Nachweisdaten dürfen nicht für Zwecke der Leistungs- und Verhaltenskontrolle von Mitarbeitern verwendet werden.
- E-Mails dürfen nicht länger gespeichert werden, als dies für die Aufgabenerfüllung erforderlich ist.

Eine Strategie-Entscheidung der niedersächsischen Landesverwaltung sieht vor, künftig in verstärktem Maße die elektronische Signatur und Verschlüsselungstechniken einzusetzen. Hierfür ist eine geeignete Infrastruktur zur Signatur und Verschlüsselung von E-Mails aufzubauen. Verbleibende Restrisiken der Vertraulichkeit sind durch organisatorische Maßnahmen wirksam abzusichern. Hierzu gehört auch eine angemessene Sensibilisierung der Mitarbeiter im Umgang mit personenbezogenen Daten und anderen vertraulichen Informationen.

Verschlüsselung bei Speicherung und Übermittlung

Der technisch-organisatorische Datenschutz umfasst die Maßnahmen, die nach § 7 des Niedersächsischen Datenschutzgesetzes bzw. nach der Anlage zu § 9 des Bundesdatenschutzgesetzes zu treffen sind, um die dort niedergelegten Ziele zu erreichen und einen datenschutzgerechten Umgang mit personenbezogenen Daten sicherzustellen. Die technische Umsetzung dieser Anforderungen war in der Vergangenheit im Wesentlichen darauf abgestellt, Unbefugten den Zugang zu den Räumen, Maschinen und Netzwerken, in denen Datenverarbeitung stattfindet, zu verwehren und die befugte Nutzung von Räumen, Maschinen und Kommunikationswegen nachvollziehbar zu protokollieren.

Der Aufwand, auf diesem Wege ein hohes Maß an Sicherheit zu erreichen, hat in verschiedenen Bereichen wie z.B. der Netzwerkabsicherung eine Größenordnung erreicht, die von kleineren Organisationen nur noch bedingt zu leisten ist. Im Gegensatz zu klassischen Maßnahmen der baulichen Absicherung von technischen Betriebsräumen und Kommunikationswegen, die sich in den letzten Jahren im Kern nur in bescheidenem Umfang verändert haben, ist der Bereich der Netzwerkabsicherung förmlich explodiert. In dem Maße, wie die öffentlichen Stellen sich verstärkt offener, technisch nicht kontrollierbarer Kommunikationswege bedienen, sind die Aufwendungen für die Absicherung der internen Netze in die

Höhe geklettert. Um die Kosten in einigermaßen erträglichen Grenzen zu halten, sind häufig zentrale Übergangsstellen zwischen internen und externen Netzen gebildet worden. Diese Firewalls sind meist in gesicherten Räumen ordnungsgemäß untergebracht. An diesen Übergangsstellen wird mit einem immer größer werdenden technischen Aufwand versucht, die möglichen Bedrohungen aus dem externen Netz soweit möglich zu begrenzen. Dennoch bieten die in dieser Weise abgesicherten zentralen Übergangspunkte oftmals nur einen trügerischen Schutz, da technisch nicht hinreichend sichergestellt werden kann, dass es wirklich keine „Nebenstrecken" zu Fremdnetzen gibt.

Dies zeigt, dass die herkömmlichen Maßnahmen im Grunde vordringlich auf eine Absicherung der „Datenumgebung" gerichtet sind; es werden räumliche Sicherungen installiert, Zutrittskontrollen durchgeführt, Zugangskontrollen installiert usw. Zur Sicherung der Daten selbst stehen bislang außer der Zuordnung von Zugriffsrechten unterschiedlicher Qualität kaum praktisch relevante Verfahren zur Verfügung. Die theoretisch denkbare Verwendung vom kryptografischen Methoden zur Absicherung der Daten während der Speicherung und Übermittlung scheitert bislang an organisatorischen, technischen und rechtlichen Problemen bei der Vergabe und Verwaltung geeigneter Schlüsselpaare. Erst wenn es gelingt, hierarchisch strukturierte Gruppenschlüssel in ausreichender Anzahl in geeigneter Weise bereitzustellen, wären die technischen Grundlagen geschaffen, um den technischen Datenschutz im engeren Sinne voranzutreiben. Die bei der flächendeckenden Ausstattung der niedersächsischen Landesverwaltung anfallenden Kosten für Crypto-Cards, Lesegeräte und Software wären durch den Zuwachs an Sicherheit für personenbezogene Daten in allen Stufen der Verarbeitung gerechtfertigt. Ob Einsparpotentiale entstehen, wenn innerhalb der Landesverwaltung alle schützenswerten Daten nur noch in verschlüsselter Form gespeichert oder übermittelt werden, wäre gesondert zu betrachten. Dabei muss jedoch bedacht werden, dass die Zugangssicherungen einen wesentlichen Beitrag zur Verfügbarkeit der Daten leisten, der ausschließlich über kryptografische Verfahren nicht sichergestellt werden kann.

Elektronische Signatur / Crypto-Card Niedersachsen

In den verschiedensten Bereichen des IuK-Technikeinsatzes und in der Kommunikation halten verstärkt kryptografische Methoden Einzug, um die Sicherungsziele Authentizität, Integrität und Verfügbarkeit bei der Verarbeitung von personenbezogenen Daten zu erreichen. Eine nachhaltige Nutzung dieser Methoden bedingt den Einsatz geeigneter Chipkartensysteme. In Niedersachsen findet für einen Teilbereich der Verwaltung eine Signatur-Karte der TeleSec Anwendung. Vor diesem Hintergrund erscheint es sinnvoll, Modelle für einen erweiterten Einsatz dieser Karten-Technologie zu entwickeln, die den weitergehenden Einsatz von Signatur und Verschlüsselung vorsehen und somit zu einer wesentlichen Verbesserung des Datenschutzniveaus in der niedersächsischen Landesverwaltung beitragen können.

Auf der in der niedersächsischen Landesverwaltung verwendeten Crypto-Card der TeleSec sind zwei Schlüsselpaare hinterlegt; ein Schlüsselpaar dient der gesetzeskonformen Signatur, das andere kann für die Verschlüsselung von Mailinhalten genutzt werden. Da der private Schlüsselteil für den persönlichen

Verschlüsselungsschlüssel ausschließlich auf der Karte vorgehalten wird, ist der Zugriff auf verschlüsselte Dokumente nur mit der persönlichen Karte möglich. Ist der Inhaber der Karte längerfristig nicht verfügbar oder hat ein unberechtigter Nutzer die Karte durch Falscheingabe der PIN gesperrt, sind die verschlüsselten Dokumente endgültig verloren. Dieses hohe Risiko hat sicherlich mit dazu beigetragen, dass die Crypto-Card außerhalb der Kernfunktionalität der automatisierten Haushaltsbewirtschaftung (P53) derzeit nur begrenzte praktische Verwendung findet.

Durch hierarchische Gruppenschlüssel ließe sich dieses Risiko reduzieren und der erwünschte Mehrnutzen erreichen. Hierzu wäre es erforderlich, auf den eingesetzten Chips zusätzliche Speicherbereiche bereitzustellen, die vom Nutzer in eigener Verantwortung belegt werden können. Leider sieht diese Erweiterung die bei der TeleSec ab Mitte 2003 verfügbare „neue“ Chipkarte noch nicht vor. Bis zur Realisierung derartiger Chipkarten muss für den Einsatz von organisationsgebundenen Schlüsseln auf reine Softwarelösungen ausgewichen werden. Unter Einbeziehung der weiterhin vorhandenen persönlichen Schlüssel für Signatur und Verschlüsselung könnten so mehrstufige Hierarchien aufgebaut werden. Die Generierung und Verwaltung dieser Organisationsschlüssel sollte zentral für die jeweilige Organisation erfolgen.

Die Crypto-Card des Landes Niedersachsen hat sich bei P53 und in Ansätzen bei der Mail-Verschlüsselung bewährt. Die einer Erweiterung ihrer Einsatzmöglichkeiten bislang entgegenstehenden technischen Probleme könnten durch Einführung einer verbesserten Chip-Karte befriedigend gelöst werden. Damit würden sich für Niedersachsen eine ganze Reihe neuer Anwendungsfelder erschließen, zum Beispiel im Bereich der Kommunikations- und Datensicherheit und beim verstärkten Einsatz der Signatur in der öffentlichen Verwaltung. Eine Arbeitsgruppe des IMA-IuK, an der ich aktiv mitarbeite, untersucht Einsatzmöglichkeiten und Möglichkeiten der technischen Realisierung.