ARBEITSPAPIERE

aus der Begleitforschung zum Städtewettbewerb Multimedia *MEDIA*@Komm

MEDIA @Komm

5/2001

E-Government – Grundlegende Aufgaben der Kommunen aus sicherheitstechnischer Sicht

Roland Krüger/Berthold Weghaus

TÜV Informationstechnik GmbH (TÜViT)

Stand: August 2001

Herausgeber: Deutsches Institut für Urbanistik

Impressum

Autoren
Roland Krüger/Berthold Weghaus
TÜV Informationstechnik GmbH (TÜViT)

Redaktion
Klaus-Dieter Beißwenger
Uwe Krüger

Textverarbeitung und Layout
Christina Blödorn

Deutsches Institut für Urbanistik
Straße des 17. Juni 110
10623 Berlin

Telefon: (030) 39001-0
Telefax: (030) 39001-100
E-Mail: difu@difu.de
Internet:http://www.difu.de

Schutzgebühr Euro 7,50/DM 15,–

Berlin, August 2001

Inhalt

1. Grundlagen: Nutzung von EDV und Internet durch die Verwaltungen

Noch vor wenigen Jahren waren jene Kommunen in der kommunalen Landschaft Vorreiter, die ein Angebot im Internet bereitstellten, das den Besuchern der Seiten wie eine Visitenkarte mehr oder weniger umfangreiche und qualifizierte Informationen bot. Aus sicherheitstechnischer Sicht lässt sich ein solches Internetangebot leicht realisieren. Auf einem Stand-alone-System können die Informationen für Bürgerinnen und Bürger bereitgestellt werden. Die Risiken, die hier bedacht werden müssen, sind nur gering. So kann es zu Angriffen auf die Verfügbarkeit des Dienstangebots kommen oder im schlimmsten Fall zu einer Veränderung der dargestellten Inhalte. Hier helfen einfache technische Schutzmaßnahmen, aber auch die simple Kontrolle der dargestellten Informationen – wie sie zum Teil schon aus Aktualisierungsgründen stattfinden wird – weiter. Eine Gefahr für die IT-Infrastruktur der Kommunen besteht nicht. Auch eine Gefährdung des Bürgers ist nicht zu vermuten, schlimmstenfalls steht dieser z.B. vor einem geschlossenen Hallenbad.

Neben der Erwartung an aktuelle und umfassende Online-Informationen im Internet werden in der (Fach-)Öffentlichkeit mittlerweile auch die Nutzung von Online-Kommunikation und Online-Transaktionen mit dem „Elektronischen Rathaus“ diskutiert und zunehmend für selbstverständlich erachtet. So muss etwa im Verhältnis von Unternehmen und Wirtschaft zur Verwaltung einer Kommune das qualifizierte und umfassende Online-Dienstleistungsangebot als ein neuer Standortfaktor angesehen werden. Die Risiken wachsen hier mit den technischen Möglichkeiten: Die Erweiterung der kommunalen Angebote im Netz in Richtung Kommunikation und Transaktion setzt die Anbindung an die verwaltungsinternen Geschäftsprozesse, Datenstrukturen und die IT-Infrastruktur voraus. Dabei entwickelte sich die Infrastruktur aus Computern und deren Vernetzungen in den vergangenen zwanzig Jahren aber weder einheitlich noch strategisch geplant, sondern in Etappen am jeweiligen Bedarf und am aktuellen Stand der Technik orientiert. Dies führte zu einem Durcheinander aus verschiedenen Rechnern und Programmanwendungen: sehr viel Großrechnerarchitektur aus der Anfangszeit der Datenverarbeitung hier, eine wachsende Anzahl neuerer PC-Anwendungen dort, die nicht miteinander kommunizieren können.

So haben sich vor allem im letzten Jahrzehnt durch den rasanten Fortschritt bei den IuK-Technologien erhebliche Herausforderungen für die Verantwortlichen in den Kommunalverwaltungen ergeben (vgl. Übersicht).

Übersicht: Trends des IuK-Einsatzes in der Verwaltung*

Von ...	... hin zu
Großrechnern, Abteilungsrechnern	Client-/Server-Systemen
Isolierten Fachanwendungen, getrennten Großanwendungen	verbundenen Anwendungen, integrierten Anwendungssystemen
starren Textmasken	graphischen, intuitiven Oberflächen
Prozeduralen Programmen	objektorientierten Programmen
Hierarchischen Datenbanken	relationalen Datenbanken
Eigenentwicklungen	individuellen Anpassungen von Standard-software
proprietären Systemen (Anbietermarkt)	offenen Systemen (Käufermarkt)
lokalen, monomedialen Daten	ubiquitären, multimedialen Daten
Flickenteppich von Daten	geordneten und abgestimmten Datenstruktu-ren
angelerntem EDV-Personal	hochqualifizierten Experten
Expertenzentrierter Softwareentwicklung	Modellierungsmethoden unter Einbeziehung von Anwendern
Anwendungssoftware mit hohem Wartungs-aufwand und tendenzieller Veränderungsre-sistenz	flexibel an geänderte Benutzeranforderun-gen angepasster IuK-Unterstützung

*Quelle: Zusammenstellung des Deutschen Instituts für Urbanistik nach *Heinrich Reinermann*, Entscheidungshilfen und Datenverarbeitung, in: Klaus König und Heinrich Siedentopf (Hrsg.), Öffentliche Verwaltung in Deutschland, Baden-Baden 1997, S. 477-496, hier: S. 492 f.

Diese technologischen Veränderungstendenzen fallen mit den Anforderungen der Kommunen im Hinblick auf das Angebot von Online-Dienstleistungen der Verwaltung zusammen und führen zu einer Vielzahl von offenen Fragen und notwendigen neuen Lösungskonzepten. So ergeben sich etwa beim Anschluss eines behördeninternen Intranets an das Internet über ein kommunales Portal in technischer und sicherheitstechnischer Hinsicht eine Vielzahl neuer Aufgaben, verbunden mit einer Reihe von Problemen.

Technik allein stellt aber noch kein Vertrauen her – Vertrauen als Voraussetzung für die Akzeptanz durch die Bürgerinnen und Bürger. Auch Recht allein bietet keinen realen Schutz für eine vertrauenswürdige Kommunikation. Vertrauensbildung ist ein komplexer gesellschaftlicher Entwicklungsprozess. Die IT-Sicherheit bildet hierin einen wichtigen vertrauensbildenden Faktor.[1]

1 http://www.europaeische-akademie-aw.de/projecte/digur.html. Die Europäische Akademie wurde am 11. März 1996 gegründet und hat die Rechtsform einer gemeinnützigen Gesellschaft mit beschränkter Haftung. Gesellschafter sind das Land Rheinland-Pfalz und das Deutsche Zentrum für Luft- und Raumfahrt e.V. (DLR). Geschäftsführer der Gesellschaft und Direktor der Europäischen Akademie ist

Für die in der Kommune bislang auch schon digitalisiert bearbeiteten und archivierten Informationen sowie die wünschenswerten Kommunikationen und Transaktionen gelten aus rechtlicher und sicherheitstechnischer Sicht die gleichen Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit, wie sie auch ansonsten im Alltag an Informationsangebote, Verwaltungsverfahren, Zahlungs- und Geschäftsprozesse gestellt werden.

Durch den Einsatz neuer Medien und vernetzter IuK-Techniken sind neue Formen der Verletzlichkeit oder Verwundbarkeit unserer hochentwickelten Dienstleistungsgesellschaft entstanden, denn IT-Systeme können über Schwachstellen vorsätzlich und gezielt angegriffen werden. Sie sind Ziele der Wirtschafts- und Konkurrenzspionage. Gezielte Angriffe auf informationsverarbeitende Systeme können auch zur Durchsetzung von wirtschaftlichen und politischen Interessen genutzt werden. Aber auch einfache Unkenntnis oder Sorglosigkeit – sowohl auf Betreiber- als auch auf Benutzerseite – können zu Schwachstellen und unkalkulierbaren Risiken führen. Die Anbindung an das Internet und die weltweit voranschreitende Vernetzung der Rechner- und Computersysteme potenzieren diese Risiken. Heute ist es praktisch von jedem Punkt der Erde möglich, über Schwachstellen in der Informationstechnik mit mehr oder minder großem Aufwand gezielt in IT-gestützte Systeme einzudringen, diese auszuspähen, zu manipulieren, zu stören oder auszuschalten. Die IT-Sicherheit entwickelt sich so gesehen zu einer wichtigen wirtschaftspolitischen Herausforderung und zu einem Eckpunkt einer zukunftsorientierten Sicherheitspolitik.

Weltweit wird die IT-Sicherheit als Begriff noch nicht einheitlich verstanden und in der Praxis oft widersprüchlich umgesetzt. Das heutige Bild ist – mit einigen lobenswerten Ausnahmen – immer noch von dem Einsatz einzelner Sicherheitsmaßnahmen geprägt, die zwar von der Verschlüsselung von Mails bis zum Einsatz von Firewalls reichen, jedoch in dieser Form (isoliert voneinander) nicht die Vorteile eines konsequenten, verwaltungsweiten Sicherheitsmanagements bieten können.

Besonders kritisch zeigt sich in der Praxis die Situation in den Kommunen, die aus unterschiedlichen Gründen bisher kaum Sicherheitsanalysen durchführen und teilweise nicht einmal über eine Strategie zur Erreichung der internen IT-Sicherheit verfügen. Nicht selten stellt sich hier Resignation, ein oder es werden für relativ viel Geld einzelne Sicherheitslösungen in Form von Hard- und/oder Software angeschafft, die eigentlich die viel komplexeren und zum Teil auf anderen Ebenen angesiedelten Sicherheitsprobleme der Verwaltung nicht lösen können und insgesamt unbefriedigend sind. Immer noch trifft man in der Praxis auf Verantwortliche, die erst aufgrund der Jahr-2000-Diskussion oder aktueller Virenwarnungen wie vor „love-letter“ auf die IT-Sicherheitsproblematik aufmerksam geworden sind; sie würden nun gerne einiges in dieser Richtung tun, doch sie haben den Eindruck, damit fachlich und auch finanziell überfordert zu sein. Es fehlt der gangbare Weg. Nicht alle Bereiche sind hochsensibel. Es fehlt eine Basis, auf die gegebenenfalls Speziallösungen für einzelne sicherheitskritische Transaktionen aufsetzen können. Die im Rahmen des *MEDIA@*Komm-Projekts[2] geplanten Online-Dienstleistungen der Kommunen sind allerdings gerade solche Internet-

---

Professor Dr. phil. Carl Friedrich Gethmann. Das Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie beteiligt sich an der Finanzierung im Rahmen seiner Projektförderung.

2 http://www.mediakomm.net

Transaktionen, die über das bisher übliche Informationsangebot der Kommunen – insbesondere aus sicherheitstechnischer Sicht – weit hinausgehen.

Zunächst gilt es für die Kommunen ihr bereits bestehendes Intranet abzusichern, bevor ein verantwortungsbewusster Anschluss des Intranets über definierte und kontrollierbare Zugangsmöglichkeiten an das Internet zugelassen werden kann. Eine IT-Grundabsicherung des Intranets ist die notwendige Voraussetzung für den Start in ein beherrschbares E-Government. Um eine IT-Grundabsicherung zu koordinieren und überschaubar zu halten, ist zunächst ein IT-Sicherheitsbeauftragter zu bestimmen, in dessen Verantwortung die Planungsmaßnahmen einschließlich der Ressourcenplanung, die Umsetzung einschließlich der Umsetzungskontrolle und die Fortschreibung des IT-Grundschutzes liegen. Eine Koordination und Zusammenarbeit mit den Datenschutzbeauftragten wird dringend empfohlen.

Die Basis jeder Entscheidungsfindung im Bereich IT-Sicherheit ist zunächst die Ist-Analyse der IT-Infrastruktur. Leider sind – vor allem im kommunalen Bereich – hier im Allgemeinen die ersten Defizite zu finden. Die einzelnen Verwaltungseinheiten haben sich IT-technisch gesehen oft isoliert voneinander aufgabenbezogen entwickelt. Solche heterogenen IT-Systeme werden dann mit der Zeit auch aufgabenübergreifend untereinander vernetzt. Hier gilt es sich zunächst einen Überblick zu verschaffen und Einzelverantwortlichkeiten zu koordinieren.

Für die anschließende Basisabsicherung der identifizierten und dokumentierten IT-Infrastruktur der einzelnen Kommune und den nachfolgenden Anschluss des Behördennetzes an das Internet gibt es zahlreiche Modellbeispiele und Orientierungshilfen, auf die zurückgegriffen werden kann. Als Minimalanforderung ist hier sicherlich – insbesondere für die öffentliche Verwaltung – der IT-Grundschutz nach dem Grundschutzhandbuch[3] des Bundesamtes für Sicherheit in der Informationstechnik (BSI)[4] anzusehen.

2. Einführung in den IT-Grundschutz

2.1 Hintergrund

Die Bundesverwaltung ist seit Jahren gehalten, im Zusammenhang mit IT-Rahmenkonzepten auch IT-Sicherheitskonzepte zu erstellen. Anfänglich wurden auch für eine Grundabsicherung IT-Sicherheitskonzepte anhand einer Risikoanalyse, zum Beispiel nach dem IT-Sicherheitshandbuch, erstellt. Zur Reduzierung des Aufwands und zur Optimierung der Ergebnisse wurden begleitende Schulungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) durchgeführt und Vereinfachungsansätze zur Risikoanalyse veröffentlicht.

Die Vielzahl und Vielfalt der Behörden, die ein IT-Sicherheitskonzept erstellen müssen, stellt einen repräsentativen Querschnitt von IT-Anwendern dar, aus dem man ableiten kann, dass effektive und aussagekräftige IT-Sicherheitskonzepte auf Basis von Risikoanalysen praktisch nur von erfahrenen IT-Sicherheitsfachleuten erarbeitet werden kön-

3 http://www.bsi.de/gshb/deutsch/menue.htm.
4 http://www.bsi.de/.

nen. Vor diesem Hintergrund wurde versucht, die Erstellung von IT-Sicherheitskonzepten zu vereinfachen, ohne die Qualität einzuschränken. Die Idee des IT-Grundschutzes war geboren.

Der Aufwand für IT-Sicherheitskonzepte sollte auf die hochschutzbedürftigen IT-Systeme konzentriert werden, indem für mittelschutzbedürftige IT-Systeme ein standardisiertes Verfahren, eben der IT-Grundschutz, eingesetzt wird. Ein Beispiel für die Anwendbarkeit des IT-Grundschutzes ist sicherlich die Grundabsicherung des Intranets der Kommunen als Ausgangsbasis für den Anschluss der Verwaltung an das Internet. Nachdem ein solcher IT-Grundschutz installiert ist, ist ein verantwortungsvoller Start ins E-Government möglich.

2.2 Ziel des IT-Grundschutzes

Ziel des IT-Grundschutzes ist es, durch geeignete Anwendung von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen ein Sicherheitsniveau für IT-Systeme zu erreichen, das für den mittleren Schutzbedarf angemessen und ausreichend ist und als Basis für hochschutzbedürftige IT-Anwendungen dienen kann. Solche

- infrastrukturellen,
- organisatorischen,
- personellen und
- technischen

IT-Sicherheitsmaßnahmen für eine Reihe von typischen IT-Systemen und Einsatzumgebungen werden in einem Regelwerk gebündelt.

Nach durchgeführter Ist-Aufnahme der IT-Infrastruktur muss der Anwender des entsprechenden Regelwerkes nur noch einen Soll-Ist-Vergleich durchführen, um fehlende IT-Sicherheitsmaßnahmen zu identifizieren. Da für jede einzelne Maßnahme auch Realisierungsvorschläge von IT-Experten ausgearbeitet wurden, ist die Umsetzung der IT-Grundschutzmaßnahmen kurzfristig möglich, zumal für den mittleren Schutzbedarf kostspielige Maßnahmen kaum benötigt werden.

IT-Grundschutz wird somit zu einer gemeinsamen Verständigungsbasis für Maßnahmen des mittleren Schutzbedarfs.

2.3 Grenzen des IT-Grundschutzes

Die für den IT-Grundschutz statthaften pauschalen Ansätze von Maßnahmenempfehlungen reichen jedoch nicht ohne weiteres für hochschutzbedürftige IT-Systeme aus. Systeme geringeren Schutzbedarfs sind häufig solche Systeme, die reinen Informationscharakter besitzen, eventuell zusätzlich auch eine Kommunikation über Rückmeldungen erlauben. Sensible Systeme sind zumeist im Bereich von Transaktionen zu finden, wie sie typischerweise im E-Commerce oder im Umfeld digitaler Signaturen auftreten.

In solchen Fällen erzielen individuelle Sicherheitsuntersuchungen detaillierte Ergebnisse, insbesondere hinsichtlich der Auswahl geeigneter Sicherheitsmaßnahmen unter Beachtung von Kosten- und Wirksamkeitsaspekten. Solche Analysen können über die IT-Grundschutzmaßnahmen hinaus zusätzliche oder qualitativ wirksamere Maßnahmen herausarbeiten. Grundsätzlich kann bei hochschutzbedürftigen IT-Anwendungen neben der Realisierung des IT-Grundschutzes auf individuelle Sicherheitsuntersuchungen nicht verzichtet werden.

2.4 Dynamik des IT-Sicherheitsprozesses

Das einmalige Erstellen eines IT-Sicherheitskonzepts, auch auf der Basis von IT-Grundschutz-Betrachtungen, ist für eine umfassende IT-Sicherheit nicht ausreichend. Vielmehr ist es erforderlich, den IT-Sicherheitsprozess durch einen Regelkreislauf bestehend aus der Konzeption, der Realisierung und der Kontrolle von IT-Sicherheitsmaßnahmen zu gestalten.

Diese Aufgabe ist von fundamentaler Bedeutung und muss durch den Dienstanbieter initiiert werden.

2.5 Schutzbedarfsfeststellung

Entscheidend für die Anwendbarkeit unterschiedlicher Strategien ist eine vorab durchzuführende Schutzbedarfsfeststellung, um so jene Bereiche zu identifizieren, in denen der IT-Grundschutz vollkommen ausreicht und auf aufwendige Risikoanalysen verzichtet werden kann. Bei der Schutzbedarfsfeststellung hat sich ein 5-Stufenkonzept für die Datenklassifizierung als effizient erwiesen und etabliert.

2.5.1 5-Stufenkonzept

Verwaltungsdaten – insbesondere personenbezogene Daten – werden nach dem Grad möglicher Beeinträchtigung schutzwürdiger Belange bei Missbrauch dieser Daten in fünf Schutzstufen untergliedert. Bei der Klassifizierung sind Datenfelder niemals einzeln zu bewerten. Die Betrachtung ist vielmehr auf die gesamte Datenstruktur, gegebenenfalls auf ein gesamtes IT-System, auszudehnen. Werden Daten unter einem Auswahlkriterium aufgenommen, das in der Datenstruktur nicht enthalten ist, so ist dieses Auswahlkriterium bei der Klassifizierung mit zu bewerten. Enthalten Datenstrukturen umfassende Angaben, z.B. zu einer Person (Dossiers), so sind sie in eine höhere Schutzstufe einzuordnen, als dies nach den Einzeldaten erforderlich wäre.

Es werden folgende Schutzstufen unterschieden:

- Stufe A:
  Frei zugängliche Daten, in die Einsicht gewährt wird, ohne dass der Einsichtnehmende ein berechtigtes Interesse geltend machen muss, z.B. Adressbücher, Mitgliederverzeichnisse, Benutzerkataloge in Bibliotheken.

- Stufe B:
  Personenbezogene oder verwaltungsinterne Daten, deren Missbrauch zwar keine besondere Beeinträchtigung erwarten lässt, deren Kenntnisnahme jedoch an ein berechtigtes Interesse des Einsichtnehmenden gebunden ist, z.B. beschränkt zugängliche öffentliche Dateien, Verteiler für Unterlagen.

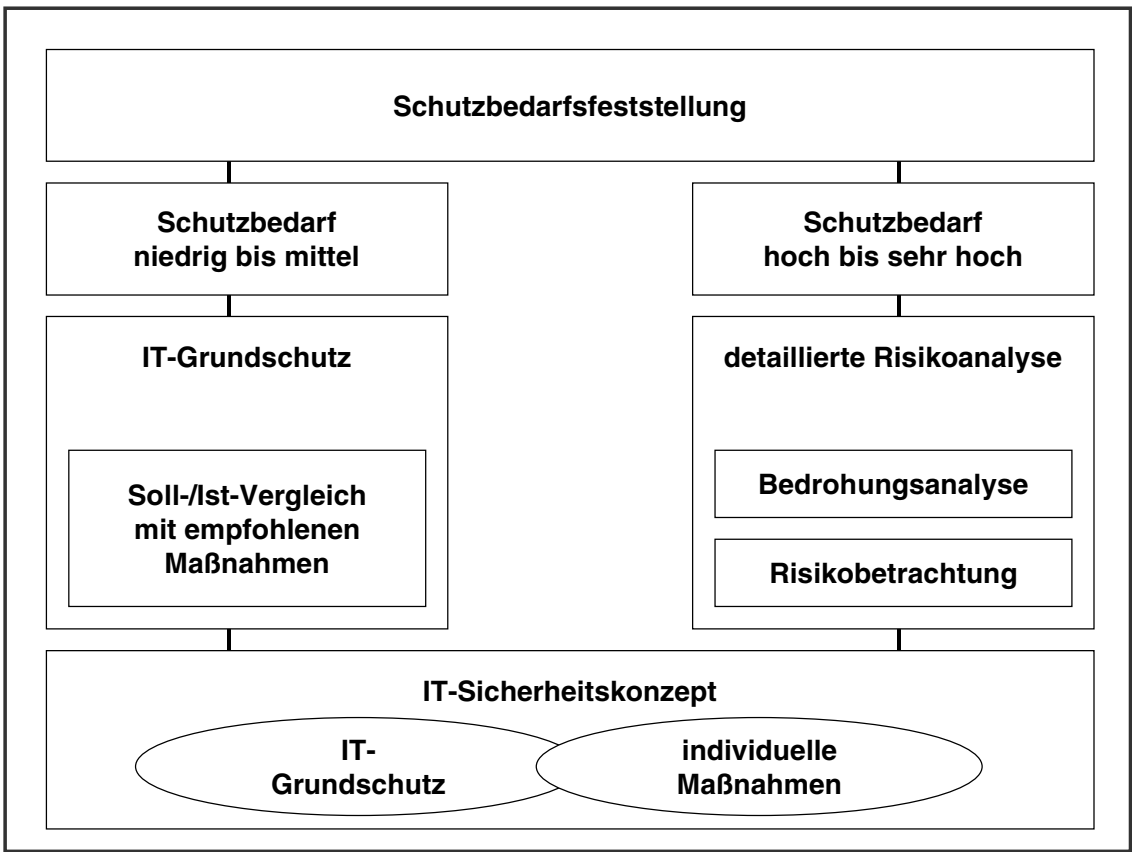
- Stufe C:
  Personenbezogene oder verwaltungsinterne Daten, deren Missbrauch den Betroffenen – sei es eine Einzelperson oder die Verwaltung insgesamt – in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann („Ansehen“), z.B. Daten zu Einkommen, Sozialleistungen, Grundsteuer, Ordnungswidrigkeiten.

- Stufe D:
  Personenbezogene Daten oder verwaltungsinterne Daten, deren Missbrauch die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen („Existenz“) oder einzelne Verwaltungsabläufe erheblich beeinträchtigen kann, z.B. Daten zu Unterbringung in Anstalten, Straffälligkeit, Ordnungswidrigkeiten schwerwiegender Art, dienstlichen Beurteilungen, psychologisch-medizinischen Untersuchungsergebnissen, Schulden, Pfändungen, Konkursen, Verfolgung von Straftaten, wesentlichen Finanztransaktionen der Verwaltung.

- Stufe E:
  Daten, deren Missbrauch Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen kann, z.B. Daten über Personen, die mögliche Opfer einer strafbaren Handlung sein können oder Daten, die die Verwaltungstätigkeit insgesamt infrage stellen.

Falls die Sensitivität nicht bekannt ist, ist von der höchsten Sensitivitätsstufe auszugehen. Insbesondere für die höheren Schutzstufen (D bis E) sind Risikoanalysen notwendig. Die Methode IT-Grundschutz ist nicht geeignet für solche Risikoanalysen, insbesondere nicht für Risikoanalysen in sicherheitstechnisch sensiblen Bereichen. Das Ziel der Methode ist letztlich die Vermeidung solcher Analysen für den mittleren Schutzbedarf, das heißt, falls ausschließlich Daten der Stufen A bis B und gegebenenfalls der Stufe C betroffen sind.

Abbildung: Schutzbedarfsfeststellung*



*Quelle: Eigene Ausarbeitung in Anlehnung an die Definitionen des BSI (vgl. hierzu IT-Grundschutzhandbuch 1997; http://www.bsi.de/gshb/deutsch/menue.htm).

Je stärker das Bedrohungsbild von den Standard-Bedrohungen abweicht, desto größer wird der individuelle Schutzbedarf. Zur Deckung dieses erhöhten Bedarfs (bei E-Commerce, Online-Dienstleistungen der Verwaltung unter Nutzung der digitalen Signatur) existieren IT-Dienstleister, die durch weitere Maßnahmen (Sicherheitsanalysen, Sicherheitstechnische Qualifizierung, Prüfungen, Validierungen, Evaluationen usw.) anderen Sicherheitsrisiken vorbeugen, Risiken diagnostizieren und auch Lösungen anbieten.

Die – wenn auch so wichtige – präventive Funktion des IT-Grundschutzes hat zudem einen wichtigen Nebeneffekt: die Erhöhung der Effektivität und insbesondere der Wirtschaftlichkeit der IT-Sicherheit. Denn es ist umso leichter, sicherer und auch wirtschaftlicher, individuelle Sicherheitsmaßnahmen festzulegen, je besser und stabiler der Grundschutz funktioniert.

So empfiehlt sich der IT-Grundschutz als wesentlicher Grundbaustein für jede systematische IT-Sicherheitsinitiative.

2.6 Kosten-Nutzenargumentation

In der Bestimmung des IT-Sicherheitsniveaus für eine Kommune spielt das Kosten/ Nutzen-Verhältnis eine entscheidende Rolle. Es ist hier wichtig zu beachten, dass das gewählte Schutzniveau des IT-Systems zur Realisierung des „elektronischen Rathauses“ nur mit einem entsprechenden Aufwand zu erreichen ist.

Die Implementierung von Grundschutz-Maßnahmen bietet ein hervorragendes Kosten/ Nutzen-Verhältnis. Wo reine Information oder Kommunikation eine Rolle spielt, reicht der IT-Grundschutz in der Regel vollkommen aus. Für sensible Bereiche des E-Commerce oder der Anwendung der digitalen Signatur muss aber stets im Einzelfall überprüft werden, ob hier – insbesondere bei Transaktionen – der IT-Grundschutz ausreicht, zumal zum einen durch das Signaturgesetz ein hoher Schutzbedarf bei der digitalen Signatur festgeschrieben ist, zum anderen auch die Bundesregierung – in Übereinstimmung mit der Arbeitsgemeinschaft der Verbraucherverbände und weiten Teilen der Wirtschaft – der Überzeugung ist, dass ein ausreichend hohes Sicherheitsniveau der digitalen Signatur Voraussetzung für die angestrebte Rechtssicherheit ist und dass das Vertrauen der Verbraucher und Nutzer der digitalen Signatur gefährdet würde, wenn Rechtsfolgen an unsichere Signaturen geknüpft wären.[5]

Als Anleitung zur Schaffung einer geeigneten Grundabsicherung dient das Grundschutzhandbuch, das über das BSI bezogen werden kann. Daneben bietet das BSI auch ein rechnergestütztes Tool an, das die Handhabung des Grundschutzhandbuches erleichtert und die Ergebnisse strukturiert präsentiert. Weiter hat der Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sich mit dem Anschluss von Netzen der öffentlichen Verwaltung an das Internet befasst und eine Orientierungshilfe zu Datenschutzfragen erarbeitet, die online[6] im Internet verfügbar ist. Alle diese Empfehlungen und Maßnahmen müssen allerdings auch technisch umgesetzt werden. Auch hierzu gibt es qualifizierte Anleitungen im Internet. Als gelungenes Beispiel sei hier der Leitfaden zur Absicherung von Rechnersystemen innerhalb des Deutschen Forschungsnetzes genannt, der in aktueller Fassung online verfügbar ist. Zahlreiche Checklisten der Landesdatenschutzbeauftragten ergänzen dieses Online-Angebot und können sowohl bei der Ist-Analyse als auch bei den Umsetzungsprüfungen wichtige Hilfestellungen bieten. Insbesondere über die Internetadresse http://www.datenschutz.de kann auf ein umfangreiches Informations- und Hilfeangebot zurückgegriffen werden. Hier werden sowohl technische als auch datenschutzrechtliche Aspekte kompetent behandelt.

Der IT-Grundschutz findet seine effiziente Anwendung in Standardsituationen. Die Situation in den Kommunen ist – was die technische Ausstattung anbelangt – allerdings häufig sehr heterogen. Oftmals sind Altsysteme integriert und werden erst nach und nach ersetzt. Es sei nochmals auf die Notwendigkeit einer sorgfältigen und dokumentierten Ist-Analyse der IT-Infrastruktur hingewiesen.

Ein komplexes und heterogenes IT-System kann aber nur sicher funktionieren, wenn Systemverwalter und Benutzer es beherrschen und sich ihrer Verantwortlichkeiten be-

---

5 http://www.datenschutz-berlin.de/jahresbe/99/doc/181_2.htm#ciii
http://www.uni-kassel.de/fb10/oeff_recht/publikationen/MMR8-00.pdf.

6 http://www.datenschutz-berlin.de/to/vnetz/index.htm.

wusst sind. Wichtig ist im Zusammenhang mit E-Government, dass sowohl der Verwaltungsbeamte in der Kommune als auch der Bürger an seinem Heim-PC als Benutzer des kommunalen IT-Systems in den Blick genommen werden. Auch hier bieten die Landesdatenschutzbeauftragten Hilfen für den Systemverwalter, den Benutzer in der kommunalen Einrichtung und für die Bürgerinnen und Bürger, die über das Internet mit den Kommunen kommunizieren.

Die neuen Medien, insbesondere die Nutzung neuer Dienste via Internet, bieten aus technischer Sicht eine Vielzahl neuer Gestaltungsmöglichkeiten. Ebenso wie in der Bio- oder Gentechnik ist auch in der Informationstechnik stets abzuwägen, welche Verfahren – rechtlich und ethisch – vertretbar sind. Ein Wirtschaftsunternehmen wird zunächst unter wirtschaftlichen und rechtlichen Gesichtspunkten eine Auswahl geeigneter informationstechnischer Dienstleitungen für seine Kundinnen und Kunden auswählen. Der Schutz des Kunden ist zunächst nur aus wirtschaftlichen Eigeninteressen und als Maßnahme gegen eine mögliche Imageschädigung relevant. Diese Interessenlage ist auch für die Kommunen gegeben. Über diese Entscheidungsfaktoren hinaus stellt sich die Situation für die Kommunen aber komplexer dar. Die Kommune ist nicht ein rein gewinnorientiertes Unternehmen, sondern vielmehr ist ihre Hauptaufgabe – selbstverständlich unter Kosten-Nutzenanalysen – die Bereitstellung einer effizienten und funktionierenden Verwaltung, die dem einzelnen Bürger das geordnete Leben innerhalb des Staatssystems ermöglicht und erleichtert. Die Kommunen sind weder Selbstzweck, noch dienen sie der Gewinnoptimierung. Daher wird neben der Kostenreduzierung und Effizienzsteigerung der Verwaltung durch den Einsatz von informationstechnischen Hilfsmitteln insbesondere das *elektronische Rathaus* als *Dienstleistungsangebot* für den Bürger und als Standortvorteil für die Kommune gesehen. Eine Dienstleistung als Hilfe und Angebot für den Bürger impliziert, dass der Bürger durch dieses Angebot einen Vorteil hat. Daher darf ein Zusatzangebot für den Bürger nicht zu dessen Schaden gereichen. Das virtuelle Rathaus ist insgesamt eine Chance für Verwaltung und Bürger; es muss von den Kommunen sorgfältig geplant und umgesetzt werden, sodass die gesteckten Ziele auch erreicht werden. Die möglichen Gefahren für den Bürger durch den Einsatz neuer informationstechnischer Medien müssen dazu im Vorfeld abgeschätzt werden – geeignete sicherheitstechnische Maßnahmen müssen gewählt werden. Diese Aufgaben für eine verantwortungsbewusste und vertrauenswürdige Einführung von E-Government werden im Weiteren zusammengefasst mit Sorgfaltspflicht bezeichnet. Die Sorgfaltspflicht des Staates gegenüber seinen Bürgerinnen und Bürgern bei der Einführung von E-Government impliziert aus informationstechnischer Sicht, dass die Kommunen ihre Bürgerinnen und Bürger unterstützen und ihnen so einen verantwortungsbewussten und abgesicherten Umgang mit dem neuen Medium *Internet als* Zugangsmedium zum *elektronischen Rathaus* ermöglichen. Nur so können Ängste und Vorbehalte überwunden und die Risiken für die Kommune und den Bürger minimiert und akzeptabel gestaltet werden. Insbesondere bedeutet dies, dass die Kommunen ihren Bürgern auch nur solche Verfahren anbieten, die sicher zu konfigurieren und zu beherrschen sind. Eine geeignete Konfiguration aus sicherheitstechnischer Sicht bedeutet hier nicht, alles technisch Mögliche zu erlauben, vielmehr die Gefahren für den Bürger zu minimieren. Als Beispiel für mögliche Gefahren seien hier aktive Steuerungselemente der Internetbrowser genannt, die unerlaubten Zugriff auf den Heim-PC des Bürgers ermöglichen und daher ohne weitere Sicherungsmaßnah-

men von den Kommunen nicht angeboten werden sollten – auch wenn die Effekte faszinieren und zur Anwendung animieren können.

E-Government bedeutet zunächst die Online-Präsenz und Öffnung der Kommune zum Internet – mit allen Chancen und Gefahren. Der nächste Schritt auf dem Weg zum E-Government ist aber sicherlich die vertrauliche elektronische Kommunikation zwischen den Verwaltungseinheiten der Kommune und zwischen Kommune und Bürgern. Der Datenschutz im Sinne der Vertraulichkeit der zu übertragenden Daten ist ein Bürgerrecht, das es auch bei der elektronischen Datenverarbeitung zu achten gilt. Dieses Bürgerrecht resultiert zum einen aus der Rechtssprechung (vgl. u.a. Volkszählungsurteil):

- Recht auf informationelle Selbstbestimmung: Dieser mit Verfassungsrang ausgestattete Grundsatz folgt bereits aus dem Wesen der Grundrechte selbst (...) als Ausdruck des Freiheitsanspruchs des Bürgers gegenüber dem Staat. Dieses Bürgerrecht darf nur aufgrund öffentlicher Interessen und verfassungsmäßiger Grundlage eingeschränkt werden.

- Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[7]

Zum anderen folgt dieses Bürgerrecht aus allgemeinen Normen:

- Artikel 12 der Allgemeinen Erklärung der Menschenrechte schreibt vor: „Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie oder seinen Briefwechsel noch Angriffen auf seine Ehre und seinen Beruf ausgesetzt werden. Jeder Mensch hat Anspruch auf rechtlichen Schutz gegen derartige Eingriffe oder Anschläge“. [8]

- Ähnlich wird in Artikel 17 des Internationalen Pakts über bürgerliche und politische Rechte von 19.12.1966 bestimmt: „Niemand darf willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, (...) und seinem Schriftverkehr (...) ausgesetzt werden. Jedermann hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen“.[9]

Darüber hinaus ist dieses Bürgerrecht als informationsethischer Grundsatz unserer Gesellschaft zu sehen. Im Kontext moderner IuK-Technologien setzt die freie Entfaltung der Persönlichkeit den Schutz vor unkontrollierter und – durch mangelnde tech-

---

7 Aus den Leitsätzen zum Urteil des Ersten Senats des Bundesverfassungsgerichts vom 15. Dezember 1983 zum Volkszählungsgesetz 1983.

8 http://www.nethics.net/nethics/de/brisant/privacy/begriffserlaeuterung.html. NETHICS e.V., gegründet Ende 1998, nimmt den Auftrag war, die UNESCO, in Deutschland die Deutsche UNESCO-Kommission (DUK), bei der Behandlung informationsethischer Fragesten zu unterstützen.

9 Ebenda.

nologische Beherrschung bedingt – unkontrollierbarer Erhebung, Speicherung, Verwendung und Weitergabe persönlicher Informationen voraus.[10]

Technisch wird der Vertraulichkeitsschutz durch Verschlüsselungsverfahren sichergestellt. Das Schlüsselmanagement ist neben rechtlichen Aspekten eine nicht zu unterschätzende technische und administrative Aufgabe. Zur Absicherung der Kommunikation zwischen unterschiedlichen Unternehmensnetzen gibt es zahlreiche Ansätze, sei es den Aufbau von Virtual Private Networks (VPNs) oder die konsequente Ende-zu-Ende-Verschlüsselung (vgl. SPHINX[11]). Für die Kommunen bieten sich unterschiedliche Lösungsstrategien an: Für die vertrauliche Kommunikation mit Individuen, z.B. einzelnen Bürgerinnen und Bürgern, geeignet ist der Einsatz von Chipkarten, da diese einerseits aus sicherheitstechnischer Sicht eine geeignete Lösung darstellen, andererseits auch zu keinen zusätzlichen Kosten führen, weil Lesegeräte und Chipkarten aufgrund des geplanten Einsatzes der digitalen Signatur den Bürgern und Kommunen bereits zur Verfügung stehen. Die eingesetzten Chipkarten integrieren neben den Signaturzertifikaten auch geeignete Verschlüsselungszertifikate. Hier gibt es bereits zahlreiche adaptierbare Konzepte, so z.B. die Leitlinie des BSI *Ende-zu-Ende-Verschlüsselung für den elektronischen Datenaustausch: Infrastruktur und Leitlinien für die Bundesverwaltung*[12]*.* Für die vertrauliche Kommunikation zwischen den Kommunen, mit Landes- und Bundesbehörden oder zukünftig europaweit wird der Anschluss an VPNs auf administrativ übergeordneter Ebene empfohlen. Zum einen werden so mögliche Interoperabilitätsprobleme gelöst, zum anderen befinden sich solche VPNs bereits im Aufbau (vgl. Projekt TESTA[13]).

Auf der einen Seite sind alle notwendigen Einzelmaßnahmen zum Datenschutz und insbesondere zur Wahrung der Vertraulichkeit durch IT-Grundschutz – technisch, administrativ oder organisatorisch – in online[14] abrufbaren Orientierungshilfen, Leitfäden und Checklisten – insbesondere vom Landesdatenschutzbeauftragten Niedersachsen[15] – detailliert beschrieben. Aus der Vielzahl unterschiedlicher Anforderungen wird aber sofort deutlich, dass nur ein wirkungsvolles Zusammenwirken der Einzelmaßnahmen für eine verantwortungsbewusste Absicherung der kommunalen IT-Infrastruktur entscheidend ist. Nur wenn das Gesamtsystem beherrscht wird und die Restrisiken bekannt sind, können Sicherheitslücken auf unterschiedlichen Ebenen vermieden werden. Spätestens bei der Einführung von Verschlüsselungstechniken – einschließlich des notwendigen Schlüsselmanagement unter technischen und rechtlichen Rahmenbedingungen – reicht der IT-Grundschutz als Katalog aus Einzelmaßnahmen nicht mehr aus, um das Gesamtsystem mit all seinen Risiken zu überschauen und zu beherrschen. Insbesondere beim Austausch von sensiblen Daten wird die Notwendigkeit eines umfassenden Sicherheitskonzepts augenscheinlich. Allein die Beurteilung der Sensibilität übertragener Daten und die Auswahl geeigneter Schutzmaßnahmen sind umfangreiche Aufgaben.

---

10 Ebenda.
11 http://www.bsi.de/aufgaben/projekte/sphinx/index.htm.
12 http://www.bsi.de/aufgaben/projekte/sphinx/bsipol081.pdf.
13 Trans-European Services for Telematics between Administrations: Projektsteuerung Deutschland durch das Innenministerium Thüringen, Herrn Wilke, Leiter Referat IT, und die Deutsche Telekom AG, Niederlassung Erfurt, Herrn Koch, BV ÖA&D, Frau Holfeld, PL TEC.
14 http://www.ld.parlanet.de/technik/.
15 http://www.lfd.niedersachsen.de.

Der notwendige Überblick und die Kontrolle über ein komplexes System aus technischen, organisatorischen und administrativen Maßnahmen wird durch die verantwortungsvolle Erstellung, Umsetzung und Fortschreibung eines IT-Sicherheitskonzepts erreicht. Entscheidend ist hierbei ein strukturiertes Vorgehen, das im günstigsten Fall mit dem Aufbau der IT-Infrastruktur einhergeht. Andernfalls werden aus sicherheitstechnischer Sicht oft bedenkliche Entwicklungen eingeleitet, deren spätere Absicherung zusätzliche Kosten und Ressourcenverbrauch bedeutet. Insbesondere sind hier die geplanten Angebote der Kommunen zu erwähnen; aktive Inhalte sind in diesen Angeboten zu vermeiden.

3. Sicherheitskonzept

3.1 Analyse

Grundsätzlich gilt, dass ein Sicherheitskonzept die Maßnahmen zur Wahrung der Informationssicherheit abdeckt. Hierzu zählen die Sicherheitspolitiken, Praktiken, Verfahren, Organisationsstrukturen und technischen Maßnahmen (Hardware/Software). Diese Maßnahmen sind zur Erfüllung der spezifischen Sicherheitsziele festzulegen. Es ist entscheidend, die Sicherheitsanforderungen zu identifizieren. Bei der Identifikation spielen drei Aspekte eine wesentliche Rolle:

1. Risiken identifizieren
   Die Risikoanalyse ermöglicht die Identifizierung von Bedrohung für die Werte, die Bewertung der Schwachstellen und der Wahrscheinlichkeit des Auftretens eines Risikos sowie die Analyse der möglichen Auswirkungen.

2. Rechtliche Aspekte beachten
   Es geht hier um Anforderungen, die sich aus Gesetzen (z.B. Datenschutz, SigG/SigV), Politik, Richtlinien und Verträgen ergeben, die – einschließlich von Dienstanbietern (z.B. Service Providern) – erfüllt werden müssen.

3. Informationsverarbeitung
   Dies betrifft die spezifischen Prinzipien, Ziele und Anforderungen der Informationsverarbeitung, die zur Unterstützung der Workflow-Prozesse entwickelt wurden.

Sicherheitsanforderungen werden durch eine methodische Analyse der Sicherheitsrisiken identifiziert. Der Aufwand der Maßnahmen muss gegenüber dem wirtschaftlichen und rechtlichen Schaden, der sich aus Sicherheitsversagen ergibt, abgewogen werden. Die Ergebnisse dieser Analyse unterstützen die Bestimmung von angemessenen Aktionen und Prioritäten bei der Verwaltung von Informationssicherheitsrisiken sowie die Implementierung zum Schutz gegen diese Risiken ausgewählten Maßnahmen. Grundlegende Informationen über Maßnahmen bietet z.B. das IT-Grundschutzhandbuch des BSI. Grundsätzlich gilt: Die im IT-Grundschutzhandbuch aufgelisteten Maßnahmen definieren eine Mindestanforderung an die IT-Sicherheit, die als Basis dienen kann. Werden diese Maßnahmen erfüllt, so können hierauf aufbauend IT-Sicherheitsmaßnahmen definiert werden, die für besonders sensible Bereiche einen hohen Schutz bieten. Diese sensiblen Bereiche sind innerhalb der angesprochenen Risikoanalyse zu identifizieren, wobei auch gesetzliche Anforderungen zu berücksichti-

gen sind. Anwendungen, die digitale Signaturen betreffen, sind nach SigG/SigV und insbesondere aus Anwendersicht grundsätzlich im Bereich eines hohen Schutzbedarfs anzusiedeln. Als Basis ist aber auch hier ein Grundschutz sinnvoll, der geeignet ergänzt wird.

3.2 Weitere Anforderungen an Sicherheitskonzepte

Um die Sicherheit durch ein Sicherheitskonzept aufrecht erhalten zu können, muss das Sicherheitskonzept regelmäßig an aktuelle Anforderungen und Entwicklungen angepasst werden. Hierbei müssen die Anpassung einer Bewertung unterzogen und die Umsetzung überprüft werden.

Um den Bereich Informationssicherheit überschaubar zu machen, kann man ihn beispielsweise in eine eigene Infrastruktur einbetten. Diese Infrastruktur besteht aus einem Managementforum, welches Verantwortungen an Management-Teams überträgt. Diese wiederum haben spezielle Aufgaben, bei denen sie als Ansprechpartner für sicherheitstechnische Belange dienen oder aber Maßnahmen zur Informationssicherheit in Abstimmung mit betreffenden Teams einleiten und durchsetzen. Dies wirft natürlich die Frage der personellen Sicherheit auf. Ziel der personellen Sicherheit muss es sein, dass die Risiken durch menschlichen Irrtum reduziert und Diebstahl, Betrug oder Missbrauch der Einrichtung verhindert werden. Dies kann durch entsprechende Arbeitsverträge und Vertraulichkeitsvereinbarungen mit den Sicherheitsverantwortlichen erreichen werden. Gleichzeitig sollte eine Überprüfung dieser Personen stattfinden. Ein weiterer wichtiger Aspekt ist das Verhalten bei Sicherheitsvorfällen und Störungen der Informationssysteme. Die sicherheitsrelevanten Vorfälle müssen über entsprechende Managementkanäle gemeldet werden. Dies setzt voraus, das alle Angestellten und Auftragnehmer mit dem Meldeverfahren für die verschiedenen Arten von Vorfällen (Sicherheitsverstoß, Bedrohung, Schwachstelle oder Störung), die Auswirkungen auf die Sicherheit der organisationseigenen Werte haben könnten, vertraut gemacht werden.

Die sicherheitssensiblen informationstechnischen Systeme müssen zudem an physikalisch sicheren Orten aufgestellt werden. Damit werden unberechtigter Zugang, Beschädigung sowie Störung der Geschäftsräume und Information verhindert. Der Schutz sollte den festgestellten Risiken (Risikoanalyse) angemessen sein.

Weiterhin müssen die Benutzer der Informationssysteme geschult werden. Dies sollte gewährleisten, dass Benutzer sich der Bedrohung und Bedenken bezüglich der Informationssicherheit bewusst sind, und dass sie bei ihrer normalen Arbeitsverrichtung über Mittel zur Unterstützung der organisationseigenen Sicherheitspolitik verfügen. Des Weiteren müssen Strategien hinsichtlich der Verfügbarkeit der angebotenen Dienste ausgearbeitet und in das Gesamtkonzept integriert werden.

Bestehende Sicherheitskonzepte für Teilaspekte können zur Aufwands- und Kostenreduzierung in das zu erstellende Gesamtkonzept integriert werden. Als Beispiel seien hier die Registrierungsstellen nach SigG/SigV genannt. Wird auf bestätigte Stellen zurückgegriffen, so können die bei der Bestätigung dieser Stellen vorgelegten Konzepte integriert werden, ansonsten sind eigene Konzeptlösungen zu qualifizieren und zu bestätigen (vgl. SigV §12,13 und zugehörige Begründung).

Als Anleitung für ein strukturiertes Vorgehen kann den Kommunen der Leitfaden zur Planung, Erstellung und Umsetzung von IT-Sicherheitskonzepten des Landesdatenschutzbeauftragten Schleswig-Hostein dienen. Um einen ersten Eindruck über die unterschiedlichen Aufgaben zu erhalten, sei hier als Beispiel für behördentypische Anwendungsfälle der Leitfaden für Datensicherheit beim Betrieb eines Landkreis-Behördennetzes des bayerischen Landesdatenschutzbeauftragten genannt.

Neben Bundesdatenschutzregelungen sind von den Kommunen auch die landesspezifischen Regelungen zum Datenschutz zu beachten, die beim zuständigen Landesdatenschutzbeauftragten erfragt werden können und in das IT-Sicherheitskonzept zu integrieren sind. Zahlreiche Checklisten der Landesdatenschutzbeauftragten – insbesondere jene aus Niedersachsen – können zur Überprüfung des Ist-Zustands und bei der späteren Umsetzungsprüfung des Sicherheitskonzepts sehr hilfreich sein. Diese Checklisten decken sowohl prinzipielle IT-Sicherheitsaspekte als auch datenschutzrelevante Regelungen ab.

Fragen zum Thema IT-Sicherheit stellen sich durch fortschreitende technische Entwicklungen und Erkenntnisse stets von Neuem. Dies beinhaltet neben einer notwendigen Fortschreibung des Sicherheitskonzepts auch die Fortschreibung und Neuerstellung der Leitfäden, Orientierungshilfen und Checklisten. Daher wird zukünftig eine Auswahl qualifizierter und hilfreicher Dokumente zur IT-Sicherheit als Online-Dokumente auf dem Internetportal http://www.mediakomm.net verfügbar sein. Daneben werden auch stets die aktuellen Online-Bezugsquellen der einzelnen Dokumente genannt werden, sodass sich die Kommunen über aktualisierte oder neuerstellte Dokumente zum Thema IT-Sicherheit informieren können. Die Online-Dokumente unter http://www.mediakomm.net werden auch alle im vorliegenden Dokument genannten Leitfäden, Checklisten und Orientierungshilfen umfassen.

4. Digitale Signatur

Die bisher beschriebenen Maßnahmen als Basis für ein verantwortungsbewusstes E-Government können wie folgt zusammengefasst werden:

- Basisabsicherung der bestehenden IT-Infrastruktur als Vorbereitung für den Internetanschluss der Kommunen – das heißt Kommune online;
- Vertraulichkeitsschutz durch
  - Virtual Private Networks (VPNs) zwischen Verwaltungseinheiten,
  - Ende-zu-Ende-Verschlüsselung zwischen Individuen, z.B. bei der Kommunikation mit dem Bürger;
- Sicherung des Gesamtsystems durch ein IT-Sicherheitskonzept. Ein solches Konzept integriert u.a. die Verantwortlichkeiten und Maßnahmen zur Basisabsicherung, zum Firewall-Konzept für den Internetanschluss und das Schlüsselmanagement.

E-Government ist aber weit mehr als ein vertraulicher Nachrichtenaustausch zwischen Bürger und Kommune. Es sollen als Ziel rechtsverbindliche Transaktionen via Internet

ermöglicht werden. Die bisher beschriebenen Maßnahmen bilden die technische Plattform. Zur Absicherung solcher Transaktionen im Hinblick auf einen möglichen Integritätsschutz und Urheberschaftsnachweis kann die digitale Signatur nach dem deutschen Signaturgesetz, d.h. im Umfeld einer gesicherten und rechtsverbindlichen Public-Key-Infrastruktur, eingesetzt werden. Die Bundesregierung hat durch das Signaturgesetz die Weichen in Richtung verbesserte Rahmenbedingungen für rechtsverbindliche elektronische Transaktionen, z.B. über das Internet, gestellt. Das Gesetz benennt allerdings keine (bereits existierenden?) Sicherheitsstandards, die von den Behörden übernommen werden können. Dies bedeutet allerdings nicht, dass Sicherheit keine entscheidende und grundlegende Anforderung ist. Nur vertrauenswürdige Verfahren zur digitalen Signatur können aus sicherheitstechnischer Sicht mit der Unterschrift von Hand gleichgesetzt werden. Begründetes Vertrauen ist neben der Nutzerfreundlichkeit ein entscheidendes Kriterium für die Akzeptanz seitens der Bürgerinnen und Bürger. Durch die Änderungen am Signaturgesetz zu SigG-E aufgrund der EU-Richtlinie haben sich zwar die rechtlichen Rahmenbedingungen im Detail geändert, ein verantwortungsbewusster Umgang mit der digitalen Signatur setzt aber auf eine vertrauenswürdige Technik. Insbesondere aus Bürgersicht bedeutet dies die Notwendigkeit einer gegenseitigen Authentisierung und des Einsatzes akkreditierter Signaturen.

4.1 Akkreditierte Signaturen im öffentlichen Bereich[16]

Nach § 15 Abs. 2 SigG-E können für den öffentlichen Bereich qualifizierte elektronische Signaturen, die auf einem qualifizierten Zertifikat eines akkreditierten Zertifizierungsdiensteanbieters beruhen, durch Rechtsvorschrift verlangt werden. Da nur bei diesen Signaturen eine nachgewiesene Sicherheit und dauerhafte Überprüfbarkeit gegeben ist, werden sie im Interesse der Rechtssicherheit aller Beteiligten (Bürger, Unternehmen, Staat) im öffentlichen Bereich in vielen Fällen als Äquivalent zur eigenhändigen Unterschrift erforderlich sein.

Mit dieser Regelung macht die Bundesregierung von der zweiten Öffnungsklausel der Richtlinie 99/93/EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektrononische Signaturen (RLeS)[17] Gebrauch. Nach Art. 3 Abs. 7 RLeS wird den Mitgliedstaaten für den öffentlichen Bereich ein eigener Entscheidungsspielraum geschaffen, indem sie den Einsatz elektronischer Signaturen „zusätzlichen Anforderungen“ unterwerfen dürfen. Durch diese Vorschrift wird klargestellt, dass „der Einsatz elektronischer Signaturen im öffentlichen Bereich (z.B. Gesundheitswesen)“ aus dem Anwendungsbereich der Richtlinie „ausgenommen ist“.

Da nur akkreditierte, nicht aber qualifizierte Signaturverfahren über eine nachgewiesene Sicherheit verfügen, kann § 15 Abs. 2 SigG-E – im Rahmen des Art. 3 Abs. 7 RLeS – die ausschließliche Verwendung akkreditierter Zertifizierungsdienste im öffentlichen Bereich ermöglichen. § 15 Abs. 2 SigG-E bestimmt den Einsatz akkreditierter

16 Prof. Dr. jur. A. Rossnagel: Auf dem Weg zu neuen Signaturregelungen – Zu den Novellierungsentwürfen für das SigG, das BGB und die ZPO, in: Multimedia und Recht 8/2000.

17 Abl. EG Nr. L13 v. 19.1.2000, S. 12.

Signaturverfahren jedoch nicht selbst. Solche Regelungen bleiben den jeweils einschlägigen Rechtsvorschriften vorbehalten. § 15 Abs. 2 SigG-E bildet zur Sicherstellung der Einheitlichkeit des Einsatzes elektronischer Signaturen im öffentlichen Bereich die Referenzvorschrift, auf die sich andere Rechtsvorschriften beziehen können. Um einen Wildwuchs der möglichen zusätzlichen Anforderungen für den Einsatz elektronischer Signaturen im öffentlichen Bereich, soweit er in die Zuständigkeit des Bundes fällt, zu vermeiden, ist als einzig zulässige „zusätzliche Anforderung“ das Verfahren der freiwilligen Akkreditierung nach § 15 SigG-E vorgesehen. Damit soll der Beschränkung des Art. 3 Abs. 7 RLeS Rechnung getragen werden, wonach die Anforderungen an den Einsatz elektronischer Signaturen im öffentlichen Bereich objektiv, transparent und verhältnismäßig sein müssen sowie nicht diskriminierend sein dürfen. Diese Beschränkung muss jedoch nicht nur bei der Referenzvorschrift, sondern auch bei jeder Anordnung dieser „zusätzlichen Anforderung“ in der einschlägigen Anordnungsvorschrift beachtet werden.

4.2 Exkurs: Stellungnahme der Gesellschaft für Informatik (GI) vom 13.12.2000 zum Entwurf der Bundesregierung für ein Gesetz über Rahmenbedingungen für elektronische Signaturen

Die GI besteht seit dreißig Jahren als Fachgesellschaft zur Förderung der Informatik. In ihr haben sich 22 000 Mitglieder aus Wissenschaft, Forschung und Anwendung zusammengefunden, um in über 120 Fach- und Arbeitsgruppen die Entwicklung der Informatik zu begleiten, sich selbst weiterzubilden und Stellung zu aktuellen Informatikthemen zu nehmen.

Die GI begrüßt die im Regierungsentwurf vorgesehene Novellierung des Signaturgesetzes als gelungene Umsetzung der europäischen Richtlinie für elektronische Signaturen und als zutreffende Konsequenz aus der Evaluierung des Signaturgesetzes. Insbesondere unterstützt sie

- die neuen Regelungen zur Haftung und Deckungsvorsorge,
- die Bußgeldregelung,
- die Vorschriften zur Anerkennung von Prüf- und Bestätigungsstellen sowie vor allem
- die Möglichkeit zur freiwilligen Akkreditierung von Zertifizierungsstellen.

Die GI sieht in den Regelungen zur Akkreditierung von Signaturverfahren den Schlüssel für die erforderliche Sicherheit im elektronischen Rechtsverkehr. Nur akkreditierte Zertifizierungsstellen verfügen über eine nachgewiesene Sicherheit ihrer organisatorischen Prozesse und ihrer technischen Komponenten. Nur die Akkreditierung bringt durch ihre Vorabprüfung für viele Bereiche des elektronischen Rechtsverkehrs, in denen die Gewissheit sicherer Verfahren erforderlich ist, die erforderliche Rechtssicherheit. Um alle Möglichkeiten des Electronic Business und Electronic Government ausschöpfen zu können, tritt die GI für eine breite Marktvielfalt und einen Wettbewerb zwischen Signaturverfahren mit und ohne vorab nachgewiesener Sicherheit ein. Um diesen Wettbewerb zu ermöglichen, muss das Angebot höherwertiger Sicherheit durch das staatliche Verfahren der Akkreditierung unterstützt werden. Aufgrund der hohen

Bedeutung, die der Akkreditierung für sichere Signaturverfahren und sichere Electronic Business- und Electronic Government-Lösungen zukommt, fordert die GI,

- in § 2 eine eigene Definition für die akkreditierte Signatur zu schaffen, auf die die Vorschrift des § 15 Abs. 2 (diese Vorschrift sollte systematischer als neuer Absatz in § 1 gefasst werden) und die des § 23 Abs. 2 verweisen können,
- an der staatlichen Aufsicht und Akkreditierung durch die Regulierungsbehörde für Telekommunikation und Post festzuhalten, weil nur diese die notwendige wirtschaftsneutrale Prüfung der Sicherheit der Signaturverfahren gewährleisten kann. Eine Akkreditierung nur durch Privatunternehmen würde das für Electronic Business und Electronic Government erforderliche Vertrauen der Teilnehmer am Rechtsverkehr gefährden.
- Wurzelzertifikate der Regulierungsbehörde nur akkreditierten Zertifizierungsstellen vorzubehalten, weil nur diese von der Regulierungsbehörde vorab überprüft wurden. Staatliche Wurzelzertifikate auch für ungeprüfte Zertifizierungsstellen würden die notwendige Unterscheidung zwischen vorab und nicht vorab geprüften Zertifizierungsstellen verwischen und die notwendige Markttransparenz beseitigen.
- an der von der Bundesregierung vorgeschlagenen Regelung in § 13 Abs. 2 festzuhalten, dass die Regulierungsbehörde nur die Zertifikate akkreditierter Zertifizierungsstellen übernimmt, wenn diese ihren Betrieb einstellen. Eine Ausdehnung dieser Regelung auch auf Zertifizierungsstellen, die nicht vorab überprüft wurden, würde ein notwendiges Unterscheidungsmerkmal zwischen akkreditierten und nicht akkreditierten Zertifizierungsstellen nivellieren. Eine Ausdehnung dieser Regelung würde außerdem die Regulierungsbehörde hinsichtlich des organisatorischen Aufwands und der Kosten überfordern. Sie müsste diese Dienstleistung für eine unabsehbar große Zahl von Zertifizierungsstellen und Zertifikaten anbieten, ohne – mangels Zulassungsverfahren – auf die Interoperabilität der Zertifikate, Dokumente und Verfahren Einfluss nehmen zu können. Dies würde die Signaturverfahren unnötig verteuern. Schließlich ist es praktisch nicht möglich, diese Dienstleistung für alle ausländischen Verfahren ebenfalls anzubieten. Dadurch würden aber qualifizierte Signaturverfahren aus anderen Mitgliedstaaten der Europäischen Union diskriminiert. Eine solche Regelung für qualifizierte Signaturverfahren nach § 4 wäre daher ein Verstoß gegen die europäische Richtlinie für elektronische Signaturen. Die GI tritt daher dafür ein, in den Regierungsentwurf eine Definition für akkreditierte Signaturen aufzunehmen und diesen ansonsten unverändert zu verabschieden.

5. Sicherheitstechnische Aspekte zu E-Government aus Sicht der Bürgerinnen und Bürger

Beim E-Government stehen die Bürgerinnen und Bürger vor neuartigen Technologien, deren Möglichkeiten und Gefahren im Allgemeinen nicht leicht zu überblicken sind. Die Kommunen verstehen sich nicht mehr allein als Informationsanbieter via Internet, vielmehr möchten sie zum einen ihren Bürgern eine Vielzahl von Behördengängen ersparen, zum anderen die Effizienz ihrer Verwaltungen erhöhen. Transaktionen via Internet,

einfach, schnell und rechtsverbindlich, natürlich ohne Medienbrüche und die anfallenden Gebühren gleich mittels E-Commerce-Verfahren integriert – so soll der Standort Deutschland auch durch eine Modernisierung der Verwaltung gefördert werden.

Nach dem derzeitigen Stand der Technik beginnt für die Bürgerinnen und Bürger das E-Government – wie es innerhalb der *MEDIA@*Komm-Projekte geplant ist – mit dem Erhalt einer Signatur-Chipkarte. Technisch gesehen können elektronische Geschäftsvorfälle nur mittels der digitalen Signatur vertrauenswürdig abgeschlossen werden. Dieser Chipkarte und ihrer Sicherheit muss der Bürger vertrauen, um sie akzeptieren und verantwortungsbewusst einsetzen zu können. Im Falle einer akkreditierten Signatur nach dem Signaturgesetz kann die Chipkarte auch als vertrauenswürdig angesehen werden: Sowohl die technische Seite der Chipkarte als auch der Herausgeber der Signaturkarte sind im Fall einer akkreditierten Signatur von Experten auf ihre Sicherheit in einem Zulassungsverfahren überprüft worden. Die Vertrauenswürdigkeit des Herstellers und seiner Produktionsumgebung ist hier besonders wichtig: Werden die geheimen Informationen auf der Chipkarte anderweitig – sei es fahrlässig oder bewusst – preisgegeben, so hilft dem Bürger die Sicherheit der Chipkarte nur wenig. Die Chipkartensicherheit schützt den Bürger nur vor unbefugtem Zugriff auf die geheimen Daten auf der Chipkarte. Sind die geheimen Daten auch direkt beim Hersteller – etwa durch einen Angriff via Internet oder durch unzuverlässiges Personal – abrufbar, so kann der Bürger nichts zu seinem persönlichen Schutz beitragen. Natürlich bleibt der Klageweg im Falle eines Missbrauchs. Für eine Akzeptanz von E-Government durch die Bürgerinnen und Bürger ist es unerlässlich, dass der Chipkartenausgeber und seine Infrastruktur vertrauenswürdig sind.

Nach Erhalt einer vertrauenswürdigen Chipkarte stellt sich den Bürgerinnen und Bürgern die Frage, wie diese zu benutzen ist:

Hier kann man sich zum einen an betreute Kiosksysteme der Kommunen wenden. Die Sorgfaltspflicht des Staates den Bürgerinnen und Bürgern gegenüber gebietet, dass die Kommunen für vertrauenswürdige Kiosksysteme Sorge tragen und die Daten des Bürgers vertrauensvoll weiterverarbeiten. Bei betreuten Kiosksystemen kann man darauf vertrauen, dass die Kommunen die technischen Vorgänge geeignet absichern (vgl. Sicherheitskonzept) – Bedienhinweise und Anleitungen erhält der Bürger direkt vor Ort.

Zum anderen steht den Bürgerinnen und Bürgern der Weg über das Internet offen – einschließlich aller Gefahren und Unsicherheiten. Zunächst muss der Bürger für eine vertrauensvolle Anbindung seines Heim-PCs an das Internet Sorge tragen.

- Auswahl geeigneter Komponenten
  Die Vertrauenswürdigkeit und Sicherheit der Komponenten und Applikationen kann aber nicht durch den einzelnen Bürger beurteilt werden. Hier muss der Bürger auf geeignet zertifizierte Komponenten und Applikationen zurückgreifen, sodass er auf das Urteil von Experten innerhalb der Zulassungsverfahren setzen kann. Als Beispiel seien hier nach SigG bestätigte Chipkartenleser genannt, die eine PIN-Eingabe direkt am Kartenleser erlauben. Durch eine Sicherheitsüberprüfung solcher Chipkartenleser wird unter anderem garantiert, dass eine eingegebene PIN nur an die Chipkarte, nicht aber an den angeschlossenen Rechner weitergeleitet wird. Ein Abhören der PIN über das Internet wird so verhindert. Neben den techni-

schen Komponenten benötigt der Bürger aber auch geeignete Applikationen zur Abwicklung der Geschäftsvorfälle via Internet – sei es eine Applikation für die Kommunikation mit einem Geschäftspartner oder für die mit der öffentlichen Verwaltung. Wer garantiert dem Bürger, dass er wirklich das bestellt und signiert, was er auch auf dem Bildschirm sieht? Einen Ausweg aus der Darstellungsproblematik für downloadbare Formulare können in Zukunft digitale Wasserzeichen aufzeigen, wie sie unter anderem vom Fraunhofer Institut[18] erforscht werden.

Bei der Auswahl geeigneter Komponenten ist auf Verfahren zu achten, die dem nachgewiesenen Sicherheitsstandard der akkreditierten Signatur genügen. Hier wird den Bürgerinnen und Bürgern eine Dienstleistung geboten: Vertrauenswürdigkeit durch nachgewiesene Sicherheit. Eine eigenständige Sicherheitsüberprüfung ist dem einzelnen Bürger nicht möglich. Bei ungeprüften Komponenten kann er bestenfalls auf Herstelleraussagen setzen („was alle machen, ist schon gut"), einen Nachweis der Vertrauenswürdigkeit hat er aber nicht. Sicherheitsüberprüfungen, denen sich die Hersteller unterziehen, sind somit nicht nur ein Service und eine einzufordernde Notwendigkeit, sie erhöhen auch die Akzeptanz der neuen Technologien. Die nachgewiesene Sicherheit der akkreditierten Signaturverfahren kann zur Absicherung der gesamten Geschäftsvorfälle einschließlich der Bezahlvorgänge genutzt werden. Die Sicherheit von E-Commerce-Lösungen basiert allerdings nicht allein auf den Verschlüsselungsverfahren und deren Schlüssellänge nach dem Kommunikationsaufbau, sie ist sehr vielschichtig, und nur ein sicheres Gesamtkonzept kann hier die Bürgerinnen und Bürger schützen. Dazu ist es allerdings notwendig, dass der „Geschäftspartner" des Bürgers, sei es eine Kommune oder ein Geldinstitut, auch geeignete Verfahren anbietet, die für den Bürger akzeptabel sind.

- Hilfe bei Installation, Konfiguration und Einhaltung der Sorgfaltspflicht
  Der nächste Schritt auf Seiten der Bürgerinnen und Bürger ist es, die ausgewählten vertrauenswürdigen Komponenten geeignet zu konfigurieren. Eine geeignete Konfiguration aus sicherheitstechnischer Sicht bedeutet hier nicht, alles technisch Mögliche zu erlauben, vielmehr die Gefahren zu minimieren. Als Beispiel seien hier aktive Steuerungselemente der Internetbrowser genannt, die unerlaubten Zugriff auf den Heim-PC ermöglichen und daher von den Kommunen nicht angeboten werden sollten – auch wenn die Effekte faszinieren und zur Anwendung animieren können.

  Ebenso ist den Bürgerinnen und Bürgern zu erläutern, dass ein bedenkenloses Surfen auf beliebigen Internetseiten unkalkulierbare Risiken mit sich bringt. Hier gibt es bereits geeignete Sicherheitshinweise z.B. der Datenschutzbeauftragten, welche die Kommunen ihren Bürgerinnen und Bürgern zur Verfügung stellen können. Solche allgemeinen Anleitungen und Hilfe müssen nur um die individuellen Besonderheiten der Kommunen ergänzt werden. Voraussetzung ist allerdings auch hier, dass die Kommunen auch Verfahren anbieten, die sicher zu konfigurieren und beherrschbar sind. Dies sollte allerdings eine Selbstverständlichkeit für die Kommunen sein, sei es aus deren Sorgfaltspflicht dem Bürger gegenüber oder aus

18 http://www.igd.fhg.de/igd-a8/.

dem einfachen Grund heraus, dass Schädigungen des Bürgers durch E-Government einen immensen Image-Schaden für die Kommune und das Projekt *MEDIA@*Komm sowie für E-Government insgesamt bewirken und die Akzeptanz der neuen Technologien verhindern.

- Gegenseitige Authentisierung & Verschlüsselung
  Im Regelfall, insbesondere bei E-Commerce-Anwendungen, geschieht nur eine einseitige Authentisierung, die der Geschäftspartner vom Bürger verlangt. Eine solche einseitig angeforderte Authentisierungspflicht bedeutet: Der Bürger muss, z.B. mittels des PIN-TAN-Verfahrens, seine Identität nachweisen. Diese Authentisierungspflicht liegt im berechtigten Interesse des Geschäftspartners, z.B. eines Geldinstituts. Das Geldinstitut möchte im Allgemeinen nur wissen, gegen welches Konto sie den Geschäftsvorfall verrechnen kann. Kann das Geldinstitut den transferierten Geldbetrag zuordnen, ist der Geschäftsvorfall abgeschlossen.

  Wie sieht aber die Situation für die Bürgerinnen und Bürger aus? Der Bürger ist beim E-Commerce in einer vergleichbar ungünstigeren Position. Er muss darauf vertrauen, dass die ihm angebotenen Dienste, z.B. Transaktionen via Internet, auch wirklich von seinem Geschäftspartner angeboten werden. Er hat im Allgemeinen keine Möglichkeit zu überprüfen, wer der wirkliche Dienstanbieter ist. Sitzt auf der anderen Seite vielleicht ein Hacker, der dem Bürger nur das Internetportal seiner Kommune vorspielt? Daher kann nur dann von einer vertrauenswürdigen Geschäftsbeziehung via Internet ausgegangen werden, wenn beide Seiten, die Kommune oder das Geldinstitut auf der einen, der Bürger oder Kunde auf der anderen Seite, sich gegenseitig authentisieren. Nur ein Nachweis der Echtheit des Gegenübers im Internet kann Sicherheit und damit Vertrauen für beide Seiten schaffen. Daher gebietet es die Sorgfaltspflicht der Kommunen, ihren Bürgerinnen und Bürgern Verfahren anzubieten, die eine gegenseitige Authentisierung erlauben. Hier kann *MEDIA@*Komm als der Start des E-Government zum Maßstab für sichere Transaktionen via Internet werden. Gleiches gilt für die zu integrierenden E-Commerce-Anwendungen.

Dass bei der eigentlichen Transaktion die übertragenen Daten aus Vertraulichkeitsgründen geeignet verschlüsselt und zum Integritätsschutz gegebenenfalls signiert werden müssen, sei hier – da Stand der Technik – nur der Vollständigkeit halber erwähnt. Das Schlüsselmanagement – insbesondere für die Verschlüsselung – ist eine sehr komplexe Aufgabe. Die Kommunen müssen festlegen, wer Zugriff auf welche Daten haben darf – hier sind auch Vertretungsregelungen und Notfallsicherungen zu integrieren, sodass es nicht zu einem Datenverlust kommt, weil die Daten nur noch verschlüsselt vorliegen. Weiterhin ungelöst – auch wenn erste Ergebnisse vorliegen – ist die Frage nach der Interoperabilität der Public-Key-Infrastruktur, sowohl für die digitale Signatur nach dem Signaturgesetz als auch für die Verschlüsselungs- und Authentisierungsverfahren. Eine Einigung ist Grundvoraussetzung für die Verbreitung der akkreditierten Signatur.

Nur sichere Verfahren können E-Government und E-Commerce zum Durchbruch verhelfen und somit zum Standortvorteil werden.

Der IT-Grundschutz reicht für vertrauenswürdige IT-Systeme, die Konzepte von „elektronischen Rathäusern“ mit umfassenden Kommunikations- und vor allem Transaktionsangeboten (mit/ohne Payment) realisierbar machen sollen, nicht aus. Auch die Einbettung der Komponenten in ein Sicherheitskonzept sagt über die Qualität und Vertrauenswürdigkeit der eingesetzten Einzelkomponenten nichts aus. Um die Risiken überschaubar zu machen und begründetes Vertrauen zu schaffen, hat der Gesetzgeber bewusst in SigG/SigV sowohl Anforderungen an die technischen Komponenten zur Erzeugung und Prüfung digitaler Signaturen als auch an die Sicherheit der Gesamtlösung gestellt. Betrachtet man die Einzelkomponenten im Umfeld digitaler Signaturen, so sind nach SigG/SigV so genannte *bestätigte* Komponenten einzusetzen. Eine Bestätigung nach SigG/SigV von technischen Komponenten umfasst als Zulassungsvoraussetzung eine erfolgreiche Evaluation solcher Komponenten nach ITSEC, hier nach den Stufen E2 hoch bzw. E4 hoch, neuerdings auch nach den international harmonisierten Common Criteria in entsprechenden Stufen.

Als technische Komponenten sind hier insbesondere zu nennen:

- personalisierte Chipkarten (Schlüsselerzeugung in einer Zertifizierungsstelle oder direkt auf der Chipkarte): Evaluation nach ITSEC E4 hoch zuzüglich der Bestätigung nach SigG/SigV;
- Komponenten zur Signaturerstellung und Prüfung von Signaturen und Zertifikaten, einschließlich der Darstellungskomponente ;
- private Nutzung (z.B. privater PC): Evaluation nach ITSEC E2 hoch zuzüglich der Bestätigung nach SigG/SigV;
- gewerbliche Nutzung (z.B. Kioskbetrieb): Evaluation nach ITSEC E4 hoch zuzüglich der Bestätigung nach SigG/SigV.

Für weitere Komponenten, so z.B. entsprechende TV- oder Handykomponenten, ist im Hinblick die notwendige Evaluationsstufe die gedachte Einsatzumgebung entscheidend: Bei einer rein privaten Nutzung ist die ITSEC-Evaluationsstufe E2 hoch ausreichend (z.B. Handy oder TV im Heimbereich), bei einer auch öffentlich genutzten Komponente (z.B. TV im Eingangsbereich einer Behörde), ist aber eine Evaluation und Bestätigung gemäß ITSEC E4 hoch erforderlich.

Die Anforderung, einzelne Komponenten nach ITSEC evaluieren zu lassen, resultiert zum einen aus gesetzlichen Auflagen (SigG/SigV), zum anderen kann sie als Analyseergebnis aus dem Sicherheitskonzept stammen, begründet in der Verantwortung der Kommunen für eine sichere Gesamtlösung und aus der gebotenen Sorgfaltspflicht gegenüber den Bürgerinnen und Bürgern. Für bestimmte Bereiche – vor allem beim verantwortungsbewussten Umgang mit der digitalen Signatur – werden besondere Anforderungen an die IT-Sicherheit der eingesetzten Produkte gestellt. Ob ein Produkt diese erfüllt, kann auf verschiedene Arten verifiziert werden. Zum einen kann man einer Herstellerzusage, zum anderen dem Prüfergebnis eines unabhängigen Dritten vertrauen, der ein solches Produkt nach anerkannten Kriterien (z.B. ITSEC) überprüft (evaluiert). Wichtig ist es festzuhalten: Nicht alle Bereiche sind hochschutzbedürftig. Dies bedeutet: Nicht jede Komponente des Gesamtsystems muss evaluiert werden. Vielmehr werden innerhalb einer Risikoanalyse die sicherheitssensiblen Bereiche identifiziert, die

einer genaueren Betrachtung und Überprüfung, als es zum Beispiel mittels IT-Grundschutz und Checklisten möglich ist, bedürfen. Neben sicheren Einzelkomponenten ist die Sicherheit des Gesamtsystems entscheidend. Die technische Überprüfung des Gesamtsystems erfolgt jedoch nicht durch eine Evaluation, da solche Verfahren für komplexe Systeme zu aufwendig sind. Hier sollte auf Alternativen wie eine sicherheitstechnische Qualifizierung (SQ) zurückgegriffen werden. Mit solchen Methoden kann das korrekte Zusammenwirken einzelner Systeme überprüft werden, ebenso die adäquate Konfiguration einzelner Systeme wie etwa einer Firewall und deren Filterregeln. Die Einbettung aller Einzelmaßnahmen in den Gesamtablauf geschieht im Rahmen der Abnahme des Sicherheitskonzepts. Das Sicherheitskonzept kann sich hierbei auf bestätigte Einzelkomponenten oder sicherheitstechnische Qualifizierungen (SQ) abstützen. Es sei aber im Zusammenhang mit der Einführung digitaler Signaturen nochmals eindringlich auf die Notwendigkeit gegenseitiger Authentisierungsmaßnahmen hingewiesen, insbesondere aus Anwendersicht.

6. Exkurs: Einführung in die ITSEC

Unter der Abkürzung ITSEC versteht man die europäisch harmonisierten Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik, genauer: Information Technology Security Evaluation Criteria, Harmonised Criteria of France, Germany, the Netherlands, the United Kingdom, Version 1.2 vom 28. Juni 1991.

Wie auch die deutschen IT-Sicherheitskriterien gehen die ITSEC von drei Grundbedrohungen aus: Verlust von Vertraulichkeit, Integrität und Verfügbarkeit. Diesen Bedrohungen soll mit einer vertrauenswürdigen Implementation von Sicherheitsfunktionen entgegengewirkt werden. Am Anfang des Designs der Sicherheitsfunktionen muss daher eine ausführliche Bedrohungsanalyse stehen. Die ITSEC unterscheiden in diesem Zusammenhang den Begriff *IT-System*, das eigenständig in einer bekannten Umgebung eingesetzt werden soll und für das reale Bedrohungen bekannt sind sowie den Begriff *IT-Produkt*, dessen Einsatzumgebung nicht vorhersehbar ist und für das ein fiktives Bedrohungsmodell aufgestellt werden muss. Diese Unterscheidung wird im Folgenden jedoch vernachlässigt.

Die Evaluation eines IT-Produkts nach den ITSEC bedeutet eine Bewertung der Vertrauenswürdigkeit der in diesem Produkt zum Zwecke der Einhaltung definierter Sicherheitsziele verwirklichten technischen Sicherheitsmaßnahmen, welche im folgenden als Sicherheitsfunktionen bezeichnet werden. Unter Vertrauenswürdigkeit versteht man hierbei die Eigenschaft des Produkts, die das Maß an Vertrauen in die Korrektheit und Wirksamkeit der Implementierung der angegebenen Sicherheitsfunktionen ausdrückt. Den Maßstab für die Bewertung bildet die vom Antragsteller der Evaluation vorgegebene Evaluationsstufe (E0, E1, E2, ... E6). Im Zusammenhang mit der Bestätigung technischer Komponenten nach SigG/SigV ergeben sich die Sicherheitsziele aus den in SigG/SigV definierten Anforderungen, die relevanten Evaluationsstufen sind die Stufe E4 für die technischen Komponenten, die direkt mit privaten Signaturschlüsseln operieren, und die Stufe E2 für die übrigen Komponenten nach SigG/SigV.

Neben den Evaluationsstufen, die ein Maß für die Prüftiefe und somit die Vertrauenswürdigkeit sind, wird bei einer Evaluation auch die Stärke der eingesetzten Sicherheitsmechanismen bewertet. Die Sicherheitsmechanismen dienen zur Realisierung der Sicherheitsfunktionalität. Die Stärke der Sicherheitsmechanismen ist ihre Fähigkeit, einem direkten Angriff zu widerstehen. Die Analyse der Mechanismenstärke stützt sich auf die folgenden Aspekte: Fachkenntnisse, geheime Absprache, Zeit und Ausstattung eines potenziellen Angreifers. Nach den ITSEC-Kriterien werden die Mechanismenstärken in die Kategorien niedrig, mittel und hoch eingeteilt, wobei nach SigG/SigV eine hohe Mechanismenstärke gefordert ist, unabhängig von der Prüftiefe bzw. Evaluationsstufe.

6.1 Kurzcharakterisierung der Qualitätsstufen

- Stufe E0:
  - unzureichende Vertrauenswürdigkeit
- Stufe E1:
  - Sicherheitsvorgaben müssen vorliegen
  - informelle Beschreibung des Architekturentwurfs
  - funktionale Tests auf Erfüllung der Sicherheitsvorgaben
- Stufe E2 (zusätzlich zu E1):
  - informelle Beschreibung des Feinentwurfs
  - Bewertung der funktionalen Tests
  - Konfigurationskontrollsystem muss vorhanden sein
  - genehmigtes Distributionsverfahren muss vorhanden sein
- Stufe E3 (zusätzlich zu E2):
  - Bewertung des den Sicherheitsmechanismen entsprechenden Quellcodes
  - Bewertung der Tests der Sicherheitsmechanismen
- Stufe E4 (zusätzlich zu E3):
  - formales Sicherheitsmodell (für ein Betriebssystem z.B. Bell-La-Padula-Modell)
  - sicherheitsspezifische Funktionen, Architekturentwurf und Feinentwurf in semiformaler Notation
- Stufe E5 (zusätzlich zu E4):
  - enger Zusammenhang zwischen Feinentwurf und Quellcode
- Stufe E6 (zusätzlich zu E5):
  - sicherheitsspezifische Funktionen, Architekturentwurf in formaler Notation, wobei Konsistenz zum unterliegenden Sicherheitsmodell gefordert ist.

6.2 Beurteilungsaspekte

Die Evaluation soll das Vertrauen in die Tatsache bewerten, dass die in einem IT-System implementierten Sicherheitsfunktionen auch das Sicherheitsziel erreichen. Dabei wird einerseits das Vertrauen in die Korrektheit der Implementierung und anderer-

seits das Vertrauen in die Wirksamkeit der implementierten Mechanismen beurteilt. Letztere Prüfung gliedert sich wie auch die Prüfung der Korrektheit in zwei Life-Cycle-Phasen, nämlich die Phase der Herstellung bzw. Konstruktion und in die des Betriebs. Bei der Wirksamkeit werden im einzelnen folgende Aspekte betrachtet:

Wirksamkeitskriterien

- Konstruktion
  - Aspekt 1: Eignung der Funktionalität
  - Aspekt 2: Zusammenwirken der Funktionalität
  - Aspekt 3: Stärke der Mechanismen
  - Aspekt 4: Konstruktionsschwachstellen

- Betrieb
  - Aspekt 1: Benutzerfreundlichkeit
  - Aspekt 2: Bewertung der operationalen Schwachstellen

Da für die Prüfung der Wirksamkeit eine Schwachstellenanalyse anzufertigen ist, die sich auf Informationen stützt, die in der Korrektheitsbewertung erarbeitet werden, wird diese Prüfung nach Darlegung der Kriterien für die einzelnen Qualitätsstufen betrachtet.

Der Korrektheitsaspekt bei der Vertrauenswürdigkeit eines EVG wird formal unter folgenden Gesichtspunkten betrachtet:

Konstruktion

- Entwicklungsprozess
  - Phase 1: Anforderungen
  - Phase 2: Architekturentwurf
  - Phase 3: Feinentwurf
  - Phase 4: Implementierung

- Entwicklungsumgebung
  - Aspekt 1: Konfigurationskontrolle
  - Aspekt 2: Programmiersprachen und Compiler
  - Aspekt 3: Sicherheit beim Entwickler

Betrieb

- Betriebsdokumentation
  - Aspekt 1: Benutzerdokumentation
  - Aspekt 2: Systemverwalter-Dokumentation

- Betriebsumgebung
  - Aspekt 1: Auslieferung und Konfiguration
  - Aspekt 2: Anlauf und Betrieb

Um zu einem vollständigen und transparenten Verständnis zu gelangen, ob das Produkt seine definierten Sicherheitsziele mit dem Grad des Vertrauens erfüllt, welcher durch den Evaluationslevel vorgegeben ist, müssen Dokumente bezüglich der Konstruktions- und der Betriebsphase des Produkts zur Verfügung gestellt werden.

Exemplarisch wird nachfolgend die benötigte Mindestdokumentation für die Stufen E2 und E4 angegeben, da diese Evaluationsstufen nach SigG/SigV relevant sind. Hierbei werden diejenigen Anforderungen für die Stufe E4, die für E2 nicht erforderlich sind, durch *Kursivsetzung* hervorgehoben.

Vom Produkthersteller wird erwartet, dass er die unten spezifizierten Dokumente im Hinblick auf Inhalt, Form und Nachweise gemäß ITSEC, S. 62-69 bzw. S. 79-87 (Korrektheit) und S. 37-43 (Wirksamkeit) erstellt und der beauftragten Prüfstelle (Prüfstelle für IT-Sicherheit der TÜV Informationstechnik GmbH) zur Verfügung stellt. Nach einer erfolgreich verlaufenen Evaluation wird durch eine Bestätigungsstelle (Bestätigungsstelle nach SigG/SigV der TÜV Informationstechnik GmbH) bestätigt, dass eine erfolgreich durchgeführte Evaluation die Sicherheitsziele nach SigG/SigV abdeckt und die technischen Komponenten somit nach SigG/SigV als bestätigte Komponenten zugelassen werden können.

Sicherheitsvorgaben

Die Sicherheitsvorgaben sind das zentrale Dokument und bilden die Grundlage für alle weiteren während des Evaluationsprozesses zu erstellenden Dokumente. Sie beinhalten eine Produktbeschreibung, die die Art des Produkteinsatzes, die vorgesehene Einsatzumgebung, die zu erreichenden Sicherheitsziele und die angenommenen Bedrohungen des Produkts darlegen. Zudem ist eine Spezifikation der vom Produkt geforderten Sicherheit (Sicherheitsfunktionen), die Mindeststärke der die Sicherheitsfunktionen realisierenden Sicherheitsmechanismen (niedrig, mittel oder hoch) sowie die angestrebte Evaluationsstufe im Rahmen der Sicherheitsvorgaben anzugeben.

Formales Sicherheitsmodell

Bei den Evaluationsstufen ab E4 muss ein in formaler Notation spezifiziertes Sicherheitsmodell definiert oder ein Verweis auf ein solches angegeben werden, welches die vom Evaluationsgegenstand durchgesetzte Sicherheitspolitik festlegt. Es muss gezeigt werden, dass die Sicherheitsvorgaben die zugrunde liegende Sicherheitspolitik umsetzen und keine Funktionen enthalten, die zu dieser Politik im Widerspruch stehen.

Architekturentwurf

Der Architekturentwurf stellt zusammen mit dem nachfolgenden Feinentwurf die für die Evaluation notwendige Designbeschreibung dar. Architektur- und Feinentwurf ergänzen sich und bilden zwei Ebenen der Beschreibungshierarchie. Der Architekturentwurf ist die obere Ebene, die über eine Top-Level-Zuordnung abstrakter Funktionen zu logi-

schen und physischen Komponenten verdeutlicht, wie die in den Sicherheitsvorgaben festgelegten Sicherheitsfunktionen zur Verfügung gestellt werden.

Feinentwurf

Der Feinentwurf stellt eine Verfeinerung der Architekturbeschreibung dar, in der die Funktionalität der einzelnen Komponenten sichtbar wird. Die Beschreibung erfolgt dabei bis hin zu einem Detaillierungsgrad, der als Basis für die Programmierung und/oder Hardware-Konstruktion verwendet werden kann. Der Feinentwurf expliziert über die Spezifikation von Sicherheitsmechanismen, auf welche Weise die Sicherheitsfunktionen realisiert werden.

Testdokumentation

Die Testdokumentation ist das Mittel, mit dem überprüft wird, ob die Implementierung des Feinentwurfs mit den Sicherheitsvorgaben übereinstimmt. Sie beinhaltet neben Testplänen, -zielen, -verfahren und -ergebnissen auch die Bibliothek der Testprogramme und -werkzeuge, die für die Tests benutzt wurden.

Quellcode/Hardware-Konstruktionszeichnungen

Für alle sicherheitsspezifischen und -relevanten Komponenten müssen der Quellcode bzw. die Hardware-Konstruktionszeichnungen sowie eine Zuordnungsbeschreibung, die den Bezug zwischen Quellcode/Hardware-Konstruktionszeichnungen und dem Feinentwurf darstellt, zur Verfügung gestellt werden.

Konfigurationsliste

Die Konfigurationsliste identifiziert eindeutig das Produkt (Version), seine Komponenten und alle für die Evaluation zur Verfügung gestellten Dokumente.

Konfigurationskontrolle

Dieses Dokument gibt Informationen über das *durch Werkzeuge unterstützte* Konfigurationskontrollsystem, das heißt die Kontrollen, die der Entwickler des Produkts hinsichtlich seiner Entwicklungs-, Produktions- und Wartungsprozesse durchgeführt hat, und wie das Konfigurationskontrollsystem im Entwicklungsprozess zusammen mit dem Qualitätsmanagementverfahren angewendet wird.

Zusätzlich muss die Entwicklung durch ein Abnahmeverfahren unterstützt worden sein, welches Objekte, die während des Entwicklungs-, Produktions- und Wartungsprozesses erstellt wurden, eindeutig in ein Konfigurationskontrollsystem einbezieht.

Programmiersprachen und Compiler

In diesem Dokument sind sämtliche für die Implementierung benutzten Programmiersprachen und implementierungsabhängigen Optionen der Programmiersprachen klar definiert. Zudem sind für alle benutzten Compiler die gewählten Implementierungsoptionen dokumentiert.

Sicherheit beim Entwickler

Dieses Dokument verdeutlicht über die Beschreibung materieller, organisatorischer, personeller und anderer Sicherheitsmaßnahmen, dass aus der Herkunft des Produkts keine Gefahren zu befürchten sind. Es zeigt, wie die Integrität des Produkts und die Vertraulichkeit der zugehörigen Dokumente gewährleistet werden.

Benutzer- und Systemverwalterdokumentation

Die Dokumente stellen sicher, dass alle Benutzer und mit Privilegien ausgestattete Systembediener und -verwalter über die sicherheitsrelevanten Aspekte umfassend, verständlich und eindeutig informiert sind, um das Produkt sicher benutzen und verwalten zu können.

Auslieferungs- und Konfigurations-Dokumentation

Diese Dokumente verdeutlichen, wie die Sicherheit während des Transports des Produkts oder seiner Komponenten zum Anwender hinsichtlich der Erstauslieferung und auch hinsichtlich später folgender Modifikationen gewahrt bleibt. Dazu muss ein für diese Stufe vom BSI zugelassenes Verfahren Anwendung finden.

Anlauf- und Betriebs-Dokumentation

Die Dokumente geben Informationen, wie die Sicherheit des Produkts während des Anlaufs und des Betriebs aufrechterhalten bleibt. Die Verfahren, die beispielsweise ein Systemverwalter zum sicheren täglichen Betrieb des Produkts benutzt, sind hier darzulegen. *Verfahren müssen vorhanden sein, die den Evaluationsgegenstand nach einem Systemausfall oder nach einem Hard- oder Softwarefehler in einen sicheren Zustand zurückversetzen können.*

Analyse der Eignung

Dieses Dokument analysiert die Eignung der Sicherheitsfunktionen, den in den Sicherheitsvorgaben zitierten Bedrohungen entgegenzuwirken. Die Analyse muss zeigen, dass und auf welche Art allen identifizierten Bedrohungen durch die Sicherheitsfunktionen begegnet wird.

Analyse des Zusammenwirkens

Dieses Dokument analysiert die Fähigkeit der Sicherheitsfunktionen und der sie realisierenden Mechanismen, in einer Weise zusammenzuwirken, dass sie sich gegenseitig unterstützen (Synergieeffekte). Die Analyse muss zeigen, dass die Gesamtheit der Sicherheitsfunktionen zusammen mit der Beschreibung ihres Zusammenwirkens entsprechend den Angaben des Architekturentwurfs alle Sicherheitsziele erfüllt, das heißt alle in den Sicherheitsvorgaben aufgeführten Bedrohungen abdeckt.

Analyse der Stärke der Mechanismen

Dieses Dokument analysiert die Fähigkeit der Sicherheitsmechanismen, einem direkten Angriff zu widerstehen. Die Analyse stützt sich bei der Bewertung der Stärke der Mechanismen auf die folgenden Aspekte: Fachkenntnisse, geheime Absprache, Zeit und Ausstattung eines potenziellen Angreifers. Nach den ITSEC-Kriterien werden die Mechanismenstärken in die Kategorien niedrig, mittel und hoch eingeteilt, wobei nach SigG/SigV eine hohe Mechanismenstärke gefordert ist, unabhängig von der Prüftiefe bzw. Evaluationsstufe.

Liste der bekannten Schwachstellen in der Konstruktion

Dieses Dokument analysiert die Auswirkungen jeder bekannten Konstruktionsschwachstelle, das heißt von Schwachstellen, die irgendeine während der Konstruktion eingebrachte Eigenschaft des Evaluationsgegenstands ausnutzen. Es müssen Maßnahmen zur Abhilfe aufgezeigt werden, sodass in der definierten Einsatzumgebung die Sicherheit des Produkts nicht kompromittiert werden kann.

Analyse der Benutzerfreundlichkeit

Bei diesem Aspekt der Wirksamkeit wird geprüft, ob der Evaluationsgegenstand in einer Weise konfiguriert oder genutzt werden kann, die unsicher ist, die aber von einem Systemverwalter oder Endanwender berechtigterweise für sicher gehalten würde.

Liste der bekannten Schwachstellen in der operationellen Nutzung

Dieses Dokument analysiert die Auswirkungen jeder bekannten Schwachstelle im Betrieb, das heißt von Schwachstellen, die Schwächen nichttechnischer Gegenmaßnahmen ausnutzen, um die Sicherheit des Evaluationsgegenstands zu verletzen. Es müssen Maßnahmen zur Abhilfe aufgezeigt werden, sodass in der definierten Einsatzumgebung die Sicherheit des Produkts nicht kompromittiert werden kann.

Nach diesem Exkurs wird deutlich, dass der Aufwand für die nach SigG/SigV verbindliche Evaluation und Bestätigung der technischen Komponenten leicht unterschätzt wird, sodass gegebenenfalls auf bereits evaluierte und bestätigte Komponenten zurückgegriffen werden sollte. Auf diese Komponenten kann dann eine technische Plattform zu-

rückgreifen, die das beabsichtigte Dienstangebot bereitstellt. Eine solche Plattform ist in ein Sicherheitskonzept einzubetten, um die Sicherheit der Gesamtlösung gewährleisten zu können. Ein naheliegender Gedanke hinsichtlich der technischen Plattformen und der einzelnen technischen Komponenten ist der Versuch der Nutzung bzw. Übertragbarkeit von bereits entwickelten Lösungen aus dem E-Commerce-Bereich. Ließen sich derartige Lösungen ohne größere Schwierigkeiten übertragen, dann könnten insgesamt sicherlich in erheblichem Maße Ressourcen eingespart werden. Technische Plattformen aus dem E-Commerce-Bereich sind im Allgemeinen zwar fähig, digitale Signaturen auszustellen und zu prüfen, sie sind aber nicht generell nach SigG/SigV bestätigte Komponenten, sodass auch aufgrund SigG/SigV Erweiterungen notwendig werden können. Zumindest sind entsprechende Bestätigungen der technischen Komponenten beizubringen. Neben jenen aufgrund von SigG/SigV bestehen noch weitere Anforderungen, z.B. aus dem Bereich des Datenschutzes und der Verfügbarkeit angebotener Dienste. E-Commerce-Lösungen erfüllen zwar auch gewisse Anforderungen an den Datenschutz, insbesondere bei der Übertragung von der Kundenseite zur Bank. Allerdings sind Datenschutzaspekte innerhalb von Banken einschließlich der Mitarbeiterschaft häufig kein Thema. Innerhalb der Städte stellt sich diese Situation indes deutlich anders dar.

Insgesamt zeigt sich, dass die Aufgaben der Städte sehr umfangreich sind. Die Anforderungen an die Gesamtlösung entstammen aus unterschiedlichen Bereichen. Alle Anforderungen müssen gesammelt und behandelt werden. Neben der Einführung der digitalen Signatur sollen Geschäftsvorfälle elektronisch abgewickelt werden, soll elektronisch bezahlt werden. Allein diese drei Bereiche, ohne hier auf Datenschutz und Verfügbarkeit einzugehen, sind Probleme, die bisher technisch nicht zufriedenstellend – auch nicht in Einzelprojekten – gelöst sind. Die Städte haben die schwierige Aufgabe, diese Einzelprojekte zusammenzuführen. Dabei sollen die eingesetzten Verfahren möglichst interoperabel sein. Der Aspekt der Interoperabilität und die Einforderung von Standards ist allerdings kein sicherheitstechnischer Bewertungsaspekt.

Der Aufwand für die nach SigG/SigV verbindliche Evaluation und Bestätigung der technischen Komponenten für akkreditierte Signaturen wird leicht unterschätzt. Dies heißt nicht, dass der Aufwand für die vertrauenschaffende Evaluation von IT-Komponenten für den Hersteller übertrieben ist. Die nachgewiesene Sicherheit der Komponenten ist ein Qualitätsmerkmal, auf das der Kunde achten sollte. Der Nachweis der Sicherheit ist Aufgabe des Herstellers, nicht des Kunden bzw. hier der Kommune. Daher sollten die Kommunen auf die Evaluation der Komponenten und damit auf ihre eigene Sicherheit beharren. Zudem entwickelt sich das aktuelle Marktangebot an evaluierten und bestätigten Komponenten zurzeit sehr positiv, sodass die Kommunen durchaus auf solche Komponenten zurückgreifen können. Auf diese Komponenten kann dann eine technische Plattform aufbauen, die das beabsichtigte Dienstangebot bereitstellt.

7. E-Commerce

Die digitale Signatur ist aber nur eine – wenn auch wichtige – Säule für E-Government. Eine weitere Aufgabe bei E-Government – als Vorteil sowohl für den Bürger als auch für die Kommune – ist die Integration von Bezahlvorgängen in den Transaktionsprozess via Internet, neudeutsch: die Integration von E-Commerce-Anwendungen. Ein naheliegender Gedanke hinsichtlich der technischen Plattformen für digitale Signaturen ist daher der Versuch der Nutzung bzw. Übertragbarkeit von bereits bestehenden Lösungen aus dem E-Commerce-Bereich. Ließen sich derartige Lösungen ohne größere Schwierigkeiten übertragen, ließen sich insgesamt in erheblichem Maße Ressourcen sparen. Technische Plattformen aus dem E-Commerce Bereich sind im Allgemeinen zwar fähig, digitale Signaturen auszustellen und zu prüfen, sind aber nicht generell nach SigG/SigV bestätigte Komponenten, sodass auch unter dem Hintergrund SigG/SigV Erweiterungen notwendig werden können. Zudem basieren die in Deutschland gängigen E-Commerce-Verfahren im Allgemeinen auf einer einseitigen Authentisierung. Aus Anwendersicht ist – ebenso wie für Signaturanwendungen – auch im E-Commerce-Bereich eine Erweiterung in Richtung einer gegenseitigen Authentisierung erforderlich. Steht bei den Kommunen und den Bürgern die IT-Infrastruktur für die digitale Signatur bereit, so ist es sinnvoll, die Sicherheitsmechanismen der digitalen Signatur in die E-Commerce-Anwendungen zu integrieren. Die digitale Signatur kann für die Rechtsverbindlichkeit einer Transaktion, den Urheberschaftsnachweis und die Absicherung eines integrierten Bezahlvorgangs genutzt werden. Ein vertrauenswürdiges Verfahren für Transaktionen via Internet ist somit gegeben, das sowohl von der Kommune als auch von den Bürgerinnen und Bürgern verantwortungsbewusst genutzt und akzeptiert werden kann. Als erster Überblick über die sicherheitstechnischen Aspekte kann aus der Schriftenreihe zur IT-Sicherheit (Band 10) des Bundesanzeigers *Sicherheitsaspekte bei E-Commerce* dienen. Für aktuellste Entwicklungen in diesem Bereich sei auf die regionalen E-Commerce-Kompetenz-Zentren[19] hingewiesen.

8. Systemtechnischer Ansatz als Ergänzung zur formalen Evaluierung gemäß ITSEC[20]

Auf der Ebene von Produkten mit Sicherheitsfunktionen werden seit einigen Jahren systematische Prüfungen und Bewertungen durchgeführt. Ein bekanntes Verfahren ist die formale Evaluation nach den Information Technology Security Evaluation Criteria (ITSEC) oder den Common Criteria (CC).

Die nun reichlich vorhandenen Erfahrungen zeigen, dass eine in allen formalen Ansprüchen akkurat und vollständig durchgeführte formale Evaluation nicht für alle IT-Systeme gleichermaßen praktikabel ist. Evaluierbare und zertifizierbare Prüfgegenstände sind typischerweise überschaubare und relativ kleine Software-Produkte.

TÜViT hat aufgrund vieler Jahre praktischer Arbeit mit der Sicherheit von Informationstechnik ein standardisiertes Verfahren der Sicherheitstechnischen Qualifizierung

19 http://www.ec-net.de/index.html.

20 http://www.tuvit.de „Sicherheitstechnische Qualifizierung und Zertifizierung von vertrauenswürdigen IT-Installationen“, Version 8.2, Stand Mai 2000 bzw. im Anhang.

(SQ) von vertrauenswürdigen IT-Installationen entwickelt. Das Verfahren erlaubt die Untersuchung von umfangreichen IT-Installationen in angemessener Weise unter besonderer Berücksichtigung von Heterogenität, Komplexität und Dynamik solcher IT-Systeme.

Das Verfahren der Sicherheitstechnischen Qualifizierung ist durch eine erheblich höhere Effizienz im Vergleich mit einer klassischen formalen Evaluation gekennzeichnet. Die verfügbaren Ressourcen können deutlich stärker auf die für die Sicherheit wirklich wesentlichen und kritischen Punkte fokussiert werden. Unmittelbares Feedback aus den laufenden Untersuchungen erlaubt eine schnelle und angemessene Reaktion auf erkannte Probleme. Alle Verfahrenselemente lassen sich an spezifische Anforderungen oder Gegebenheiten individuell anpassen.

Standardisierte Anforderungsprofile ermöglichen die Qualifizierung und Zertifizierung des Sicherheitsniveaus einer IT-Installation.

IT-Sicherheit ist die angenommene sicherheitstechnische Verlässlichkeit eines IT-Systems, in dem die Risiken, die beim Einsatz dieses IT-Systems aufgrund von Bedrohungen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß beschränkt sind.

Wenn sich Vertrauen in die IT-Sicherheit allein oder wesentlich auf (guten) Glauben stützt, kann dies sehr risikoreich sein; es ist für das Vertrauen in ein IT-System vielmehr dringend erforderlich, dass ein vom Benutzer des IT-Systems anerkannter, unabhängiger und kompetenter Gutachter wie die TÜV Informationstechnik GmbH die IT-Sicherheit des IT-Systems überprüft und bescheinigt.

Folgende Quellen dienen als Grundlage zur Erlangung von Vertrauen in ein IT-System:

- Schutzmaßnahmen im IT-System,
- Transparenz des IT-Systems,
- Überprüfungen am IT-System,
- Analyse des IT-Systems.

Aus den erkannten Quellen des Vertrauens in die IT-Sicherheit eines IT-Systems werden folgende Aspekte zur Bewertung der IT-Sicherheit abgeleitet. Mithilfe dieser Bewertungsaspekte wird das erreichte Sicherheitsniveau einer IT-Installation festgestellt.

- Technische Sicherheitsanforderungen und Vorgaben,
- Systemdokumentation,
- Sicherheit der verwendeten IT-Komponenten,
- Benutzer-, Administrations- und sonstige Betriebsdokumentation,
- Mittel des Systemmanagements,
- Verfahren und technische Mittel des Änderungsmanagements,
- Tests und Inspektionen,
- Sicherheitsanalysen.

Eine IT-Installation wird durch „Zerlegung“ in IT-Subsysteme und IT-Komponenten, Klassifizierung der IT-Subsysteme und IT-Komponenten, Einzelprüfungen von IT-Komponenten, Einzelanalysen und Einzelsicherheitskonzepte sicherheitstechnisch qualifiziert.

Nach dieser Zerlegung der IT-Installation werden die einzelnen IT-Subsysteme und IT-Komponenten in die Kategorien

- sicherheitsspezifisch,
- kritisch und
- unkritisch

klassifiziert.

Sicherheitsspezifisch sind jene IT-Subsysteme und IT-Komponenten, die unmittelbar zur Durchsetzung der IT-Sicherheit beitragen.

Als kritisch werden jene IT-Subsysteme und IT-Komponenten bezeichnet, die zwar nicht sicherheitsspezifisch sind, für die aber bekannt ist oder nicht ausgeschlossen werden kann, dass sie die IT-Sicherheit der IT-Installation im Sinne ihrer technischen Sicherheitsanforderungen verletzten können.

Als unkritisch werden jene IT-Subsysteme und IT-Komponenten bezeichnet, die weder kritisch noch sicherheitsspezifisch sind.

Die Klassifizierung dient der Fokussierung der Prüfaufwände auf die für die IT-Sicherheit wichtigen Bereiche, sodass vor allem sicherheitsspezifische und kritische IT-Subsysteme und IT-Komponenten untersucht und die vorhandenen Resourcen sinnvoll eingesetzt werden.

Nach den Untersuchungen und der Erstellung der notwendigen Dokumente kann auf der Basis des Anforderungsprofils für bestimmte IT-Installationen ein Zertifikat erteilt werden.

9. Resümee

Insgesamt zeigt sich, dass die Aufgaben der Kommunen sehr umfangreich sind. Die Anforderungen an die Gesamtlösung entstammen unterschiedlichsten Bereichen. Alle Anforderungen müssen gesammelt und abgearbeitet werden. Die Städte haben die schwierige Aufgabe, diese Einzelprojekte zusammenzuführen. Dabei sollen die eingesetzten Verfahren möglichst interoperabel sein. Die Interoperabilität und die Einforderung von Standards sind allerdings keine sicherheitstechnischen Bewertungsaspekte, sondern eine Forderung, die die Akzeptanz und Verbreitung der eingesetzten Verfahren gewährleistet. Gleiches gilt für die Standardisierung der beteiligten Geschäftsvorfälle. Der eigentliche Vorteil des E-Government – sowohl für die Bürgerinnen und Bürger als auch für die Kommune – ist gegeben, wenn es bei den Transaktionen zu keinen Medienbrüchen kommt. Workflow-Prozesse sind neu zu überdenken und gegebenenfalls zu reorganisieren. Als Beispiel für die Vielzahl der neuen Aufgaben seien die Archivierungssysteme genannt, die auf digitale Dokumente umgestellt werden müssen. Als Lösungsmöglichkeiten bieten sich hier revisionssichere Dokumentenmanagementsysteme an, wobei stets beachtet werden muss, dass digitale Signaturen nur eine begrenzte Zeit lang überprüfbar sind.

Geschäftsprozesse allein auf der Basis digitaler Dokumente sind eine Zukunftsvision, die nicht vollständig erreicht werden kann. Es wird immer auch Papierdokumente geben, zumindest bis alle Anwendungen auf die Verarbeitung digitaler Dokumente umgestellt sind. Leider hat die digitale Signatur eines Dokuments einen entscheidenden Nachteil: Wird ein digital signiertes Dokument ausgedruckt oder konvertiert (z.B. in eine neue Wordversion), so verliert das neue Dokument die Überprüfbarkeit der Signatur, da es technisch verändert wurde, auch wenn der Inhalt unverändert geblieben ist. Hier sind künftig die Techniken digitaler Wasserzeichen von großer Bedeutung. Insbesondere bei elektronischen Formularen kommt es entscheidend auf den Inhalt und weniger auf das Darstellungsformat an. Das Fraunhofer Institut[21] ist hier als besonders qualifizierter Know-how-Träger zu nennen. Dass digitale Wasserzeichen nicht nur ein theoretisches Forschungsgebiet sind, sondern auch moderne Anwendungen hervorbringen, zeigen Kooperationen mit am Markt erfolgreichen Softwareanbietern, die diese neuen Technologien einsetzen und vermarkten.

Um nicht auf Insellösungen zu setzen, ist die Standardisierung der Geschäftsvorfälle mit marktüblichen E-Commerce-Verfahren zu kombinieren. Aus sicherheitstechnischer Sicht sind solche E-Commerce-Lösungen geeignet, die zur Wahrung der Integrität, zur gegenseitigen Authentisierung und zum Urheberschaftsnachweis die digitale Signatur und akkreditierte Public-Key-Infrastrukturen nach dem Signaturgesetz integrieren. Die Vertrauenswürdigkeit überprüfter Sicherheit kann somit auch für Bezahlvorgänge, z.B. via Internet, als Grundprinzip und Vorteil für eine breite Akzeptanz genutzt werden. Leider steht die Standardisierung von Geschäftsvorfällen und E-Commerce-Lösungen erst am Beginn ihrer Entwicklung. Zudem sind E-Commerce-Lösungen überaus zahlreich, und mögliche Standards werden teilweise von aktuellen Entwicklungen überholt. Neue M-Commerce- (Mobile Commerce-)Verfahren drängen auf den Markt. Eine kontinuierliche Marktbeobachtung ist hier notwendig, um nicht den Anschluss zu verpassen. Der Standort Deutschland kann nur so seinen Vorteil durch den Vorsprung im Bereich der digitalen Signatur und einer zugehörigen vertrauenswürdigen Public-Key-Infrastruktur dauerhaft nutzen. Die Entwicklungen im Bankenbereich sind hier von besonderem Interesse, da die Marktbeherrschung der Banken zu Standardisierungen im E-Commerce führen kann, die sich als *Bankenstandard* möglicherweise durchsetzen. Die Politik kann hier den Schutz der Bürgerinnen und Bürger bei E-Government und E-Commerce durch den Einsatz gegenseitiger Authentisierungsverfahren mittels digitaler Signaturen fordern und die Verbreitung vertrauenswürdiger Verfahren durch Modellprojekte – wie z.B. *MEDIA@*Komm – fördern. Eine vertrauensbildende Maßnahme stellt hierbei die Anwendung akkreditierter Signaturen dar, die die Bürgerinnen und Bürger beim Einsatz gegenseitiger Authentisierungsverfahren gegen Missbrauch schützt und von ihnen als vertrauenswürdig akzeptiert werden kann.

21 http://www.igd.fhg.de/igd-a8/.

Anhang

Sicherheitstechnische Qualifizierung und Zertifizierung von vertrauenswürdigen IT-Installationen

Security Qualification and Certification of Trustworthy IT-Installations

Datum:	22.05.00
Version:	8.2
Autor(en):	Christoph Sutter Markus Bartsch
Kurztitel:	SQ-Verfahren
Dateiname:	SQ82.doc

Inhaltsverzeichnis

1 Einführung

Sicherheits-risiken

Einige Sicherheitsrisiken bei der Anwendung von Informationstechnik (IT) sind so gravierend, daß sie in ihren Konsequenzen das Image von Organisationen schwer schädigen und sogar ihre Existenz in Frage stellen können. Betreiber von sicherheitssensitiven IT-Installationen übernehmen die Verantwortung für die Wahl angemessener Schutzmaßnahmen. Hierzu benötigen sie verläßliche technische Informationen und sicherheitstechnische Bewertungen.

Grenzen der ITSEC

Auf der Ebene von Produkten mit Sicherheitsfunktionen (Security) werden seit einigen Jahren systematische Prüfungen und Bewertungen durchgeführt. Ein bekanntes Verfahren hierzu ist die formale Evaluation nach den Information Technology Security Evaluation Criteria (**ITSEC**) oder den Common Criteria (**CC**).

Die nun reichlich vorhandenen Erfahrungen zeigen, daß eine in allen formalen Ansprüchen akkurat und vollständig durchgeführte formale Evaluation nicht für alle Systeme der IT-Technik gleichermaßen praktikabel ist. Evaluierbare und zertifizierbare Prüfgegenstände sind typischerweise überschaubare und relativ „kleine“ SW-**Produkte**.

Begrenzter Nutzen von Produktzertifikaten

Die Ergebnisse einer Produktevaluation nach ITSEC oder CC sind für sich alleine nicht befriedigend, weil zertifizierte Produkte in der Praxis in größeren Systemzusammenhängen auftreten. Aus den nur vereinzelt vorhandenen Produktzertifikaten lassen sich nicht ohne weiteres Sicherheitsaussagen für die gesamte IT-Installation ableiten.

Aufgaben

Die objektive Identifikation und angemessene Behebung von Sicherheitsrisiken sind das unmittelbare Anliegen eines Systemintegrators oder Betreibers einer IT-Installation. Darüber hinaus muß das erreichte Sicherheitsniveau qualifiziert werden und Wege zur weiteren Verbesserung müssen aufgezeigt werden.

Soweit erforderlich, sollte eine Zertifizierung den erarbeiteten Sicherheitsstandard gegenüber Dritten demonstrieren.

SQ

Die TÜV-Informationstechnik GmbH (TÜViT) und die SWISSiT Informationstechnik AG haben aufgrund vieler Jahre praktischer Arbeit mit der Sicherheit von Informationstechnik aus den als sachgerecht und pragmatisch erkannten Methoden ein standardisiertes Verfahren der

Sicherheitstechnischen Qualifizierung (SQ)
von vertrauenswürdigen IT-Installationen

entwickelt.

Das Verfahren erlaubt die Untersuchung von umfangreichen IT-

Installationen in angemessener Weise unter besonderer Berücksichtigung der in der Regel anzutreffenden Heterogenität, Komplexität und insbesondere Dynamik solcher Installationen.

Effizienz und Flexibilität

Das Verfahren der SQ ist durch eine erheblich höhere **Effizienz** gegenüber einer klassischen formalen Evaluation gekennzeichnet. Die verfügbaren Ressourcen können deutlich stärker auf die für die Sicherheit wirklich wesentlichen und kritischen Punkte fokussiert werden. **Unmittelbares 'Feedback'** aus den laufenden Untersuchungen erlaubt eine schnelle und angemessene Reaktion auf erkannte Probleme. Alle Verfahrenselemente lassen sich an spezifische Anforderungen oder Gegebenheiten **individuell anpassen**.

Evaluation und Systemakkreditierung

Die Sicherheitstechnische Qualifizierung SQ von IT-Installationen ist das **Bindeglied** zwischen der formalen Evaluation von einzelnen Komponenten und dem Security Management. Auf der einen Seite werden vorhandene Evaluationsresultate oder gleichwertige Qualitätsaussagen in die Bewertung konsequent einbezogen. Auf der anderen Seite liefert die SQ die notwendigen sicherheitstechnischen Aussagen über die IT-Installationen als Teil des Gesamtsystems. Die Durchführung von Sicherheitstechnischen Qualifizierungen ist daher eines der „Controls" im Rahmen eines umfassenden Risikomanagements.

Systemzertifizierung

Standardisierte Anforderungsprofile ermöglichen die **Qualifizierung** und **Zertifizierung** des Sicherheitsniveaus einer IT-Installation. Das Verfahren erlaubt die schrittweise Verbesserung des Sicherheitsniveaus einer IT-Installation über Zwischenstufen bis zu einem vom Betreiber als sinnvoll und notwendig erachteten Sicherheitsstandard.

2 Überblick über die Bewertungsaspekte

Das erreichte Sicherheitsniveau einer IT-Installation wird auf der Basis von erfüllten Mindestanforderungen festgestellt. Dabei wird eine Reihe von **Bewertungsaspekte** in die Untersuchung einbezogen (s. nachfolgende Tabelle 1).

Tabelle 1: Bewertungsaspekte für die Sicherheit von IT-Installationen

- Technische Sicherheitsanforderungen und Vorgaben
- Dokumentation der IT-Installation
- Sicherheit der verwendeten Komponenten
- Benutzer-, Administrations- und sonstige Betriebsdokumente
- Mittel des Systemmanagement
- Verfahren und technische Mittel des Änderungsmanagements
- Tests und Inspektionen
- Operationelle Anforderungen
- Sicherheitsanalysen

2.1 Technische Sicherheitsanforderungen und Vorgaben

Eine Untersuchung der Sicherheit ist nur sinnvoll, wenn ausreichend deutlich ist, welchen Anforderungen die fragliche IT-Installation genügen und welche Eigenschaften diese haben soll. Nur gegenüber definierten (deutlichen) Anforderungen als Maßstab ist überhaupt erkennbar, was eigentlich Thema einer Prüfung und damit Bewertung sein soll. Eine zentrale Mindestforderung ist also, daß eine für die Zwecke der Untersuchung geeignete Spezifikation der Bedrohungen, Sicherheitsziele und relevanten Randbedingungen vorliegt.

2.2 Dokumentation der IT-Installation

Eine für die Untersuchungszwecke angemessene Dokumentation der IT-Installation ist erforderlich. Zum einen dient diese zur Vorbereitung oder Interpretation von Tests und Inspektionen, zum anderen müssen Sicherheitsanalysen notwendigerweise auf Informationen über die Spezifikationen der IT-Installation, ihrer Subsysteme sowie ihrer Architektur und Abläufe basieren. Das Bewertungskriterium ist somit, ob die IT-Installation ausreichend transparent ist und ihre einzelnen Elemente und ihre Beziehungen erkennbar und verständlich sind.

2.3 Sicherheit der verwendeten Komponenten

Das Vertrauen in die Sicherheit der Subsysteme und der darin verwendeten Komponenten (z. B. bestimmte Produkte) ist im Regelfall eine notwendige Voraussetzung für die Sicherheit der gesamten Installation. Nur dort, wo

gegebene Randbedingungen oder Eigenschaften der Gesamtarchitektur vorhandene Schwachstellen anderweitig sichern, kann auf Anforderungen an die Basiskomponenten ggf. verzichtet werden.

2.4 Benutzer-, Administrations- und sonstige Betriebsdokumente

Die IT-Installation wird ihren Sicherheitszielen letztendlich nur dann gerecht, wenn ihr Verhalten und ihre Eigenschaften von denen, die mit der Installation direkt oder indirekt interagieren (Benutzer, Anwender u. a.), verstanden wird. Nur dann werden die tägliche Arbeit mit und Eingriffe in die IT-Installation sachgerecht und sicher sein. Hierzu ist alles zu bewerten, was der Information der Betroffenen über äußerlich wahrnehmbare Funktionen, Eigenschaften und Einflußmöglichkeiten an der Installation dient (Bedienung, Schnittstellen, Operating, Maintenance usw.).

2.5 Mittel des Systemmanagements

Für das Systemmanagement müssen angemessene technische Mittel bereitstehen. Der stets sichere Zustand der IT-Installation im Betrieb und die sichere Beherrschung von Ausnahmesituationen kann nur gewährleistet werden, wenn angemessene technische Mittel hierzu bereitstehen.

2.6 Verfahren und technische Mittel des Änderungsmanagements

Eine ‘laufende’ IT-Installation verändert sich. Veränderungen werden in der Regel Auswirkungen auf das Ausmaß der Erfüllung der Sicherheitsanforderungen haben. Veränderungen dürfen also nicht unkontrolliert geschehen. Falls notwendig, müssen Veränderungen rechtzeitig im Hinblick auf die Sicherheitsauswirkungen untersucht und verstanden werden. Ggf. sind Analysen und Unterlagen anzupassen oder vorzubereiten. Für die Planung und Durchführung von Änderungen muß ein Konzept vorliegen, um Risiken und Konsequenzen für die Sicherheit adäquat bewerten zu können.

2.7 Tests und Inspektionen

Jede IT-Installation kann versagen. Die regelmäßige oder anlaßgemäße Überprüfung des Zustandes, der Eigenschaften und des Verhaltens ist notwendig, um die ständige Wirksamkeit der IT-Installation im Sinne der Sicherheitsanforderungen belegen zu können. Ein Anlaß ist der Konstruktionsvorgang selbst.

2.8 Operationelle Anforderungen

Jede noch so sichere IT-Installation wird nur dann optimal bestimmten Sicherheitsanforderungen genügen, wenn sie von den Personen, die diese bedienen oder verwalten, fachkundig eingesetzt wird. Ebenso muß eine sichere IT-Installation innerhalb bestimmter räumlicher Gegebenheiten eingebettet werden, so daß die Zugangssicherung zur Installation in ihrer Wirkung nicht untergraben werden kann.

2.9 Sicherheitsanalysen

Die vorher genannten Bewertungsaspekte sind Voraussetzungen für eine erfolgreiche Bewertung der IT-Installation. Erst die tatsächlich durchgeführte und ggf. ständig geübte Analyse der Eigenschaften unter Beachtung der ergänzenden Aspekte sowie der Ergebnisse von Überprüfungen gibt schließlich die verlangte Auskunft über die IT-Installation.

3 Bewertungskriterien

Für jeden der in Kap. 2 benannten Bewertungsaspekte gibt es jeweils eine Reihe von genau definierten Kriterien, welche die Anforderungen für die Sicherheitstechnische Qualifizierung einer IT-Installation festlegen. Diese Anforderungen mit allen in dem Qualifizierungsverfahren einbezogenen Teilaspekten sind in Tabelle 2 stichpunktartig dargestellt und in den folgenden Abschnitten näher erläutert.

Tabelle 2: Teilaspekte: Einzelheiten der Bewertungsaspekte

Bewertungsaspekte	Teilaspekte
Technische Sicherheitsanforderungen und Vorgaben	• Darstellung der Rahmenbedingungen (Bedrohungen, Sicherheitspolitik, Voraussetzungen) • Darstellung der Sicherheitsleistungen (Sicherheitsziele und Sicherheitsfunktionen)
Dokumentation der IT-Installation	• Dokumentation der statischen Struktur (Zerlegung - flächendeckend und punktuell) • Dokumentation der dynamischen Struktur (Nutzungsbeziehungen, Datenflüsse) • Dokumentation der Sicherheitsarchitektur (Separierungsstruktur, Kryptoarchitektur, ggf. anderes)
Sicherheit der verwendeten Komponenten	• Dokumentation über die Subsysteme • Sicherheitsqualität der Subsysteme
Benutzer-, Administrations- und sonstige Betriebsdokumente	• Allgemeines Handbuch der IT-Installation • Dokumentation zu Subsystemen • Sicherheitshandbuch der IT-Installation
Mittel des Systemmanagements	• Monitoring der IT-Installation • Konfigurationsmanagement
Verfahren und technische Mittel des Änderungsmanagements	• Security Maintenance Plan (SMP) • Anpassung von Unterlagen • Regelung der Verantwortlichkeit • Analyse der Änderungen • Planung von Verbesserungen
Tests und Inspektionen	• Allgemeine funktionale Korrektheit • Belege zur Struktur der IT-Installation • Nachweis der Sicherheitsfunktionen • Konfigurationsanalyse • Penetrationstests

Bewertungsaspekte	Teilaspekte
Operationelle Anforderungen	• personelle Verantwortlichkeiten • physikalische Sicherheit
Sicherheitsanalysen	• Schwachstellenermittlung • Wirksamkeit der Sicherheitsfunktionen • Klassifizierung der Subsysteme und Komponenten

3.1 Technische Sicherheitsanforderungen und Vorgaben

Es werden technische Sicherheitsanforderungen erstellt. Diese müssen die Sicherheitspolitik und die Bedrohungen sowie die Sicherheitsleistungen darlegen. Die Informationen zu den technischen Sicherheitsanforderungen dürfen keine inhaltlichen Widersprüche aufweisen.

3.2 Dokumentation der IT-Installation

Eine Darstellung der statischen Struktur der IT-Installation, die mindestens die Zerlegung in grundlegende Subsysteme darlegt, wird erstellt. Die Zerlegung in Subsysteme muß in dieser Darstellung dann ggf. bis auf Komponenten verfeinert werden, wenn ein Subsystem als sicherheitsspezifisch erkannt wurde. Die Nutzungsbeziehungen und Datenflüsse zwischen den identifizierten Subsystemen werden dargelegt.

3.3 Sicherheit der verwendeten Komponenten

Für alle Komponenten und Subsysteme der Zerlegung müssen funktionale Spezifikationen erkennbar sein. Darlegungen der externen Schnittstellen der Installation müssen bereitgestellt werden. Die Sicherheitsanforderungen von sicherheitsspezifischen Subsystemen müssen erkennbar sein. Für wesentliche sicherheitsspezifische Subsysteme werden Darlegungen der Sicherheitsanforderungen erstellt.

3.4 Benutzer-, Administrations- und sonstige Betriebsdokumente

Handbücher zur IT-Installation sowie zu den sicherheitsspezifischen und kritischen Subsystemen müssen existieren.

3.5 Mittel des Systemmanagements

Ein Konfigurationsmanagement der sicherheitsspezifischen Komponenten ist vorhanden und ein Monitoring ist möglich.

3.6 Verfahren und technische Mittel des Änderungsmanagements

Ein Security Maintenance-Plan wird erstellt. Dieser muß darlegen, in welcher Weise Dokumentation und Sicherheitsanalysen bei Änderungen an der IT-Installation regelmäßig zumindest nachträglich angepaßt werden. In dieses Verfahren müssen mindestens die Dokumentation der Struktur der IT-Installation (Zerlegung) und die Technischen Sicherheitsanforderungen eingeschlossen sein.

3.7 Tests und Inspektionen

Über eine Inspektion an der IT-Installation werden die sicherheitsspezifischen Komponenten identifiziert und ihr Vorhandensein in der angenommenen Version vollständig bestätigt. Der Betreiber legt für die Prüfer erkennbare Nachweise über vollständige und erfolgreiche Tests aller Sicherheitsfunktionen vor.

3.8 Operationelle Anforderungen

Es müssen geeignete operationelle Bedingungen vorliegen, die eine einwandfreie Funktionsweise des zu untersuchenden Systems unterstützen. Die personellen Verantwortlichkeiten und räumlichen Gegebenheiten gewährleisten den fachkundigen Einsatz und die Zugangssicherung der Installation.

3.9 Sicherheitsanalysen

Die Prüfer geben fundierte Aussagen zu den Schwachstellen der Installation. Resultierende Vermutungen über die Klassifizierung der Subsysteme und die Wirksamkeit der Sicherheitsfunktionen werden gegeben.

4 Zertifizierung

Auf der Basis der Bewertungskriterien für die Sicherheitstechnische Qualifizierung (SQ) (siehe Kapitel 3) kann bei Erfüllung aller Teilaspekte für die untersuchte IT-Installation ein **Zertifikat** ausgesprochen werden. Jeweils ein deutsches und englisches Zertifikat ist in den nachfolgenden Abbildungen dargestellt. Die Bewertungsaspekte sind jeweils auf der Rückseite abgedruckt.

Zertifikat

Die Zertifizierungsstelle der
TÜV Informationstechnik GmbH bescheinigt hiermit
der
<Firma>
<Straße>
<PLZ, Ort>

die
Sicherheitstechnische Qualifizierung

für die Installation der
<Bezeichnung der Installation>

Der Umfang der in der Qualifizierung einbezogenen System-Teile und die mit der <Bezeichnung der Installation> verfolgten Sicherheitsziele sind in dem Dokument <Name, Version nn>, spezifiziert.

Die Qualifizierung wurde durchgeführt von
der Firma
TÜV Informationstechnik GmbH
Am Technologiepark 1
D-45307 Essen

auf der Grundlage der Anforderungen in der Spezifikation SQ, Version 8.2.
Eine Zusammenfassung der Anforderungen wird umseitig wiedergegeben.

Dieses Zertifikat gilt nur in Verbindung mit dem Qualifizierungsbericht
<Name, Version nn> vom <Datum> sofern die Maßgaben für
die Installation eingehalten werden.

99

Zertifikat Register Nr.: TUVIT SQ99xx.99

Essen, xx.yy.1999
Zertifizierungsstelle

TÜV Informationstechnik GmbH - ein Unternehmen der (N)TÜV Gruppe
Am Technologiepark 1 45307 Essen

Abbildung 1: Deutsches Musterzertifikat

TÜViT

Certificate

The certification body of TÜV Informationstechnik GmbH
hereby confirms that

the company
<name of the company>
<address>
<postal code, city>

has passed the
Security Qualification

for the installation of:
<name of the installation>

The extent of the parts of the installation included in this qualification
as well as the considered security objectives are specified
in the document <name, version> as of <date>.

The qualification was performed
by
TÜV Informationstechnik GmbH
An Technologiepark 1
D-45307 Essen

on the basis of the requirements of the specification SQ, version 8.2.
A summary of the requirements is printed overleaf.

This certificate is valid only in conjunction with the
qualification report «name, version» as of «date» provided that
the measures for the installation described therein are respected.

Certificate Registration No.:
TUVIT-SQ0xxx.99

Essen, 1999-month-day
Certification Body

TÜV Informationstechnik GmbH - Subsidiary of the RWTÜV Group
An Technologiepark 1, D-45307 Essen

Abbildung 2: Englisches Musterzertifikat