Michael Hange

Wirksamkeit von Regelungen und Empfehlungen in der IT-Sicherheit

Durchgreifende Umwälzungen in der Informationstechnologie haben auch qualitativ neuartige Bedrohungen der IT-Sicherheit zur Folge und offenbaren technologische Schwachstellen von neuer Komplexität. Das Internet und die Mobilkommunikation haben in den letzten zehn Jahren die Entwicklung der Informationstechnik maßgeblich geprägt. Mit der rasanten Ausbreitung hat das Internet als Plattform erst übergreifende Konzepte für digitale Dienstleistungen des E-Business und E-Government ermöglicht. Trotz inzwischen zurückhaltender Erwartungen bei den Internet-Unternehmen hat das Internet bereits heute zu einer Veränderung in Wirtschaft und Verwaltung geführt. Künftig werden die digitalen Anwendungen und Dienstleistungen selbst die treibenden Kräfte der Fortentwicklung des Internets sein.

In vielen Staaten sind Programme aufgelegt, um E-Government im Zeitraum von 2003 bis 2005 in die Praxis umzusetzen. Mit der Initiative Bund-Online 2005 verfolgt die Bundesregierung die Zielsetzung, bis 2005 durch E-Government für den Bürger mehr und qualitativ bessere Dienstleistungen online bereitzustellen und das Verwaltungshandeln effizienter zu gestalten. Entscheidender Faktor für eine breite Akzeptanz der angebotenen digitalen Dienstleistungen wird das Vertrauen der Bürger in die IT-Sicherheit des Internets sein – insbesondere der Bürger, die für die Nutzung der Onlinedienste noch gewonnen werden müssen. Auch eine erfolgreiche Überwindung der »digitalen Spaltung« in Nutzer und Nicht-Nutzer wird maßgeblich davon abhängen, vertrauenswürdige sowie sichere rechtliche und technologische Rahmenbedingungen zu schaffen.

Wirkung von Regelungen und Empfehlungen auf die Verbesserung der IT-Sicherheit

Nachfolgend werden einige ausgewählte Regelungsbereiche und Empfehlungen vorgestellt, die im Kontext von E-Government eine Rolle spielen.

Beispiele für Regelungen im Bereich IT-Sicherheit
- Bundesdatenschutzgesetz (BDSG)
- Signaturgesetz (SigG)

Beispiele für Empfehlungen im Bereich IT-Sicherheit
- IT-Grundschutzhandbuch
- E-Government-Handbuch

Beispiele für Selbstregulierung durch die Wirtschaft im Bereich IT-Sicherheit
- Interoperabilitätsstandard ISIS-MTT für elektronische Signaturen
- ISO-Standard ITSEC/CC für die Sicherheitszertifizierung von IT-Produkten.

Die Aufzählung ist beispielhaft, denn es fehlen u.a. bereichsspezifische Regelungen für das E-Government, die teilweise noch nicht verabschiedet sind sowie u.a. das Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (EGG), das zum Ziel hat, einen modernen und verlässlichen Rechtsrahmen für den elektronischen Geschäftsverkehr zu schaffen.

Für die Bewertung der Wirksamkeit von Regelungen und Empfehlungen in der IT-Sicherheit können folgende Kriterien zugrunde gelegt werden:

- Anwendbarkeit auch bei Technikveränderung – insbesondere keine Behinderung des Fortschritts der Technik,
- Überprüfbarkeit der Einhaltung; dies bedeutet, dass eine Regelung oder Empfehlung eindeutig und verständlich formuliert sein muss,
- positiver Aufwand-Nutzen-Effekt bei Umsetzung für den Betroffenen und
- Schaffen eines allgemeinen Vertrauensvorteils.

Bisherige Erfahrungen

1. Im **Bundesdatenschutzgesetz** aus den siebziger Jahren waren in §9 die so genannten zehn Gebote enthalten, in denen die technisch-organisatorischen Regelungen zur Datensicherheit (z.B. Speicherkontrolle) beschrieben wurden. Die Regelungen orientierten sich weitgehend an der Arbeitsweise in Großrechenzentren – d.h. der Rechnerwelt vor ca. 25 Jahren. Mit Einführung der Client-Server Architekturen in den achtziger Jahren entsprachen die in §9 beschriebenen Sicherheitsmaßnahmen nicht mehr dem Stand der IT-Sicherheit. Dies ändert aber nichts an der Tatsache, dass das BDSG in den letzten 25 Jahren nachhaltig zu einem gesteigerten Datenschutzbewusstsein bei den Bürgern geführt und auch in der Praxis zu einer Verbesserung der Vertrauensbasis für den Einsatz von IT beigetragen hat.
   Mit Novellierung des BDSG im Jahre 2001 ist auf eine technikbezogene Spezifizierung der Sicherheits- und Kontrollmaßnahmen verzichtet worden.
2. Das 1997 verabschiedete Signaturgesetz (SigG) sah in einer der ersten Fassungen neben der Signaturverordnung einen ausführlichen **Katalog von Sicherheitsmaßnahmen** vor, in dem konkret die Umsetzung der rechtlichen in technische Anforderungen beschrieben wurde. Insbesondere wurden in dem 300-seitigen Maßnahmenkatalog, der mit Wirtschaft und Wissenschaft ausführlich erörtert wurde, die hohen Sicherheitsanforderungen an die eingesetzten Sicherheitskomponenten (z.B. Chipkarten) detailliert beschrieben. Obwohl die Wirtschaft auf der Ebene der Experten an dem Maßnahmenkatalog aktiv mitgearbeitet hatte und die Qualität der aufgezeigten Sicherheitsmaßnahmen allgemein anerkannt wurde, lehnten im Anhörungsverfahren die betroffenen Wirtschaftsverbände den Katalog weitgehend ab. Es wurde die Auffassung vertreten, dass durch die Beschreibung der für Sicherheitsmaßnahmen geeigneten

Technologien andere mögliche Lösungen benachteiligt und technische Innovation behindert würden.

3. Es wurde daraufhin entschieden, den Maßnahmenkatalog als Handbuch des BSI mit Empfehlungscharakter herauszugeben. In dieser Form hat er sich sowohl bei der Entwicklung von Sicherheitsprodukten wie auch bei der Errichtung von Trust-Centern als nützliche Orientierungshilfe bewährt.
4. Anfang der neunziger Jahre wurde der Bundesverwaltung die Durchführung von Risikoanalysen und die Erstellung von Sicherheitskonzepten in der Bundesverwaltung verpflichtend vorgegeben. Von jeder Bundesbehörde mussten bei IT-Vorhaben auch IT-Sicherheitskonzepte zur Genehmigung der Haushaltsmittel vorgelegt werden. Die Erstellung der Sicherheitskonzepte mit aufwändigen Bedrohungs-, Schwachstellen-, und Risikoanalysen orientierte sich an dem **IT-Sicherheits-Handbuch**. Das Verfahren der Risikoanalysen führte vielfach zu umfangreichen Untersuchungen, deren Ergebnisse in keinem Verhältnis zu den Aufwänden standen. Das IT-Sicherheits-Handbuch hat sich trotz Empfehlung in der Bundesverwaltung als Standardwerk in der Breite nicht durchsetzen können.
5. Das alternativ im BSI entwickelte **IT-Grundschutzhandbuch** wurde daher bei der Einführung zunächst nur als Hilfsmittel zur Selbsthilfe den Verwaltungen und Wirtschaftsunternehmen empfohlen. Entscheidendes Kriterium für die Akzeptanz der im Grundschutz-Handbuch beschriebenen Vorgehensweise waren die Qualität der erzielten Ergebnisse sowie der positive Aufwand-Nutzen-Effekt des Verfahrens. Mit Bewährung des Grundschutz-Handbuches in der Praxis wurde es in einigen Verwaltungen und Wirtschaftsunternehmen in Selbstregulierung als verbindliches Standardwerk festgelegt.

Regelungen und Empfehlungen im E-Government

Die von der Bundesregierung gestartete Initiative BundOnline 2005 hat das Ziel, bis zum Jahr 2005 alle internetfähigen Dienstleistungen der Bundesverwaltung online anzubieten.

Rahmenbedingungen für die Umsetzung von IT-Sicherheit im E-Government

- Bei der Kommunikation und bei Transaktionen über das Internet sind Rechtssicherheit und der Schutz der Verbraucherinteressen sicherzustellen. Hierzu bedarf es **rechtlicher Rahmenbedingungen**. Daneben sind bereichsspezifisch zusätzliche Regelungen zu treffen.
- Die Interoperabilität von Sicherheitstechnologien im Kommunikationsbereich ist zwingende Voraussetzung, um mit E-Government alle Bürger erreichen zu können. In **Selbstregulierung** bedarf es zwischen den betroffenen Hersteller- und Anwendergruppen der Festlegung interoperabler

Schnittstellenspezifikationen. Darüber hinaus würde auch die Einführung von Sicherheitszertifikaten das erreichte Sicherheitsniveau von Online-Dienstleistungen transparenter machen. In Selbstregulierung könnten die Internetdienstleister über Sicherheitszertifikate das Vertrauen der Verbraucher in das Internet erhöhen.

– Im Bereich der Wirtschaft und ebenso aufgrund der föderalen Struktur in den deutschen Verwaltungen haben **Empfehlungen** zur IT-Sicherheit einen hohen Durchdringungs- und Verbreitungsgrad. Ursache hierfür sind die Praxisnähe, der Zeitfaktor und die formale Unverbindlichkeit von Empfehlungen. Ein geschicktes Marketing durch die Implementation in Pilotverfahren, durch das Publizieren von beispielhaften Lösungen (Best Practise) sowie durch gemeinsame Initiativen von Wirtschaft und Verwaltung (Public Private Partnership) können Empfehlungen eine hohe Verbreitung und breite Akzeptanz verschaffen.

Aktionsplan zur Umsetzung von BundOnline 2005

Regulativer Rahmen

– SigG und BDSG wurden im Jahre 2001 novelliert. Aufgrund der Gleichstellung der elektronischen mit der manuellen Unterschrift müssen in Folge auch weitere Gesetze und Verordnungen novelliert werden. Moderne Sicherheitstechnologien (z. B. Signaturverfahren), versehen mit Sicherheitszertifikaten bzw. -bestätigungen sollen in der Umsetzung den Schutz der Internetnutzer sowie den Anspruch an Rechtssicherheit – insbesondere bei Transaktionen über das Netz – gewährleisten.

Selbstregulierung

– Im Online-Sektor sollte Selbstregulierung die Gesetzgebung ergänzen. So bietet sich u.a. die Festlegung von Schnittstellen des elektronischen Geschäftsverkehrs zwischen Wirtschaft und Verwaltung für Vereinbarungen unterhalb gesetzlicher Regelungen an.

  Der Aufbau einer Public Key Infrastruktur für elektronische Signaturen und Verschlüsselung ist eine der zentralen Herausforderungen in der Realisierung des E-Governments, um innerhalb der Verwaltung sowie mit der Wirtschaft und den Bürgern formgebundene und inhaltlich sensitive Nachrichten sicher zu kommunizieren. Zwingende Voraussetzung für die sichere Kommunikation über das Internet ist die Interoperabilität der eingesetzten Sicherheitsprodukte und -systeme. Die Definition von entsprechenden Interoperabilitätsstandards wie beispielsweise ISIS-MTT für den Bereich der Elektronischen Signaturen kann nicht von staatlichen Stellen vorgegeben werden, sondern obliegt den einschlägigen Herstellerverbänden. Die Selbstregulierung der Interoperabilität durch die Hersteller sichert den Wettbewerb der Produkte auf dem Markt sowie deren innovative Weiterentwicklung für die Zukunft.

– Einen Beitrag zur Vertrauensbildung im Internet kann auch die Einführung von Sicherheitszertifikaten für Internetangebote darstellen. Analog zu dem Ansatz von Gütesiegeln (Trustmarks), die Qualitätsaussagen von Internetangeboten auf der Grundlage klar definierter Qualitätskriterien bestätigen, können auch Sicherheitszertifikate das erreichte Sicherheitsniveau im Internet transparenter machen und so das Vertrauen auf Seiten des Bürgers erhöhen. Hierzu hat das BSI im Frühjahr 2002 auf Basis des IT-Grundschutz-Handbuches ein Qualifizierungs- und Zertifizierungsschema veröffentlicht. Damit können grundsätzlich auch für Internetangebote Sicherheitszertifikate vergeben werden. Es wird angestrebt, gemeinsam mit den Dienstleistern im Bereich der Internet-Wirtschaft auf der Basis des IT-Grundschutzes und der Common Criteria so genannte Schutzprofile zu entwickeln, die das Sicherheitsniveau für die Vergabe von Sicherheitszertifikaten definieren. Die Entscheidung, ein Zertifizierungsverfahren in Selbstverpflichtung einzuführen, bleibt den Internetserviceprovidern in Eigenverantwortung überlassen.

Empfehlungen

– Zur Unterstützung des Programms BundOnline 2005 veröffentlicht das BSI ein E-Government-Handbuch. Das Handbuch präsentiert verschiedene Themen als eigenständige Module, ergänzt um nützliche Werkzeuge. Die gesammelten Empfehlungen aus der Beratungspraxis sollen nicht reglementieren, sondern werden als arbeitsökonomisches Hilfsmittel angeboten. Sie sollen den Behörden bei der Einführung von internetbasierten Verwaltungsdienstleistungen unterstützen und insbesondere Empfehlungen und Hinweise für die Implementierung der erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen geben. Das Handbuch bietet auch eine Plattform für die Darstellung von Modellprojekten als Best Practise. Beispiele für E-Government-Modellprojekte sind die Projekte E-Vergabe und Digitaler Dienstausweis.
– Public private Partnerships sind geeignete Instrumente, um die Nutzung und Akzeptanz des Internets in Gesellschaft und Verwaltung voranzutreiben. Ein Beispiel für das gemeinsame Engagement von Staat und Wirtschaft ist die Initiative D21, die inzwischen von mehr als 130 Unternehmen unterstützt wird. Gemeinsam mit der Bundesregierung werden hier Konzepte für den Übergang in die Informationsgesellschaft erarbeitet und umgesetzt. In der Arbeitsgruppe 5 »Sicherheit im Internet« der Initiative D21 wurden zu diesem Zweck vier Projektgruppen mit Experten aus Wirtschaft und Verwaltung eingerichtet. Die in den Projektgruppen erzielten Arbeitsergebnisse werden als Empfehlungen im Rahmen der Informationskampagnen von D21 publiziert. Im Einzelnen haben die Projektgruppen folgende Empfehlungen erarbeitet:
  – Zum Aufbau so genannter Computer Emergency Response Teams, deren Aufgabe es ist, auf Schwachstellen hinzuweisen und vor Angriffen aus dem Internet zu warnen,

- zum Aufbau und Ausbau von übergreifenden Public-Key-Infrastrukturen, die gemeinsam von Wirtschaft und Verwaltung genutzt werden können,
- zum Einsatz von Chipkarten als Träger von Sicherheitsmechanismen und
- zur Anwendung geeigneter IT-Sicherheitskriterien für die Erstellung von Sicherheitskonzepten; hierzu wurde ein Leitfaden erstellt.

Mit den Sicherheitsempfehlungen sollen nicht nur Spezialisten, sondern auch Führungskräfte angesprochen werden. Ausgehend von Umfragen, die besagen, dass drei Viertel aller deutschen Unternehmen ihre E-Business-Strategie durch mangelnde IT-Sicherheit bedroht sehen, muss über Aufklärung und Sensibilisierung ein Bewusstsein dafür gestärkt werden, dass Sicherheitslösungen keinen Luxus, sondern einen Erfolgsfaktor bei der Einführung digitaler Dienstleistungen darstellen.

Schlussfolgerung:

Aus den oben dargestellten Beispielen lassen sich einige Grundprinzipien ableiten, an welchen Stellen Bürger, Unternehmen bzw. Behörden Regelungen für die IT-Sicherheit benötigen, wo das Instrument der Selbstregulierung besser greift und wo Empfehlungen besser geeignet erscheinen:

- Gesetzliche Regelungen sind erforderlich für den Rechtsrahmen zum Schutz der Internetnutzer sowie zur Rechtssicherheit von elektronischen Transaktionen.
- Rechtliche Regelungen sollten technikneutral und entwicklungsoffen formuliert werden.
- Initiativen zur Selbstregulierung des Internets sind in den Bereichen sinnvoll, in denen staatliche Regulierung nicht notwendig oder nicht möglich ist. So kann die Einführung von Sicherheitszertifikaten für Internetangebote (analog zu Gütesiegeln in Bezug auf die Qualität von Internetangeboten) ein Weg sein, über den das Vertrauen der Bürger in die Sicherheit von Online-Dienstleistungen nachhaltig erhöht werden kann.
- Empfehlungen sind ein sehr erfolgversprechender Ansatz zur Erhöhung der IT-Sicherheit, wenn es um die Festlegung von Standards, den Aufbau von Sicherheitsinfrastrukturen (z. B. CERT) sowie um die Implementation von IT-Sicherheit in Anwendungen insbesondere unter engen Zeitvorgaben geht. Public Private Partnerships sind geeignete Instrumente, um Empfehlungen eine breite Akzeptanz zu verschaffen und somit das Vertrauen in die sichere Nutzung des Internets in Gesellschaft und Verwaltung zu fördern.