Politik zwischen E-Government und Überwachungsstaat I. Teil

Lothar Binding 12.7.04

Der Begriff „E-Government“ – Electronic Government – steht als Synonym für eine moderne und effiziente Verwaltung mit optimalen Kommunikationsmöglichkeiten zwischen Bürgern und Verwaltung.

Es besteht kein Zweifel, dass wir uns kontinuierlich vom Industrie- zum Informationszeitalter entwickeln. Der Übergang zur Wissensgesellschaft hat zu einer neuen Qualität der Beziehung zwischen Bürgerinnen und Bürgern und öffentlicher Verwaltung geführt. Die buzz-words sind Kundenorientiertheit, Effizienz, Geschwindigkeit und Transparenz, sie sind die neuen Merkmale einer real verfügbaren virtuellen bzw. einer virtuell verfügbaren realen Verwaltung.

Der Einsatz neuer Medien ermöglicht es den Behörden, Dienstleistungen, über den traditionellen Weg hinaus, einer breiteren Öffentlichkeit zugänglich zu machen. Besonders das Internet hat zu einem qualitativen Fortschritt in der Kommunikation zwischen Verwaltung und Bürgern beigetragen. Inzwischen wird eine Vielzahl an Informationen im Web angeboten. Allerdings: Viele Menschen verfügen über keinen Online-Zugang zur weiten Welt der offenen Kommunikation.

Die öffentliche Verwaltung – vergleiche etwa *http://www.service-bw.de*, das E-Government-Portal des Landes Baden-Württemberg – geht langsam dazu über, alle Verfahrensschritte, so genannte Transaktionen, vom Antrag oder Auftrag bis zur Erledigung online anzubieten. Formulare brauchen in Zukunft nicht mehr heruntergeladen zu werden, sondern können direkt am Bildschirm ausgefüllt, elektronisch signiert und abgesandt werden. Erledigungen der Verwaltung, Bescheide und sonstige Schriftstücke müssen nicht mehr auf dem Postweg zugestellt werden. Sofern gewünscht, kann die Zustellung elektronisch erfolgen. In Heidelberg gibt es für diese Vorgänge Unterstützung in den dezentral eingerichteten Bürgerämtern.

Die elektronische Abwicklung von Amtswegen bedeutet nicht nur für Bürgerinnen und Bürger Veränderungen. Auch innerhalb der Verwaltung ist eine Reorganisation von Arbeitsabläufen und Kommunikationswegen notwendig. Von den Mitarbeiterinnen und Mitarbeitern in öffentlichen Verwaltungen wird dabei eine hohe Flexibilität im Umgang mit den neuen Technologien verlangt. Hier bilden die Vorschläge der KGSt eine hervorragende Basis. (Die KGSt ist der von Städten, Gemeinden und Kreisen gemeinsam getragene Fachverband für kommunales Management. Er wurde am 1. Juni 1949 in Köln als „Kommunale Gemeinschaftsstelle für Verwaltungsvereinfachung“ gegründet.)

E-Government führt daher nicht nur zu einer Neuorientierung hinsichtlich der Kommunikation zwischen Bürgerinnen, Bürgern und Behörden, die Entwicklung des Internet und neuer Technologien schafft eine Reihe von innovativen Ansätzen für die Teilnahme an demokratischen Entscheidungsprozessen. Insbesondere das Internet bietet die Chance einer stärkeren Beteiligung der Bevölkerung an der Gestaltung unserer Gesellschaft:

- Internet-Chats mit politischen Entscheidungsträgern.

- Bürgerbeteiligungsverfahren können einer breiten Öffentlichkeit zugänglich gemacht werden.

- Öffentliche Diskussionsforen.
- Die Beteiligung an Verfahren bei Gesetzesvorhaben oder kommunalen Planungen wird möglich.
- Auch die Teilnahme an Wahlen ist denkbar.

Bevor aber diese positiven Erwartungen umfassend Realität werden, gibt es die Aufgabe, verschiedene Spannungsfelder aufzuheben. Deshalb werden hier einige Begriffe definiert, Problemlagen angesprochen und der rechtliche wie politische Rahmen kurz dargestellt.

Verschlüsselung und Sicherheitsinteressen

In der aktuellen Diskussion über Kryptographie im Internet stehen sich zwei konträre Sicherheitsinteressen gegenüber. Auf der einen Seite das Interesse des einzelnen Anwenders, seine Daten vor dem Zugriff Dritter zu schützen. Das spricht für Kryptographie. Auf der anderen Seite aber das Interesse der Gesellschaft, kriminellen Missbrauch aufzudecken, und Kriminellen keine Chance zu geben, ihre Aktivitäten geheim zu halten. Das ruft nach einem Kryptographie-Verbot.

Spam

Als Spam werden unerwünschte E-Mails bezeichnet. In der Fachsprache unterscheiden wir „UCE“, für unsolicited commercial email, und „UBE“, unsolicited bulk email. Im täglichen Sprachgebrauch ist das Wort Spam jedoch das Schlagwort schlechthin für alle Arten von Werbe- und anderen unerwünschten Massenmails geworden. Spam gibt es mittlerweile nicht nur in Form von E-Mail sondern auch als Newsletter, Fax und SMS.

So werden im Massenversand unangeforderte Werbe-E-Mails verschickt, es erscheinen Werbebeiträge in Newsgroups, die nichts mit dem Thema der Newsgroup zu tun haben, und es gibt Kettenbriefe mit Sex-Offerten, Medikamentenwerbung oder mit „Dummenfang“, in der man aufgefordert wird, irgendwohin Geld zu überweisen, etwas weiterzusenden etc. Das Wort Spam ist eigentlich der Markenname eines amerikanischen Dosenfleisches (*www.spam.com*). Als die entsprechende Firma wegen Copyright und Geschäftsschädigung gegen die Zweckentfremdung und negative Belegung ihres Produktnamens klagte, war der Begriff schon zu etabliert, um ihn aufzuhalten …

Spionageprogramme

Neben Spam, Viren und Würmern wird auch die Schnüffel-Software zur Plage des Internet-Nutzers. Hunderte Spione sammeln Informationen über unsere Hobbys, Surfgewohnheiten und sammeln fremde Bookmarks. Das Recht des einzelnen Nutzers auf Datenschutz und Diskretion im Internet wird durch oft unbemerkt installierte Hintergrundanwendungen, Plug-Ins und Dateien gefährdet. Schutz davor bieten verschiedene Programme und der sorgfältige Umgang im Netz, die Installation einer Firewall, das Surfen mit alternativen Browsern (z.B. Mozilla, Opera etc.), das Benutzen von alternativen E-Mail Programmen anstatt Outlook Express, oder am besten ein anderes Betriebssystem (z.B. Linux).

Auf der Homepage des Bundesamtes für Sicherheit in der Informationstechnik (BSI), oder direkt unter *www.bsi-fuer-buerger.de* findet man eine gute Übersicht und Informationen zur IT-Sicherheit sowie eine Toolbox mit Programmen zu Viren- und Dialerschutz, Verschlüsselung, Web-Filter, Kinderschutz und Firewall. Dieser Internetauftritt ist eine Weiterentwicklung der CD-ROM „Ins Internet – mit Sicherheit!“, die Bundesinnenminister Otto Schily beim BSI in Auftrag gegeben und auf der CeBIT 2002 vorgestellt hat. Das BSI hat die CD-ROM über 650.000-mal kostenlos an Bürgerinnen und Bürger verteilt.

Übrigens benutzt der deutsche Bundestag Mozilla als Hauptbrowser, das Mailsystem von Mozilla als E-Mail-Programm und Linux auf seinen Servern.

Hacker

Hacker werden Personen genannt, die versuchen, auf illegale Weise über Datennetze in fremde Computersysteme einzudringen. Sie löschen, verändern, ge- oder missbrauchen geschützte Datenbestände oder Programme.

Denial-of-Service-Attacken

Eine Art, ein System außer Dienst zu setzen, ist die Denial-of-Service-, oder kurz DoS-Attacke. Bei DoS-Attacken wird ein Server gezielt mit so vielen Anfragen bombardiert, dass das System die Aufgaben nicht mehr bewältigen kann und im schlimmsten Fall zusammenbricht. Es gibt verschiedene Formen einer DoS-Attacke: Das Syn Flooding, das Ping Flooding, das Mailbombing und natürlich auch kombinierte Attacken, so genannte verteilte Denial-of-Service-Attacken (Distributed Denial of Service [DDoS]).

Beteiligte an diesen Aktivitäten sind zum einen die Verursacher, die Spammer, und auf der anderen Seite die „Opfer“ der Angriffe, die Zielpersonen. Doppelte Opfer sind Administratoren: als Zielpersonen mit besonders hohem Spam-Aufkommen und als Anlaufstelle für Beschwerden. Sie werden bei einem Zusammenbruch des Systems meist als erste – aber oft zu unrecht – verantwortlich gemacht.

Zentrale Spam-Abwehr

Wie die Spamflut unter Kontrolle zu bekommen sei, ist im In- und Ausland unter Experten wie Laien ein viel diskutiertes Thema. Häufige Aussagen gehen in die Richtung: es wird sich doch eine technische Lösung finden lassen… es muss eine technische Lösung geben… wir müssen uns einfach mal mit Fachleuten zusammensetzen… wir leben in einem Hightech-Land… etc.

Tatsächlich ist es juristisch und in der Umsetzung allerdings nicht einfach, gesetzlich gegen Spamming vorzugehen. Die im Moment wohl einfachste und wirkungsvollste Methode für den privaten Nutzer sind die Spamfilter der großen E-Mail-Dienstanbieter (wie gmx, web.de etc.), die alle unbekannten Absender zunächst in extra Ordner sortieren. Im Posteingang landen dann nur Nachrichten von im Adressbuch verzeichneten Kontakten. Der Nachteil dieser Methode ist der hohe Zeitaufwand bis wirklich alle erwünschten Absender gekennzeichnet sind. Des Weiteren ist dies auch nur eine Möglichkeit für private E-Mailkonten. Für Personen und Institutionen, die in der Öffentlichkeit stehen und ständig neue E-Mail-Eingänge von wechselnden Absendern haben, ist diese Methode praktisch nicht realisierbar (z.B. Internationale Organisationen, Unternehmen mit vielen Außenkontakten, aber auch Abgeordnetenbüros).

Die technische Lösung

Das Erkennen von SPAM ist technisch nicht ganz einfach. Eine Methode ist beispielsweise die Analyse des Betreffs. Zeilen wie „Order VIAGRA Now!“ mögen leicht zu erkennen sein. Die Spammer brauchen jedoch nur „Order V1AGRA Now!“ zu schreiben, und für einen Rechner oder ein Programm ist nicht mehr VIAGRA zu lesen, sondern eine Buchstaben-Zahlen-Kombination.

Selbst wenn man diese Zeile dem Programm beibringt, braucht der Spammer den Betreff nur in „Order V°IAGRA Now!“ zu ändern, und das Wort VIAGRA wird vom Programm wieder nicht mehr erkannt. Hier beziehe ich mich auf genauere Betrachtungen in einem unveröffentlichten Aufsatz von Edith Petermann über Spam: „SPAM oder HAM – Informationen und Lösungsansätze zum traurigen Kapitel Müll-Mails“, Edith Petermann, Mai 2003, Universitätsrechenzentrum Mannheim.

Die aktuelle Gesetzeslage macht eine zentrale Abwehr auch deshalb schwierig, weil nach §303 a, StGB, sich „(s)trafbar macht..., wer Daten löscht, unterdrückt, unbrauchbar macht oder verändert“.

Die Verwaltung organisiert sich

Am 1. September 2001 wurde im Rahmen der Neuorganisation des Bundesamtes für Sicherheit in der Informationstechnik das Referat CERT-Bund neu aufgestellt. CERT-Bund steht für „Computer Emergency Response Team für Bundesbehörden".

Ziel von CERT-Bund ist die Bereitstellung einer zentralen Anlaufstelle für präventive und reaktive Maßnahmen in Bezug auf sicherheits- und verfügbarkeitsrelevante Vorfälle in Computer-Systemen.

Zu den Aufgaben von CERT-Bund

- präventive Handlungsempfehlungen zur Schadensvermeidung erstellen und veröffentlichen;
- auf Schwachstellen in Hardware- und Software-Produkten hinweisen;
- Maßnahmen zur Behebung von bekannten Sicherheitslücken vorschlagen;
- bei besonderen Bedrohungslagen, bezogen auf Informationstechnik, warnen bzw. alarmieren;
- reaktive Maßnahmen zur Schadensbegrenzung oder -beseitigung empfehlen.

Die Dienstleistungen von CERT-Bund stehen in erster Linie den Bundesbehörden zur Verfügung und umfassen derzeit,

- eine 24-Stunden-Rufbereitschaft,
- den Betrieb eines Lagezentrums,
- die Analyse von Vorfallsmeldungen,
- die Erstellung daraus abgeleiteter Empfehlungen,
- das Betreiben eines Warn- und Informationsdienstes,
- die aktive Alarmierung der Bundesverwaltung bei akuten Gefährdungen.

BSI-Zertifizierung

Das BSI hat gemäß BSI-Errichtungsgesetz die Aufgabe, für Produkte (Systeme oder Komponenten) der Informationstechnik Sicherheitszertifikate zu erteilen. Die Zertifizierung eines Produktes wird auf Veranlassung des Herstellers oder eines Vertreibers durchgeführt.

Bestandteil des Verfahrens ist die technische Prüfung – Evaluierung – des Produktes gemäß den vom BSI öffentlich bekannt gemachten oder allgemein anerkannten Sicherheitskriterien. Die Prüfung wird in der Regel von einer vom BSI anerkannten Prüfstelle durchgeführt. Diese Anerkennung wird nach Abschluss eines erfolgreich durchlaufenen Akkreditierungsverfahrens ausgesprochen. Jede Evaluierung wird mit dem Ziel, eine einheitliche Vorgehensweise und Methodik sicherzustellen, durch Mitarbeiter der Zertifizierungsstelle begleitet. Die Prüfberichte der Prüfstellen werden von diesen Mitarbeitern der Zertifizierungsstelle abgenommen. Es erfolgt hierbei ein Abgleich der Bewertungen mit denen aus anderen Zertifizierungsverfahren. Das Ergebnis wird in einem Bericht festgehalten. Hierin enthalten sind u. a. das Sicherheitszertifikat als zusammenfassende Bewertung und der detaillierte Zertifizierungsbericht. Er enthält die sicherheitstechnische Beschreibung des zertifizierten Produktes, die Einzelheiten der Bewertung und Hinweise für den Anwender. Die erteilten Zertifikate und Zertifizierungsreporte werden – sofern der Antragsteller dem zustimmt – durch die Zertifizierungsstelle veröffentlicht.

E-Commerce

Zur Regelung des E-Commerce gibt es von der EU eine E-Commerce-Richtlinie. Diese sieht als wichtigste Regelung das Herkunftslandprinzip vor. Das bedeutet, dass Dienstanbieter sich nur an den Gesetzen des Staates, in dem sie niedergelassen sind, orientieren

müssen, auch wenn sie ihre Dienste im Ausland anbieten. Am 21. Dezember 2001 trat das EGG, das Gesetz zum elektronischen Geschäftsverkehr in Kraft. Damit ist das Herkunftslandprinzip auch im deutschen Recht umgesetzt.

Verlässliche Kommunikation

Elektronischer Geschäftsverkehr braucht verlässliche Kommunikation. Es ist wichtig zu wissen, von wem eine Information stammt, d.h. die Authentizität einer Nachricht muss sichergestellt sein. Weiter ist es wichtig zu wissen, dass keine nachträglichen Veränderungen an der Nachricht vorgenommen wurden, das bedeutet, das Prinzip der Integrität muss gewährleistet bleiben; und es muss ersichtlich und verlässlich sein, wann eine Nachricht versendet wurde, d.h. eine zeitliche Fixierung muss mittels Zeitstempels gesichert sein.

Elektronische Signatur: Erste rechtliche Ansätze

Zur Umsetzung einer elektronischen Signatur gibt es bereits erste rechtliche Ansätze: Die maßgeblichen Vorschriften zur Einführung der Elektronischen Signatur wurden im Signaturgesetz (SigG) festgeschrieben und in der Signaturverordnung (SigV) explizit erläutert. Zuständige Behörde für alle Belange des SigG ist die Regulierungsbehörde für Telekommunikation und Post (RegTP).

Weitere rechtliche Schritte stellen das Formanpassungsgesetz sowie eine EU-Richtlinie dar: Das Formanpassungsgesetz regelt die Gültigkeit elektronischer Signaturen im herkömmlichen Rechtsverkehr, indem das Bürgerliche Gesetzbuch an den entsprechenden Stellen angepasst wird.

Einheitliche EU-Richtlinie

Die Kommunikation und der elektronische Geschäftsverkehr innerhalb der EU wurden oft durch unterschiedliche rechtliche Regelungen zur Anerkennung elektronischer Signaturen kompliziert. Um diese Schranken aus dem Weg zu räumen, hat das Europäische Parlament zusammen mit dem Rat der EU am 19. Januar 2000 eine vereinheitlichende Richtlinie veröffentlicht.

Das E-Commerce-Signaturgesetz

Digitale Signaturen, mit denen Dateien vor ihrer Versendung versehen werden, können verschiedene Anforderungen erfüllen. Das Signaturgesetz unterscheidet dabei

- die einfache elektronische Signatur
- die fortgeschrittene elektronische Signatur
- die qualifizierte elektronische Signatur

Während eine einfache elektronische Signatur nur der Authentifizierung, also der Bestimmung des Absenders, dient, garantiert die fortgeschrittene elektronische Signatur auch die Integrität – Unverfälschtheit – einer Mitteilung. Sie unterscheidet sich nach § 2 Ziff. 2 SigG von der einfachen elektronischen Signatur dadurch,

- dass sie ausschließlich dem Signaturschlüsselinhaber zugeordnet ist
- dass sie die Identifizierung des Signaturschlüsselinhabers ermöglicht
- dass sie mit Mitteln erzeugt wird, die der Signaturschlüsselinhaber unter seiner alleinigen Kontrolle halten kann
- dass sie mit den Daten, auf die sie sich bezieht, so verknüpft wird, dass eine nachträgliche Veränderung der Daten erkannt werden kann

Die qualifizierte elektronische Signatur schließlich entspricht einer fortgeschrittenen elektronischen Signatur, sichert also ebenfalls Authentizität und Integrität der mit ihr verknüpften Daten, bietet aber ein qualitativ höheres Maß an Sicherheit. Die qualifizierte elektronische Signatur beruht auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat.

Die EU-Richtlinie zum Datenschutz

Die EU-Richtlinie 2002/58/EG zum Datenschutz in der elektronischen Kommunikation sieht zwingend eine vorhergehende Einwilligung der Nutzerinnen und Nutzer vor, bevor Werbe-E-Mails und Werbefaxe zugestellt werden dürfen, die „Opt-In-Lösung“, die USA sind dagegen auf eine „Opt-out-Regelung“ orientiert: das bedeutet, dass an jeden, der sich nicht ausdrücklich dagegen ausspricht, jede Menge Spam geschickt werden darf.

Das Urheberrecht

Am 10. September 2003 trat das Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft in Kraft. Im Spannungsfeld der unterschiedlichen Interessen von Verlagen auf der einen, Bildungseinrichtungen und Pädagogen auf der anderen Seite wurde nun in § 52a geregelt, dass es zulässig ist, veröffentlichte kleine Teile eines Werkes, Werke geringen Umfangs sowie einzelne Beiträge aus Zeitungen oder Zeitschriften zur Veranschaulichung im Unterricht an Schulen, Hochschulen ... für einen begrenzten Kreis – etwa begrenzt auf das jeweilige Intranet – öffentlich zugänglich zu machen.

Das Strafgesetzbuch

Es folgen die für unser Thema zentralen Paragraphen des StGB.

§ 202a – Ausspähen von Daten

(1) Wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden

§ 263a – Computerbetrug

(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, dass er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflusst, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

§ 265a – Erschleichen von Leistungen

(1) Wer die Leistung eines Automaten oder eines öffentlichen Zwecken dienenden Telekommunikationsnetzes, die Beförderung durch ein Verkehrsmittel oder den Zutritt zu einer Veranstaltung oder einer Einrichtung in der Absicht erschleicht, das Entgelt nicht zu entrichten, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

§ 303a – Datenveränderung

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

§ 303b – Computersabotage

(1) Wer eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dadurch stört, dass er ...eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

Das Gesetz gegen den unlauteren Wettbewerb

Beim UWG ist der Paragraph 17 zentral.

§ 17 – Verrat von Geschäfts- oder Betriebsgeheimnissen

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer als Angestellter, Arbeiter oder Lehrling eines Geschäftsbetriebs ein Geschäfts- oder Betriebsgeheimnis, das ihm vermöge des Dienstverhältnisses anvertraut worden oder zugänglich geworden ist, während der Geltungsdauer des Dienstverhältnisses unbefugt an jemand zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Geschäftsbetriebs Schaden zuzufügen, mitteilt.

(2) Ebenso wird bestraft, wer zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Geschäftsbetriebs Schaden zuzufügen,

1. sich ein Geschäfts- oder Betriebsgeheimnis durch

a) Anwendung technischer Mittel,

b) Herstellung einer verkörperten Wiedergabe des Geheimnisses oder

c) Wegnahme einer Sache, in der das Geheimnis verkörpert ist, unbefugt verschafft oder sichert oder

2. ein Geschäfts- oder Betriebsgeheimnis, das er durch eine der in Absatz 1 bezeichneten Mitteilungen oder durch eine eigene oder fremde Handlung nach Nummer 1 erlangt oder sich sonst unbefugt verschafft oder gesichert hat, unbefugt verwertet oder jemandem mitteilt.

Anmerkung der Redaktion: Der zweite Teil des Beitrags von Lothar Binding wird in den BenutzerNachrichten 2004-4 veröffentlicht. Er ist dem Schwerpunkt „Mehrwertdiensterufnummern“ gewidmet.