Innenausschuss
A-Drs. 16(4)570 E

Stellungnahme zum Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes

Die Bundesregierung befindet sich mitten in der Umsetzung einer Gesamtstrategie für die informationstechnische Infrastruktur dieses Landes. Sie ist geprägt von Begriffen wie Deutschland Online, iD2010 oder e-Government 2.0. Das Bundesministerium des Innern ist personell, organisatorisch und politisch federführend in der Umsetzung dieser Strategie. Das Bundesamt für Sicherheit in der Informationstechnik soll in Zukunft Verantwortung übernehmen für einen Eckpfeiler der neuen IT-Strategie, nämlich die Sicherheit in der Informationstechnik und soll dafür die - aus Sicht der Bundesregierung - notwendigen, wesentlich erweiterten Befugnisse erhalten.

Die vorliegende Stellungnahme zum Gesetzentwurf der Bundesregierung befasst sich mit folgenden Aspekten dieses Gesetzentwurfs:

1) das "System" BMI - Umsetzung der IT-Strategie der Bundesregierung und damit verbundener Projekte und die Stellung sowie neuen Aufgaben des Bundesamt für Sicherheit in der Informationstechnik (BSI) in diesem Kontext,

2) die Darstellung des Risikos als Begründung für die Notwendigkeit des neuen Gesetzes,

3) die Erhebung und Auswertung von Protokolldaten entsprechend Par. 5 des Gesetzentwurfs,

3) die Marktmacht des BSI nach den Vorgaben dieses Gesetzentwurfs - Par. 8 und folgende

Sofern zu anderen Vorschlägen des Gesetzentwurfs keine Anmerkungen gemacht sind, ist dies zunächst der Zeitknappheit bei der Erarbeitung dieser schriftlichen Stellungnahme geschuldet und sollte nicht gleichgesetzt werden mit kommentarloser Zustimmung zu den nicht kommentierten Passus.

1 Das "System BMI", Stellung und neue Aufgaben des BSI in diesem Kontext

Das Bundesministerium des Innern (im Folgenden nur noch "BMI") versteht sich selbst als "IT-Ministerium", "e-Government-Ministerium", "Organisationsministerium" und als verantwortlich für die Sicherheit der Informationstechnik [1609]. So formulierte es jedenfalls der Staatssekretär im BMI, Dr. Bernhard Beus, der neben seiner Haupttätigkeit im Ministerium auch noch die Funktion des "IT-Beauftragten der Bundesregierung" ("Bundes-CIO") wahrnimmt.

1.1 Aktuelle strategische IT-Vorhaben der Bundesregierung

Und es ist in der Tat beachtlich, welche Aktivitäten das BMI im Zusammenhang mit Informations- und Kommunikationstechniken in dieser Legislaturperiode bereits ergriffen hat und welche Ergebnisse dabei erzielt wurden. Zu letzteren sind auch Gesetzgebungsvorhaben zu zählen, wie die Vorratsdatenspeicherung, das ATD/GDG-Gesetz und insbesondere natürlich das BKA-Gesetz.

Die strategischen Vorhaben bezüglich der Informations- und Kommunikationstechnik wurde, modern in der Sprache und up-to-date in den Methoden, in Pakete mit wohlklingendem Namen verpackt, wie

- Deutschland Online
- e-Government 2.0
- iD2010 - Informationsgesellschaft Deutschland 2010
- Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI)
- e-Identity oder
- eHealth

Die wichtigsten, *erklärten* Absichten hinter diesen Vorhaben sind

- der zügige Aufbau einer sicheren Kommunikationsinfrastruktur für die Verwaltungen auf Bundes-, Länder- und kommunaler Ebene,
- die elektronische Zusammenarbeit von Behörden auf allen Ebenen und weitestgehend elektronischer Datenaustausch auf der Basis einheitlicher, verbindlicher Standards,
- die Steigerung der *"digitalen Integration"*, durch weitgehend elektronische Kommunikation und Prozessabwicklung zwischen Verwaltungen, Bürgern und Unternehmen.

Die Bundesregierung hat ihre Absicht zum Ausdruck gebracht, auf diesen Gebieten *"vermehrt gestalterische Funktionen"* zu übernehmen, ähnlich wie man dies zuvor in der Daseinsvorsorge oder Gesundheitsbetreuung getan habe und ihre diesbezüglichen Ziele formuliert wie folgt:

- *"Die Kommunikationswege sind verlässlich. Informationen und Daten können sicher über die elektronischen Wege transportiert werden.*
- *Jeder Teilnehmer (an e-Government-Prozessen / d. Verf.) verfügt über eine eindeutige Identität im Netz und eine Mailadresse, die es ermöglicht, Daten und Informationen verbindlich zu empfangen bzw. zuzustellen.*
- *Die Verwaltung ist umfassend und uneingeschränkt elektronisch erreichbar.*
- *Wirtschaft und Verwaltung arbeiten durchgängig elektronisch zusammen.*[1]

Das Bundesministerium des Innern ist mit der Umsetzung dieser Strategie beauftragt. Diese hat längst begonnen:

1.1.1 Identifizierung, die "e-identity-Strategie"

Bei der so genannten 'e-Identity-Strategie" geht es darum, den für sich selbst oder eine juristische Person Handelnden eindeutig zu identifizieren. Dies ist insofern ein echtes Problem in der Informationstechnik, als Datenbanken lediglich mit "virtuellen Abbildern" von Personen umgehen. Sie speichern Daten über Personen, wie die Namensangaben und Geburtsdaten, ggf. beschreibende Merkmale usw.

Doch kann man nie sicher sein, dass sich ein bestimmtes Personen-Abbild in einer Datenbank - korrekt - auf eine ganz bestimmte Person bezieht. Da gibt es reihenweise Doubletten in den Datenbanken, die zwar "eigentlich" auf ein- und dieselbe Person gemünzt sind, was die Technik aber nicht erkennen kann, da einzelne Daten (wie z.B. der Familienname Meier, Meyer, Mayer) unterschiedlich geschrieben sind. Ebenfalls nicht selten gibt es den umgekehrten Fall, dass nämlich ein Datensatz nicht vollständig genug ist, sodass er sich auf mehr als eine Person in der Wirklichkeit beziehen kann (z.B. Martin Schulze, geb. 13.05.1943), was wenig erwünscht ist, wenn dann der falsche Martin Schulze einer polizeilichen Maßnahme anheim fällt.

Hier hat der Wunsch nach Identifizierung seine eigentlichen Wurzeln: Nur wenn jede Person eindeutig identifiziert ist (z.B. durch biometrische Angaben), diese ebenfalls in den Datenbanken gespeichert werden ***UND*** gewährleistet ist, dass die Zuordnung eines bestimmten Datensatzes (z.B. in einem Bundesmelderegister) sich *eineindeutig* auf eine bestimmte Person bezieht, wäre das o. g. Problem gelöst.

Die Bundesregierung - federführend das BMI - ist mit Hochdruck dabei, ihre umfassende e-Identity-Strategie in die Tat umzusetzen. Es gehören dazu

- der neue, elektronisch lesbare Personalausweis
- der bereits eingeführte, maschinenlesbare Reisepass
- die elektronische Gesundheitskarte,
- der elektronische Einkommensnachweis, sowie eine
- qualifizierte elektronische Signatur

Gemeinsam ist den **e-Cards**, dass sie neben den üblichen, von Menschen lesbaren Angaben auch einen Chip aufweisen, aus dem Informationen elektronisch ausgelesen werden können. Das eCard-Konzept sieht vor, dass sich ein Ausweisinhaber einmal bei einer vertrauenswürdigen Stelle als der identifiziert, der er zu sein vorgibt und dass ihm dann - nach Überprüfung seiner Identität - ein Ausweisdokument ausgestellt wird, das diese Identität bestätigt.

Für rund 40 Millionen Arbeitnehmer wird der **elektronische Einkommensnachweis (ELENA)** eingeführt, für die Millionen von gesetzlich Krankenversicherten kommt zusätzlich die **elektronische Gesundheitskarte (eKG).** Seit November 2007 dient der **ePass** Millionen von Inhabern als maschinen-lesbares Reisedokument, seine informationstechnischen Merkmale entsprechen international einheitlichen Standards, er kann also überall elektronisch gelesen werden, wo entsprechende Lesegeräte vorhanden sind. Neben Personalien und beschreibenden Angaben über Körpergröße und Augenfarbe enthält der ePass eine (biometrisch auswertbare) Gesichtsfotografie, sowie zwei Fingerabdrücke, die auch auf dem Chip gespeichert sind. Ab 1. November 2010 soll der **neue, elektronische Personalausweis(ePA)** den bisherigen Personalausweis ablösen. Neben ähnlichen Funktionen als Reisedokument, wie sie der ePass aufweist, soll der ePA verpflichtend auch einen elektronisch lesbaren Nachweis der Identität seines rechtmäßigen Inhabers aufweisen. Diese Funktionalität erhält in der weiteren e-Government-Strategie der Bundesregierung eine Schlüsselrolle, als in der Kommunikation und im Rechtsverkehr über das Internet zunehmend der neue Personalausweis eingesetzt werden soll, um sich gegenüber dem Kommunikationspartner "elektronisch" zu identifizieren. Auf freiwilliger Basis soll der EPA ferner eine qualifizierte elektronische Signatur einhalten, mit der elektronisch rechtsverbindliche und mit dem Signaturgesetz konforme elektronische Unterschriften möglich werden.

Diese qualifizierte elektronische Signatur (QES) dient dazu, nur elektronisch vollzogene Rechtshandlungen in gleicher Weise rechtssicher zu bestätigen, wie dies bisher durch eine Unterschrift geschehen ist. Ein auf diese Weise signiertes elektronisches Dokument kann die notwendige Schriftform bei Rechtsgeschäften ersetzen. Sie werden beispielsweise nach dem Umsatzsteuergesetz als "Unterschrift" auf elektronischen Rechnungen verlangt und sollen in Kürze auch notwendig werden für die Abgabe z.B. einer Umsatzsteuervoranmeldung im ELSTER-Verfahren. Wer einen entsprechenden Signatur(schlüssel) benötigt, muss sich bei einem entsprechend akkreditierten und bei der Bundesnetzagentur registrierten Zertifizierungsdienst anmelden. Der Schlüssel wird verge-

ben, nachdem die Identität des Antragssteller von der ausgebenden Stelle überprüft wurde, um die bei der "elektronische Unterschrift" verwendete Identität der Rechtsperson sicher feststellen zu können.

Die beschriebenen Maßnahmen der Identitätsfeststellung und -Zertifizierung erfordern es, dass Diensteanbieter, Geräte und Verfahren sich in Übereinstimmung mit vorgegebenen (Sicherheits-)Anforderungen befinden. Diese Prüfung und Bewertung, Zertifizierung und Akkreditierung ist eine der wesentlichen, neuen Aufgaben des Bundesamts für Sicherheit in der Informationstechnik.

1.1.2 Registrierung

Seit dem 1. September 2006 ist die ausschließliche Gesetzgebungskompetenz für das Meldewesen auf den Bund übergegangen. Ein Projekt von höchster Priorität im Rahmen des Aktionsplans "Deutschland Online" ist der Aufbau eines **Bundesmelderegisters** bis zum Jahr 2010. Aus den dort erhobenen Daten wird sich Deutschland ferner am **europaweiten Zensus 2010** beteiligen, womit "*direkte Auskunftspflichten für Bürgerinnen und Bürger entfallen*".[2]

1.1.3 Datenaustausch und Interoperabilität

Auch "Datenaustausch" ist ein Wort, das sich leicht spricht, jedoch auf immense praktische Probleme stößt. Deren Ursachen liegen nicht nur in der oben beschriebenen Mehrdeutigkeit zwischen "Datenbankabbild" und natürlicher Person. Vor allem ist die historische Entwicklung daran schuld: Denn es haben sich in den letzten 40 Jahren tausende von Datenbanksystemen in den Verwaltungen dieses Landes entwickelt, die sich schlicht nicht verstehen. Der Grund liegt darin, dass diese Datenbanken unterschiedliche Datenbankstrukturen verwenden, d.h. intern jeweils anders "eingerichtet" sind.

Man stelle sich pro Datenbank eine große Lagerhalle vor mit Hochregallagern und Fächern darin. Jedes Regal ist für Informationen einer bestimmten Art (z.B. Personen, Firmen, Adressen) zuständig. Jedes Fach in einem Regal ist zuständig zur Aufnahme eines bestimmten Merkmals (Familienname, Vorname, Geburtsdatum usw.). Jede der vielen Datenbanken in den Verwaltungen entspricht einer anderen Lagerhalle und ist innen anders eingerichtet. Daher ist es nicht möglich, Daten automatisch von Datenbank zu Datenbank zu schicken und zu erwarten, dass das Zielsystem weiß, was es damit soll.

Das Problem ist längst erkannt. Seit Jahren arbeitet man in den deutschen Verwaltungen bereits an so genannten "Datenaustauschstandards". Mit denen werden Datenaustauschprogramme "gefüttert", die dann dafür sorgen, dass die Daten von einer Datenbank A "übersetzt" werden in die Struktur, die die Datenbank B erwartet. Sehr vereinfacht ausgedrückt. Wer sich besser vorstellen möchte, welche Mammutaufgabe dies darstellt, möge sich für "XÖV" bei Google interessieren. Damit sichergestellt werden kann, dass die Daten aus einer Datenbank A sich auf die gleiche Person (z.B. Hans Mustermann) beziehen, wie in einer Datenbank B, möchte die Bundesregierung eine *"verlässliche, einheitliche, elektronische Identifizierung"*[1] einführen, faktisch also ein eindeutiges, elektronisch auswertbares Personenkennzeichen.

Inzwischen hat man festgestellt, dass zur "Verständigung" zwischen unterschiedlichen Partnern im e-Government, auf Verwaltungsebene oder im Law Enforcement, mehr gehört als nur Datenaustauschstandards. Das neue Schlagwort für den umfassenden Ansatz lautet "Interoperabilität" und soll auch die Geschäftsprozesse aufeinander abstimmen und zu einer Vereinbarung von gemeinsamen Standards führen. Es ist dies ein Thema, das derzeit auch in der deutschen Polizeilandschaft herausragende Aufmerksamkeit genießt, nicht zuletzt auch wegen den gewachsenen Anforderungen an Datenaustausch zwischen Polizeibehörden in Deutschland und über die Bundesgrenzen hinaus.

1.1.4 Ein einheitliches Kommunikationsnetz für die Deutsche Verwaltung

Im Rahmen des Vorhabens "Deutschland Online Infrastruktur" wurde im 2. Halbjahr 2006 eine Bestandsaufnahme durchgeführt über die bestehenden Behörden-Kommunikationsnetze. Schwerpunkt der Untersuchung waren die vorhandenen Flächennetze auf Bundes-, Länder- und Kommunenebene, sowie die Anforderungen von Fachverfahren an die Netzinfrastrukturen. Wesentliches Ergebnis der Untersuchung war die Feststellung, dass es an einer übergreifenden, nationalen Kommunikationsinfrastruktur fehlt. Nach Aufbau der notwendigen Betreiberstruktur DOI-Netz e.V., dem der Bund, vertreten durch das BMI und alle 16 Länder angehören, wurde Anfang März 2009 an T-Systems der Auftrag vergeben für den Aufbau des DOI-Netzes, also des "gemeinsamen Netzes der deutschen Verwaltung", in das bis September 2009 100 Teilnehmermetze migriert sein sollen.[3] Das Vorgängernetz TESTA wird dadurch abgelöst.

1.1.5 Bürgerportal und De-Mail

Mit besonderem Nachdruck betreibt die Bundesregierung im Rahmen ihrer E-Government-Strategie die Einführung von so genannten Bürgerportalen und De-Mail.[4] Bei den Bürgerportalen soll es sich um einen Verbund von staatlich zertifizierten, privat oder staatlich betriebenen Kommunikationsplattformen handeln, mit deren Hilfe das Versenden und Empfangen von nachrichten und Dokumenten im Internet so einfach, sicher und verbindlich gestaltet werden kann, wie dies heute im Briefverkehr mit der traditionellen Post der Fall ist. Die zertifizierten Provider von Bürgerportalen werden - nach einer sicheren Erstregistrierung - für natürliche und juristische Personen Email-Adressen zur Verfügung stellen. "

> *"Mit Hilfe der Bürger-Portale können Bürgerinnen und Bürger elektronische Nachrichten einfach mit anderen Bürgerinnen und Bürgern, mit der Wirtschaft und Verwaltung auf unterschiedlichen Kanälen, in verschiedenen Formaten und auf klar definierten Sicherheitsstufen austauschen. Nachrichten werden vertraulich und nicht anonym übertragen und (falls erforderlich qualifiziert) signiert. Die Adressierbarkeit der Bürgerinnen und Bürger im elektronischen Raum wird durch eine eindeutige elektronische Adresse gewährleistet, die – analog zur physikalischen Meldeadresse – auch auf dem elektronischen Personalausweis festgehalten werden kann. Auch juristische Personen können sich Organisationspostfächer auf Bürger-Portalen einrichten. An diese können Bescheide und andere elektronische Dokumente sicher und verbindlich zugestellt werden*[5]

Das BSI ist bei der konzeptionellen Gestaltung maßgeblich beteiligt.

1.2 Aufgaben und Ausstattung des BMI

Das BMI ist federführend für die Umsetzung der e-Government-Strategie der Bundesregierung und der verwandten, o.g. strategischen Vorhaben. Die für die fachgerechte Umsetzung dieser Aufgaben notwendige personelle und fachliche Kapazität wurde teilweise im BMI, teilweise auch in nachgeordneten Behörden und Einrichtungen aufgebaut.

Im Ministerium selbst arbeitet eine IT-Abteilung unter Leitung des IT-Direktors. Dessen Stellvertreter ist gleichzeitig auch stellvertretender Leiter des Bundesamts für Sicherheit in der Informationstechnik. Der Staatssekretär im BMI, Dr. Bernhard Beus, ist, wie von Fachverbänden beklagt wurde, "nebenberuflicher" "IT-Beauftragter der Bundesregierung", umgangssprachlich auch "Bundes-CIO" (CIO = Chief Informations Officer) genannt, ferner Mitglied in der IT-Steuerungsgruppe des Bundes, sowie Vorsitzender des Rates der IT-Beauftragten des Bundes. Und sowohl im Vorstand, als auch in der Geschäftsführung des Vereins DOI-Netz e.V., der für Aufbau und Vertrieb des neuen Verwaltungsnetzes zuständig ist, finden sich Angehörige des Bundesministeriums des Innern.

Dem BMI unterstellt sind zahlreiche Behörden und Einrichtungen, von denen für den vorliegenden Themenkosmos relevant ist,

- **der Cluster der Polizei- und Sicherheitsbehörden:** Das BMI ist vorgesetzte Behörde für die Bundespolizei mit ihren +40.000 Mitarbeitern, für das Bundeskriminalamt mit rund 5.500 Mitarbeitern und das Bundesamt für Verfassungsschutz. Im Rahmen des vorliegenden Gesetzentwurfs soll das BSI die

Aufgabe erhalten, die Polizeien und Strafverfolgungsbehörden, sowie den Bundesnachrichtendienst bei der Wahrnehmung ihrer jeweiligen gesetzlichen Aufgaben zu unterstützen.

- **Der Cluster der IT-relevanten Behörden und Einrichtungen**, zu denen das Beschaffungsamt des BMI zählen, das jährlich Aufträge im Volumen von rund 3 Milliarden Euro vergibt, ferner der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, das Bundesamt für die Sicherheit in der Informationstechnik sowie die Bundesstelle für Informationstechnik (BIT) im BVA. Letztere verwaltet zusätzlich einen jüngst ergebenen Rahmenauftrag über 75.000 Personentage an Beratungs- und Unterstützungsleistung durch fünf Anbieterkonsortien (Quelle).
- Nicht zuletzt, der **Cluster der für die Infrastruktur der Kommunikationsnetze** des Bundes zuständigen Einrichtungen, nämlich die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS), sowie der bereits erwähnte, vor kurzem gegründete jüngst gegründete DOI-Netz e.V.

1.3 Die neuen Aufgaben des BSI

Eingangs ist festzustellen, was der Gesetzentwurf gerade **nicht** enthält: Enttäuscht wird nämlich die Erwartung des Rezipienten, Bürgers und Politikers, der sich das BSI als die zuständige Zentralstelle des Bundes für die ***Informationssicherheit*** vorgestellt haben mag. Das BSI selbst definiert in einem seiner grundlegenden Standards[6]

> *"**Informationssicherheit** hat als Ziel den Schutz von Informationen jeglicher Art und Herkunft. Dabei können Informationen sowohl auf Papier, in Rechnersystemen oder auch in den Köpfen der Nutzer gespeichert ein. IT-Sicherheit beschäftigt sich an erster Stelle mit dem Schutz elektronischer gespeicherter Informationen und deren Verarbeitung… Die Sicherheit von Informationen wird nicht nur durch vorsätzliche Handlungen bedroht (z.B. Computer-Viren, Abhören der Kommunikation, Diebstahl von Rechnern. …"*
> *… Die Unterscheidung, ob Informationen mit Informationstechnik, mit Kommunikationstechnik oder auf Papier verarbeitet werden, [ist] nicht mehr zeitgemäß. Der Begriff **Informationssicherheit** statt IT-Sicherheit ist daher umfassender und besser geeignet". ."*

Demgegenüber beschränkt sich der Gesetzentwurf nur noch auf einen Teilaspekt der Informationssicherheit, nämlich den der ***Sicherheit in der Informationstechnik***, der in Par. 2, Ziff. 2 definiert wird wie folgt:

> *"**Sicherheit in der Informationstechnik** im Sinne dieses Gesetzes bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen*
> *1. in informationstechnischen Systemen, Komponenten oder Prozessen oder*
> *2. bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen. "*

Das Gesetz lässt offen, in wessen Verantwortungsbereich in Zukunft der Schutz der Informationssicherheit in Bundesbehörden gestellt wird, die nach den Ausführungen im o.g. Standard auch bedroht ist durch

- höhere Gewalt, aufgrund derer Datenträger oder IT-Systeme in Mitleidenschaft gezogen werden, sodass Daten und Dokumenten, IT-Systeme oder Dienste nicht mehr wie gewünscht zur Verfügung stehen.
- missglückten Software-Update, aufgrund dessen Anwendungen nicht mehr funktionieren oder Daten unbemerkt verändert wurden oder
- vertrauliche Informationen versehentlich von einem Mitarbeiter an Unbefugte weitergegeben werden, weil Dokumente nicht als vertraulich gekennzeichnet wurden oder Daten nicht ausreichend vor unberechtigtem Zugriff geschützt wurden.

Es mag sein, dass diese Aufgaben, sowie die damit verbundene Beratungs-, Unterstützungs- und Standardisierungsleistung weiterhin vom BSI erbracht wird. Zu hinterfragen ist allerdings, warum dies in der Neufassung des Gesetzes dann nicht auch ausdrücklich erwähnt wurde.

Folgt man den - teils bemerkenswert dramatisierenden - Darstellungen im Gesetzentwurf, so können Energie- und Wasserversorgung zusammenbrechen, öffentliche Verkehrsmittel zum Stillstand kommen und der bargeldlose Zahlungsverkehr zum Erliegen, wenn IKT-Strukturen ausfallen. Auf den tatsächlichen Zusammenhang solcher Ereignisse **mit der Informations- und Kommunikationsinfrastruktur von Bundesbehörden** wird im weiteren Verlauf des Gesetzentwurfes jedoch nicht weiter eingegangen. Diese Risiken sollen hier nicht verharmlost werden. Ganz im Gegenteil wäre eine zentrale, vertrauenswürdige, technisch-kompetente, neutrale Instanz wünschenswert, die die Sicherheit von Anwendungen im Internet beobachtet, zeitnah Warnungen für Bürger, Unternehmen und andere Verwaltungen herausgibt und Beratung und

Unterstützung anbietet.

Faktisch ist dem BSI hier auch wenig vorzuwerfen:

- Es unterhält unter der Bezeichnung 'BSI-fuer-Buerger' ein umfassendes Informations- und Beratungsangebot im Internet,
- und bietet mit dem 'Bürger-CERT' einen Warn- und Informationsdienst, um Bürger und kleine Unternehmen "schnell und kompetent, kostenfrei und absolut neutral", von Viren, Würmern und Sicherheitslücken in Computeranwendungen in Kenntnis zu setzen.

Umso bedauerlicher ist es, dass Warnungen gegenüber der Öffentlichkeit im Par. 7 des vorliegenden Gesetzentwurfes lediglich als "Kann-Bestimmung" ausgelegt sind, und es ausdrücklich in das Ermessen des BSI gestellt wird, dass "entdeckte Sicherheitslücken oder Schadprogramme, nicht allgemein bekannt werden" sollen.

Es verstärkt diese Tatsache den generell vorhandenen Eindruck, dass Risikoszenarien aus dem Leben des Normalbürgers bzw. der Infrastruktur zur Begründung für die Notwendigkeit bestimmter, im Gesetzentwurf vorgesehener Maßnahmen zwar herangezogen werden, dass aber im Übrigen nicht auch ausgewogen Informationssicherheit und Sicherheit der Informationstechnik des Bürgers und Unternehmens berücksichtigt ist, sondern - noch dazu nur äußerst sparsam offen gelegte - Interessen und Absichten des BSI bzw. BMI den Gesetzentwurf dominieren.

Hinzu kommt, dass die Definitionen für Sicherheit bzw. angeführten Beispiele von Risiken, sowie die Aufgabe, Befugnisse und Maßnahmen für das BSI sehr einseitig orientiert scheinen an allem, was mit Internet zu tun hat. ***Zur IT-Sicherheit, wie auch der oben bereits angeführten Informationssicherheit gehört jedoch wesentlich mehr. Es ist bedauerlich, dass diese Aspekte im Gesetzentwurf nicht angemessen berücksichtigt sind bzw. zu hinterfragen, warum dies so ist.***

Im Übrigen bleibt im Gesetzestext selbst diffus und unkonkret, welche Aufgaben und Befugnisse das BSI in Zukunft wahrzunehmen hat. Mehr Klarheit darüber bringt erst die zeitaufwändige Untersuchung der diversen strategischen Maßnahmen der Bundesregierung zur Umsetzung von eGovernment 2.0 bzw. Deutschland Online, in Umsetzung begriffene Projekte, wie der elektronische Identitätsnachweis und die elektronische Signatur, sowie aktuelle Gesetzesvorhaben in diesem Kontext unter denen besonders der am 08.04.2009 im Deutschen Bundestag eingebrachte Entwurf eines Gesetzes zur Regelung von Bürgerportalen zu beachten ist.

Deutlich wird die Absicht, das BSI unter Berufung auf Sicherheitserfordernisse zur zentralen Instanz im Kosmos des BMI zu machen, die zuständig ist für

- **Die Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes,**
- die Sammlung und Auswertung von Informationen über Sicherheitsrisiken …,
- die Forschung im Bereich der gesetzlichen Aufgaben des Amtes,
- die Herstellung von Schlüsseldaten und Betrieb von Krypto- und Sicherheitsmanagementsystemen …,
- **die Entwicklung von so genannten IT-Sicherheitsprodukten und Bereitstellung für Stellen des Bundes_bis hin zur zentralen und verpflichtenden Versorgung von Stellen des Bundes mit solchen Produkten,** sowie die
- **Prüfung und Bewertung, sowie Zertifizierung von IT-Komponenten, sowie der Akkreditierung von Anbieterfirmen und deren Personal.**

Die drei, in der obigen Aufstellung hervorgehobenen Bereiche sind im Folgenden eingehender betrachtet.

Davor jedoch ist eine kurze Diskussion über die im Gesetzentwurf dargestellten Risiken erforderlich, da sie die Notwendigkeit zur aktuellen Umsetzung dieser Gesetzesvorschlages maßgeblich begründen:

2 Risikodarstellung im Gesetzentwurf

Obwohl an mehreren Stellen Anläufe genommen werden, lässt der Gesetzentwurf eine ernsthafte und plausible, sowie konkrete Erklärung der Gefahren und Risiken, die man abzuwehren gedenkt, vermissen.

Ein erster Ansatz findet sich bereits in der Einleitung, Ziff. 1 - Problem und Ziel: Die dort erwähnten Gefährdungen betreffen Energie- oder Wasserversorger, Verkehrsunternehmen, bargeldloser Zahlungsverkehr im

Einzelhandel oder bei der Auszahlung von Renten genannt. Es folgt die recht dramatische Darstellung von Unfällen mit "unmittelbaren Auswirkungen auf Leben und Gesundheit vieler Menschen" die auf Angriffe auf IKT-Strukturen zurückgehen.

Diese Begründungen mögen zutreffen im Bereich des Schutzes kritischer Infrastrukturen (KRITIS), eines ebenfalls vom BMI betreuten Projektes. Im Übrigen wird die Möglichkeit des Zutreffens dieser Behauptung hier gar nicht bezweifelt, wohl aber darauf hingewiesen, dass dies alles **für die Informationsverarbeitung bzw. Kommunikation zwischen Bürgern, Unternehmen und Bundesbehörden** nicht zutreffend ist. Insofern muss die Frage erlaubt sein, was mit dieser dramatischen Überhöhung eigentlich bezweckt wird.

Weiter heißt es dann im gleichen Abschnitt, dass "*die zunehmende Vernetzung sehr inhomogener IT-Systeme*" es erschwere, einheitliche Sicherheitsstandards einzuführen. Diese Behauptung ist, mit Verlaub, in keiner Weise nachvollziehbar, sollten doch Sicherheitsstandards gerade völlig unabhängig sein von den beschafften Systemen bzw. sollten nur solche Systeme beschafft sein, die den minimalen Sicherheitserfordernissen entsprechen. Konkrete Belege für diese Behauptung könnten zu mehr Verständnis beitragen. Ansonsten wäre sie zu streichen.

Fortgeführt wird mit der Behauptung, dass "*Schwachstellen an einer Stelle ein Eindringen in die IT-Systeme einer Vielzahl von Behörden ermöglichen*". Diese Behauptung unterstellt, dass schon heute die Behörden untereinander völlig schutzlos miteinander kommunizieren, was sicher nicht den Tatsachen entspricht.

Die abschließende Bemerkung, dass "*dieser Gefahr nur durch die Festlegung einheitlicher und strenger Sicherheitsstandard durch eine zentrale Stelle begegnet werden kann*" ist unstrittig, unterschlägt jedoch, dass das BSI diese Aufgabe(n) bereits seit 1991 durchaus erfolgreich wahrnimmt, sodass sich die Frage nach der Neuigkeit dieser Aussage ebenso stellt, wie nach der Notwendigkeit von Veränderungen in diesem Bereich.

In mehreren anderen Unterlagen von Bundesregierung, BMI bzw. BSI werden Gefahren aus dem Internet in sehr dramatischer Weise dargestellt, z.B. *"Trotz vielfältiger Anstrengungen ist die Kommunikation über das Internet heute gefährlicher denn je. Spam-, Wurm- und Phishing-Mails überfluten die E-Mail-Postfächer" Einfach und kostengünstig anzuwendende Identifizierungs- und Absicherungsverfahren fehlen ..."*[7] Gerne würde man zu solchen Behauptungen harte Fakten finden.

Die **öffentlich verfügbare PKS-Statistik des Bundeskriminalamts**, leider in der jüngsten aktuellen Version nur verfügbar für das Berichtsjahr 2007, weist für die Computerkriminalität Fallzahlen von insgesamt 62.944 erfassten Fällen aus, was einem Anstieg gegenüber dem Vorjahr um 6,4% entspricht. Davon beziehen sich rund 25.000 Fälle mit rechtswidrig erlangten Debitkarten mit PIN, also das Ausspähen privater Bankdaten[8]. Dies geschieht, wie man aus anderer Quelle weiß, jedoch hauptsächlich durch manipulierte Geldautomaten, nicht jedoch im Internet. ***Diese Statistik ist also wenig geeignet, die von der Bundesregierung konstatierte, dramatische Entwicklung zu untermauern. Es fällt das Missverhältnis auf zwischen der tatsächlicher Internet-Nutzung - d.h. hunderten von Millionen von gesendeten / empfangenen Emails pro Jahr und einer noch viel größeren Zahl von "angeklickten Links" und den genannten Fallzahlen.*** Dass also so erfreulich wenig tatsächlich passiert, liegt am umsichtigen und vorsichtigen Verhalten von i. d. R. wohl informierten Nutzern. Selbst der private Internet-Nutzer weiß inzwischen, dass Email-Anhänge von unbekannten Absendern besser nicht geöffnet und Links in fremden Emails besser nicht angeklickt werden und verhält sich entsprechend. Das BSI hat einen verdienstvollen Anteil an dieser "Fortbildung" des Anwenders. ***Der so häufig von staatlicher Seite proklamierte "mündige Bürger" existiert also längst im Internet und bedarf daher keiner staatlichen Regularien.***

Vor wenigen Wochen ging BKA-Chef Ziercke erneut in die Presse-Offensive[9] und sprach von einer *"dramatisch gestiegenen Zahl von mit Schadprogrammen infizierten Computern in Deutschland" "Schätzungen gehen heute von etwa einer Million mit Schadprogrammen infizierten Rechnern in Deutschland aus*." Das sei "*etwa in Drittel mehr als vor einem Jahr*." Abgesehen davon, dass Herr Ziercke selbst schon von "Schätzungen" spricht, die jedoch plausibler würden, wenn ihnen eine Quellenangabe beigefügt wäre, besteht ein erheblicher Unterschied zwischen infizierten und "virulenten" Computern. Jeder Computernutzer, der sich des Risikos von Viren (=Schadprogramme) bewusst ist, setzt einen Virenscanner ein. Dieser läuft ständig mit, erkennt mögliche Viren bereits bevor sie Schaden anrichten können bzw. bietet die Möglichkeit, den Festplattenbestand in regelmäßigen Abständen auf infizierte Dateien zu untersuchen. Erkannte Risikokandidaten können also isoliert werden, "in Quarantäne" gesteckt werden. Solche Schadprogramme sind dann zwar noch auf Computern vorhanden, können jedoch keinen Schaden anrichten. Im weiteren Verlauf nennt Herr Ziercke auch die aktuellen (wohl aus 2008

stammenden) Fallzahlen im Bereich der Informations- und Computerkriminalität, die nunmehr auf 37.000 gestiegen seien, wovon erneut das Gros entfällt auf das Ausspähen privater Bankdaten, also mit Internet-Nutzung nichts zu tun hat.

Bisher fehlt ein glaubwürdiger, anhand objektiver Quellen plausibel nachvollziehbarer Beweis für die von Regierungsseite so dramatisch dargestellten Risiken durch das Internet. Daraus folgt für den vorliegenden Gesetzentwurf, dass die dargestellte Notwendigkeit, die sich ja im Wesentlichen auf Schutz und Sicherheit gegenüber Gefahren aus dem Internet bezieht, bisher nicht nachgewiesen ist.

3 Erhebung und Auswertung von Protokolldaten … - zu Par. 5

In Kurzfassung besagt Par. 5 des Gesetzentwurfs, dass das BSI zur Abwehr von Schadprogrammen ***UND*** zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes die Befugnis erhält, "*Protokolldaten, die beim Betrieb von Kommunikationstechnik des Bundes anfallen*" zu erheben und automatisiert auszuwerten, sowie die an den "*Schnittstellen der Kommunikationstechnik des Bundes anfallenden Daten"* einschließlich der Kommunikationsinhalte automatisiert auszuwerten.

3.1 Klärung von Begriffen und Grundlagen

3.1.1 Informations- ./. Kommunikationstechnik

Par. 3, Abs. 1, Ziffer 1 erwähnt in der summarischen Auflistung als *eine* Aufgabe des BSI die der "*Abwehr von Gefahren für die Sicherheit der* ***Informationstechnik*** *des Bundes".* Dieser Terminus wird in Par. 4, Abs 2, Ziff. 1 wiederholt im Zusammenhang mit der Sammlung und Auswertung von Informationen über Schadensursachen, Schadprogramme bzw. Angriffe. Abweichend davon wird dann in Par. 5 allerdings von "Gefahren für die ***Kommunikationstechnik*** des Bundes" gesprochen.

Die Legaldefinition in Par. 2, Abs. 3 führt aus, dass "**Kommunikationstechnik** *des Bundes im Sinne dieses Gesetzes …* " die ***Informationstechnik*** (sic!) (ist), *"die von einer oder mehreren Bundesbehörden oder im Auftrag von einer oder mehrerer Bundesbehörden betrieben wird und der Kommunikation oder dem Datenaustausch der Behörden untereinander oder mit Dritten dient."*

Da es im Begriffsrahmen dieses Gesetzes wohl kaum informationstechnische Systeme gibt, in die Daten / Informationen **nicht** im Wege des Datenaustausch mit anderen Behörden oder Dritten bzw. im Zuge von Kommunikationsprozessen gelangen, erscheint die Unterscheidung zwischen Informations- und Kommunikationstechnik an dieser Stelle entbehrlich und könnte sowohl die Verständlichkeit des Textes, wie auch die Rechtssicherheit bezüglich des künftigen Gesetzes erhöhen.

3.1.2 "… Kommunikationstechnik des Bundes …"?!

Im Juni 2006 wurde durch einen Beschluss der Bundeskanzlerin und der Regierungschefs der Länder der Aktionsplan Deutschland Online (DOL) als E-Government-Strategie von Bund, Ländern und Kommunen ins Leben gerufen. Ziel des Aktionsplanes ist es, eine vollständig integrierte E-Government-Landschaft in Deutschland zu schaffen[10]. Diese erhielt den Namen Deutschland-Online-Infrastruktur - DOI.

In Phase 1 wurde eine Bestandsaufnahme der bestehenden Behördennetze durchgeführt. In der zweiten Projektphase (bis April 2007) wurde eine ebenenübergreifende Infrastruktur geplant und die Anforderungsanalyse vertieft. Ziel der aktuellen, letzten Projektphase (bis September 2009) ist die Errichtung des DOI-Netzes und die Schaffung der organisatorischen Voraussetzungen für dessen Betrieb. Für die Vergabe des DOI-Netzes und dessen Betriebsführung wurde der DOI-Netz e.V. gegründet, dessen Gründungsmitglieder neben dem Bund, vertreten durch das BMI, alle sechzehn Länder sind. Die Geschäftsführung obliegt zwei Mitarbeitern aus dem

BMI ein weiterer Vertreter des BMI ist Mitglied des Vorstands[11].

Der DOI-Netz.e.V. hat am 06.03.2009 einen Rahmenvertrag mit T-Systems zum Aufbau eines modernen Kommunikationsnetzes der öffentlichen Verwaltung in Bund, Ländern und Kommunen unterzeichnet. *"Die neue Infrastruktur soll die deutschen Verwaltungsnetze von Bund, Ländern und Kommunen flächendeckend und sicher verbinden. Es löst das bisherige TESTA-D-Netz ab."* [12]

In Kenntnis dieser Entwicklung und aktuellen Ergebnisse ist zu fragen, was im zeitgleich zu Phase 3 des DOI-Netzprojekts vorgelegten Gesetzentwurf konkret mit "Kommunikationstechnik des Bundes" gemeint ist, insbesondere ob überhaupt noch von einem physikalisch abgrenzbaren "Kommunikationsnetz" des Bundes gesprochen werden kann und wenn ja, wie dies begründet wird.

3.1.3 "Protokolldaten"

3.1.3.1 Daten eines Datenübertragungsprotokolls

Ebenfalls uneinheitlich wird im Gesetzentwurf, sowie der folgenden Begründung mit dem Begriff "Protokolldaten" umgegangen. Eine Legaldefinition findet sich in Par. 2, Abs. 8:

> *"Protokolldaten im Sinne dieses Gesetzes sind **Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung**, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind. Protokolldaten können Verkehrsdaten gemäß § 3 Nummer 30 des Telekommunikationsgesetzes und Nutzungsdaten nach § 15 Absatz 1 des Telemediengesetzes enthalten."*

Diese Definition lässt sich für den Techniker in Einklang bringen mit dem Begriff des "Datenübertragungs-protokolls" (bedeutungsgleich auch "Kommunikationsprotokoll") und den Daten, die ein solches Protokoll erzeugt.

Definition Datenübertragungsprotokoll:

> *Damit Kommunikationspartner überhaupt miteinander kommunizieren können, müssen sie bestimmte Vereinbarungen und Regeln einhalten. Diese Regeln sind die Protokolle. Ein einzelnes Protokoll arbeitet immer einen bestimmten Funktionsbereich ab, der bei der Datenkommunikation der Funktionalität einer Schicht des OSI-Schichtenmodells entsprechen kann.*

OSI-Schichtenmodell:

> *Das OSI-Schichtenmodell der Internationalen Standardisierungs-Organisation/ISO wurde ab 1977 als Grundlage für die Bildung von Kommunikationsstandards entworfen. Ziel von der Open Systems Interconnection (OSI) ist die Kommunikation in heterogenen Netzen, insbesondere zwischen verschiedenen Rechnerwelten auf der Grundlage anwendungsunterstützender Grunddienste. Diese Grunddienste sind z.B. die Dateiübertragung, das virtuelle Terminal, der Fernzugriff auf Dateien und der Austausch elektronischer Post. Für diese und alle weiteren Kommunikations-Anwendungen benötigt man neben den eigentlichen Anwendungsdaten strukturelle und prozedurale Zusatzinformationen, die als OSI-Protokolle festgelegt sind.* [5]

3.1.3.2 Protokoll-Daten technischer Systeme (Logfiles)

Eine gegenüber der Legaldefinition in Par. 2, Abs. 8 abweichende Definition liefert der 2. Absatz "zu § 5, zu Absatz 1" in Teil B der Begründung.

> *"Gemäß Nummer 1 kann das BSI **Protokolldaten, also sog. Logfiles von Servern, Firewalls usw.** erheben und automatisiert auswerten. Dies erfolgt zum einen, um Anzeichen für bevorstehende IT-Angriffe zu finden. Hierzu können die Logfiles automatisiert ausgewertet werden, z. B. hinsichtlich des Datenvolumens oder durch das automatisierte „Absurfen" von aus dem Bundesnetz heraus aufgerufenen URLs, um sog. Phishingseiten zu identifizieren."*

Eine Logdatei "engl. Logfile) beinhaltet das automatisch erstellte Protokoll von allen oder bestimmten Prozessen bzw. Aktivitäten von Nutzern, Anwendungen oder Geräten auf einem Computersystem.

Der wesentliche Unterschied zwischen den beiden Begriffen besteht darin, dass beim Datenübertragungs-

protokoll sehr wohl auch die **Kommunikationsinhalte** mit dem entsprechenden technischen Analysewerkzeugen erschlossen und "gelesen" werden können, während aus den Prozessprotokollen Zeitstempel für bestimmte Aktivitäten, deren Verursacher und weitere Einzelheiten ablesbar sind, aber die Kommunikationsinhalte nicht enthalten sind. ***Der Gesetzentwurf sollte zwischen den Begriffen und den sich ergebenden unterschiedlichen Auswertungsmöglichkeiten deutlich unterscheiden.***

3.1.4 Automatisierte Auswertung von Protokolldaten

Die Erhebung und automatisierte Auswertung der Protokoll-Daten (Logfiles), wie auch der anderen (Protokolldaten (aus analysierter Datenübertragung), legt aus technischer Sicht nahe, dass dafür (mindestens) zwei verschiedene Werkzeuge verwendet werden.

Die Erhebung und automatisierte Auswertung von Daten, die von Datenübertragungsprotokollen stammen, ist die Aufgabe von so genannten Protokollanalysekomponenten (engl. protocol analzer). Sie werden auf der Kommunikationsstrecke zwischen Sender und Empfänger zwischengeschaltet (z.B. "hinter" dem Webserver eines Behördensubnetzes). Je nach Einstellung sind diese Geräte / Komponenten in der Lage, die Daten eines ganz bestimmten Datenübertragungsprotokolls auf einer ganz bestimmten Ebene (des OSI-Schichtenmodells) herauszufiltern, darzustellen und auch auszuwerten. Die Protokollanalyse kann man sich vorstellen, wie den Einblick mit dem Röntgengerät "in" einen Körper. Man sieht also z.B. für eine Email nicht nur den Sender und Empfänger, sowie die Betreffsangabe und den Inhalt der Email im Klartext, sondern erhält die auf der Ebene des Webbrowsers oder Email-Programme sonst nicht darstellten technischen Zusatzinformationen, die die Datenübertragungsprotokolle zur Steuerung des Übertragungsprozesses benötigen und erzeugen.

Mit diesen "Röntgeneinblicken" werden Eingriffe auf technischer Ebene in den Kommunikationsprozess sichtbar, ferner können die tatsächlichen physikalischen (IP-)Adressen des Senders bzw. Empfängers decodiert werden, auch wenn diese, was bei Spam-Emails häufig geschieht, auf der Anzeigeebene "gefaked", d.h. verfälscht dargestellt werden.

Protokollanalysegeräte werden von mehreren Herstellern entwickelt, angeboten und vertrieben. Beispielhaft erwähnt sei die amerikanische Firma Wildpackets (http://www.wildpackets.com), die nach eigenen Angaben mehr als 80% der in der Forbes-1000-Liste genannten Institutionen und Unternehmen zu ihren Kunden zählt, darunter auch die Deutsche Telekom, T-Systems, T-Mobile, die Deutsche Bank. Wildpackets unterhält eine deutsche Niederlassung in München. Wildpackets versorgt auch Regierungseinrichtungen mit leistungsfähigen und kostengünstigen Lösungen für die Erkennung der Netzwerkaktivitäten in Echtzeit.

Es darf nicht unerwähnt bleiben, dass solche und verwandte Werkzeuge nicht nur passiv erheben und auswerten, was "über die Kommunikationskanäle" kommt, sondern auch in der Lage sind, automatisch aktiv in den Kommunikationsvorgang einzugreifen. ***Solche Eingriffe durch das Bundesamt bzw. durch Stellen des Bundes sollten im Gesetz ausdrücklich ausgeschlossen werden.***

3.1.5 Eigentum an und und Nutzung der Daten

Die Vorstellung von der praktischen Umsetzung der in Par. 5 genannten Maßnahmen wirft die Frage auf, wer eigentlich - ganz konkret - tätig wird und wer Eigentümer der so erhobenen Protokolldaten werden soll.

Wie an anderer Stelle bereits erwähnt, dürfte das im Gesetzentwurf dargestellte Bild von einer einheitlichen und abgegrenzten Kommunikationslandschaft "des Bundes" nicht den Tatsachen entsprechen. Man liegt wohl näher an der Wirklichkeit mit der Vorstellung von einer ganzen Reihe verschiedener Subnetze von Behörden und Einrichtungen, für deren Verbindung untereinander bisher das TESTA-Netz (oder auch andere mögliche Backbones) verwendet wurden, und wofür in Zukunft das DOI-Netz benutzt werden soll. Wenn diese Vorstellung grundsätzlich falsch sein sollte, wäre es hilfreich, eine "richtige" Vorstellung vermittelt zu bekommen.

Der Gesetzentwurf läßt eine Erläuterung darüber vermissen, wie ganz konkret das BSI Zugang und Zugriff erhält, um anfallende Protokolldaten in irgendwelchen Stellen des Bundes zu erheben, wie in Par. 5, Abs. 1, Ziff. 1 formuliert. Werden dazu entsprechende, vom BSI zertifizierte Geräte / Komponenten in den Netzen von Bundesbehörden und -einrichtungen installiert? Wer bedient diese Komponenten? Wie und wo geschieht die Auswertung der erhobenen Daten? Werden sie gesammelt und an das BSI

transferiert? Oder geschieht die Auswertung direkt vor Ort? Fragen über Fragen, deren Beantwortung wesentlich mehr Klarheit erwarten lässt, als bisher vorhanden.

Diese Fragen stellen sich in analoger Weise auch für Protokolldaten, die an den Schnittstellen der Kommunikationstechnik des Bundes anfallen. Darf also in Vorwegnahme der Inbetriebnahme von DOI-Netz unterstellt werden, dass an den entsprechenden Übergabepunkten zwischen Backbone (DOI-Netz) und den angeschlossenen Subnetzen entsprechende Erhebungs- und Auswertungswerkzeuge des BSI installiert werden?

Dass, wie im Gesetzentwurf vorgesehen, ein völlig "spurenloses" Löschen technisch nicht machbar ist, wurde von mehreren Seiten bereits zutreffend bemerkt.

Ferner enthält der Gesetzentwurf keine Regelungen über die Übermittlung der erhobenen Protokolldaten. Nach dem Motto "was nicht ausdrücklich verboten ist, ist demzufolge erlaubt", könnten Protokolldaten bzw. darauf basierende Auswertungen und Auswertungszwischenergebnisse somit auch übermittelt werden an andere Einrichtungen, was gerade im Hinblick auf die Polizeien, Strafverfolgungsbehörden, das Bundesamt für Verfassungsschutz und den Bundesnachrichtendienst, mit deren Unterstützung das BSI ja beauftragt ist bzw. beauftragt werden soll, durchaus nachvollziehbar erscheint.

3.1.6 Abwehr von Schadprogrammen

Hinsichtlich der Technik der Erkennung von Schadprogrammen weist z.B. Prof. Hartmut Pohl in einem in der Zeitschrift 'Datenschutz und Datensicherheit' erschienenen Beitrag[13] darauf hin, dass *"Schadprogramme, wie Viren, Würmer und Trojanische Pferde, sich durch sog. Virensuchprogramme erkennen (lassen),* ***sofern diese die Schadprogramme kennen****."* (Hervorhebung vom Verf.) Im aktuellen Lagebericht 2009 des BSI[14] heißt es zum gleichen Thema: *"Es gibt Millionen von Schadprogrammen, deren Anzahl immer schneller wächst. Jeden Monat kommen Zehntausende hinzu."*

Jedem Internet-Nutzer sind die Namen von Firmen, wie Kaspersky, Norton, Antivir, McAfee, Avira etc. bekannt, die sich auf die Entwicklung und ständige Aktualisierung von Virenscan-Programmen spezialisiert haben. Dahinter steckt ein entsprechender technischer und personeller Aufwand, mit dem das BSI, jedenfalls mit den im Gesetzentwurf genannten, zusätzlichen personellen und finanziellen Ressourcen, wohl kaum ernsthaft konkurrieren kann.

Vor allem aber vermag der Gesetzentwurf selbst nicht zu erklären, inwiefern eine flächendeckende Erhebung und automatisierte Auswertung von Protokolldaten (siehe dazu auch 3.2.1) für die Abwehr von (nicht genauer bezeichneten) Gefahren aus Schadprogrammen geeignet sein soll. Im Lagebericht 2009 des BSI[10] wird dieses Thema zwar gestreift: "

> *"Bislang arbeitet Schutzsoftware hauptsächlich signaturbasiert, das heißt, ein Virenschutzprogramm erkennt nur bereits bekannte Schadprogramme. Diese Technik ist an ihre Grenzen gestoßen, so dass intensiv an Technologien gearbeitet wird, die neue Schadprogramme auch an ihren Eigenschaften bzw. ihrem Verhalten erkennen können. Das Problem dabei: Verhaltensbasierte Erkennungsverfahren führen immer zu einer höheren Anzahl von unberechtigten Alarmen (so genannte false positives). Dies ist für die Nutzer der Schutzsoftware jedoch problematisch, insbesondere, wenn dadurch fälschlicherweise wichtige Betriebssystemprogramme deaktiviert oder sogar gelöscht werden. "*

Doch auch hier findet sich kein weiterer Hinweis darauf, inwiefern die Erhebung von Protokolldaten zielführend für die Abwehr von Schadprogrammen in der Bundesverwaltung werden kann.

Aus dem Entwurfstext und der Begründung erschließt sich ferner nicht präzise, was eigentlich mit dem Terminus "Abwehr von Schadprogrammen" gemeint ist. Wahrig's Deutsches Wörterbuch bestätigt das zunächst intuitive Verständnis des Lesers, dass 'Abwehr' gleichzusetzen ist mit 'Verteidigung', 'Schutz' bzw. 'Zurückweisung', so dass es in Folge einer erfolgreichen Abwehr eines Schadprogramms nicht zum Eindringen desselben in ein IKT-Netz bzw. -System kommen kann. Ferner unterstellt der Leser ohne weitere semantische Erläuterung durch den Verfasser des Gesetzes, dass die Abwehr einen Angriff voraussetzt und dies wiederum auf einer Absicht beruhen muss, also vorsätzlich geschieht.

- In Teil B, Zu Par. 2, Zu den Absätzen 5 und 6, dort im 2. Textabsatz, ist die Rede davon, dass

Schadprogramme *"dem Zweck dienen, unbefugt unerwünschte Funktionen auszuführen".* Und dass "*unbeabsichtigte Sicherheitslücken in normalen Programmen*" damit nicht gemeint seien. (*1)

- In den Begründungen "zu §5, zu Absatz 4" wird dann lapidar festgestellt, dass "Angriffe auf die Informationstechnik des Bundes mittels Schadprogrammen "*zugleich auch Straftaten oder eine Gefahr für die öffentliche Sicherheit dar(stellen."* (*2)
- Daraus wird die Befugnis abgeleitet, solche Daten auch an die zuständigen Behörden zu übermitteln, sofern dies zur Verfolgung einer Straftat von erheblicher Bedeutung oder einer mittels Telekommunikation begangener Straftat erforderlich ist. (*3)

Ob der oben mit ('1) gekennzeichneten Abschnitt tatsächlich geeignet ist, dem Strafverfolger ausreichende Mittel in die Hand zu geben, um die Zweckbestimmung, die nicht vorhandene Befugtheit und die (vom wem?) nicht erwünschte Funktion eingrenzen und auch beweisen zu können, mögen rechtskundigere Fachleute bewerten. Die Erfahrung der Verfasserin besagt jedenfalls, dass selbst einschlägig tätige Staatsanwaltschaften für Internet-Kriminalität weder über Mitarbeiter mit sonderlich ausgeprägten technischen Fähigkeiten und Kenntnissen verfügen, noch über das Werkzeug, um entsprechende Nachweise führen zu können. Dass auch Staatsanwaltschaften die Erfolgsaussichten ihrer Bemühungen in Relation zum vermutlich notwendigen Aufwand setzen und entsprechende Entscheidungen treffen, kommt hinzu.
Zu der mit (*2) gekennzeichneten Passage ist unklar, welche Strafgesetze oder strafrechtlichen Nebengesetze hier konkret greifen sollen, doch werden Rechtsexperten diese Frage wahrscheinlich eindeutig beantworten können.
Zum Absatz (*3) wird, wie schon von vielen anderen Kommentatoren, darauf hingewiesen, dass Begehrlichkeiten, beispielsweise der Unterhaltungsindustrie, nach dem Zugriff auf solche Daten bekannt sind, so dass sich die Frage stellt, ob hier entsprechende "Vorkehrungen" bereits in das Gesetz eingebaut wurden.

3.2 Einzelheiten zur beabsichtigten Erhebung und Auswertung von Protokolldaten

3.2.1 Umfang der Erhebung von Protokolldaten

Die Formulierung in Par. 5, Abs. 1 Ziff. 1 weist auf ein klassisches "Henne-Ei-Problem" hin, das den Verfassern möglicher Weise entgangen ist: Es wird dort die Befugnis geregelt, "*Protokolldaten zu erheben und auszuwerten, "**soweit dies** zum Erkennen Eingrenzen oder Beseitigen von Störungen oder Fehlern …. erforderlich"* ist. Es impliziert diese Formulierung, dass **vorher bekannt** ist, ob sich aus den Daten, Indikationen für das Erkennen, Eingrenzen oder Beseitigen von Fehlern … ergeben. Dies wird wohl nicht der Fall sein, ***sodass bei konsequenter Verfolgung dieses Ziels zunächst einmal sämtliche Protokolldaten erhoben und ausgewertet werden müssen; was im Übrigen ja auch der Betriebsweise von einschlägig bekannten Protokollanalysesystemen entspricht.***
Analoges trifft zu auf den zweiten Spiegelstrich, wo es um die Auswertung der an den Schnittstellen der Kommunikationstechnik des Bundes anfallenden Daten geht.

3.2.2 Auswertung der Inhalte, insbesondere enthaltener Links und "Absurfen" dieser Links

Für völlig überzogen und unverhältnismäßig hält die Verfasserin das Ansinnen, welches im vierten Absatz der Begründung zu Par. 5, Abs. 1 am deutlichsten ausgeführt ist. Es soll nämlich erlaubt werden, die Kommunikationsinhalte zu scannen auf das Vorkommen von darin enthaltenen Links (auf Seiten im Inter- bzw. Intranet). Anschließend soll diese Seiten "automatisiert" aufgesucht werden, um deren Inhalte darauf zu untersuchen, ob sie Schadsoftware enthalten, die versucht, sich automatisch auf dem Rechner des Benutzers zu installieren. Einmal ganz abgesehen von der rechtlichen Frage, ob diese Online-Durchsuchung von Webseiten ohne jeglichen Bezug zu der Kommunikationsinfrastruktur des Bundes, überhaupt zulässig ist, ist damit der Möglichkeit für die Erstellung von Interessenprofilen von Nutzern Tür und Tor geöffnet. Dies gilt insbesondere, wenn man den vorliegenden Gesetzentwurf in den größeren Kontext stellt der in Kapitel 1.1 skizzierten

Bestrebungen des BMI

- zur Online-Identifizierung von Nutzern (auch mit Hilfe des neuen elektronischen Personalausweises),
- der Einführung von "Bürgerportalen", die jedem Bürger eine virtuelle Zustelladresse zuweisen und ihn eindeutig "online" identifizieren,
- den Bemühungen des BMI um die Zusammenführung von personenbezogenen Daten aus diversen Behördenquellen mit dem Ziel der Erstellung eines umfassenden "Personendossiers und
- nicht zuletzt mit den jüngsten Beschlüssen mit dem Ziel der Eindämmung von Kinderpornographie, zu deren Werkzeugen es auch gehört, dass vom Bundeskriminalamt, täglich aktualisiert, eine Liste inkriminierter Webseiten erstellt und publiziert wird, die von Providern geblockt bzw. umgeleitet werden sollen.

3.2.3 Mögliche Betroffene

Auch wenn der Gesetzentwurf den Eindruck zu erwecken sucht, es ginge ja "nur" um die Kommunikationstechnik des Bundes, was somit auch Sache des Bundes sei, sieht die Wirklichkeit doch ganz anders aus. Federführend vorangetrieben durch das BMI, arbeitet die Bundesregierung an einer umfassenden "e-" bzw. "online"-Strategie. Der gerade vergebene Auftrag für das neue "Netz der deutschen Verwaltung" ist ein Baustein, die Absicht, bis zum Jahr 2012 die gesamte Kommunikation zwischen Unternehmen und Behörden online abzuwickeln[15], ein weiterer Indikator.

Visionen, wie sie in den einschlägigen Werbebroschüren des BMI bzw. BSI entwickelt werden, beschreiben die "schöne neue Welt":

> *"Mal eben zwischendurch einen Meldeantrag zu Hause am Sofa ausfüllen, im Café bei Espresso und Kuchen Einspruch gegen einen Bescheid erheben, vom Strandkorb aus die Steuererklärung verfassen - all das ist keine Zukunftsmusik mehr, sondern bereits heute möglich."* [16]

Unternehmen sollen sich mit dem Gedanken an e-Government anfreunden mit solchen Beispielen:

> *"Im Rahmen der gesetzlichen Meldepflichten der Unternehmen zur amtlichen Statistik können die Daten aus den Rechnungswesensystemen der Unternehmen elektronisch und automatisiert an das statistische Bundesamt und die statistischen Landesämter übermittelt werden.*
> *"Sämtliche Prozesse und IT-Verfahren der Warenflusskontrolle (z.B. bei Versendern, Spediteuren und Empfänger), der Sicherheitskontrollen der Behörden (Zoll, Bundesamt für Güterverkehr, Gesundheitsbehörden) sind aufeinander abzustimmen. Meldepflichten und redundante Datenerfassung können bei allen Beteiligten reduziert werden.*[17]

Im Zusammenhang mit der letztgenannten Vision sind auch die Bemühungen des BSI um den sicheren RFID-Einsatz zu sehen, jene kleinen aktiven Chips, die zur Warenkennzeichnung verwendet werden und das Bild vom "Internet der Waren" geprägt haben.

Damit liegen die umfassenden Absichten deutlich erkennbar auf dem Tisch. Und ergibt sich daraus folgerichtig, dass die Erhebung und Auswertung von "Protokolldaten" eben nicht nur irgendwelche Kommunikationseinrichtungen auf Bundesebene oder Bedienstete des Bundes betrifft, sondern in naher Zukunft jeden Bürger und jedes Unternehmen erfassen würde. Im Zusammenhang mit dem Bestrebungen nach "sicherer Identifizierung" und dem erkennbaren Ansatz, "anonymes Surfen" zu unterbinden, ein aus Sicht der Verfasserin geradezu atemberaubender Versuch des Eingriffs des Staates in die informationelle Selbstbestimmung der einzelnen natürlichen und juristischen Person.

Nicht unerwähnt bleiben dürfen im Übrigen die Bediensteten in den Verwaltungen auf allen Ebenen, deren Online-Aktivitäten ebenfalls lückenlos von solcher Art Protokolldatenauswertung erfasst würde.

4 Die Marktmacht des BSI - Anmerkungen zu den Paragraphen 8 und folgende

Völlig neu gegenüber dem BSI-Errichtungsgesetz von 1991 ist Par. 8 des Gesetzentwurfs, der kurz gefasst, besagt, dass das Bundesamt befugt ist,

- "Mindeststandards" für die "Sicherung" der Informationstechnik festzulegen,

- diese in Form von Verwaltungsvorschriften als verpflichtend zu erklären für alle Stellen des Bundes,
- ferner technische Richtlinien zu erlassen, die verpflichtende Vorgaben für Vergabenverfahren für de stellen des Bundes darstellen und zwar
  a) hinsichtlich der "Eignung", d.h. Anforderungen an den Auftragnehmer, sowie
  b) hinsichtlich der Anforderungen an die IT -Sicherheitsprodukte und
- Eigenentwicklung durchzuführen.
- Aufgrund eines Beschlusses des Rats der IT -Beauftragten der Bundesregierung kann ferner festgelegt werden, dass "die Bundesbehörden" verpflichtet sind, diese Produkte beim BSI abzurufen.

4.1 Klärung von Begriffen und Grundlagen

4.1.1 …"Sicherung der Informationstechnik"

Es heißt im Gesetzentwurf, dass das Bundesamt "Mindeststandards **für die Sicherung der Informationstechnik** des Bundes festlegen" kann. Bis dahin war im Gesetzentwurf von **der Sicherheit der Informationstechnik** die Rede, der in Par. 8 verwendete Begriff der "Sicherung" ist weder eingeführt, noch legal definiert.

Handelt es sich um eine versehentlich falsche Wortwahl? Wenn ja, wäre es klarer, auch hier von "Sicherheit in der Informationstechnik" zu sprechen. Wenn nein, sollte erläutert werden, was eigentlich unter "Sicherung der Informationstechnik" zu verstehen ist.

4.1.2 "Mindeststandards"

Ebenfalls ungeklärt und undefiniert ist, was eigentlich "Mindeststandards" sind. Die Begründung nimmt zwar Bezug auf das heutige Grundschutzhandbuch[18] oder auf Prüfvorschriften.

Zu ersterem ist allerdings zu bemerken, dass es sich um ein Werk mit 3.800 Seiten in vier Ordnern handelt und nicht etwa technische Standards, sondern vor allem Prozesse definiert. Allein das Volumen dieses Werks steht im krassen Widerspruch zum Wort "Mindeststandards". Zu den Prüfvorschriften sei angemerkt, dass solche, wenn man der Bedeutung des Wortes traut, Vorgaben für die Prüfung von Komponenten machen. Im vorliegenden Falle allerdings geht es um Leistungsmerkmale und Eigenschaften von technischen Komponenten, die eingehalten sein wollen, wenn der entsprechende Hersteller weiterhin "im Geschäft" mit Bundesbehörden bleiben bzw. einen neuen Geschäftskontakt aufbauen möchte.

Aufgrund der somit gravierenden geschäftlichen Auswirkungen für ein Unternehmen hinsichtlich der weiteren Teilnahme am IT-Markt mit Bundesbehörden bzw. des Marktzutritts, sollte fairer Weise verlangt werden, dass sich die Verfasser des Gesetztes etwas präziser zu ihren Vorstellungen und beabsichtigten Regelungen über solche Vorgaben als faktische Marktzutrittsbarrieren äußern.

4.1.3 Technische Richtlinien

Bei den in Par. 8, Abs. 2 genannten technischen Richtlinien soll es sich nach Par. 3, Abs. 1, Nummer 10) um *"**sicherheitstechnische Anforderungen** an die einzusetzende Informationstechnik des Bundes"* handeln. Abweichend davon wird dann in der Begründung zu §8, Abs. 2 erläutert, dass das BSI ermächtigt werden soll, *"für die **Beschaffung von Informationstechnik verbindliche Richtlinien** zu verfassen"* und weiter ausgeführt, dass es sich dabei z.B. um *"Vorschriften zur Risikoanalyse, zur Auswahl und zu den IT-Sicherheitsanforderungen"*, handelt.

Im Gesetzentwurf sollte geklärt werden, ob nun

a) technische Richtlinien zur Definition von sicherheitsbezogenen Anforderungen an die Leistung bzw. die Eigenschaften von informationstechnischen Systemen gemeint sind oder

b) "abstrakte Qualitätskriterien" (so die Begründung) für die Beschaffung von Informationstechnik.

Gleiches gilt sinngemäß für die Anforderungen an die Eignung von Auftragnehmern.

4.1.4 Anforderungen an die Eignung

Vollends "schwammig" bleibt der Gesetzentwurf bei der Frage, was eigentlich "*sachgerechte Anforderungen an Auftragnehmer (Eignung)"* sein sollen. Objektiv nachvollziehbare, offen gelegte und für alle gleiche Standards dazu setzt das Vergaberecht. Es werden z.B. Nachweise verlangt über die finanzielle Leistungsfähigkeit des Anbieters, Belege über pünktlich angemeldet bzw. bezahlte Steuern und Sozialabgaben, über die personelle Ausstattung etc. ***Wenn im Rahmen dieses Gesetzes weitergehende fachliche Kriterien für die Bemessung der Eignung des Anbieters notwendig sind, sollten diese benannt und offen gelegt werden und verbindlich für alle Auftragnehmer angewendet werden. Ferner wäre zu regeln, welche Rechtsmittel für abgewiesene Anbieter zur Verfügung stehen.***

4.2 Einzelheiten zu den "Vorgaben ..:"

Die Verfasserin anerkennt durchaus die Notwendigkeit von einheitlichen Minimalanforderungen an technische Systeme und Auftragnehmer, wie auch an die Gestaltung von Ausschreibungsunterlagen und Durchführung von Vergabeverfahren. Unklar und im Gesetzentwurf auch nicht begründet ist, warum dies für die Bundesverwaltung nun ausgerechnet im BSI-Gesetz geregelt werden muss bzw. wo in den bisherigen Regularien Lücken enthalten sein sollen, die diese Neuregelung erforderlich machen. Über die hier unterschwellig angedeutete, schwankende Qualität von Ausschreibungsunterlagen, unzureichend definierte Anforderungen an Technik und Personal müsste das Beschaffungsamt des Bundsministerium des Innern Auskunft erteilen können, das seit langer Zeit solche Aufträge vergibt in einer Größenordnung von rund 3 Milliarden Euro pro Jahr.

In ihren Auswirkungen sind diese geplanten "Vorgaben" durch das BSI geeignet, den Markt für informationstechnische Systeme und Services für die Bundesverwaltung in der Bundesrepublik Deutschland komplett der Gestaltungs- und Entscheidungshoheit des Bundesamts für die Sicherheit in der Informationstechnik zu unterwerfen.

Es ist zutreffend, dass das Bundesamt auch aufgrund seiner bisherigen gesetzlichen Aufgaben bereits Zertifizierungsstelle für informationstechnische Systeme oder Komponenten war. Bisher allerdings beschränkte sich diese Aufgabe auf die Prüfung von Anträgen auf Erteilung eines Sicherheitszertifikats im Hinblick auf die Konformität des zu prüfenden Produkts mit den vom Bundesamt festgestellten oder allgemein anerkannten Sicherheitskriterien.

Über die Zertifizierung hinaus soll das BSI mit dem neuen Gesetz ermächtigt werden, Standards und Richtlinien zu Vorgaben für technische Leistungsmerkmale und Eigenschaften zu machen (obwohl dies, wie oben ausgeführt, nicht klar definiert ist), sowie Anforderungen an die Auftragnehmer zu definieren. Diese Vorgaben unterliegen allein dem Gutdünken des BSI.

- Anders, als im noch geltenden BSI-Gesetz sind sämtliche Bezüge auf allgemein anerkannte Standards (BSI-Errichtungsgesetz §4, Abs. 2) gestrichen worden. Es gelten somit nur noch Prüf- und Bewertungskriterien, die vom Bundesamt nach eigenem Gutdünken festgelegt werden.
- Ergänzend sei erwähnt, dass es im gerade im Bereich der Informationssicherheit eine ganze Reihe von offenen Standards[19] gibt, von denen einige vom BSI selbst erarbeitet und veröffentlicht worden sind, andere auf ähnliche Arbeiten einer britischen Regierungseinrichtung zurückgehen (ITIL) und wieder andere auf Standards nach IEC / ISO sowie auf veröffentliche, so genannte Best Practices.
- Anders als im noch geltenden BSI-Gesetz ist auch die Möglichkeit der Mitsprache des Antragstellers (bei Zertifizierungsverfahren) gestrichen, wie sie bisher im BSI-Errichtungsgesetz §4, Abs. 2 enthalten war.
- Ferner fehlt im Gesetzentwurf jegliche Verpflichtung des BSI zur Offenlegung solcher Kriterien. Ein potenzieller Anbieter bzw. Antragsteller hat somit nicht einmal die Chance, z.B. das Qualitätsmanagement seines Unternehmens oder die fachliche Qualifikation seiner Mitarbeiter bereits im Vorfeld von Vergabeverfahren zu verbessern. Dass es im Einzelfall die Anforderung geben mag, fachliche Qualifikationen oder bestimmte gewünschte Leistungsmerkmale eines Systems oder Services aufgrund

ihrer Sicherheitsrelevanz nicht zu veröffentlichen, ist nichts Neues und stellte auch bisher keinen Anlass zur Einführung entsprechender gesetzlicher Regularien dar. Nach wie vor existiert die Möglichkeit, auch Mitarbeiter aus der freien Wirtschaft zur Geheimhaltung zu verpflichten und Unternehmen in die Geheimschutzbetreuung aufzunehmen.

Sollte das hier vorgeschlagene "System" in die Praxis umgesetzt werden, besteht die Gefahr der Ausbildung einer Monokultur von solchen Anbietern, die den Zuschlag in Vergabeverfahren erhalten haben, weil ihr Angebot konform war mit (ggf. unveröffentlichten) Anforderungen des BSI. Dies schafft zwangsläufig einen Wettbewerbsvorsprung gegenüber "Nicht-Insidern".

Aus Sicht der ausschreibenden Behörde / Dienststelle mag es einen Pluspunkt für einen bestimmten Anbieter darstellen, dass er überhaupt schon Zuschläge in solchen Vergabeverfahren erhalten hat, sodass man geneigt sein könnte, solchen Anbietern bei zukünftigen Ausschreibungen den Vorzug zu geben. Wie einfach dies zu gestalten ist, liegt auf der Hand, wenn die "sachgerechten Anforderungen an die Eignung" einem bestimmten Anbieter problemlos "auf den Leib" geschneidert werden können, was insbesondere für Vergabeverfahren des BSI selbst gilt.

4.3 Das BSI als Entwickler und Vertreiber von IT-Sicherheitsprodukten

Ohne jegliche fachliche oder technische Einschränkung wird dem BSI die Aufgabe und Befugnis zuerkannt, IT-Sicherheitsprodukte zu entwickeln und *"für Stellen des Bundes"* bereitzustellen. Vorgesehen ist sogar, dass eine Verpflichtung für diese zum Bezug solcher Komponenten beim Bundesamt besteht und Eigenbeschaffungen (durch Behörden) nur noch im begründeten Ausnahmefall möglich sind.

Die Entwurfsfassung des Gesetzestexts ist in diesem Punkt rigide und schränkt nicht etwa auf bestimmte, besonders sicherheitsrelevante Produkte ein. In den Erläuterungen zu Absatz 3 (von Par. 8) wird zwar zunächst von *"bestimmten Sicherheitsprodukten (z.B. Virenscanner, Firewalls, Verschlüsselungstechnik usw.)"* gesprochen. Im weiteren Verlauf heißt es jedoch, dass das BSI auch dann von dieser Befugnis Gebrauch machen kann, wenn "*durch die zentrale Bereitstellung (durch Mengenrabatte) Kosten gespart"* werden können.

Der Entwurf lässt alle weiteren Fragen in diesem Zusammenhang offen. Dazu gehört, ob ein Bundesamt für die Sicherheit in der Informationstechnik die richtige Instanz ist und die passende logistische, fachliche, technische und vertriebliche Struktur und notwendigen Ressourcen hat, um solche Entwicklungen durchzuführen. Oder ob die notwendige Objektivität gewahrt sein kann, wenn die Leistungsbeschreibungen, Entwicklung, Prüfvorschriften, Zertifizierung und die Überwachung im späteren Betrieb in ein- und derselben Hand liegen. Oder ob faire Marktpreise gewahrt sind, wenn eine Bundesbehörde eine monopolistische Anbieterstellung einnimmt.

Hinsichtlich der erwähnten Mengenrabatte sei darauf hingewiesen, dass das Beschaffungsamt des BMI seit Jahren Praxis darin hat, Rahmenverträge zu vergeben, um bestmögliche Konditionen im Hinblick auf das gegebene Einkaufsvolumen von einem oder mehreren Anbietern zu erhalten. Zu erwähnen ist in diesem Zusammenhang ein vor kurzem vergebener Rahmenvertrag über 75.000 Personentage (entsprechend überschlägig berechnet 375 Mannjahre) an externer Beratungsleistung, der an fünf Firmenkonsortien vergeben wurde und von der "Schwester" des BSI, der Bundesstelle für Informationstechnik des Bundes (BIT) verwaltet wird[20].

4.4 Faktische Marktmacht des BSI

Wie in Kapitel 1 bereits dargelegt wurde, hat das BSI schon heute zentrale Bedeutung für die wesentlichen Projekte und Vorhaben im Rahmen von e-Government und Deutschland Online. Das BSI ist ferner Unterstützer und Berater der dem BMI nachgeordneten Polizei- und Sicherheitsbehörden, sowie - dies neu im Rahmen des vorliegenden Gesetzentwurfs - auch Unterstützer des Bundesnachrichtendienstes bei dessen gesetzlichen Aufgaben.

Dazu kommt nach dem vorliegenden Gesetzentwurf die soeben diskutierte, umfassende Ermächtigung des BSI zum Erlass von technischen und fachlich/personellen Vorgaben für die Informationstechnik in Bundesbehörden und -einrichtungen.

Ergänzt wird die ohnehin schon dominierende Stellung des BSI, weil seine Vorgaben implizite Bedeutung auch für andere, Nicht-Bundes-Behörden, sowie für Dritte haben. Denn Vorgaben für z.B. die informations- und kommunikationstechnische Infrastruktur des Bundes ziehen zwangsläufig die Notwendigkeit nach sich, dass sich der Partner, der mit der entsprechenden Stelle des Bundes "online" in Kontakt kommen möchte, an dessen technischen Standards ausrichtet. Diese werden allein und ohne Abstimmung mit irgendwelchen Dritten nur vom BSI vorgegeben. Gemessen an der Tatsache, dass das Gesamtvolumen des IT-Marktes mit der öffentlichen

Verwaltung mehr als 15 Milliarden Euro pro Jahr ausmacht, ist die hier vorgesehene, faktische Marktmacht des BSI daher immens***. Es bedeutet dies in der Praxis, dass der Hersteller bzw. Vertrieb bzw. Service-Auftragnehmer entweder - relativ rechtlos - sich in die Hände der Vorgaben und Entscheidung des BSI zu begeben hat oder mittelfristig aus dem IT-Markt mit öffentlichen Einrichtungen auszusteigen gezwungen ist.***

4.5 Systemische Gestaltung kann korrumptive Entwicklungen befördern

Die hier nur kurz skizzierte Anlage der Entscheidungsmacht und Entscheidungswege beim BSI (bzw. BMI) birgt das Risiko der Entwicklung von korrumptiven Strukturen in sich, da relativ wenige Entscheider faktisch über einen immensen Gestaltungsspielraum und Entscheidungsmacht verfügen.

Dabei muss es nicht nur um die Gewährung und Annahme **persönlicher Vorteile** durch den Entscheider beim Auftraggeber gehen. Ebenso vorstellbar ist vielmehr ein ***Vorteilsgewährung auf systemischer Ebene***, die z.B. darin besteht, dass ein Anbieter, der ins Geschäft kommen bzw. bleiben möchte, sich entweder auf finanzielle Zusagen einlassen muss (Preisdumping) bzw. auf die Zusage von "technischen Leistungsmerkmalen", ggf. unter der Zusatzbedingungen, dass diese nicht gegenüber Dritten zu kommunizieren sind. ***Ganz automatisch würde dies auch dafür sorgen, dass immer weniger Menschen, geschweige denn Nicht-Angehörige des "Kosmos BSI" überhaupt noch wissen und beurteilen können, was die dort entwickelten bzw. betriebenen Systeme tatsächlich leisten und wie sie funktionieren.***

Inhalt

Literatur- und Quellenverzeichnis

1 E-Government 2.0 - Das Programm des Bundes, 2009, Bundesministerium des Innern
2 IT-Projekte im Überblick: Bundesmelderegister, Bundesministerium des Innern
3 DOI. T-Systemes vernetzt Bund, Länder und Kommunen, 05.03.2009, portel.de
4 DBT-Drs 16/12598
5 (1), Seite 21
6 BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS), Bundesamt für Sicherheit in der Informationstechnik
7 (1), Seite 15
8 Auszug aus der polizeilichen Kriminalstatistik für das Berichtsjahr 2007, Bundeskriminalamt
9 Immer mehr Hackerangriffe, 26.03.2009, Südddeutsche Zeitung Online
10 Landschaftspflege im deutschen E-Government: Deutschland-Online-Infrastruktur Verwaltungsnetz wird ausgeschrieben. 03.2008, Innovation und Kommunalverwaltung
11 Deutschland Online Infrastruktur, Stand und Ausblick, Vortrag zur Cebit 2009 von Rudi Grimm, Geschäftsführer von DOI-Netz e.V:
12 Vertrag für Infrastruktur, 06.03.2009, move-online.de
13 Zur Technik der heimlichen Online-Durchsuchung, Prof. Dr. Hartmut Pohl, Datenschutz und Datensicherheit 31 (2007)
14 Die Lage der IT-Sicherheit in Deutschland 2009, Bundesamt für Sicherheit in der Informationstechnik
15 Einführung eGovernment mit der Wirtschaft bis 2012
16 (001 712)
17 siehe (1)
18 IT-Grundschutz-Handbuch, Bundesamt für Sicherheit in der Informationstechnik
19 Standards für IT-Sicherheit
20 Beratung in neuer Dimension, 17.04.2009, move-online.de