Bayerischer Kommunaler
Prüfungsverband

BKPV

Geschäftsbericht

2002

- auszugsweise -

Bayerischer Kommunaler Prüfungsverband
Renatastraße 73, 80639 München
Telefon: (089) 1272-0, Telefax: (089) 168 86 46
E-Mail: geschaeftsstelle@bkpv.de
Internet: www.bkpv.de

Auszug aus dem Inhaltsverzeichnis

C. Aktuelle Fragen aus der Prüfungs- und Beratungstätigkeit

Eingruppierung von Sachbearbeitern in Führerscheinstellen (Fahrerlaubnisbehörden)

Verfasser: Berthold-Edwin **Anger**
Willi **Müller**

In diesem Beitrag befassen wir uns mit der Bewertung der Sachbearbeiterstellen im Fahrerlaubniswesen. Anlaß hierzu gaben die europaweite Angleichung des Fahrerlaubnisrechts, die mit der seit 01.01.1999 geltenden neuen Fahrerlaubnisverordnung (FEV) umgesetzt wurde, mit der die Anforderungen an die Sachbearbeiter allgemein nicht unerheblich gestiegen sind, und die vielen daraufhin an uns gerichteten Fragen bezüglich der tariflichen Auswirkungen.

In unseren Geschäftsberichten 1996, S. 34 ff., und 2000, S. 66 ff., hatten wir uns mit der **Personalbemessung** in Kraftfahrzeug-Zulassungsstellen und in Führerscheinstellen befaßt. Auf die **tarifliche Bewertung** der Stellen der Sachbearbeiter in **Zulassungsstellen** sind wir in unseren BKPV-Mitteilungen 2/1999 RdNr. 14 eingegangen. Aufgrund des Ergebnisses unserer damaligen Erhebungen und Zählungen kamen wir zu der Auffassung, daß die Sachbearbeiter der Zulassungsstellen - mit der geschilderten grundsätzlichen Allzuständigkeit - im tariflichen Sinne „Fachkenntnisse“ einzusetzen haben, die qualitativ als „gründlich“ und ihrem Umfang nach insgesamt bereits als „vielseitig“ zu bezeichnen sind. Daraus folgte eine tarifliche Bewertung mit VergGr. VII Fallgr. 1 b. Früher waren wir davon ausgegangen, daß sich die von einem Sachbearbeiter im Schalterdienst der Zulassungsstelle einzusetzenden „gründlichen (näheren) Fachkenntnisse“ auch bei zusammenfassender Betrachtung gemäß § 22 Abs. 2 UAbs. 2 Satz 2 BAT auf ein eng abgegrenztes Teilgebiet bzw. Wissensgebiet im Sinne der tariflichen Begriffsdefinition und der Arbeitsrechtsprechung beschränken und somit den Begriff der „vielseitigen“ Fachkenntnisse in VergGr. VII Fallgr. 1 b (bzw. VI b Fallgr. 1 b nach sechsjähriger Bewährung) noch nicht erfüllen.

Bei den **Führerscheinsachbearbeitern** bejahten wir schon bisher regelmäßig die Notwendigkeit des Einsatzes „gründlicher“ Fachkenntnisse in „vielseitigem“ Umfang und somit die VergGr. VII Fallgr. 1 b. Die Umstellung des Fahrerlaubnisrechts hat, wie sich heute eindeutig feststellen läßt, für die Sachbearbeiter in zweifacher Hinsicht höhere Anforderungen gebracht. Zum einen haben sich die Zahl der anzuwendenden Vorschriften und das daraus resultierende Fachwissen deutlich erhöht. Zum anderen ist die Sachbearbeitung zu einem erheblichen Teil - qualitativ - anspruchsvoller geworden.

a) Unsere Erhebungen und Zählungen ergaben, daß der Begriff der „vielseitigen“ Fachkenntnisse nunmehr eindeutig erfüllt wird und bisher etwa vorhandene Zweifel hinsichtlich

der tariflichen Vielseitigkeit nicht mehr möglich sind, daß andererseits aber „umfassende“ Fachkenntnisse in der tariflich vorausgesetzten Breite nicht vorliegen.

„**Fachkenntnisse**“ sind nach der Interpretation der Tarifpartner „Kenntnisse von Gesetzen, Verwaltungsvorschriften und Tarifbestimmungen usw.“ des Aufgabenkreises. Wie sich aus dem Zusatz „usw.“ ergibt, können sich diese Kenntnisse auch auf die etwa notwendige Kenntnis von - normierten oder nicht normierten - Ablaufregelungen und Verfahrensabläufen oder auch auf irgendwelche sonstigen Fachkenntnisse außerhalb der Fachkenntnisse im eigentlichen Verwaltungsbereich[1] beziehen (z.B. Gesprächsführung, Umgangsformen, psychologisches Einfühlungsvermögen, Organisationstalent). Fachkenntnisse sind solche, die unerläßlich sind, um die übertragenen Aufgaben ordnungsgemäß erfüllen zu können. Zu den Fachkenntnissen im tariflichen Sinne rechnet auch Erfahrungswissen.[2] Bloße Lebenserfahrung, die unabhängig von der speziellen Tätigkeit des Angestellten erworben wird, sowie Allgemeinwissen sind allerdings nicht als „Fachkenntnisse“ anzusehen.[3] Ein Arbeitsvorgang, bei dem „Fachkenntnisse“ nicht einzusetzen sind (VergGr. VIII Fallgr. 1 a), darf aus Rechtsgründen mit einem Arbeitsvorgang, der „Fachkenntnisse“ erfordert, nicht zu einem Arbeitsvorgang zusammengefaßt werden.[4]

„**Gründliche**“ Fachkenntnisse im Sinne des Tarifmerkmals haben ein qualitatives und ein quantitatives Element.[5]

– Qualitativ müssen die „gründlichen“ Fachkenntnisse nach der tariflichen Klammerbemerkung zur VergGr. VII Fallgr. 1 a „*nähere*“ Kenntnisse sein. Nach der Rechtsprechung des LAG Bayern[6] soll der Angestellte aufgrund der „näheren“ Kenntnisse in der Lage sein, in seinem Aufgabengebiet ordnungsgemäß zu arbeiten. Dies ist anzunehmen, wenn er den Normalfall (der untersten Wertigkeitsstufe, in der erstmals Fachkenntnisse verlangt werden) in seiner verschiedenen Abwandlung sachlich richtig bearbeiten kann. Die Fachkenntnisse müssen in dem Sinne „nähere“ sein, daß sich der Angestellte jederzeit auf sie stützen und verlassen kann. Lediglich oberflächliche Kenntnisse reichen somit nicht aus.[7] Jedoch kann bereits eine wenig schwierige Auswertung „gründliche“ Fachkenntnisse (nämlich nähere Kenntnisse der betreffenden Vorschriften oder der sonstigen Regelungen) erfordern.

– Quantitativ genügt es, wenn sich die „gründlichen“ (näheren) Fachkenntnisse auf ein „*eng abgegrenztes*“ Teilgebiet bzw. Wissensgebiet beschränken. Ein ganz unerhebliches Maß an Fachkenntnissen reicht aber nicht aus.[8] Die Erfüllung der quantitativen

---

1 BAG, Urteile vom 24.08.1983, vom 14.08.1985 und vom 22.10.1986, AP Nrn. 78, 109 und 126 zu §§ 22, 23 BAT 1975

2 BAG, Urteile vom 27.06.1962, AP Nr. 87 zu § 3 TO.A, und vom 29.08.1984, AP Nr. 94 zu §§ 22, 23 BAT 1975

3 BAG, Urteil vom 29.08.1984, AP Nr. 94 zu §§ 22, 23 BAT 1975

4 BAG, Urteil vom 01.09.1982, AP Nr. 65 zu §§ 22, 23 BAT 1975

5 BAG, Urteil vom 24.08.1983, AP Nr. 78 zu §§ 22, 23 BAT 1975

6 siehe insbesondere Urteil vom 11.08.1962 - Sa 887/61 -

7 siehe Fußnote 5

8 siehe Fußnote 5

Anforderungen kann sich aus der zusammenfassenden Betrachtung (gemäß § 22 Abs. 2 UAbs. 2 Satz 2 BAT) der bei der Erledigung der Tätigkeit in Frage kommenden Fachkenntnisse ergeben.[9]

„**Vielseitige**“ Fachkenntnisse erfordern gegenüber den „gründlichen“ Fachkenntnissen (im quantitativen Sinne) eine Erweiterung der Fachkenntnisse dem Umfang nach. Dabei ist nicht jeweils nur auf den einzelnen Arbeitsvorgang, sondern auf deren Summe abzustellen; die Vielseitigkeit der Fachkenntnisse kann nämlich in der Regel erst bei einer Gesamtbetrachtung mehrerer Arbeitsvorgänge festgestellt werden.[10] Das Gebiet, auf dem nähere Kenntnisse von Vorschriften usw. im obigen Sinne tatsächlich einzusetzen sind, darf nicht mehr eng abgegrenzt bzw. eng bemessen sein. Es muß vielmehr eine gewisse Breite aufweisen und so gestaltet sein, daß es nach seinem Umfang „vielseitige“ Fachkenntnisse erfordert. Die Vielseitigkeit kann sich auf die Mannigfaltigkeit und Unterschiedlichkeit des einzusetzenden Fach- bzw. Erfahrungswissens beziehen.[11] Da der Begriff „vielseitig“ (nur) quantitativ aufzufassen ist,[12] ist für sein Vorliegen die Menge der anzuwendenden Bestimmungen bzw. Regelungen einschließlich des Erfahrungswissens maßgebend. Auf die Zahl der Rechts- bzw. Fachgebiete, in denen der Angestellte Fachkenntnisse einzusetzen hat, kommt es dabei nicht an, sondern - wie erwähnt - auf den Umfang der insgesamt benötigten Fachkenntnisse.[13] Das Merkmal „vielseitige“ Fachkenntnisse ist in § 22 Abs. 2 UAbs. 2 Satz 2 BAT als Musterbeispiel dafür angeführt, daß eine tarifliche Anforderung auch (erst) bei zusammenfassender Betrachtung vorliegen kann, d.h., daß das Merkmal zwar beim einzelnen Arbeitsvorgang für sich betrachtet noch nicht, jedoch in der Summe der Arbeitsvorgänge erfüllt wird. Die verlangte Qualität der Fachkenntnisse entspricht der der „gründlichen“ (= näheren) Fachkenntnisse in VergGr. VIII 1 b und VII 1 a. Daraus folgt unter anderem, daß zu „vielseitigen“ Fachkenntnissen nur solche Fachkenntnisse addiert werden können, die ihrerseits „gründliche“ (nähere) Fachkenntnisse sind.

„**Umfassende**“ Fachkenntnisse setzen nach der Klammerbemerkung zur VergGr. V b Fallgr. 1 a bezüglich des einzusetzenden Fachwissens eine Steigerung der Breite (und auch der Tiefe) voraus. Die geforderte Steigerung der Breite nach, also in der Quantität der Fachkenntnisse, ist nach der Rechtsprechung des BAG erst dann gegeben, wenn ein breites, d.h. nach dem (quantitativen) Umfang der Kenntnisse bedeutendes Wissen eingesetzt werden muß.[14]

b) Die Arbeitsvorgänge (Bearbeitungs- oder Auskunftsfälle, jeweils einschließlich Zusammenhangstätigkeiten) mit höheren Anforderungen, insbesondere bei

- sogenannten Umtauschfällen (mit Besitzstandswahrung),
- Umschreibungen aufgrund einer ausländischen Fahrerlaubnis,
- Nachuntersuchungen Facharztgutachten (außer Normalfälle),
- Nachuntersuchungen MPU-Gutachten,
- nicht einzelfallbezogenen Auskünften nicht einfacher Art,

---

[9] siehe Fußnote 5

[10] BAG, Urteil vom 25.11.1981, AP Nr. 51 zu §§ 22, 23 BAT 1975

[11] LAG Bayern, Urteile vom 04.07.1961 - 3 Sa 619/61 -, 31.07.1962 - 6 Sa 99/62 N - und 16.04.1962 - 3 Sa 904/61 -

[12] siehe Fußnote 10

[13] siehe Fußnote 3

[14] BAG, Urteil vom 28.03.1962, AP Nr. 85 zu § 3 TO.A, und BAG in AP Nr. 12 zu § 23 a BAT

nehmen den Führerscheinsachbearbeiter nach unseren Ermittlungen aufgrund der Änderungen durch das neue Fahrerlaubnisrecht in einem zeitlichen Ausmaß in Anspruch, daß wir nunmehr im Regelfall die **VergGr. VI b Fallgr. 1 a** als erfüllt betrachten. Diese Vergütungs- und Fallgruppe setzt neben „gründlichen und vielseitigen“ Fachkenntnissen zu mindestens einem Fünftel „selbständige Leistungen“ voraus.

„**Selbständige Leistungen**“ erfordern nach der tariflichen Begriffsdefinition in den Klammersätzen zu den Vergütungsgruppen VI b 1 a und V c 1 a/1 b ein den vorausgesetzten „vielseitigen“ Fachkenntnissen entsprechendes selbständiges Erarbeiten von Ergebnissen unter Entwicklung eigener geistiger Initiative, wobei eine leichte geistige Arbeit nicht ausreicht. Es genügt - was häufig verkannt wird - nicht, wenn Leistungen nur im Sinne des allgemeinen Sprachgebrauchs selbständig erbracht werden, also z.B. ohne Anweisung und ohne Anleitung von Vorgesetzten. Vielmehr ist eine ***nicht leichte*** gedankliche Umsetzarbeit dahingehend zu entwickeln, daß Ergebnisse eigenständig „erarbeitet“ werden. Einfacher Gesetzesvollzug (bzw. Vollzug sonstiger Normen und Regelungen) erfüllt dieses Merkmal nicht. Erforderlich ist eine Gedankenarbeit, die hinsichtlich des einzuschlagenden Weges wie auch hinsichtlich des zu findenden Ergebnisses eine eigene Beurteilung mit eigenem Entschluß enthält.[15] Kennzeichnend für selbständige Leistungen in diesem Sinne können Ermessens-, Beurteilungs-, Gestaltungs- oder Entscheidungsspielräume (wie auch immer geartet, also ohne Bindung an die verwaltungsrechtlichen Fachbegriffe) sein.[16] Es werden Abwägungen verlangt, Anforderungen an das Überlegungsvermögen gestellt. Der Angestellte muß also unterschiedliche Informationen verknüpfen, untereinander abwägen und zu einer Entscheidung kommen. Dieser Prozeß kann bei entsprechender Routine durchaus schnell ablaufen. Gleichwohl bleibt das Faktum der (nicht leichten) geistigen Arbeit bestehen. Diese wird erbracht, wenn sich der Angestellte bei der Arbeit fragen muß: Wie geht es nun weiter? Worauf kommt es nun an? Was muß als nächstes geschehen?[17] Eine „selbständige Leistung“ kann darin liegen, daß vorgegebene oder zu ermittelnde Daten und Fakten aufgrund entsprechender Fachkenntnisse in ein neues Ergebnis umgewandelt werden. Eine rein rechnerische „Bearbeitung“ anhand der vier Grundrechenarten reicht nicht aus.

Eine „gedankliche Umsetzarbeit“ ist dann als lediglich leichte geistige Arbeit zu bezeichnen, wenn sie in Anbetracht der sich wiederholenden oder ähnelnden Fälle als schematisch gelten muß. Die Arbeit darf sich zum Beispiel nicht in der Sammlung oder Übertragung feststehender Fakten erschöpfen, ohne daß hinsichtlich des einzuschlagenden Weges und des zu findenden Ergebnisses eine Wahl- oder Entscheidungsmöglichkeit besteht oder eine besondere Überlegung notwendig ist. Das jeweilige Arbeitsergebnis darf nicht aus tatsächlichen oder rechtlichen Gründen von vornherein feststehen, wie z.B. im Fall von Wegstrecken- und Mitnahmeentschädigungen im Reisekostenrecht; es müssen vielmehr Möglichkeiten der Entscheidung bestehen.[18]

Andererseits sind „selbständige Leistungen“ nicht erst dann anzunehmen, wenn die Tätigkeit etwa besondere Schwierigkeit bereitet oder überhaupt schwierig ist,[19] sondern schon dann, wenn ein Ergebnis aufgrund eigener Initiative erarbeitet wird und darin nicht lediglich eine leichte geistige Arbeit liegt. Eine „schwierige“ Tätigkeit ist demgegenüber erst in

[15] BAG, Urteile vom 25.07.1962 und vom 26.06.1963, AP Nrn. 92 und 99 zu § 3 TO.A

[16] BAG, Urteil vom 14.08.1985, AP Nr. 109 zu §§ 22, 23 BAT 1975

[17] BAG, Urteil vom 18.05.1994, AP Nr. 178 zu §§ 22, 23 BAT 1975

[18] BAG, Urteil vom 23.02.1983 Nr. 4 AZR 209/80 (nicht in AP abgedruckt)

[19] BAG, Urteil vom 10.12.1969, AP Nr. 27 zu §§ 22, 23 BAT

VergGr. V b 1 a/1 b und IV b gefordert; sie ist mit der „nicht leichten“ geistigen Arbeit in den darunterliegenden Vergütungsgruppen nicht mehr identisch. Somit bedeuten die in VergGr. VI b 1 a und V c 1 a/1 b vorausgesetzten „selbständigen (= nicht leichten) Leistungen“ nicht zugleich auch die Schwierigkeitsanforderung, die in VergGr. V b 1 a/1 b und IV b aufgrund der verlangten Steigerung der *Tiefe* nach gestellt ist (neben der erforderlichen Steigerung der Breite nach).

Unterschriftsbefugnis wird für das Vorliegen „selbständiger Leistungen“ nicht vorausgesetzt; sie sind schon dann gegeben, wenn Angestellte entsprechende (nicht leichte geistige) Arbeiten ohne fremde Hilfe unterschriftsreif fertigstellen. Das Vorhandensein einer Aufsicht, Überwachung oder Kontrolle macht tatsächlich erbrachte „selbständige Leistungen im Tarifsinne“ nicht zu unselbständigen.[20] Die Verwendung von Formblättern schließt in diesem Sinne „selbständige Leistungen“ nicht von vornherein aus.[21] Allerdings wirkt sich die Verwendung von Vordrucken regelmäßig auf die Bearbeitungsdauer eines Arbeitsvorgangs und somit auf den zeitlichen Umfang der „selbständigen Leistungen“ aus.

Arbeitsvorgänge mit und Arbeitsvorgänge ohne „selbständige Leistungen“ dürfen nicht zu einem (einheitlichen) Arbeitsvorgang im Tarifsinne zusammengefaßt werden.[22]

Wenn „selbständige Leistungen“ in einem Arbeitsvorgang in rechtserheblichem Ausmaß anfallen, so sind sie mit der gesamten Dauer des Arbeitsvorgangs einschließlich der Zusammenhangsarbeiten zu berücksichtigen.[23] Wenn beispielsweise ein Arbeitsvorgang mit allen Nebenarbeiten (Heraussuchen der Akte und sonstiger Unterlagen, Aktenstudium, eigene Erarbeitung des Ergebnisses unter Einsatz nicht leichter Gedankenarbeit, Fertigung eines Schreibens, Schlußkontrolle, Ablage) einen größeren Zeitaufwand verursacht, die „Erarbeitung der Lösung“ selbst aber lediglich einen Teil hiervon in Anspruch nimmt, ist in diesem Fall der gesamte Zeitaufwand - und nicht etwa nur die reine „Erarbeitungszeit“ - unter das Tätigkeitsmerkmal der „selbständigen Leistungen“ zu subsumieren.

Unser Bewertungsergebnis (VergGr. VI b 1 a) geht von folgenden organisatorischen Verhältnissen aus:

– Vorgesetzte nehmen die allgemeinen Leitungs- und Führungsaufgaben wahr und werden in „schwierigen“ oder „besonders schwierigen“ Angelegenheiten/Fragen insbesondere bei

  - vorzeitiger Erteilung der Fahrerlaubnis,
  - Versagung der Fahrerlaubnis,
  - Eignungsüberprüfung,
  - Verstoß gegen das Betäubungsmittelgesetz,
  - Entzug der Fahrerlaubnis,

[20] BAG, Urteile vom 02.03.1960, AP Nr. 60 zu § 3 TO.A, und vom 17.02.1961, AP Nr. 3 zu § 611 BGB

[21] siehe Fußnote 10

[22] BAG, Urteile vom 02.12.1981, AP Nr. 53 zu §§ 22, 23 BAT 1975, und vom 05.12.1990 Nr. 4 AZR 244/90, ZTR 1991, 159

[23] BAG, Urteile vom 14.02.1979, 19.03.1986, 20.10.1993 und 18.05.1994, AP Nrn. 15, 116, 172 und 178 zu §§ 22, 23 BAT 1975, und Beschluß vom 22.03.1995, ZTR 1995, 361

- Neuerteilung der Fahrerlaubnis nach Entzug,
- Nachuntersuchung

tätig.

– Mehrfachtäterangelegenheiten, Fahrschul- und Fahrlehrerwesen sind auf bestimmte Dienstkräfte konzentriert („spezialisierte“ Aufgabenwahrnehmung).

– Sogenannte Umtauschfälle und Fahrgastbeförderungsfälle sind auf die Führerscheinsachbearbeiter (gleichmäßig) verteilt, also nicht „spezialisiert“.

Ergänzend weisen wir in diesem Zusammenhang auf unsere Ausführungen zur Organisation in Führerscheinstellen in Abschnitt 5 unseres Beitrags „Personalbemessung in Führerscheinstellen“ im Geschäftsbericht 2000, S. 74/75, hin.

Die **VergGr. V c Fallgr. 1 a**, die mindestens zu einem Drittel „selbständige Leistungen“ im Tarifsinne voraussetzt, kann bei einem Führerscheinsachbearbeiter dann erfüllt sein, wenn ihm etwa zusätzlich Mehrfachtäterangelegenheiten übertragen sind und/oder er - aus welchen Gründen auch immer - Tätigkeiten erledigen muß, die normalerweise von einer vorgesetzten Dienstkraft wahrgenommen werden sollten.

Aufwandserstattung oder Anliegerregie für die Grundstücksanschlüsse zu Wasserversorgungs- und Entwässerungseinrichtungen

Verfasser: Hans **Rausch**

Inhaltsübersicht Seite

1. Einführung

Mit dem Gesetz zur Änderung des Kommunalabgabengesetzes (KAGÄndG) vom 25.07.2002 (GVBl S. 322) hat der Gesetzgeber die Bestimmungen über die Grundstücksanschlüsse zu Wasserversorgungs- und Entwässerungseinrichtungen entscheidend geändert. Dabei ging es dem Gesetzgeber zunächst um zweierlei. Zum einen sollte es den Kommunen ermöglicht werden, die nach früher geltendem Recht zulässige sogenannte Anliegerregie für in öffentlichem Straßengrund liegende Teile von Hausanschlüssen wieder zuzulassen. Zum andern sollte der kommunale Einrichtungsträger, der nicht die Anliegerregie, sondern eine kommunale Bewirtschaftung der Einrichtung wählt, wie bislang auf die Erstattung des Aufwands für die nicht im öffentlichen Straßengrund liegenden Teile der Einrichtung beschränkt bleiben. Derartige Erstattungsansprüche können jetzt abgelöst oder im Rahmen städtebaulicher Verträge übernommen werden.

In unserem Geschäftsbericht 1995, S. 94 bis 99, hatten wir zu Fragen, die in der kommunalen Praxis bei der Geltendmachung von Aufwandserstattungsansprüchen für Grundstücksanschlüsse nach Art. 9 Abs. 1 des Kommunalabgabengesetzes (KAG) aufgetreten sind, Stellung genommen. Diese Ausführungen werden nunmehr - unter Berücksichtigung der zwischenzeitlichen Gesetzesänderungen - aktualisiert.

Zu den hier aufgeworfenen Fragen und zu den weiteren Bestimmungen des KAGÄndG 2002 ist noch die bei der Gesetzesbehandlung im Landtag angekündigte Vollzugsbekanntmachung des Bayerischen Staatsministeriums des Innern abzuwarten.[1] In der Literatur wurde bereits die rückwirkende Regelung zur Zulassung der Anliegerregie kritisiert.[2]

2. KAG-Änderung 1992

Art. 9 Abs. 1 KAG wurde durch § 1 Nr. 7 des Gesetzes zur Änderung des KAG vom 28.12.1992, GVBl S. 775, wie folgt gefaßt:

„Die Gemeinden, Landkreise und Bezirke können bestimmen, daß ihnen der Aufwand für die Herstellung, Anschaffung, Verbesserung, Erneuerung, Veränderung und Beseitigung sowie für die Unterhaltung des Teils eines Grundstücksanschlusses an Versorgungs- und Entwässerungseinrichtungen, der sich nicht im öffentlichen Straßengrund befindet, in der tatsächlichen Höhe oder nach Einheitssätzen (§ 130 BauGB) erstattet wird."

Die Möglichkeit der Geltendmachung von Erstattungsansprüchen wurde durch diese Neufassung des Art. 9 Abs. 1 KAG auf den Teil des Grundstücksanschlusses beschränkt, der sich nicht im öffentlichen Straßengrund befindet. Die Aufwendungen für den Teil der Anschlußleitung im öffentlichen Straßengrund waren somit jedenfalls in den Fällen, in denen die Kommune für die Herstellung, Unterhaltung etc. des Grundstücksanschlusses zuständig ist, von ihr selbst

[1] siehe hierzu Hesse, „Die KAG-Novelle 2002", BayGT 10/2002

[2] so Bötsch, „Kanalanschlüsse im öffentlichen Straßengrund - eine unendliche Geschichte", BayVBl 2003, S. 76

zu tragen. Sie können entweder (soweit beitragsfähig) in die Beitragssätze einfließen oder (falls sie nicht durch Beitragssätze gedeckt werden) über die Kalkulation von Kosten nach betriebswirtschaftlichen Grundsätzen durch Benutzungsgebühren finanziert werden. Auf Grund einer Übergangsbestimmung (Art. 19 Abs. 3 KAG) waren Satzungsregelungen mit einem Erstattungsanspruch gemäß Art. 9 KAG a.F. bis 01.01.1997 der geänderten Rechtslage anzupassen.

Nach der Begründung des Entwurfs zum o.a. Gesetz vom 28.12.1992 (Landtags-Drucksache 12/8082, S. 10) sollte die Änderung des Art. 9 Abs. 1 KAG *„vor allem dazu dienen, den Erstattungsanspruch auf den Aufwand zu begrenzen, der für Maßnahmen an dem Teil des Grundstücksanschlusses entsteht, der sich nicht im öffentlichen Straßengrund befindet. Das bedeutet, daß der Teil des Grundstücksanschlusses, der im öffentlichen Straßengrund liegt, stets zur öffentlichen Einrichtung gehört und ein hierfür entstehender Aufwand stets über Beiträge und/oder Gebühren geltend zu machen ist (vgl. Art. 62 Abs. 2 GO)“*.

Vor Inkrafttreten des „KAG-Änderungsgesetzes 1992“ bestand jedenfalls für Entwässerungseinrichtungen neben der Möglichkeit der satzungsmäßigen Normierung uneingeschränkter Aufwandserstattungen für Grundstücksanschlüsse auch die weitere Variante

„in der Stammsatzung anordnen zu können, daß der Anschließer den Anschluß selbst und auf eigene Kosten zu bewirtschaften hat (sogenannte Anliegerregie)“[3]***.***

Nach Inkrafttreten des KAG-Änderungsgesetzes 1992 (und auch nach Ablauf der Übergangsfrist zum 01.01.1997) vertraten viele Kommunen weiter die Auffassung, man könne den Grundstückseigentümern Herstellung, Unterhaltung usw. der gesamten Grundstücksanschlüsse auf ihre Kosten überlassen und dadurch die Anwendung des Art. 9 Abs. 1 KAG n.F. vermeiden. Wir hatten zu einem solchen Verfahren bereits in unserem Geschäftsbericht 1995, S. 96, unter anderem bemerkt:

„Abgesehen von dem rechtlichen Risiko einer derartigen Regelung (die davon ausgeht, daß ein nach Art. 9 Abs. 1 KAG zu erstattender Aufwand in diesem Fall nicht entsteht) ist zu berücksichtigen, daß der Einrichtungsträger ggf. auch weitgehend seinen Einfluß auf die Bauausführung bei der Errichtung und Änderung von Grundstücksanschlüssen aus der Hand gibt.“

Ferner haben wir auf mögliche hygienische Bedenken gegen eine solche Übertragung auf die Grundstückseigentümer bei der Wasserversorgung hingewiesen.

Außerdem besteht zur Gestaltung und Finanzierung für Grundstücksanschlüsse nach wie vor die Möglichkeit, den gesamten Anschluß der kommunalen Einrichtung zuzuordnen und über Beiträge und/oder Gebühren zu finanzieren. Wenn der Anschluß ganz übernommen wird, entfallen die Probleme, die bei einer Teileinbeziehung zwangsläufig entstehen (Aufteilung der Kostenanteile). [4]

[3] zum Begriff der „Anliegerregie“ siehe ausführlich Hasl-Kleiber, „Zum Entwurf einer KAG-Novelle“, KommunalPraxis BY 2002, S. 166

[4] IMS vom 28.10.1996 Nr. IB4-1524.4-4, GK 29/1997 Nr. 1 Buchstabe a

3. Rechtsprechung des BayVGH zur sogenannten „Anliegerregie“

Der BayVGH hat mit Normenkontrollbeschluß vom 12.07.2000 Az. 4 N 98.3522[5] eine Entwässerungssatzung insoweit für nichtig gehalten, als sie die Anliegerregie im öffentlichen Straßengrund vorsah. Dem Beschluß ist unter anderem folgendes zu entnehmen:

„Die Satzung für die öffentliche Entwässerungsanlage der Stadt ... ist nichtig, soweit sie in § 1 Abs. 3 i.V. mit § 8 und § 12 Abs. 2 bestimmt, daß die im öffentlichen Straßengrund befindlichen Teile der Grundstücksanschlüsse nicht zur Entwässerungsanlage der Stadt gehören und von den Grundstückseigentümern hergestellt, erneuert, geändert und unterhalten werden.“

Der BayVGH begründete dies wie folgt:

„So wie es der Gesetzgeber als durch Art. 9 Abs. 1 KAG a.F. ermöglicht ansah, daß die Gemeinden die Grundstücksanschlüsse insgesamt von der Zugehörigkeit zu ihrer öffentlichen Einrichtung ausnehmen, gleichzeitig aber auf Kosten der einzelnen Grundstückseigentümer selbst herstellen und unterhalten lassen konnten, gebietet er durch Art. 9 Abs. 1 KAG in der seit 01.01.1993 geltenden Fassung, daß die im öffentlichen Straßengrund befindlichen Anschlußteile zur öffentlichen Einrichtung gehören und ihr Herstellungs- und Unterhaltungsaufwand von der Gemeinschaft der Anschlußberechtigten und -pflichtigen über Beiträge und/oder Gebühren getragen wird (vgl. BayVGH vom 22.06.1999 Nr. 23 B 98.3202, U.A. S. 10; Hölzl/Hien, GO, Exkurs F. 6 zu Art. 22). Nur so wird vermieden, daß die Grundstückseigentümer, deren Grundstücke weiter von der Hauptleitung entfernt liegen als andere, und diejenigen, deren Grundstücke an in verkehrsreichen Straßen verlegten Hauptleitungen angeschlossen sind, im Verhältnis zu den anderen Grundstückseigentümern bei der Herstellung und Unterhaltung der Grundstücksanschlüsse einseitig mit Mehrkosten belastet werden, deren Ursache nicht den privaten Grundstücksgegebenheiten zuzurechnen ist und denen auch kein besonderer Vorteil gegenüber steht ...

Das läßt es - spätestens ab 01.01.1997 (vgl. die Übergangsvorschriften des Art. 19 Abs. 3 KAG) - nicht (mehr) zu, daß die Gemeinden dennoch die Grundstücksanschlüsse von der Zugehörigkeit zu ihrer öffentlichen Einrichtung auch hinsichtlich des im öffentlichen Straßengrund liegenden Teils ausnehmen und damit weiterhin in Kauf nehmen, daß einzelnen Grundstückseigentümern bei der Herstellung und Unterhaltung der Grundstücksanschlüsse nicht grundstücksbedingte Mehrkosten zugemutet werden ...“

Auf der Basis dieser Entscheidung wäre bei einer entsprechenden Umstellung des Finanzierungssystems mit Beitrags- und/oder Gebührenerhöhungen bei den hiervon betroffenen Kommunen zu rechnen, da die Errichtung und Unterhaltung der zu den einzelnen Anwesen führenden Grundstücksanschlüsse (soweit sie im öffentlichen Straßengrund liegen) nach keiner Satzungsvariante mehr von den einzelnen Grundstückseigentümern, sondern von der Solidargemeinschaft gleichmäßig zu finanzieren wären.

Die Entscheidung des VGH war Anlaß für die - unter der folgenden Nr. 4 erläuterte - erneute Änderung des Art. 9 KAG.

[5] FSt 299/2000

4. Wiederzulassung der Anliegerregie für die im öffentlichen Straßengrund liegenden Teile der Grundstücksanschlüsse

Durch § 1 Nr. 5 KAGÄndG[6] wurde dem Art. 9 KAG folgender Absatz 5 angefügt:

„Ortsrechtliche Regelungen auf Grund eines Anschluß- und Benutzungszwangs, wonach die Bewirtschaftung des Grundstücksanschlusses einschließlich der in Absatz 1 genannten Maßnahmen auch im öffentlichen Straßengrund vom Anlieger in eigener Regie und auf eigene Kosten vorzunehmen ist, werden durch dieses Gesetz nicht beschränkt."

Damit korrespondierend wurde durch § 1 Nr. 7 Buchstabe a/bb KAGÄndG dem Art. 19 Abs. 3 KAG folgender Satz 2 angefügt:

„Die Einbeziehung der Grundstücksanschlüsse im öffentlichen Straßengrund in eine öffentliche Einrichtung mit Anschluß- und Benutzungszwang und damit ihre Bewirtschaftung durch den Einrichtungsträger sind von den Eigentümern und sonst Berechtigten unentgeltlich zu dulden, wenn es in der Benutzungssatzung angeordnet wird."

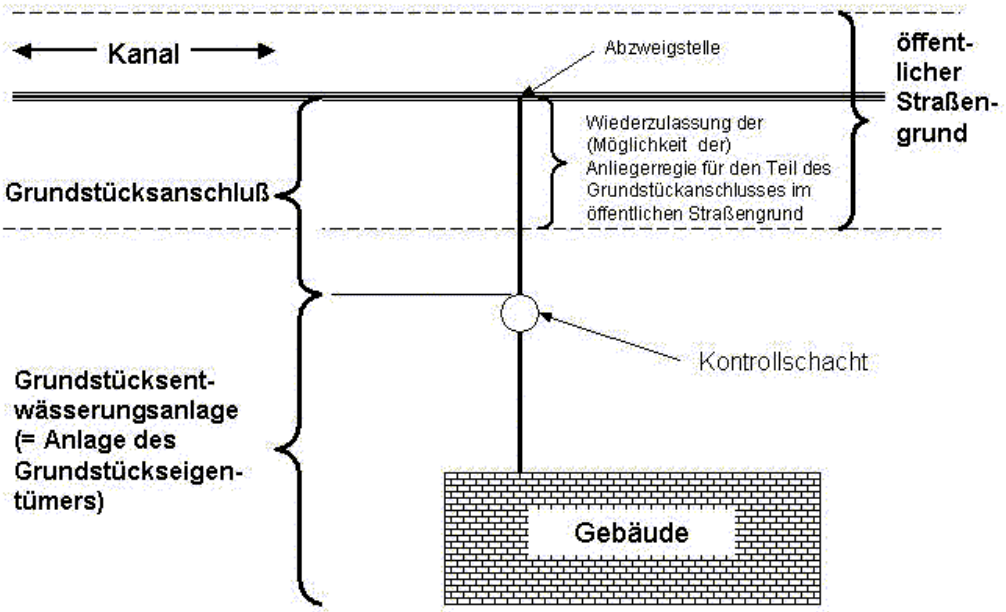
Diese Änderungen wurden durch § 2 Abs. 2 KAGÄndG wie folgt mit Rückwirkung versehen:

„Abweichend von Absatz 1 treten in § 1 Nr. 5 der Art. 9 Abs. 5 und in § 1 Nr. 7 der Art. 19 Abs. 3 Satz 2 mit Wirkung vom 01.01.1993 in Kraft."

[6] Gesetz zur Änderung des Kommunalabgabengesetzes (KAGÄndG) vom 25.07.2002 (GVBl S. 322)

Die praktischen Auswirkungen der Wiederzulassung der (Möglichkeit der) Anliegerregie für den Teil des Grundstücksanschlusses im öffentlichen Straßengrund werden am folgenden Schaubild (am Beispiel einer Entwässerungseinrichtung) dargestellt:

Grundstücksanschluß zur Entwässerungseinrichtung
(Neuregelung durch KAGÄndG vom 25.07.2002)



In der Begründung des Regierungsentwurfes zum KAGÄndG[7] ist zu den erwähnten Neuregelungen unter anderem folgendes ausgeführt:

„Art. 9 Abs. 5 will die Zulässigkeit der Anliegerregie auch im öffentlichen Straßengrund sicherstellen. Zu diesem Zweck wird bestimmt, daß die Bewirtschaftung durch den Anlieger nicht entsprechend Art. 9 Abs. 1 im Bereich des öffentlichen Straßengrundes ausgeschlossen ist, weil es sich nicht um einen Fall der Abgabenerhebung handelt. Das Gesetz geht dabei davon aus, daß sich die Befugnis zur Anordnung der Anliegerregie aus dem Anschluß- und Benutzungszwang ergibt. Der Begriff der Bewirtschaftung umfaßt dabei für die Anliegerregie im wesentlichen die in Art. 9 Abs. 1 genannten Maßnahmen (Herstellung, Anschaffung, Verbesserung, Erneuerung, Veränderung, Beseitigung, Unterhaltung), soll aber auch für atypische Fälle die Verantwortung des Anliegers klarstellen.

Das Gesetz verfolgt in erster Linie die Wiederherstellung der kommunalen Wahlfreiheit im Bereich Anliegerregie:

Die Entscheidung, ob Grundstücksanschlüsse vom Einrichtungsträger oder vom Anlieger bewirtschaftet werden, ist grundsätzlich von den jeweiligen örtlichen Gegebenheiten abhängig - unterschiedliches Ortsrecht ist dabei als Kehrseite der kommunalen Selbstverwaltung in Kauf

[7] Landtags-Drucksache 14/9151

zu nehmen. Nur für den Fall, daß sich der Einrichtungsträger für die kommunale Bewirtschaftung entscheidet, so daß eine Refinanzierung der kommunalen Kosten durch Abgaben notwendig wird, soll es bei der zwingenden gesetzlichen Vorgabe in Abs. 1 bleiben, daß für im öffentlichen Straßengrund entstandene Kosten keine Erstattung beim Anlieger, sondern nur Beiträge oder Gebühren erhoben werden können ...

Die Zulässigkeit der Anliegerregie auch im öffentlichen Straßengrund wird rückwirkend zum Inkrafttreten der Neufassung des Art. 9 Abs. 1 (01.01.1993) festgelegt:

Für die Rückwirkung besteht ein zwingendes öffentliches Interesse (vgl. BVerfGE 72, 302). Der Haushalt zahlreicher Kommunen soll vor schwer abschätzbaren und als überraschend empfundenen Erstattungsansprüchen aus der Zeit von 1993 bis zum Inkrafttreten dieses Gesetzes geschützt werden, die Anlieger wegen vermeintlich rechtsgrundloser Eigeninvestitionen an die Einrichtungsträger stellen könnten. Die Rechtslage rechtfertigt eine rückwirkende Klärung ...

Dieses Bedürfnis nach rückwirkender Klärung überwiegt das Vertrauen der Haus- und Grundbesitzer in die neuere Rechtsprechung. Zwar ist die Regelung zunächst mit einer Belastung verbunden - Haus- und Grundbesitzer müssen weiter selbst auf eigene Kosten bewirtschaften, während nach dem Ansatz des BayVGH die Lasten auf die Schultern aller Beitrags- und Gebührenzahler verteilt worden wären. Dabei ist allerdings zu bedenken, daß durch den vermehrten Verwaltungsaufwand auch zusätzliche Kosten entstanden wären, den die Eigentümer mitzutragen gehabt hätten, wobei die Kommunen auch eine vollständige Beitragsfinanzierung hätten wählen können. Die Grundeigentümer konnten also zu keinem Zeitpunkt auf einen unentgeltlichen Anschluß im öffentlichen Straßengrund vertrauen ...“

Die Kommunen, die sich dafür entscheiden, die Anliegerregie für die Teile der Grundstücksanschlüsse im öffentlichen Straßengrund für ihre Entwässerungseinrichtung[8] einzuführen, sollten beachten, daß dann frühere und künftige Investitionsaufwendungen für die im öffentlichen Straßengrund liegenden Teile der Grundstücksanschlüsse nicht durch Beiträge und Gebühren finanziert werden dürfen (siehe im übrigen auch die Hinweise zu Änderungen des Finanzierungssystems für Grundstücksanschlüsse in unserem Geschäftsbericht 1995, S. 97 ff.).

5. Besonderheiten bei der Wasserversorgung

Für Grundstücksanschlüsse[9] zu Wasserversorgungseinrichtungen ist wegen der vorrangig geltenden Vorschriften der *„Verordnung über Allgemeine Bedingungen für die Versorgung mit Wasser (AVBWasserV)“* vom 20.06.1980 (BGBl I S. 750, berichtigt BGBl I S. 1067) die Anliegerregie nur sehr eingeschränkt zulässig.

In § 35 Abs. 1 dieser Verordnung ist bestimmt:

„Rechtsvorschriften, die das Versorgungsverhältnis öffentlich-rechtlich regeln, sind den Bestimmungen dieser Verordnung entsprechend zu gestalten; unberührt bleiben die Regelungen

[8] zu Wasserversorgungseinrichtungen siehe die folgenden Hinweise zur Beachtung der §§ 10 und 35 AVBWasserV

[9] Die Definitionen der Grundstücksanschlüsse und der Hausanschlüsse sind im wesentlichen inhaltsgleich (vgl. Dietzel in Driehaus, Kommunalabgabenrecht, RN 16 zu § 10 KAG NW).

des Verwaltungsverfahrens sowie gemeinderechtliche Vorschriften zur Regelung des Abgabenrechts.“

Die gemäß Art. 9 Abs. 5 KAG n.F. wieder zulässigen ortsrechtlichen Bestimmungen zur Bewirtschaftung von Grundstücksanschlüssen (auf Grund eines Anschluß- und Benutzungszwangs) durch den Anlieger („in eigener Regie“) sind keine Regelungen des Verwaltungsverfahrens oder gemeinderechtliche Vorschriften zur Regelung des Abgabenrechts im Sinne von § 35 Abs. 1, 2. Halbsatz AVBWasserV, die von der Anpassungspflicht nach § 35 Abs. 1, 1. Halbsatz AVBWasserV unberührt bleiben. Dies ergibt sich bezüglich des Abgabenrechts schon aus dem Wortlaut des Art. 9 Abs. 5 KAG n.F. („Ortsrechtliche Regelungen auf Grund eines Anschluß- und Benutzungszwangs ... werden durch dieses Gesetz nicht beschränkt.") Der unter Nr. 4 zitierten Begründung des Regierungsentwurfes zum KAGÄndG 2002 ist dazu unter anderem folgendes zu entnehmen:

„Nur für den Fall, daß sich der Einrichtungsträger für die kommunale Bewirtschaftung entscheidet, so daß eine Refinanzierung der kommunalen Kosten durch Abgaben notwendig wird, soll es bei der zwingenden gesetzlichen Vorgabe in Abs. 1 bleiben, daß für im öffentlichen Straßengrund entstandene Kosten keine Erstattung beim Anlieger, sondern nur Beiträge oder Gebühren erhoben werden können ...“

Für die Frage der Zulässigkeit der Anliegerregie sind vor allem die Regelungen für Hausanschlüsse[10] nach § 10 AVBWasserV zu beachten. Nach § 10 Abs. 3 Sätze 1 und 2 AVBWasserV gilt:

„Hausanschlüsse gehören zu den Betriebsanlagen des Wasserversorgungsunternehmens und stehen vorbehaltlich abweichender Vereinbarung in dessen Eigentum. Sie werden ausschließlich von diesem hergestellt, unterhalten, erneuert, geändert, abgetrennt und beseitigt, müssen zugänglich und vor Beschädigungen geschützt sein.“

In § 35 Abs. 2 AVBWasserV wurde zwar allgemein bestimmt, daß die bei Inkrafttreten dieser Verordnung geltenden Rechtsvorschriften (Inkrafttreten der Verordnung nach deren § 37 Abs. 1 am „1. April 1980“), die das Versorgungsverhältnis regeln, bis zum 01.01.1982 an diese Verordnung anzupassen waren. Nach § 10 Abs. 6 AVBWasserV können jedoch Regelungen „hinsichtlich des Eigentums am Hausanschluß und der daraus folgenden Pflichten zur Herstellung, Unterhaltung, Erneuerung, Änderung, Abtrennung und Beseitigung, die von § 10 Abs. 3 AVBWasserV abweichen“ und bei Inkrafttreten der AVBWasserV (am 01.04.1980) bereits bestanden hatten, beibehalten werden.

Dementsprechend ist in der Anlage 2 Nr. 2.2 der IMBek vom 13.07.1989[11] unter anderem folgendes ausgeführt:

„Soweit in Satzungen, die am 1. April 1980 bereits in Kraft waren, die Pflichten zur Herstellung, Unterhaltung, Erneuerung, Änderung, Abtrennung und Beseitigung des Grundstücksanschlusses abweichend geregelt sind, können diese Regelungen auch künftig beibehalten werden (vgl. hierzu § 10 Abs. 6 AVBWasserV) ...“

---

[10] siehe hierzu Fußnote 9

[11] VollzBek zum Muster für eine gemeindliche Wasserabgabesatzung vom 13.07.1989 Nr. I B 1 - 3003 - 16/6/86 (AllMBl 1989, S. 579)

Das Modell der Anliegerregie für Grundstücksanschlüsse zu Wasserversorgungseinrichtungen[12] ist somit nur im Fall des § 10 Abs. 6 AVBWasserV zulässig, also bei der ununterbrochenen Fortführung entsprechender Regelungen, die vor dem 01.04.1980 getroffen worden sind, also bei *„denjenigen Versorgungsunternehmen, nach deren Versorgungsbedingungen die Hausanschlüsse seinerzeit im Eigentum der Anschlußnehmer standen und bei denen die Anschlußnehmer deshalb auch für alle den Hausanschluß betreffenden Maßnahmen verantwortlich waren".*[13]

Die nach Art. 9 Abs. 5 KAG n.F. wieder grundsätzlich zulässige Anliegerregie für Teile der Grundstücksanschlüsse im öffentlichen Straßengrund kann daher für Wasserversorgungseinrichtungen nicht mehr neu eingeführt werden. Dies gilt auch für Einrichtungsträger, die nach der (unter Nr. 2 erläuterten) KAG-Änderung 1992 eine frühere Anliegerregie für Grundstücksanschlüsse zur Wasserversorgung aufgegeben haben.

6. Zulassung der Ablösung und der vertraglichen Übernahme der Erstattungsansprüche für Grundstücksanschlüsse im Rahmen städtebaulicher Verträge

Durch § 1 Nr. 5 KAGÄndG wurde weiter folgender neuer Absatz 4 an Art. 9 KAG angefügt:

„(4) Der Abgabeberechtigte kann die Ablösung des Erstattungsanspruchs vor dessen Entstehung gegen eine angemessene Gegenleistung zulassen. Das Nähere ist in der Abgabesatzung (Art. 2) zu bestimmen. Die vertragliche Übernahme erstattungsfähiger Aufwendungen ist auch im Rahmen städtebaulicher Verträge möglich; § 11 BauGB gilt entsprechend."

Die neue Vorschrift entspricht dem Regierungsentwurf, der wie folgt begründet wurde:[14]

„Eine Ablösung des Erstattungsanspruchs sah das Gesetz bislang nicht vor, obwohl wegen der Besonderheit jedes Grundstücksanschlusses ein Konflikt mit dem Äquivalenzprinzip noch weniger nahe liegt als bei Beiträgen. Es wird daher in Anlehnung an Art. 5 Abs. 9 eine entsprechende Ablösungsmöglichkeit eingeführt. Der Gesetzentwurf will darüber hinaus im Interesse einer Erleichterung vertraglichen Verwaltungshandelns Rechtssicherheit zur Anwendbarkeit der städtebaulichen Verträge auch im Bereich der Erstattungsansprüche schaffen. Soweit auch die Errichtung und Bewirtschaftung von Grundstücksanschlüssen durch die Gemeinde außerhalb ihrer Einrichtung als ‚städtebauliche Maßnahmen' von § 11 BauGB erfaßt werden, sollen sich die Grenzen allein aus dem Bundesrecht ergeben. Insoweit gilt die Begründung zu Art. 5 Abs. 9 Satz 3 sinngemäß."

Diese Neuregelung ist nach § 2 Abs. 1 KAGÄndG am 01.08.2002 in Kraft getreten.

Bisher wurde im Umkehrschluß zu Art. 5 Abs. 9 KAG die vertragliche Ablösung erstattungsfähiger Kosten als unzulässig angesehen.[15]

---

[12] umfassend die Teile der Grundstücksanschlüsse im öffentlichen Straßengrund und im Privatgrund

[13] vgl. Hasl-Kleiber, „Zum Entwurf einer KAG-Novelle", KommunalPraxis BY 2002, S. 166, ebenso Ecker, Kommunalabgaben in Bayern, 71.04.3.1, Stand 01.04.2001

[14] Bayerischer Landtag, Drucksache 14/9151

[15] Hasl-Kleiber in Ecker, Kommunalabgaben in Bayern, Nr. 73.01.3, Stand 01.04.2001

Firewallsysteme
Ein elementarer Teil der Sicherheit in der Informationstechnik (IT)
Wozu werden sie benötigt, was können sie und wie werden sie eingesetzt?

Verfasser: Herbert **Gruschka**
Andreas **Schneider**

Inhaltsübersicht Seite

1. Zusammenfassung

Das Thema „Firewall“ hat in den letzten Jahren durch den Anschluß lokaler Netze an externe Weitverkehrsnetze und die Nutzung von Internetdiensten durch die Kommunen und deren Verwaltungen eine zunehmende Bedeutung erlangt. Angesichts des großen Nutzens, den das Internet und die dort verfügbaren Dienste bieten, wird allzu oft vernachlässigt, daß im Internet auch viele Gefahren lauern, denen begegnet werden muß. Diese Gefahren werden aus unserer Sicht noch steigen, wenn im Rahmen der vielerorts anzutreffenden eGovernment-Initiativen eigene Internet-Dienste bereitgestellt werden oder interaktive Anwendungen rund um die Uhr erreichbar sein sollen. Dieser Beitrag wendet sich daher an alle IT-Entscheider und -Verantwortlichen, um diese für ein aus unserer Sicht sehr wichtiges Thema zu sensibilisieren, die Notwendigkeit einer Absicherung lokaler Netze durch eine Firewall deutlich zu machen und die grundlegenden Unterschiede von Firewallösungen aufzuzeigen.

Folgende Punkte sind aus unserer Sicht besonders zu beachten:

– Ein ungesicherter Anschluß des lokalen kommunalen Netzes an das Internet oder an andere unsichere Weitverkehrsnetze ist in vielfacher Hinsicht (Strafrecht, Datenschutz, Kassensicherheit, Verfügbarkeit) unzulässig.

– Die Sicherung lokaler Netze durch eine Firewall setzt eine klare Strategie (IT-Sicherheitsziele, Sicherheitskonzept) und eine gewissenhafte Umsetzung dieser Vorgaben durch organisatorische und technische Maßnahmen voraus. Dies ist kein einmaliger Vorgang, sondern eine Daueraufgabe.

– Aufbau und Betrieb einer Firewall erfordern ein entsprechendes Fachwissen, welches in der Regel erst ab einer gewissen Größenordnung wirtschaftlich vorgehalten werden kann. Wird die Größenordnung nicht erreicht, ist es zweckmäßig, die damit zusammenhängenden Aufgaben einem vertrauenswürdigen Dritten zu übertragen oder eine interkommunale Zusammenarbeit (z.B. Landkreis-Behördennetz) anzustreben.

– Eine Firewall muß nicht immer am Standort selbst stehen, sondern kann auch zentral für mehrere Standorte vorgehalten werden, wenn die Übertragungsstrecken vom Standort bis zur Firewall ausreichend sicher sind.

– Maschinen, die von außen erreichbar sein müssen, da sie Internet-Dienste anbieten, gehören stets in ein besonders abgesichertes Teilnetz und sollten nicht direkt mit dem lokalen Netz verbunden sein.

– Auch bei einem Anschluß an das Bayerische Behördennetz (BYBN) hat jede Stelle für ihren Verantwortungsbereich sicherzustellen, daß ihre Daten und Programme nicht von Unbefugten eingesehen, verändert oder gelöscht werden können. Für die Einhaltung der datenschutzrechtlichen und haushaltsrechtlichen Vorschriften zur IT-Sicherheit ist jede Stelle selbst verantwortlich.

2. Einführung

Im Rahmen unserer überörtlichen Rechnungsprüfung haben wir in den letzten Jahren neben dem sparsamen und wirtschaftlichen Betrieb der vor Ort eingesetzten Informationstechnik (IT) zunehmend auch den ordnungsgemäßen und sicheren Einsatz der Hard- und Software geprüft. Hinsichtlich der inneren und äußeren Sicherheit der IT-Systeme mußten wir dabei teilweise schwerwiegende Feststellungen treffen. Um nur einige der gravierendsten Beispiele zu nennen:

– Internetzugang des lokalen Verwaltungsnetzes ohne jegliche Schutzmaßnahmen

– keinerlei Protokollierung sicherheitsrelevanter Zugriffe

– Verwendung von Installations-Paßwörtern und/oder Trivialpaßwörtern in zentralen Netzwerkkomponenten, Serversystemen, Datenbanken und finanzwirksamen Verfahren

– keine Beschränkung und Differenzierung von Benutzerrechten in finanzwirksamen Anwendungsverfahren

– keine Sicherheitseinstellungen in den Betriebssystemen (Paßwort- und Systemrichtlinien)

– keine Kontrolle von Internetdiensten (z.B. Download aller Dateien, Zugriff auf WEB-Seiten mit pornographischen Inhalten)

– unzureichender oder fehlender Virenschutz

– fehlende oder nicht funktionsfähige Datensicherungen

Diese Vielfalt von Sicherheitsmängeln ist schon bedenklich, was die Sicherheit der IT gegenüber Ausfällen, Datenverlusten, böswilligen oder allzu neugierigen Mitarbeitern anbelangt. Besonders beunruhigend ist es aber, wenn lokale Verwaltungsnetze ungeschützt mit dem Internet und so mit der ganzen Welt verbunden sind. Angesichts der häufigen Meldungen in der Fach- und Boulevardpresse über Sicherheitslücken in IT-Systemen und über weltweite Systemausfälle durch Viren, Würmer oder Hackerangriffe ist es dringend notwendig, sich mit den Gefahren auseinanderzusetzen, die beim Anschluß lokaler Netze an das Internet entstehen, und die erforderlichen Schutzmaßnahmen zu besprechen. Angesichts der Vielzahl technischer Möglichkeiten und der daraus resultierenden Gefahrenquellen ist dies ohnehin schon ein sehr breites Thema. Um nicht zu verwirren oder abzuschrecken, wollen wir versuchen, die aus unserer Sicht wichtigsten Aspekte allgemein verständlich darzustellen. Dabei ließ es sich nicht vermeiden, zum besseren Verständnis auf bestimmte grundlegende technische Zusammenhänge hinzuweisen. Für den „technischen Laien“ wird trotzdem manches zu technisch erscheinen. Dagegen können wir für den „Experten“ in diesem Beitrag nicht alle notwendigen Details darstellen; er kann sich jedoch aus der im Anhang angegebenen Literatur weitergehend informieren.

3. Was gilt es zu schützen?

Durch die Verbindung eines lokalen, nicht öffentlichen Netzes (LAN[1]) mit einem öffentlichen und daher grundsätzlich unsicheren Netz (WAN[2]), insbesondere dem auf der ganzen Welt verfügbaren Internet, sind grundsätzlich gefährdet

- die Vertraulichkeit, Verfügbarkeit und Integrität der auf den IT-Systemen gespeicherten Daten (mögliche Schäden: Verstoß gegen rechtliche oder vertragliche Vorschriften; Beeinträchtigung des informationellen Selbstbestimmungsrechts und der Persönlichkeitsrechte),

- die Verfügbarkeit der Hard- und Software, d.h. der für den Bürger, den Verwaltungsbetrieb oder die politischen Gremien notwendigen technischen Infrastruktur (mögliche Schäden: Beeinträchtigung der Aufgabenerfüllung),

- das Ansehen der Verwaltung oder der kommunalen Gebietskörperschaft und deren Einrichtungen (mögliche Schäden: negative Außenwirkung und finanzielle Auswirkungen).

Welcher Schutzbedarf sich für die eingesetzte IT-Infrastruktur, die Anwendungen und Daten ergibt, läßt sich aus unserer Sicht am besten anhand des IT-Grundschutzhandbuches (IT-GSHB)[3] des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ermitteln. Darüber hinaus ist das IT-GSHB auch eine gute Informationsquelle und eine praxisorientierte Anleitung zum Thema IT-Sicherheit im allgemeinen. Im wesentlichen bestimmt der Schaden bzw. die Summe der Schäden mit den schwerwiegendsten Auswirkungen den Schutzbedarf eines IT-Systems (Maximum-Prinzip). Soweit wir dies überblicken können, werden nach unserer Einschätzung im kommunalen Bereich Anwendungen eingesetzt und Daten gespeichert, bei denen mindestens ein mittlerer, bisweilen ein hoher, gelegentlich ein sehr hoher Schutzbedarf[4] gegeben ist. Folgende Beispiele sollen dies verdeutlichen:

- Die in finanzwirksamen Verfahren gespeicherten Daten weisen in der Regel einen mittleren Schutzbedarf aus.

- Die in Personalinformationssystemen oder Sozialhilfeverfahren gespeicherten, personenbezogenen Daten haben regelmäßig einen hohen Schutzbedarf.

- Die in Klinik-Informationssystemen gespeicherten personenbezogenen Daten der Patienten, insbesondere deren Diagnose- und Behandlungsdaten, bedingen aus unserer Sicht einen sehr hohen Schutzbedarf.

Aufgrund dieser Einschätzung weisen wir darauf hin, daß bei einem hohen oder sehr hohen Schutzbedarf die Anwendung des IT-GSHB und die Umsetzung des dort vorgesehenen Standard-Maßnahmenkatalogs nicht ausreicht. In diesen Fällen ist eine ergänzende Sicherheitsanalyse (vgl. Kapitel 2.5 IT-GSHB) anhand des IT-Sicherheitshandbuchs notwendig, um gegebenenfalls die im IT-GSHB beschriebenen Schutzmaßnahmen sinnvoll zu ergänzen oder zu verstärken.

---

1 local area network - vgl. Begriffsdefinitionen

2 metropolitan area network, wide area network - vgl. Begriffsdefinitionen

3 vgl. www.bsi.de/gshb/index.htm

4 zur Einstufung des Schutzbedarfs vgl. Kapitel 2.2 IT-GSHB

Auch ohne nähere Risikobewertung der verwendeten Internet-Dienste ist daher schon jetzt folgendes festzustellen:

Ein ungeschützter oder unzureichend abgesicherter Zugang eines lokalen kommunalen Netzes zum Internet ist bei diesem Schutzbedarf weder mit den aktuellen technischen Sicherheitsstandards, noch mit den allgemeinen oder spezialgesetzlichen Bestimmungen zum Datenschutz (z.B. § 203 StGB, AO, SGB X, BayDSG) vereinbar. Im Schadensfall drohen den Verantwortlichen dienst- und strafrechtliche Verfahren sowie Schadensersatzforderungen.

4. Wovor muß man sich schützen?

Die Angriffsszenarien und daraus resultierenden Risiken sind vielfältig und lassen sich im Rahmen dieses Beitrags nicht erschöpfend behandeln, da immer wieder neue Angriffsmethoden und -werkzeuge, aber auch neue Unzulänglichkeiten der eingesetzten Server- und Client-Programme (sogenannte Vulnerabilities) bekannt werden.

Ausgehend von den zu schützenden Werten (vgl. vorstehende Ausführungen) möchten wir die bekannteren Angriffsmethoden kurz darstellen, um später bei der Beschreibung der Firewallfunktionalitäten einen gewissen Bezugspunkt zu schaffen. Die Darstellung der einzelnen Angriffsmethoden ist größtenteils einer vom BSI veröffentlichten Studie der debis IT Security Services[5] entnommen und wurde zum Teil mit eigenen Anmerkungen ergänzt oder entsprechend komprimiert. In der Studie finden sich außerdem zahlreiche weitere Hinweise über technische und konzeptionelle Schwachstellen in Internet-Diensten und Betriebssystemen, deren Lektüre den Sicherheitsverantwortlichen und den Systemadministratoren zu empfehlen ist:

– **Port-Scans**[6]

  Portscanner klopfen an fremde Systeme an, um in Erfahrung zu bringen, welche Dienste ein Zielrechner anbietet bzw. auf welchen TCP und UDP-Ports[7] des Zielsystems ein Server auf eintreffende Datenpakete wartet.

– **IP- und DNS-Spoofing**

  Bei Spoofing-Angriffen versucht sich der Angreifer hinter einer falschen Absender- oder Empfänger-Adresse zu verstecken. Da das derzeit verwendete Internet-Protokoll (IPv4) selbst keine wirksamen Authentifizierungsmechanismen zwischen den im Internet angeschlossenen Rechnern zur Verfügung stellt, ist es z.B. möglich, falsche Rechneradressen (IP-Spoofing) oder Rechnernamen (DNS-Spoofing) zu verwenden oder die Routing-Tabellen eines Rechners/Routers zu manipulieren.

– **Denial-of-Service-Angriffe (DoS-Attacken)**

  Gezielte Angriffe auf bekannt gewordene Sicherheitslücken oder Implementierungsfehler eines Server-Dienstes können diesen lahmlegen oder zum Absturz bringen. Auch normale Abfragen eines Serverdienstes können mit einer künstlich hohen Abfragerate den Dienst

[5] [BSI1998]

[6] vgl. Begriffserläuterungen im Anhang

[7] vgl. Kapitel 9.1 Paketfilter

außer Kraft setzen, insbesondere dann, wenn die Antwort sehr viel Rechenzeit in Anspruch nimmt. DoS-Attacken auf Schwachstellen (Vulnerabilities) des Betriebssystems können einen an das Netzwerk angeschlossenen Rechner (Host) blockieren oder diesen ebenfalls zum Absturz bringen.

– **Viren**

Unter einem Virus versteht man ein sich selbst replizierendes Programm, das sich in einem Wirtprogramm oder im Bootsektor einer Festplatte festsetzt. Es kann sich außerdem in andere Programme kopieren und diese dadurch infizieren. Ein Virus läßt sich in der Regel an einem für ihn typischen Muster (Codesequenz) identifizieren. Neuere Viren können sogar ihre Codesequenzen ändern und sind deshalb besonders schwer zu erkennen. Viren beeinträchtigen in aller Regel die Funktionsfähigkeit des befallenen Rechnersystems und können zu Datenverlusten oder Schäden an Hardware führen. In letzter Zeit treten häufig sogenannte Makro-Viren auf, die sich in elektronischen Dokumenten oder Mails verstekken.

– **Trojaner**

Ein „trojanischen Pferd“ ist ein Programm mit unerwarteter Funktionalität. Beispiel für einen Trojaner ist eine Anmelde-Prozedur, die alle verarbeiteten Paßwörter sammelt, oder ein Tastaturscanner, der alle eingegebenen Tastenanschläge aufzeichnet, und diese Informationen an einen potentiellen Angreifer weiterleitet. Von Trojanern befallene Systeme werden gelegentlich auch für DoS-Attacken auf fremde Systeme mißbraucht.

– **Würmer**

Ein Wurm verbreitet Kopien seiner selbst über ein Netz. Ein Wurm ist ein eigenständiges Programm und von keinem Wirtsprogramm abhängig. Würmer führen in der Regel aufgrund ihrer Replikationsrate zu einem erhöhten Datenverkehr, können aber auch Schadensfunktionen haben, die vergleichbar mit den Viren sind.

– **Browser-Plug-Ins, Java, JavaScript, ActiveX, Java-Applets**

Webbrowser (z.B. Microsoft Internet-Explorer oder kurz IE, Netscape-Navigator oder kurz Netscape, Mozilla) können selbst nur eine beschränkte Anzahl von Daten verarbeiten und benötigen deshalb sogenannte Viewer, um Datentypen zu verarbeiten, die die Browser selbst nicht verstehen. Die weltweit am häufigsten eingesetzten Browser (IE und Netscape) unterstützen deshalb inzwischen einen Mechanismus, der es Drittherstellern erlaubt, Plug-Ins anzubieten, die nach dem Herunterladen eine integrierte und nahtlos eingepaßte Erweiterung des eigentlichen Browsers bilden. Die meisten Browser können zusätzlich noch ein oder mehrere Erweiterungssysteme (z.B. Java, JavaScript oder ActiveX) verarbeiten, die die Leistungsfähigkeit und Flexibilität der Browser ebenfalls erweitern. Werden solche Erweiterungen aus nicht vertrauenswürdigen Quellen heruntergeladen, können diese Programme zu Schäden an den befallenen IT-Systemen oder zu anderweitigen Sicherheitsproblemen (vgl. Trojaner) führen.

– **Makrosprachen**

Makrosprachen sind in diversen Office-Paketen verbreitet und im Grunde genommen Programmiersprachen, die speziell auf die jeweiligen Anwendungen zugeschnitten sind. Sehr

bekannt und leistungsfähig sind die VBA-Sprachen der Microsoft-Office-Komponenten, die in Umfang und Mächtigkeit einer herkömmlichen Programmiersprache kaum nachstehen und auch Zugriffe auf Betriebssystemressourcen erlauben.

– **Sniffer**

  Mit Netzwerk-Sniffern wird die Datenübertragung bis hinunter zur Ebene einzelner Protokollpakete überwacht und mitprotokolliert. Da manche Protokolle das bei der Authentifizierung verwendete Paßwort im Klartext übertragen (z.B. Telnet), können hierbei ernsthafte Sicherheitsprobleme entstehen.

– **Social Engineering**

  Dies ist, rein technisch betrachtet, die einfachste Form eines Angriffs. Hier wird ganz bewußt die Gutgläubigkeit und Vertrauensseligkeit der Anwender oder Administratoren ausgenutzt, um in den Besitz von sicherheitstechnisch relevanten Informationen (z.B. Benutzerkennungen und Paßwörter) zu gelangen. Von Ausspähen (Blick über die Schulter) oder Erfragen von Paßwörtern bis hin zu modernen Köpenickiaden, wenn beispielsweise ein Angreifer als Servicetechniker getarnt Zugang zu den Rechnerräumen oder den Netzwerkverteilern erlangt, um dort einen Angriff vorzubereiten, sind vielerlei Formen dieser Methode denkbar.

Mit Ausnahme der Port-Scans, die lediglich dem Ausforschen fremder Systeme dienen, können alle weiteren Angriffsarten der Vertraulichkeit und Integrität von Daten schaden, nehmen Rechnerressourcen (z.B. Rechenzeit, Plattenplatz) in Anspruch oder blockieren Kommunikationsverbindungen und/oder die daran angeschlossenen IT-Systeme.

5. Sicherheitskonzept

Auf der Grundlage der Risikoanalyse und der Ermittlung des Schutzbedarfs gilt es, Richtlinien für die Sicherheit festzulegen (sogenannte security-policy[8]). In bezug auf die Konzeption einer Firewall empfehlen wir, sich dabei an folgenden grundlegenden Sicherheitsprinzipien zu orientieren:

– **Prinzip der minimalen Zugriffsrechte**

  Das grundlegenste Sicherheitsprinzip in der IT ist das Prinzip der minimalen Zugriffsrechte. Dieses Prinzip besagt, daß jeder Administrator oder Benutzer nur die Rechte erhält, die für die Erledigung der jeweils zugewiesenen Aufgaben benötigt werden. Unabhängig davon, wie man aus Sicht moderner Mitarbeiterführung oder aus einer liberalen Grundhaltung heraus darüber denkt, verkleinert das Prinzip der minimalen Zugriffsrechte die Angriffsfläche und verringert den Schaden, der bei eventuell auftretenden Angriffen entsteht. In gleicher Weise gilt dieser Grundsatz auch für die auf einem IT-System ablaufenden Programme oder Dienste. Auch hier sollte - soweit dies technisch realisierbar ist - darauf geachtet werden, daß diese möglichst mit eingeschränkten Rechten ausgeführt werden. In diesem Zu-

[8] vgl. Begriffsdefinition im Anhang

sammenhang verweisen wir auch auf das datenschutzrechtliche Erforderlichkeitsprinzip (vgl. Art. 16 Abs. 1 und Art. 17 Abs. 1 BayDSG), das ebenfalls eine entsprechende Beschränkung der Zugriffsrechte erfordert.

– **Mehrschichtige und vielfältige Verteidigung**

Bei Sicherheitsmaßnahmen gilt generell, daß man sich nicht nur auf einen einzigen Schutzmechanismus verlassen sollte, auch wenn er nach der Produktbeschreibung oder nach Aussagen von Fachleuten besonders stark und unüberwindbar erscheint. Es empfiehlt sich daher, grundsätzlich mehrere Mechanismen einzusetzen, die sich entweder gegenseitig sichern oder verhindern, daß bei der Durchdringung einer Sicherheitskomponente (z.B. Paketfilter) die dahinter liegende IT-Infrastruktur vollständig offenliegt. Dazu gehören unter anderem zusätzliche Paketfilter unterschiedlicher Hersteller, die Bildung überwachter Teilnetze und/oder eine Segmentierung des Netzwerks sowie der Einsatz eines Intrusion Detection Systems (IDS), um auffällige Aktivitäten schneller zu erkennen. Diese aus Sicherheitsgründen grundsätzlich wünschenswerte technische Vielfalt findet aber ihre Grenzen in einer einfachen und vom zeitlichen Aufwand her vertretbaren Administration sowie in den finanziellen Rahmenbedingungen. Einen wesentlichen Beitrag zur Sicherheit von IT-Systemen liefern daneben organisatorische Maßnahmen (z.B. Aufklärung der Benutzer über mögliche Risiken, sorgfältige Systemadministration, Auswertung von Systemprotokollen,[9] Beobachtung von Virenwarnlisten im Internet und das Lesen von Veröffentlichungen über bekannt gewordene Sicherheitslücken).

– **Eine Passierstelle**

Ein wichtiger Punkt beim Aufbau einer Verteidigungsstrategie ist die Kontrolle über den jeweiligen (Internet-)Zugang. Um es mit einem Bild aus der Literatur auszudrücken: „Durch diese hohle Gasse muß er kommen." Dies läßt sich aber grundsätzlich nur dann realisieren, wenn das lokale Netz nur **einen Übergang** in das Internet besitzt und weitere Zugänge strikt untersagt sind. Besonders gilt dies auch für alle Fernwartungs- oder Wählverbindungen, die wir im Rahmen der überörtlichen Prüfung immer wieder neben den Hauptübergängen angetroffen haben.

– **Einfachheit und Klarheit**

Sicherheitstechnische Systeme sollten grundsätzlich so einfach und überschaubar wie möglich aufgebaut und gut dokumentiert sein. Dies erfordert einerseits eine systematische Vorgehensweise bei der Planung und Installation von Firewalls. Andererseits sollten keine Produkte eingesetzt werden, deren Komplexität die Systemadministratoren nicht mehr überblicken können oder die in diesem Umfang nicht für die Lösung der sicherheitstechnischen Aufgabe nötigt sind. Wir verkennen nicht, daß der Aufbau wirksamer und sicherer Internet-Firewallsysteme ein sehr komplexes Thema ist und daß der Wunsch nach Einfachheit dabei oftmals nur schwer zu erfüllen ist. Gleichwohl sollten die zuständigen Systemadministratoren - ebenso wie sachverständige Dritte - die Firewall noch überblicken und auf ihre Wirksamkeit hin überprüfen können. Ebenso sollten Systeme vermieden werden, auf denen gleichzeitig eine Vielzahl von Diensten laufen und die daher die sicherheitstechnischen Maßnahmen unnötig komplizieren.

[9] zur datenschutzrechtlichen Zulässigkeit vgl. [DS2000]

– **Fortschreibung und Pflege**

Wegen der immer noch rasanten Entwicklung der eingesetzten Hard- und Software, neuer Kommunikationsanforderungen (z.B. im Rahmen von eGovernment) und des damit einhergehenden Einsatzes neuer Entwicklungswerkzeuge, Protokolle, Dienste und Anwendungsverfahren wandeln sich auch die Anforderungen an die IT-Sicherheitssysteme. Generell gilt: Neue Technik verursacht neue Probleme. Aus diesem Grund sind das IT-Sicherheitskonzept und die daraus resultierenden Maßnahmen als laufender Prozeß anzusehen, der eigentlich nie abgeschlossen sein wird, solange die technische Entwicklung anhält[10]. Dies bedeutet für die Verantwortlichen nicht nur, daß sie mit der technischen Entwicklung Schritt halten und die Risiken und Schwachstellen der neuen Technologien kennen und bewerten müssen, sondern erfordert auch eine ständige Anpassung der technischen und organisatorischen Sicherheitsmaßnahmen an die aktuellen Bedürfnisse.

6. Was ist eine Firewall?

Das englische Wort „Firewall“ läßt sich mit „Brandschutzmauer“ übersetzen. Dieser aus dem Hochbau stammende Begriff beschreibt die Funktionsweise einer Firewall[11] aber nur unzureichend. Im Gegensatz zur Brandschutzmauer hat eine Firewall nicht nur eine abweisende, sondern auch eine durchlassende Funktion. Um überhaupt die Dienste des Internets nutzen zu können, werden auf einer Firewall zahlreiche „Löcher“ benötigt, durch die der Datenverkehr fließt. Insoweit ist eine Firewall eher mit einem zentralen Zugangskontrollsystem eines Unternehmens vergleichbar. Auch hier achten ein oder mehrere Sicherheitsangestellte/Pförtner darauf, wer das Unternehmen betritt oder verläßt oder welchen Ansprechpartner der Besucher im Gebäude erreichen will. Gegebenenfalls werden Passanten oder deren Gepäck nach bestimmten (sicherheitsrelevanten) Kriterien durchsucht bzw. das Gepäck vom Pförtner selbst entgegengenommen, um es dann stellvertretend für den Absender an den Empfänger weiterzuleiten. Etwas abstrakter ausgedrückt, ist eine Firewall daher ein Konzept und zugleich eine technische Infrastruktur für die Verbindung zwischen einem öffentlichen und einem nichtöffentlichen Netz. Eine Firewall kann nur aus einem einzelnen Gerät oder aus mehreren Servern, Überwachungsroutern und anderen Komponenten bestehen.[12] Wir werden darauf noch ausführlicher bei den Firewallarchitekturen zu sprechen kommen. Im Grunde genommen besteht eine Firewall im wesentlichen aus der geschickten Kombination mehr oder weniger intelligenter Paketfilter[13] und Proxies[14], die mit Virenscannern[15] oder anderen Schutzprogrammen (z.B. Filter-[16], Verschlüsselungs- oder Authentifizierungsprogrammen) ergänzt werden.

---

[10] Bill Gates hat anläßlich der 20-Jahr-Feier von Microsoft Deutschland im letzten Jahr bereits die nächste digitale Dekade eingeläutet.

[11] vgl. Begriffsdefinition DFN im Anhang

[12] vgl. [Barth2001]

[13] vgl. Kapitel 9.1 Paketfilter

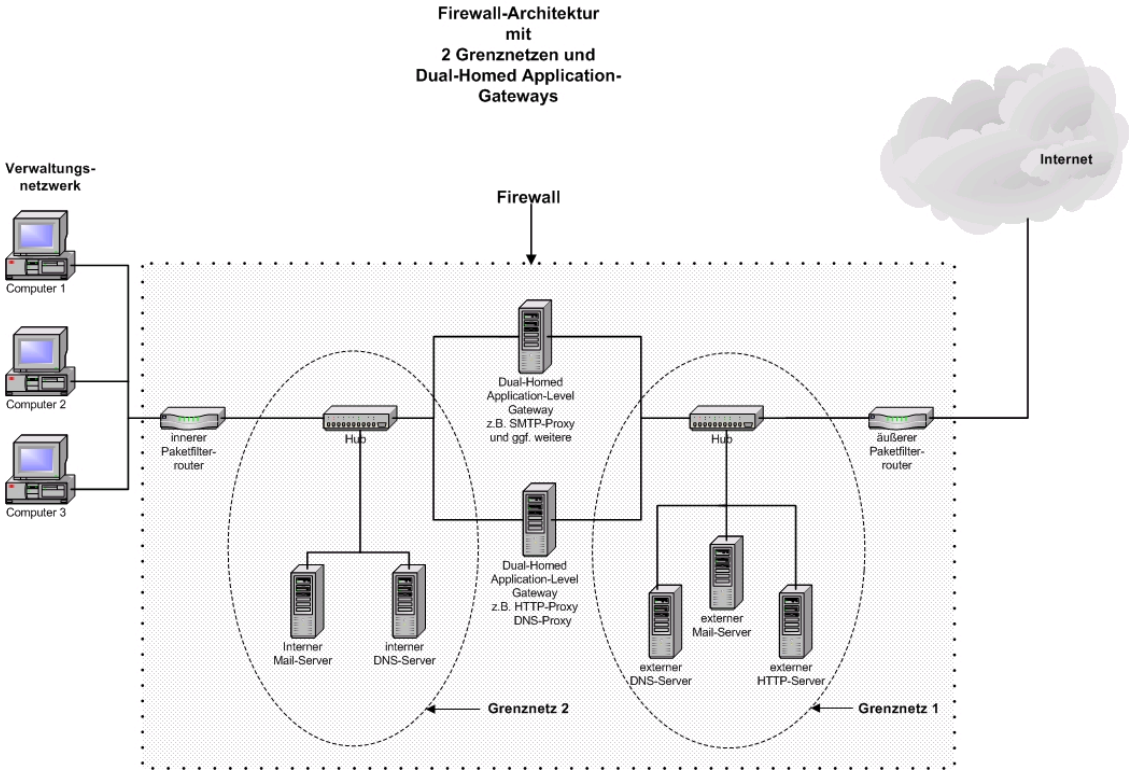
[14] vgl. Kapitel 9.2 Proxy-Systeme

[15] Virenscanner - vgl. Begriffsdefinition im Anhang

[16] z.B. URL-, Java-Script- oder ActiveX-Filter

7. Firewallarchitekturen

Wie wir bereits bei der Definition des Begriffs „Firewall“ festgestellt haben, unterscheiden sich die Firewallarchitekturen doch erheblich und können von einer Single-Box-Architektur bis hin zu Multi-Box-Architekturen mit verschiedenen Paketfilter- und Proxy-Systemen und mehreren überwachten Teilnetzen[17] reichen. Im IT-GSHB (M 2.73) sind einige dieser Firewallarchitekturen kurz schematisch dargestellt, weshalb wir an dieser Stelle darauf verweisen dürfen. Eine ausführlichere Darstellung der einzelnen Architekturen mit einer sehr detaillierten Darstellung der jeweiligen Vor- und Nachteile ist in dem Buch „Einrichten von Internet Firewalls“[18] enthalten. Die vom BSI empfohlene Architektur mit zwei überwachten Teilnetzen und einem oder mehreren Dual-homed Bastion-Hosts wollen wir nachfolgend etwas näher beleuchten, da sie alle wesentlichen Bestandteile einer wirksamen Sicherung enthält:



Bei Angriffen aus dem Internet sind naturgemäß die Maschinen am gefährdetsten, die direkt über das Internet erreichbar sind (öffentliche Adressen) und/oder Internet-Dienste anbieten oder nutzen. Es liegt also nahe, diese Maschinen in einen abgesicherten Bereich (abgesichertes Teilnetz oder Grenznetz) zu stellen, diesen besonders zu schützen und die Verbindungen am Übergang zum lokalen Netz zu trennen. Was sind nun die Vorteile einer solchen Architektur?

– Der äußere Überwachungsrouter schützt den Bastion-Host mit seinen Filterregeln und kann den Verkehr und die nutzbaren Dienste bereits erheblich einschränken. Eingehende Verbindungen lassen sich damit auf einzelne wenige Dienste (z.B. E-Mail) begrenzen.

[17] sogenanntes Grenznetz, wird gelegentlich auch als sogenannte Demilitarisierte Zone (DMZ) bezeichnet

[18] [ZCC2002]

– Zwischen dem äußeren Router und der nach außen gerichteten Netzwerkkarte des Bastion-Hosts wird ein Grenznetz gebildet, das am Bastion-Host endet. Damit wird die Struktur des zweiten (inneren) Grenznetzes und des lokalen Netzes vollständig verborgen. Maschinen, die von außen erreichbar sein müssen, wenn sie Internet-Dienste anbieten sollen (z.B. sogenannte externe Mail-, DNS- und HTTP-Server), gehören deshalb in dieses Grenznetz.

– Der Bastion-Host wickelt stellvertretend für alle im lokalen Netz befindlichen Maschinen den Internetverkehr über entsprechende Proxy-Server ab und kann darüber hinaus mit besonders wenigen Diensten sehr robust konfiguriert werden, so daß er besonders schwer angreifbar ist (sogenannte Härten).

– Zwischen der nach innen gerichteten Netzwerkkarte des Bastion-Hosts und dem inneren Router wird ein weiteres Grenznetz geschaffen, das ein weiteres Hindernis zwischen dem Angreifer und den internen Maschinen bildet, da die Struktur des lokalen Netzes auch bei einem erfolgreichen Angriff auf den Bastion-Host immer noch nicht sichtbar wäre.

– Der innere Überwachungsrouter[19] schützt das lokale Netz mit eigenen (strengeren) Filterregeln, beschränkt die zugelassenen Dienste und läßt nur Verkehr zwischen dem Bastion-Host und dem lokalen Netz zu. Der interne Verkehr im lokalen Netz wäre für einen Angreifer selbst dann nicht sichtbar, wenn er den externen Überwachungsrouter überwunden hätte und in den Bastion-Host eingebrochen wäre.

Soweit wir dies überblicken können, werden im kommunalen Bereich überwiegend Single-Box-Architekturen eingesetzt. Diese vereinen gewissermaßen die Funktionalität der Multi-Box-Architekturen in einem Gerät, da sie intern meist wie Multi-Box-Lösungen aufgebaut sind. Aus unserer Sicht ergeben sich folgende Vor- und Nachteile gegenüber Multi-Box-Lösungen:

Vorteile:

– Single-Box-Lösungen zeichnen sich in der Regel durch eine einheitliche, leicht bedienbare und verständliche Oberfläche aus, mit der sich Filter- und Access-Regeln effizienter und übersichtlicher einstellen lassen.

– Da nur ein Gerät benötigt wird, sind die Hardwarekosten bei Single-Box-Lösungen meist niedriger.

– Von den Administratoren ist nur ein Gerät zu betreuen und zu überwachen.

– Neben ausgeklügelten Paketfiltersystemen können die Single-Box-Lösungen bereits wichtige und ausgereifte Proxy-Server enthalten.

– Das sogenannte Härten des Sicherheitssystems wird bei der Installation einiger Lösungen automatisch erledigt.

Nachteile:

– Zwischen äußerem und innerem Netz befindet sich nur eine Maschine. Wenn diese überwunden wird, hat ein Angreifer vollen Zugriff auf die interne Netzstruktur.

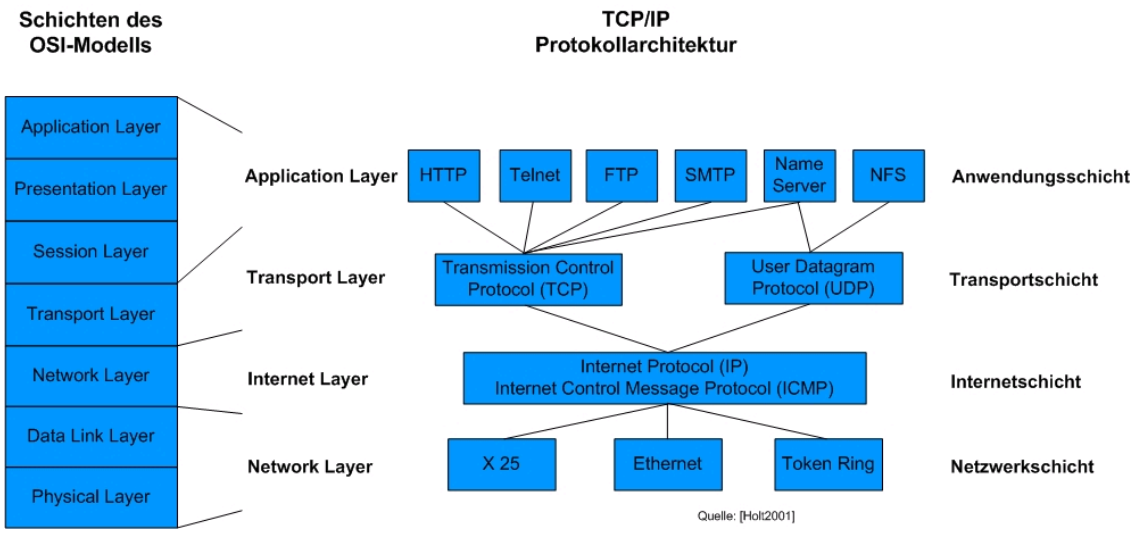
[19] manchmal als Choke-Router bezeichnet

– Die Konfiguration einer Single-Box-Lösung wird zwar durch die einheitliche Oberfläche erleichtert, teilweise werden dadurch aber auch die eigentlichen Probleme und kritischen Punkte verdeckt.

Insgesamt überwiegen aus unserer Sicht jedoch die Vorteile der Single-Box-Lösungen, zumal vielfach weder das entsprechende Wissen noch die Zeit zur Verfügung stehen, um gleichwertige Multi-Box-Lösungen aufzubauen. Allerdings wäre die zweckmäßigste und wirtschaftlichste Lösung jeweils unter Berücksichtigung der örtlichen Gegebenheiten und Sicherheitsanforderungen zu ermitteln.

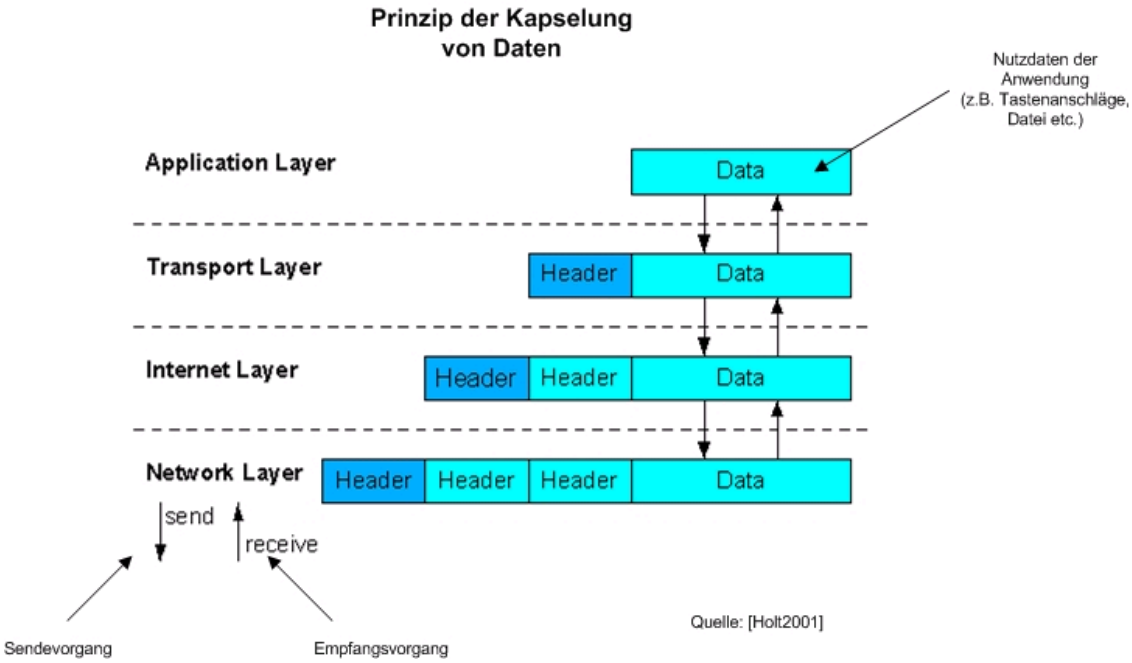
8. Protokolle und deren Pakete

Um die Vor- und Nachteile der Komponenten einer Firewall zu verstehen, müssen wir an dieser Stelle etwas näher auf das eingehen, womit Firewalls arbeiten: Protokolle und deren Pakete. Damit Informationen effizient über ein Netzwerk übertragen werden können, werden sie in kleine Teile zerlegt, die einzeln und abwechselnd gesendet werden. In IP-Netzwerken nennt man diese Teile Pakete. Da das Internet ein Netzwerk von TCP/IP-Netzen ist, wollen wir kurz den Aufbau der TCP/IP-Protokoll-Architektur in bezug auf die einzelnen Netzwerkschichten darstellen:



Für das Verständnis der weiteren Ausführungen genügt es zu wissen, daß in jeder dieser Schichten (Layer) ein Paket grundsätzlich aus zwei Teilen besteht, den relevanten Informationen für die Weiterleitung (Header) und dem Datenbereich (Data). Beim Sendevorgang behandelt jede Schicht die Informationen, die sie aus der darüberliegenden Schicht erhält, als Daten und stellt diesen Daten (Data) wiederum ihren eigenen Header voran. Dieser Vorgang wird Kapselung genannt (ähnlich wie die Häute einer Zwiebel, die darunter liegende Schichten umhüllen). Das so gebildete Gesamtpaket wird als Datagramm bezeichnet und auf der Netzwerkschicht weitergeleitet. Am anderen Ende einer Verbindung wird dieser Vorgang umgekehrt. Beim Weiterreichen der Daten von einer Schicht an die nächsthöhere Schicht wird jeder

Header (jedes Zwiebelhäutchen) von seiner entsprechenden Schicht wieder entfernt. Die nachfolgende Darstellung soll diese Abläufe verdeutlichen:



9. Firewallkomponenten

9.1 Paketfilter

Bei der Paketfilterung wird in der Regel auf den OSI-Schichten[20] drei und vier der TCP/IP-Protokollfamilie überprüft, welche Pakete an ein externes Netz oder aus einem externen Netz an die angegebene interne Zieladresse weitergereicht werden dürfen. Paketfilter stehen entweder auf Routern[21] zur Verfügung (zumeist als reine Hardwarelösungen) oder sind als reine Softwarelösungen erhältlich. Eigentlich ist die grundlegende Routing-Funktionalität schon in den meisten PC-Betriebssystemen enthalten. Während dedizierte Router ohne Paketfilter nur die optimale Verbindung für die Weiterleitung eines Pakets anhand ihrer Routing-Tabellen ermitteln, prüfen Router mit Paketfilter (gelegentlich auch als Filter- oder Überwachungsrouter bezeichnet) anhand interner Regeln, ob das Paket an das Zielsystem weitergeleitet werden darf oder nicht. Die Paketfilterung wird meistens auf sogenannten Überwachungsroutern eingesetzt, kann aber auch auf den Bastion-Hosts und dedizierten Firewallsystemen (Single-Box-Lösungen[22]) stattfinden. Die Anforderungen an einen geeigneten Paketfilter für eine Firewall hat das BSI im IT-GSHB (M 2.74) ausführlich dargestellt, weshalb wir hier nicht näher darauf eingehen wollen.

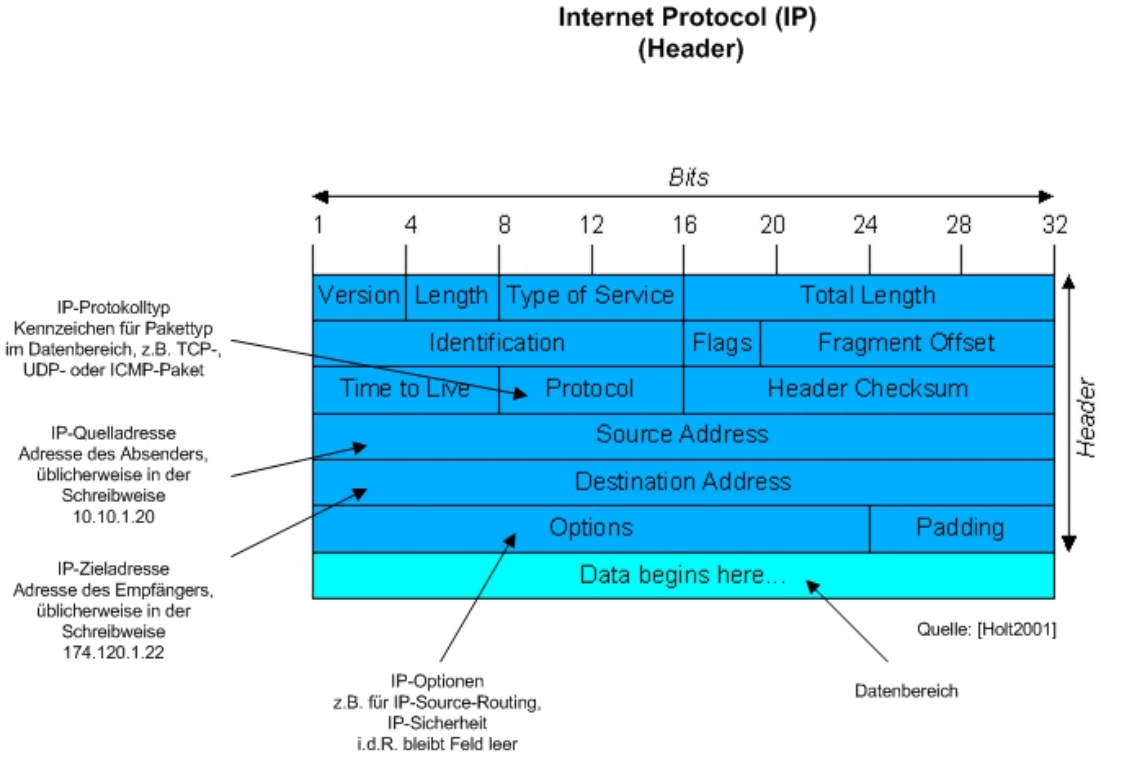
---

[20] Die Zusammenhänge zwischen dem OSI-Schichtenmodell, TCP/IP und anderen Protokollen sind in der Anlage dargestellt.

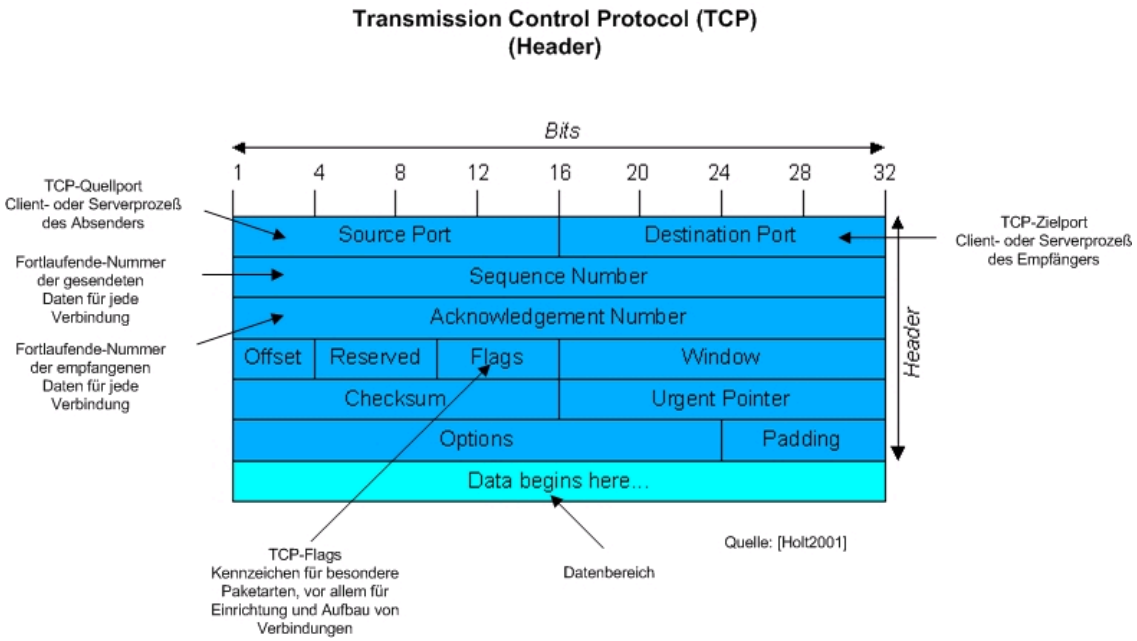
[21] Geräte, die IP-Netze miteinander verbinden, werden Router genannt.

[22] Gelegentlich werden diese auch als Firewall-Appliance bezeichnet.

Für die Paketfilterung sind vor allem die Header der Protokolle auf der Internet- und Transportschicht von Bedeutung, die (auf Basis der am weitesten verbreiteten Protokolle IP, TCP und UDP erläutert) folgende interessante Informationen enthalten:

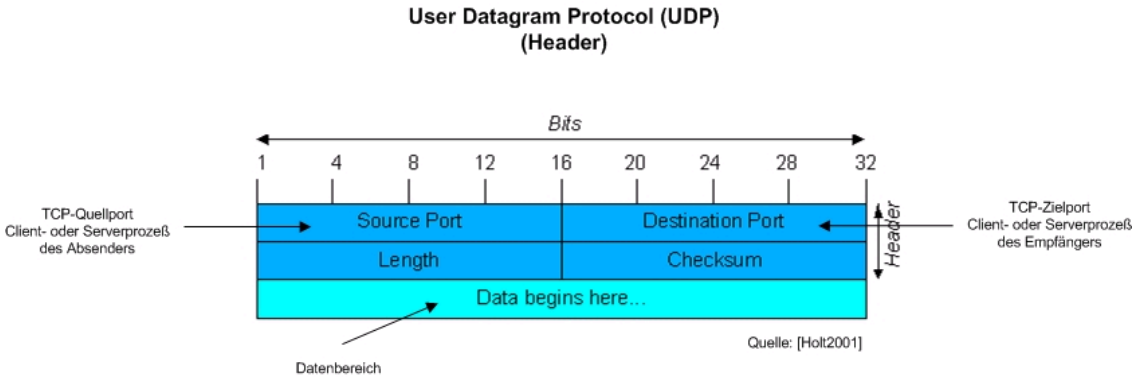


Das verbindungsorientierte[23] TCP-Protokoll trägt im sogenannten Header folgende Informationen:



[23] vergleichbar dem Telefonieren

Das verbindungslose[24] UDP-Protokoll ist dagegen im Header auf sehr viel weniger Informationen beschränkt:



Vorteile der Paketfilterung:

- Da Router ohnehin die Paket-Header vor der Weiterleitung prüfen, ist dies eine strategisch günstige Stelle, um auch weitergehende Kontrollen (Prüfungen auf Grundlage der Ziel- und Quelladresse, Auswertung der verwendeten Sitzungs- und Anwendungsports) durchzuführen.

- Paketfilter sind sehr leistungsfähig.

- Die Paketfilterung kann mit relativ wenig Aufwand betrieben werden, zumal kommerzielle Router in der Regel bereits über eingebaute Filtersysteme verfügen.

- Die Kontrolle ein- und ausgehender TCP-Verbindungen ist auf Grundlage des Drei-Wege-Initialisierungsprozesses (three-way-handshake) sehr effizient und sicher möglich. Damit können unter anderem bestimmte Arten von Port-Scans und DoS-Attacken verhindert werden.

- Mit Hilfe dynamischer (zustandsgesteuerter) Paketfilter[25] können nicht nur laufende Verbindungen überwacht, sondern auch in Abhängigkeit von bestimmten Protokolleigenschaften neue Filterregeln generiert und Ports temporär geöffnet bzw. nach Verbindungsende wieder geschlossen werden. UDP-Pakete können ohnehin nur auf Basis der dynamischen Paketfilterung einer bestehenden UDP-Verbindung zugeordnet werden. Manche dynamischen Paketfilter erlauben, wenn auch in beschränktem Umfang, neben der Überwachung des Zustands einer Verbindung auch eine Prüfung der Paketdaten auf der Ebene einiger Kommunikationsprotokolle der Anwendungsschicht.

- Paketfilter bieten sich als Sicherheitsmechanismen für Protokolle der Anwendungsschicht an, bei denen keine dedizierten Proxies verfügbar sind, die lediglich mit einem generischen Proxy[26] arbeiten oder die überhaupt nicht proxyfähig sind.

---

[24] vergleichbar dem Versenden eines herkömmlichen Briefes

[25] häufig auch als „stateful-inspection“ bezeichnet, vgl. Begriffserläuterungen

[26] Die beiden Begriffe dedizierter Proxy und generischer Proxy werden im Kapitel 9.2 erläutert.

Nachteile der Paketfilterung:

– Paketfilter sind oft schwer zu konfigurieren, da die Filterregeln sehr schnell unübersichtlich und daher komplex werden.

– Paketfilterregeln lassen sich nur aufwendig testen.

– Die Paketfiltereigenschaften mancher Produkte sind eingeschränkt und erlauben daher nicht alle Arten von Filterregeln.

– Fehler in der Konfiguration oder Implementierung von Paketfiltern führen eher zu Sicherheitsproblemen als Fehler in Proxy-Systemen.

– Paketfilter verbergen keine Strukturen des zu schützenden Netzwerks und trennen dies nicht vom unsicheren Netz.

9.2 Proxy-Systeme

Proxies (Stellvertreter) sind in der Regel besonders geschützte Rechner (z.B. Dual-Homed Bastion-Host), über die alle Verbindungen zwischen dem lokalen Netzwerk und dem Internet geleitet werden. Im Gegensatz zu Paketfiltern trennen sie jedoch die Verbindungen am Übergang zwischen den Netzen und agieren anstelle des jeweiligen Clients. Diese Technik wird einerseits dazu benutzt, um die Leistungsfähigkeit eines Internet-Zugangs zu verbessern (sogenannte Cache-Proxies), andererseits werden damit vor allem der Verbindungsaufbau und der ein- und ausgehende Datenverkehr auf Ebene der Protokolle der Anwendungsschicht kontrolliert (sogenannte Filter-Proxies). Proxies arbeiten damit auf der siebten OSI-Schicht. Das folgende Beispiel soll anhand einer WEB-Abfrage ihre Funktionsweise verdeutlichen:

Der Client eines Benutzers (z.B. Internet-Explorer) wendet sich an den HTTP-Proxy-Server des Standorts und nicht direkt an den echten HTTP-Server im Internet. Der Proxy-Server bewertet die Anfragen des Clients und entscheidet sich dann, ob er diese weiterreicht oder verwirft. Wird die Anfrage zugelassen, leitet der Proxy-Server diese an den echten HTTP-Server weiter und nimmt auch dessen Antworten entgegen. Handelt es sich um gültige Antworten, leitet der Proxy-Server diese zum Client zurück. Für den Benutzer scheint es so, als ob er direkt mit dem echten HTTP-Server im Internet kommunizieren würde, obwohl in Wahrheit der Proxy-Server stellvertretend für den Client diese Aufgaben wahrgenommen hat.

Obwohl diese Funktionsweise allen Proxy-Servern zugrunde liegt, unterscheiden sie sich hinsichtlich ihrer Leistungsfähigkeit doch sehr stark und bieten deshalb unterschiedlich starken Schutz vor Angreifern.

Ein **dedizierter Proxy-Server** bedient nur ein einziges Protokoll der Anwendungsschicht und kennt dessen Befehle genau. Ein solcher Proxy-Server wird in der Praxis auch als **Application-Level-Proxy** oder **Application-Level-Gateway (ALG)** bezeichnet. Da dedizierte Proxies die protokollspezifischen Eigenheiten kennen, bieten sie weit mehr Funktionalitäten als einfache Paketfilter. Neben der Steuerung der Verbindungen anhand der Quell- und Zieladresse sowie des Ports erlauben sie in zunehmendem Maße eine Kontrolle der mit dem Protokoll übermittelten Inhalte. Es kann mit ihnen festgestellt werden, ob die übertragenen Befehle sicher sind oder überhaupt dem jeweiligen Protokoll entsprechen. Dies ist insbesondere deshalb wichtig, weil zwischenzeitlich bestimmte Protokolle und deren Ports von mehreren unterschied

lichen Anwendungen benutzt werden. Zum Teil wird durch eine solche Kapselung von Informationen in bekannten Diensten auch versucht, die Regeln und Einschränkungen einer Firewall zu umgehen oder einfach deren Neukonfiguration zu vermeiden. Daneben bieten dedizierte Proxies bessere Protokollmöglichkeiten an, als mit anderen Mitteln erreicht werden kann.

Generische Proxy-Server bedienen dagegen mehrere Protokolle der Anwendungsschicht, ohne das Anwendungsprotokoll selbst zu kennen und zu interpretieren. Man nennt sie in der Praxis auch **Circuit-Level-Proxies**. Sie bieten gegenüber dem reinen Paketfilter nur eine höhere Sicherheit in bezug auf Fehler in Paket-Headern und bei der Fragmentierung von Paketen. Ansonsten sind sie ebenfalls auf die Kontrolle der jeweiligen Verbindung anhand der Quell- und Zieladresse sowie des verwendeten Ports beschränkt. Nachteilig ist jedoch, daß nicht alle Protokolle problemlos durch einen generischen Proxy verarbeitet werden können, insbesondere dann, wenn Portinformationen zwischen Client und echtem Server ausgetauscht werden müssen.

Die Vorteile der Filter-Proxies sind:

- Der Proxy-Server ist der einzige Rechner, der eine gültige, im Internet sichtbare IP-Adresse benötigt.

- Es besteht keine direkte Verbindung zwischen dem internen Client und dem Internet. Die Strukturen des inneren Netzwerks (z.B. Domain-Namen, IP-Adressen, Rechnername) werden komplett verborgen.

- Ein dedizierter Proxy-Server kennt die zugelassenen Befehle des jeweiligen Protokolls und läßt deshalb nur gültige Anfragen auf dem jeweiligen Port durch oder ermöglicht deren Filterung.

- Protokollierung und Kontrolle der Zugriffe sind auf einer höheren Ebene möglich und deshalb wesentlich leistungsfähiger und variabler als auf der Ebene der niedrigeren Protokolle (IP, TCP, UDP), bei denen die auswertbaren Informationen einfach durch den Aufbau des Headers begrenzt sind.

Die Nachteile der Filter-Proxies sind:

- Der Betrieb von Filter-Proxies erfordert auf Clientseite eine Proxy-taugliche Anwendungs- oder Betriebssystemsoftware oder einen entsprechenden Router, der Pakete automatisch abfängt und zum entsprechenden Proxy-Server umleitet.

- Dedizierte Proxy-Server stehen in der Praxis nur für die wichtigsten Dienste (z.B. Telnet, FTP, SMTP, DNS, NNTP, HTTP) zur Verfügung. Alle anderen Dienste müssen - sofern dies aufgrund der Protokolleigenschaften möglich ist - entweder über generische Proxies oder Paketfilter abgewickelt werden.

- Proxies haben gegenüber Paketfiltern eine geringere Geschwindigkeit beim Datendurchsatz.

9.3 Network-Address-Translation (NAT)

Dieser Begriff beschreibt grundsätzlich die Manipulation von IP-Source- und IP-Destination-Adresse im IP-Header. Damit ist es möglich, eine bestimmte Gruppe von Netzwerk-Adressen für den internen Gebrauch und eine oder mehrere Netzwerk-Adressen für die Anbindung an externe Netzwerke zu verwenden. Manchmal wird unter dem Begriff „NAT“ auch die Änderung des Port-Eintrags subsumiert, obwohl hier eigentlich präziser von einer Port-Address-Translation (PAT) gesprochen werden müßte. In der Praxis ist in modernen Firewallsystemen meist beides möglich. Die Funktionsweise von NAT[27] läßt sich kurz wie folgt beschreiben:

Wenn ein Client ein Paket an einen Server im externen Netzwerk schickt, modifiziert das NAT-System die Quelladresse so, daß es aussieht, als käme es von einem ganz anderen Client (NAT-Address-Pool). Antwortet nun der externe Server, wird die von diesem verwendete Destination-IP-Adresse vom NAT-System wieder in die tatsächliche IP-Adresse des Clients umgewandelt, so daß der Absender dann tatsächlich auch die Antwort erhält. Voraussetzung hierfür ist jedoch, daß das NAT-System das empfangene Paket der vom Client initiierten Verbindung zuordnen kann. Die Port-Umsetzung funktioniert in gleicher Weise.

Allerdings weisen wir darauf hin, daß bei einem sauber aufgebauten Netzwerk und einer Firewallarchitektur, wie wir sie in Ziffer 7 beschrieben haben, NAT wohl nicht mehr nötig ist und auch keinen zusätzlichen Sicherheitsgewinn brächte.

Die Vorteile von NAT sind:

- NAT unterstützt die Firewall bei der Kontrolle einer nach außen gerichteten Verbindung.

- Ein NAT-System, das Adressen dynamisch anpaßt, erlaubt nur solche Pakete, die zur aktuellen, von der Innenseite initiierten Verbindung gehören. Insoweit ist damit ein weiterer (kleiner) Sicherheitsgewinn verbunden, da der betreffende Client nur für die Dauer der Verbindung direkt erreichbar ist.

- Da NAT die internen Netzwerkstrukturen verbirgt, erschwert dies einem potentiellen Angreifer die Netzwerkanalyse.

Die Nachteile von NAT sind:

- Die dynamische Adreßanpassung erfordert Zustandsinformationen, die nur bei verbindungsorientierten Protokollen (z.B. TCP) zuverlässig vorliegen. Bei UDP-Paketen können Probleme auftreten.

- Die im Datenteil eines Pakets eingebetteten IP-Adressen kann NAT nicht bei allen Protokollen umsetzen.

- NAT funktioniert nicht mit Protokollen, die eingebettete IP-Adressen mit dem Schutz der Datenintegrität kombinieren (z.B. IPSec).

- Die dynamische Anpassung von IP-Adressen oder Ports kann, abhängig davon, an welcher Stelle sie vorgenommen wird, die Protokollierung des Datenverkehrs verfälschen und die Paketfilterung beeinträchtigen.

[27] In der Linux-Welt wird anstelle von NAT meistens der Begriff „IP-Masquerading“ verwendet.

10. Lösungen

a) Auswahlkriterien für Firewallsysteme

Gute Firewallsysteme gibt es zwar nicht wie Sand am Meer, dennoch sind zwischenzeitlich einige sehr leistungsfähige Lösungen verfügbar, die anhand

- des örtlichen Schutzbedarfs,
- der von den genutzten Internet-Diensten ausgehenden Risiken und
- des Preis-/Leistungs-Verhältnisses

ausgewählt werden müssen.

Bei mittlerem bis hohem Schutzbedarf empfehlen wir grundsätzlich eine Lösung einzusetzen, die die Anforderungen des IT-GSHB an eine sichere Firewall (vgl. M 2.72, M 2.74, M 2.75) erfüllt. Bei reinen Paketfiltersystemen sollte mindestens eine dynamische Paketfilterung (statefulinspection) möglich sein. Aufgrund der höheren Schutzwirkung sind dedizierte Filter-Proxies gegenüber der reinen Paketfilterung vorzuziehen. Sind nur generische Proxies für den jeweiligen Dienst verfügbar, empfiehlt sich eine Kombination von Paketfilter und Proxy. Grundsätzlich gilt: Je weiter oben die Firewall technisch im Schichtenmodell angesiedelt ist und je detaillierter protokollspezifische Inhalte kontrolliert werden können, desto höher ist ihre Schutzwirkung. In der Praxis gibt es häufig keine Standardlösung, da die Verhältnisse zu unterschiedlich sind. Mithin ist zu berücksichtigen, daß kleinere Schwächen einer bestimmten Lösung auch durch andere Schutzmaßnahmen (z.B. durch eine höhere Rechnersicherheit im Netz, Einsatz nachgeschalteter Filterproxies oder weiterer Überwachungsrouter, Verbindung über ein zusätzlich abgesichertes Netz[28]) ausgeglichen werden können.

Die Risiken, die von den jeweils genutzten Internet-Diensten ausgehen, sind unterschiedlich. Es gibt aus technischer Sicht sichere (z.B. SSH, SSL) und unsichere Dienste (z.B. ICQ, SMTP, SNMP, TELNET), wobei es aber im Einzelfall darauf ankommt, wie und in welcher Umgebung diese Dienste genutzt werden. So ist es durchaus möglich, unsichere Dienste auf gesicherte Weise zu benutzen (z.B. SMTP über eine VPN-Verbindung). Allerdings können auch mit einem sicheren Dienst unsichere Inhalte (z.B. Viren, Trojaner) übertragen werden. Insoweit ist keine pauschale Aussage über den jeweiligen Grad der Gefährdung, der durch die Benutzung eines bestimmten Internet-Dienstes entsteht, möglich. Dieser muß individuell für jeden verwendeten Dienst im Hinblick auf die örtlichen Sicherheitsanforderungen und -richtlinien (security-policy), die technische Konfiguration der IT-Systeme des Standorts und die Art und Weise der Verwendung eines Internet-Dienstes ermittelt werden. Für die sicherheitstechnische Bewertung von Diensten und Protokollen[29] gibt es in der Fachliteratur[30] und im Internet ausreichend Hinweise, die auch den halbwegs versierten Systembetreuer in die Lage versetzen, die jeweiligen Risiken zu beurteilen.

[28] beispielsweise über kommunale Behördennetze oder das BYBN

[29] zum Unterschied zwischen Diensten und Protokollen vgl. Begriffsdefinitionen

[30] vgl. Literaturhinweise im Anhang

b) Kommerzielle Lösung oder Eigenbau?

Die Frage, ob der Eigenbau einer Firewall gegebenenfalls wirtschaftlicher und zweckmäßiger ist, kann nicht von vornherein eindeutig beantwortet werden. Wie fast immer kommt es auf die näheren Umstände an:

– Ist der Eigenbau unter Berücksichtigung aller einmaligen und laufenden Kosten (der Kalkulationszeitraum sollte ca. fünf Jahre betragen) und des damit erzielbaren Nutzens die wirtschaftlichste Lösungsvariante?

– Wird mit dem Eigenbau eine ausreichende Sicherheit erreicht?

– Ist die laufende Wartung und Pflege der Firewall über die geplante Einsatzdauer sichergestellt?

– Kann die Administration der Firewall auch von einem Vertreter bewältigt werden?

Da diese Fragen oftmals nicht oder nur eingeschränkt mit „Ja“ beantwortet werden können, dürfte sich das Thema „Eigenbau“ aus unserer Sicht meistens von selbst erledigen.

Obwohl kommerzielle Systeme aufgrund ihrer durchdachten Oberflächen regelmäßig einfacher und effizienter zu administrieren sind als „selbstgestrickte“ Lösungen, geben wir zu bedenken, daß auch deren Konfiguration komplex ist und Spezialwissen erfordert, das nur bei einem größeren IT-Betrieb und mehreren Administratoren wirtschaftlich sinnvoll vorgehalten werden kann. Soweit das notwendige Fachwissen örtlich nicht vorhanden ist, empfehlen wir, die Planung, Implementierung und Pflege von Firewallsystemen an fachkundige und vertrauenswürdige Dritte mit entsprechender Erfahrung und Zuverlässigkeit zu vergeben. Im Gegensatz zu manch anderen Bereichen in der IT muß die Firewall von Anfang an richtig funktionieren; für „learning by doing“ oder Experimente ist in diesem kritischen Umfeld kein Platz.

c) Erfahrungen mit interkommunalen Lösungen

Erfolgversprechend und auch wirtschaftlich sinnvoll scheint uns in diesem Zusammenhang ein Ansatz zu sein, der sich auf Ebene der kreisangehörigen Kommunen bei Einbindung in die sogenannten Landkreis-Behördennetze abzeichnet. Die Zusammenfassung und gemeinsame Nutzung einer Sicherheits-Infrastruktur bietet aus unserer Sicht viele Vorteile, da Personal und Technik nur an einer zentralen Stelle vorgehalten werden müssen. Die interkommunale Zusammenarbeit in diesem Bereich können wir aus diesem Grund nur begrüßen. Im Hinblick auf Art. 3 des neuen IuK-Gesetzes vom 01.01.2001 und die von den kommunalen Spitzenverbänden mit der Bayerischen Staatskanzlei im Juni 2002 abgeschlossene eGovernment-Vereinbarung[31] dürfte sich diese Entwicklung wohl auch in Zukunft verstärken. Andererseits verkennen wir nicht, daß verschiedene Kommunen aus den örtlichen Gegebenheiten heraus (z.B. spezielle Anforderungen an Bandbreite und Dienste, historisch gewachsene Strukturen, spezielle Anwendungen) möglicherweise nach wie vor auf eigene Übergänge zum Internet angewiesen sind und diese dann auch selbst schützen müssen. Selbstverständlich ist auch bei letzteren immer im Hinblick auf den Grundsatz der sparsamen und wirtschaftlichen Haushaltsführung zu hinterfragen, ob nicht zwischenzeitlich andere Lösungen in Frage kommen.

[31] sogenanntes E-Government-Pakt

d) Wahl auf Grundlage des zugrundeliegenden Betriebssystems?

Eine gute Firewall ist aus unserer Sicht keine Frage des jeweiligen Betriebssystems. Es gibt hinreichend sichere und vom BSI geprüfte Firewallsysteme für UNIX- und Windows-Betriebssysteme. Im übrigen ist es gerade im Hinblick auf die Sicherheit der sogenannten Bastion-Hosts viel wichtiger, daß sich der zuständige Administrator mit der Bedienung und den sicherheitsrelevanten Einstellungen des jeweiligen Betriebssystems gut auskennt und weiß, wie er sicherheitskritische Dienste und Programme zuverlässig deaktiviert oder entfernt, als theoretische Überlegungen in bezug auf die Sicherheit von Betriebssystemen anzustellen.

11. Trends und Entwicklungen bei Firewallsystemen

a) Trends bei Firewalltechnologien

In der Vergangenheit war bei den Firewalltechnologien ein deutlicher Trend zum Einsatz von Proxy-Systemen, insbesondere der sogenannten Application-Level-Gateways, erkennbar. Dies liegt wohl darin begründet, daß die Anforderungen komplexer werden und die verfügbaren Lösungen bereits eine Vielzahl dedizierter Filterproxies und in der Regel einen leistungsfähigen generischen Proxy enthalten. Aber auch die Paketfiltersysteme der Überwachungsrouter oder kleinere Single-Box-Lösungen werden immer leistungsfähiger. Mit Hilfe von „stateful-inspection“ und anderer Überwachungsmodule, die bis hinauf zur siebten OSI-Schicht arbeiten, bieten sie schon sehr viele Schutzmechanismen. Es hängt letztlich von den genutzten Diensten, der technischen Infrastruktur, der Konfiguration der eingesetzten IT-Systeme und dem jeweiligen Schutzbedarf ab, welche Systeme als Firewall geeignet sind. Ein Paketfiltersystem mit stateful-inspection dürfte jedoch derzeit aus technischer Sicht der Mindeststandard sein.

b) Neue Anforderungen mit eGovernment

Neue Herausforderungen für die Administratoren und Firewallsysteme in den kommunalen Gebietskörperschaften werden mit den allerorts anzutreffenden eGovernment-Aktivitäten zu erwarten sein. Dies wird insbesondere dann gelten, wenn über die reine Informationsbereitstellung und den Download von Formularen hinaus interaktive Anwendungen für den Bürger oder die sogenannten Power-User (Anwälte, Notare, Detekteien, KFZ-Händler, um nur einige zu nennen) verfügbar sind. Neben den reinen Sicherheitsaspekten werden dann auch die Anforderungen an die Verfügbarkeit und Ausfallsicherheit der Systeme (7 mal 24 Std.) erheblich höher sein als bisher. Daneben werden die sichere Authentifizierung und die Weiterleitung verschlüsselter Daten durch die Firewallsysteme hindurch zuverlässig gelöst werden müssen. Um den Anforderungen der Zukunft gewachsen zu sein, empfehlen wir eine Orientierung an den aktuellen Veröffentlichungen des BSI[32] und der Datenschutzbeauftragten des Bundes und der Länder zum Thema eGovernment[33].

[32] E-Government Handbuch, www.bsi.de/fachthem/egov/3.htm

[33] vgl. [DS2001]

c) Intrusion Detection

Wie wir an anderer Stelle schon festgestellt haben, ist eine Firewall nur ein Element der IT-Sicherheit und bietet keinen umfassenden Schutz vor Angriffen, insbesondere dann, wenn sie nicht von außen, sondern von innen (z.B. durch böswillige Benutzer oder eingeschleuste Programme) gestartet werden. In letzter Zeit wurden deshalb vermehrt Forderungen laut, die Überwachungstätigkeit der Administratoren durch automatische Überwachungssysteme zu unterstützen oder zu ergänzen. Solche Systeme werden Intrusion Detection Systeme (IDS) genannt und reichen von einfachen, passiven Programmen, die Protokolldateien lesen und nach Unregelmäßigkeiten durchsuchen, bis zu extrem komplexen Systemen, die das Verhalten des Netzwerks und des Betriebssystems nach Anomalien und den Datenstrom nach bestimmten signifikanten Signaturen untersuchen. Von der Wirksamkeit und der Komplexität solcher Systeme einmal abgesehen, stellt sich die Frage nach dem Nutzen-/Kosten-Verhältnis dieser Produkte. Des weiteren muß entsprechend geschultes Personal zur Verfügung stehen, um den Betrieb eines IDS sicherzustellen und dessen Alarmmeldungen zu verstehen. Aus unserer Sicht dürfte derzeit ein IDS erst ab einer gewissen Größenordnung zweckmäßig sein und wirtschaftlich eingesetzt werden können. Allerdings haben wir selbst noch zu wenig Erfahrungen mit IDS, um uns hierzu ein abschließendes Urteil bilden zu können.

12. Betrieb und Wartung von Firewalls

Mit der Installation einer technisch ausgereiften und gut konfigurierten Firewall ist es keineswegs getan.

Eine Firewall ist, wie wir bereits bei der Definition festgestellt haben, kein statisches, sondern ein dynamisches System, das regelmäßig überprüft, gewartet und aktualisiert werden muß. Gerade die Auswertung der Log-Dateien auf sicherheitsrelevante Vorfälle (z.B. erfolglose Anmelde- oder Verbindungsversuche, eintreffende Pakete mit internen Quelladressen, wiederholte Port-Scans etc.) ist elementarer Bestandteil eines sicheren Firewallbetriebs und sollte nicht vernachlässigt werden.

Daneben sollten die Sicherheitseinstellungen und die Protokollierung sicherheitskritischer Ereignisse sowohl nach der Installation einer Firewall wie auch im laufenden Betrieb gelegentlich mit geeigneten Programmen auf ihre Wirksamkeit hin überprüft und die lückenlose Protokollierung solcher (bewußter) Angriffe kontrolliert werden. Die Log-Dateien sind, wie andere Unterlagen über den ordnungsgemäßen Systembetrieb, bis zum Ablauf der Aufbewahrungsfristen nach § 82 KommHV in digital auswertbarer Form aufzubewahren, da sonst die Ordnungsmäßigkeit des IT-Betriebs nicht festgestellt werden kann.

Sollen neue Internet-Dienste genutzt oder angeboten werden, sind zunächst die Risiken dieser Dienste zu untersuchen. Sofern der Dienst mit den Sicherheitsrichtlinien vereinbar ist, sind die Einstellungen der Firewall entsprechend anzupassen und deren Wirksamkeit bzw. auch etwaige Seiteneffekte auf bereits vorhandene Sicherheitsmechanismen zu überprüfen. Es kommt nicht selten vor, daß Firewalleinstellungen aufgrund nachträglicher Installationen von Softwarelösungen (oft kurzerhand) verändert und ohne nähere Prüfung so belassen werden, was zu (neuen) Sicherheitslücken führen kann. Zur Betreuung einer Firewall zählt darüber hinaus auch das Studium der einschlägigen Warnmeldungen (z.B. BSI, CERT, Hersteller) und das Einspielen von Updates oder Bugfixes.

Diese Tätigkeiten erfordern nahezu das gleiche Verständnis und technische Wissen wie die Planung und Implementierung von Firewallösungen, so daß auch hier die Frage zu stellen ist, ob diese Aufgaben nicht besser an einen vertrauenswürdigen Dritten übertragen werden sollen. Diese sicher nicht einfache Entscheidung hängt im wesentlichen von den verfügbaren Personalressourcen, den haushaltsrechtlichen Vorgaben und der datenschutzrechtlichen Zulässigkeit[34] der Datenverarbeitung im Auftrag (vgl. Art. 6 BayDSG) ab. Eine gewisse Kernkompetenz, die vor allem eine Kontrolle der Aufgabenerfüllung durch den Dritten gewährleistet, muß aber nach wie vor in der Verwaltung selbst vorgehalten werden.

13. Grenzen von Firewalls

Firewalls sind primär darauf ausgerichtet, ein (internes) Netz vor Angriffen aus den daran angeschlossenen (externen) Netzen zu schützen; in der Regel ist dies das Internet. Firewalls sind aber keine umfassende und vollständige Sicherheitslösung, zumal sich manche Gefahren mit Firewalls gar nicht kontrollieren lassen. Insoweit kommt dem physischen Schutz des Netzwerks und der Server, der Rechnersicherheit, dem Virenschutz auf den Clients und Servern sowie der Schulung der Benutzer eine besondere Bedeutung zu.

Firewalls schützen insbesondere nicht vor folgenden Gefahren:

- Angriffe von böswilligen und untreuen Mitarbeitern oder Hackern im eigenen Netzwerk (z.B. mittels Netzwerk-Sniffern, Paßwort-Crackern oder auf fremden Systemen installierten Tastaturscannern)

- schlecht konfigurierte oder schlecht abgesicherte Systeme (z.B. Standardinstallationen von Betriebssystemen ohne System- und Sicherheitsrichtlinien, Benutzer mit weitreichenden Berechtigungen, Verwendung von schwachen oder leicht erratbaren Paßwörtern, Verwendung von Standard- oder Installationspaßwörtern)

- Viren, Trojaner oder Würmer, wenn sie auf Datenträgern ins Netz eingeschleust werden. Den eingehenden Datenverkehr kann eine Firewall nur bis zu einem gewissen Grad auf diese Schädlinge hin überprüfen. Der von diesen Schädlingen ausgehende Datenverkehr nach außen kann, sofern er die in der Firewall zugelassenen IP-Adressen, Ports und Protokolle verwendet, von einer Firewall leider nicht kontrolliert werden.

- Verbindungen in externe Netze, die nicht über die Firewall laufen

- Dienste, die ihre Daten in zugelassenen Protokollen und Ports verstecken

Eine Firewall ist, wenn sie richtig geplant, konfiguriert und betrieben wird, gleichwohl ein wesentlicher Bestandteil der IT-Sicherheit; beim Anschluß eines lokalen Verwaltungsnetzes an ein unsicheres öffentliches Netz (z.B. Internet) ist sie unentbehrlich. Etwas drastischer ausgedrückt: Es kommt ja auch niemand auf die Idee, ein Rathaus ohne verschließbare Eingangstüren zu bauen.

[34] vgl. 20. Tätigkeitsbericht des BayDSB, Abschnitt 17.3.3, „Outsourcing von Kommunaldaten“

14. Anhang

Literaturverzeichnis

[ZCC2002] **Einrichten von Internet Firewalls**, Elizabeth D. Zwicky, Simon Cooper & D. Brent Chapman, O'REILLY-Verlag

[BSI-GSHB] **IT-Grundschutzhandbuch 2002, Standard-Sicherheitsmaßnahmen**, Bundesamt für Sicherheit in der Informationstechnik, Bundesanzeiger-Verlag, www.bsi.de/gshb/index.htm

[Barth2001] **Das Firewall Buch**, Wolfgang Barth, SuSE PRESS

[BSI1998] **Grundlagen, Forderungen und Marktübersicht für Intrusion Detection Systeme (IDS) und Intrusion Response Systeme (IRS)**, Dr. Josef von Helden, Dr. Stefan Karsch, debis IT Security Services

[Holt2001] **Einführung in TCP/IP, Standards und Protokolle**, SS2001, Heiko Holtmann, Universität Bielefeld - Technische Fakultät

[Holt1999] **Einführung in TCP/IP**, Heiko Holtmann, Universität Bielefeld - Technische Fakultät

[Raepple1998] **Sicherheitskonzepte für das Internet**, Martin Raepple, dpunkt.verlag

[DS2000] **Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet**, Konferenz der Datenschutzbeauftragten des Bundes und der Länder, www.datenschutz-bayern.de/technik/orient/int_gesch.pdf

[DS2001] Handreichung „Datenschutzgerechtes eGovernment“, Konferenz der Datenschutzbeauftragten des Bundes und der Länder, www.lfd.niedersachsen.de/functions/downloadObject/0,,c1358174_s20,00.pdf

Begriffserläuterungen

Firewall	Eine Firewall ist eine Schwelle zwischen zwei Netzen, die überwunden werden muß, um Systeme im jeweils anderen Netz zu erreichen. Durch technische und administrative Maßnahmen wird dafür gesorgt, daß jede Kommunikation zwischen den beiden Netzen über die Firewall geführt werden muß. Auf der Firewall sorgen Zugriffskontrolle und Audit dafür, daß das Prinzip der geringsten Berechtigung durchgesetzt wird und potentielle Angriffe schnellstmöglich erkannt werden (Definition Deutsches Forschungsnetz - www.dfn-cert.de/team/ue/fw/fire/node3.html)
Stateful-inspection	Gelegentlich auch als dynamische Paketfilterung bezeichnet. Stateful-inspection ist eine Firewalltechnik, die ab der dritten Schicht des OSI-Modells (network-layer) arbeitet. Im Gegensatz zur statischen Paketfilterung wird bei stateful-inspection jede Verbindung, die zwischen den Netzwerk-Interfaces einer Firewall besteht, aufgezeichnet und es wird überwacht, ob die ein- und ausgehenden Pakete weiterhin zur bestehenden Verbindung gehören. Es wird also neben dem IP-Header der aktuelle Zustand der jeweiligen Verbindung dynamisch überwacht. Manche Systeme mit stateful-inspection sind sogar in der Lage, dynamisch Ports zu öffnen und wieder zu schließen. Im Vergleich zur statischen Filterung werden IP-Pakete bereits auf der Netzwerkschicht von einem Analysemodul entgegengenommen, das nicht nur die Überwachung der Verbindung ermöglicht, sondern die Inhalte der Pakete bis hinauf in die siebte Schicht des OSI-Modells (application-layer) untersuchen kann.
Dienst	Die Aufgabe einer Schicht innerhalb eines Protokollstapels ist die Bereitstellung eines bestimmten Dienstes (für die jeweils darüber liegende Schicht). Ein Dienst ist im Gegensatz zu einem Protokoll eine Gruppe von Operationen, die eine Schicht der über ihr liegenden Schicht zur Verfügung stellt [Holt2001].
Protokoll	Alle an einer Kommunikation beteiligten Parteien müssen sich auf Regeln einigen, die beim Austausch von Nachrichten angewendet werden sollen. Eine solche Vereinbarung wird Protokoll (protocol) genannt („Protocols are formal rules of behaviour“). Die Aufgaben eines Protokolls sind – die Adressierung der Kommunikationsendpunkte, – die Steuerung des Datenflusses, – die Bereitstellung eines sicheren Datenübertragungsdienstes. Ein Protokoll ist im Gegensatz zu einem Dienst das Regelgefüge, welches das Format und die Bedeutung der von den Partnereinheiten innerhalb einer Schicht ausgetauschten „Informationen“ festlegt [Holt2001].
Virenscanner	Programm zur Überwachung und Prüfung eines Computers auf schädliche Programme (z.B. Viren, Trojaner, Würmer)
security-policy	Oberbegriff für die Sicherheitspolitik (Festlegung von Sicherheitszielen) und das daraus abgeleitete Sicherheitskonzept (organisatorische und technische Maßnahmen zur Einhaltung der Sicherheitsziele) [Barth2001]

Online-Informationen zur IT-Sicherheit bieten unter anderem folgende Institutionen/Firmen/Mailinglisten/Newsgroups:

Bundesamt für Sicherheit in der Informationstechnik	www.bsi.de oder www.bsi.bund.de
Bundesministerium für Wirtschaft und Arbeit und Bundesministerium des Innern	www.sicherheit-im-internet.de/themes
Fa. Microsoft	www.microsoft.com/germany/ms/security
Telstra Corporation	www.telstra.com.au/infor/security.html
BugTraq	www.securityfocus.com
NTBugTraq	www.ntbugtraq.com
Cert-CC	www.cert.org
First	www.first.org
Internet Engineering Task Force	www.ietf.org
World Wide Web Consortium	www.w3c.org
USENIX Association	www.usenix.org
SysAdmin, Audit, Network, Security	www.sans.org
Diverse Hersteller von Software und Sicherheitsprodukten	

Wertung von Änderungsvorschlägen und Nebenangeboten

Verfasserin: Martina **Aschl**

Inhaltsübersicht Seite

Die Wertung von Änderungsvorschlägen und Nebenangeboten wirft in der Praxis immer wieder Fragen auf. Deshalb sollen einige vor kurzem veröffentlichte obergerichtliche Entscheidungen zum Anlaß genommen werden, diese Problematik näher zu erläutern.

1. Begriffsbestimmungen

Eine Definition der Begriffe „Nebenangebot“ und „Änderungsvorschlag“ (in der Praxis auch Sondervorschläge genannt) ist der VOB nicht zu entnehmen. Aus dem Wortsinn ergibt sich, daß unter „Nebenangebot“ ein Angebot zu verstehen ist, das von einem Bieter neben dem geforderten „Hauptangebot“ eingereicht wird. Als Änderungsvorschlag kann man den Vorschlag eines Bieters bezeichnen, die Leistung in einer anderen als der vom Auftraggeber vorgesehenen Art auszuführen. In der Praxis ist es gebräuchlich, Bietervorschläge, die eine völlig andere als die geforderte Leistung zum Inhalt haben (z.B. eine Betonbrücke anstatt der ausgeschriebenen Stahlbrücke), als Nebenangebote, und solche, die sich nur auf einen Teil der Leistung beziehen (z.B. eine zusätzliche Brückenstütze, ein anderer Brückenbelag), als Änderungsvorschläge zu bezeichnen. Eine exakte Abgrenzung ist nicht möglich. Von Nebenangeboten wird auch gesprochen, wenn die Leistung unter anderen als den in den Verdingungsunterlagen vorgesehenen vertraglichen Rahmenbedingungen für die Leistung (z.B. Lohn- und Stoffpreisgleitklauseln) oder unter Abweichung von den vertraglich vorgesehenen Abrechnungsmodalitäten (z.B. Pauschalpreis anstelle von Einheitspreisen) angeboten wird. Keine Nebenangebote sind globale Preisnachlässe und Angebote mit Skonti für den Fall der Einhaltung bestimmter Zahlungsfristen (vgl. Heiermann/Riedl/Rusam, VOB, 8. Auflage, A § 25 Rdn. 70, 71, 72, 75, 76).

2. Vorteile und Risiken für Auftraggeber und Auftragnehmer

Nebenangebote und Änderungsvorschläge dienen der Verbesserung der Auftragschancen mit Hilfe technisch oder wirtschaftlich besserer Lösungen als den vom Auftraggeber vorgesehenen. Für den Auftraggeber können sie zu erheblichen Einsparungen führen. Außerdem fördern sie die notwendige technische Weiterentwicklung, die Rationalisierungsbemühungen und die Konkurrenzfähigkeit, auch im internationalen Wettbewerb (vgl. Heiermann/Riedl/Rusam, VOB, 8. Auflage, A § 25 Rdn. 69). Risiko des Auftragnehmers ist, daß er für Planung, technische Gestaltung, Kalkulation und praktische Ausführung die volle Verantwortung trägt. Im Risikobereich des Auftraggebers liegt es dagegen, daß er für preislich günstige Vorschläge möglicherweise keine gleichwertige Leistung erhält oder bei ihm neue oder ungenügend erprobte Bauweisen ausprobiert werden (vgl. Heiermann/Riedl/Rusam, VOB, 8. Auflage, A § 25 Rdn. 81, 82).

3. Voraussetzungen der Wertung von Änderungsvorschlägen und Nebenangeboten

Auftraggeber sind verpflichtet, Änderungsvorschläge und Nebenangebote wie Hauptangebote zu werten. Ausnahmen von dieser Verpflichtung gibt es nur, wenn Änderungsvorschläge und Nebenangebote

– in der Bekanntmachung oder in den Vergabeunterlagen nicht zugelassen wurden (§ 25 Nr. 5 Satz 1, Nr. 1 Abs. 1 lit. d, § 10 Nr. 5 Abs. 4 VOB/A),

– wegen Unvollständigkeit von der Wertung ausgeschlossen sind (§ 25 Nr. 1 Abs. 1 lit. b, § 21 Nr. 1 Abs. 1 Satz 3 VOB/A),

– wegen mangelnder Kennzeichnung von der Wertung ausgeschlossen werden (§ 25 Nr. 1 Abs. 2, § 21 Nr. 3 Satz 2 VOB/A).

4. Ausschluß wegen Nichtzulassung (§ 25 Nr. 5 Satz 1, Nr. 1 Abs. 1 lit. d, § 10 Nr. 5 Abs. 4 VOB/A)

Nicht zugelassene Änderungsvorschläge und Nebenangebote werden ausgeschlossen (§ 25 Nr. 1 Abs. 1 lit. d VOB/A). Nach § 10 Nr. 5 Abs. 4 VOB/A ist in den Verdingungsunterlagen anzugeben, wenn der Auftraggeber Änderungsvorschläge und Nebenangebote wünscht oder nicht zulassen will oder wenn Nebenangebote ohne gleichzeitige Abgabe eines Hauptangebots ausnahmsweise ausgeschlossen werden (letzteres sollte nur ausnahmsweise erfolgen, da sonst Betriebe, die nur zur Erbringung der im Nebenangebot angebotenen Leistungen technisch in der Lage sind, ohne ausreichenden Grund nicht zum Zuge kämen, vgl. Heiermann/ Riedl/Rusam, VOB, 8. Auflage, A § 10 Rdn. 24).

Enthalten die Verdingungsunterlagen Formulierungen, daß bestimmte Festlegungen des Leistungsverzeichnisses verbindlich sein sollen, können Änderungsvorschläge und Nebenangebote ebenfalls ausgeschlossen sein, wenn sie von diesen Festlegungen abweichen (vgl. Vergabekammer Nordbayern, ZfBR 2002, 195 und Heiermann/Riedl/Rusam, VOB, 8. Auflage, A § 25 Rdn. 87).

Hat sich der Auftraggeber zu Änderungsvorschlägen in der Bekanntmachung oder in den Verdingungsunterlagen nicht geäußert, so muß er sie genauso wie die Hauptangebote werten (§ 25 Nr. 5 Satz 1 VOB/A). Wertet der Auftraggeber ein nicht zugelassenes Nebenangebot, kann dies beim übergangenen Bieter Schadensersatzansprüche aus Verschulden bei Vertragsschluß auslösen, da das durch die Ausschreibung begründete Vertrauensverhältnis verletzt wird (vgl. Heiermann/Riedl/Rusam, VOB, 8. Auflage, A § 25 Rdn. 86).

5. Ausschluß wegen Unvollständigkeit (§ 25 Nr. 1 Abs. 1 lit. b, § 21 Nr. 1 Abs. 1 Satz 3 VOB/A)

Nach § 25 Nr. 1 Abs. 1 lit. b werden Angebote, also auch zugelassene Nebenangebote und Änderungsvorschläge, die zum Zeitpunkt der Angebotsabgabe unvollständig sind, von der Wertung ausgeschlossen. Sie entsprechen dann nicht § 21 Nr. 1 Abs. 1 und 2 VOB/A. Dort ist festgelegt, daß die Angebote die Preise und die geforderten Erklärungen enthalten sollen.

Ob ein Angebot, das die geforderten Erklärungen nicht enthält, zwingend oder nur bei Einfluß auf den Wettbewerb auszuschließen ist, ist wegen der Formulierung des § 21 Nr. 1 Abs. 1

Satz 3 VOB/A („sollen“) strittig. Von der h.M. wird der zwingende Ausschluß im Hinblick auf den klaren Wortlaut des § 25 Nr. 1 Abs. 1 lit. b bejaht (BGH, NJW 1998, 3634).

Änderungsvorschläge und Nebenangebote müssen eindeutig und erschöpfend beschrieben sein. Die Leistungsangaben des Bieters müssen den Anforderungen entsprechen, wie sie für den Bauherrn in § 9 VOB/A festgelegt sind (vgl. Ingenstau/Korbion, VOB Kommentar, 14. Auflage, A § 25 Nr. 5 Rdn. 87). Der Bieter muß sein Nebenangebot so gestalten, daß es der Auftraggeber ohne besondere Schwierigkeiten werten kann. Er muß die Gleichwertigkeit durch entsprechende Unterlagen belegen. Ein Nebenangebot muß zu diesem Zweck alle Daten enthalten, die nötig sind, damit der Auftraggeber sich ein klares Bild über den Inhalt verschaffen und das Angebot nicht manipuliert werden kann. Zum Wettbewerb gehört eine vollständige, übersichtliche und nachvollziehbare Präsentation der Angebote durch die Bieter unter Berücksichtigung der speziellen subjektiven Anforderungen und vorhersehbaren möglichen Bedenken des Auftraggebers. Fehlen in einem Nebenangebot die für die inhaltliche Bestimmung und die Wertung erforderlichen Daten oder sind sie derart allgemein gehalten, daß ein Vergleich mit anderen Angeboten nicht möglich ist, so ist das Nebenangebot auszuschließen (OLG Frankfurt a.M., NZBau 2002, 692). In dem vom OLG Frankfurt a.M. entschiedenen Fall fehlten in dem Nebenangebot Angaben zur erforderlichen Menge Stahl für eine alternative Konstruktion einer Brücke. Die Mengenangaben waren für die Prüfung der Statik und Dauerhaftigkeit, und damit für die Beurteilung der Gleichwertigkeit des Nebenangebots, zwingend erforderlich. Ein Bieter muß schlüssig und nachvollziehbar darlegen, inwieweit die von ihm angebotenen Masseneinsparungen auf der technischen Alternativlösung und nicht auf einer bloßen Reduzierung des Mengenansatzes im Leistungsverzeichnis beruhen. Die Mengeneinsparungen müssen transparent sein.

Nach einer Entscheidung des OLG Brandenburg (NZBau 2002, 694) reicht eine beigefügte Produktinformation des Herstellers, der die allgemeinen technischen Werte des Produkts zu entnehmen waren, nicht aus, die konkrete Gleichwertigkeit des Produkts zur ausgeschriebenen Leistung zu begründen. Aus dem Änderungsvorschlag oder Nebenangebot muß eindeutig hervorgehen, welche in den Verdingungsunterlagen vorgesehenen Leistungen oder vertraglichen Regelungen geändert, ersetzt oder ergänzt werden (vgl. Heiermann/Riedl/Rusam, VOB, 8. Auflage, A § 25 Rdn. 90).

6. Keine Prüfungspflicht und keine Nachverhandlungen des Auftraggebers bei nicht nachgewiesener Gleichwertigkeit eines Nebenangebots

Änderungsvorschläge und Nebenangebote sind so zu werten, wie sie abgegeben wurden.

Weist der Bieter die Gleichwertigkeit nicht mit dem Angebot nach, besteht im Regelfall keine umfassende Nachforschungs- und Prüfungspflicht des Auftraggebers. Zur Ermittlung der Gleichwertigkeit sind vielmehr Nachforschungen nur im Rahmen der verfügbaren Erkenntnismöglichkeiten und innerhalb der zeitlichen Grenzen der Zuschlags- und Angebotsfrist anzustellen (vgl. OLG Brandenburg, NZBau 2002, 694).

Fehlende Angaben zur Gleichwertigkeit des Nebenangebots darf der Auftraggeber auch nicht unzulässigerweise im Wege von Nachverhandlungen ergänzen lassen. Aufklärungsgespräche dürfen sich nur auf die Erläuterung des wirklichen Angebots, nicht aber auf fehlende, jedoch zwingende Angebotsbestandteile beziehen. § 24 Nr. 1 Abs. 1 VOB/A läßt Aufklärungsver

handlungen nur über ein feststehendes, vom Bieter aber zweifelhaft formuliertes Angebot zu. Angaben, die zum Nachweis der Gleichwertigkeit eines Nebenangebots unbedingt erforderlich sind, können dagegen nicht im Wege von Aufklärungsgesprächen nachgeholt werden, weil der Bieter den Leistungsumfang und/oder seine Kalkulation ändern und eine in seinem ursprünglichen Angebot so nicht enthaltene Leistung anbieten könnte. Damit entstünden Manipulationsmöglichkeiten und Wettbewerbsverzerrungen (vgl. OLG Frankfurt a.M., NZBau 2002, 692).

Ein danach im Einzelfall erforderliches technisches Aufklärungsgespräch oder die Hinzuziehung eines externen Sachverständigen findet ihre Grenze aus Gründen der Gleichbehandlung dann, wenn zur Bewertung Unterlagen oder Angaben des Bieters erforderlich werden, die dieser bereits zusammen mit dem Nebenangebot hätte vorlegen müssen (vgl. OLG Rostock, NZBau 2002, 696).

7. Ausschluß wegen mangelnder Kennzeichnung eines Nebenangebots (§ 25 Nr. 1 Abs. 2, § 21 Nr. 3 Satz 2 VOB/A)

Auftraggeber haben die Möglichkeit, Änderungsvorschläge und Nebenangebote nicht zu werten, wenn sie nicht auf besonderer Anlage gemacht und als solche deutlich gekennzeichnet werden (§ 25 Nr. 1 Abs. 2, § 21 Nr. 3 Satz 2 VOB/A). Die Bieter sollen so gezwungen werden, zur Transparenz des Vergabeverfahrens beizutragen.

8. Wertung eines Hauptangebots als Nebenangebot

§ 21 Nr. 1 Abs. 2 VOB/A untersagt dem Bieter Änderungen an den Verdingungsunterlagen. Ändert der Bieter die Verdingungsunterlagen, ist sein Angebot nach § 25 Nr. 1 Abs. 1 lit. b VOB/A von der Wertung als Hauptangebot auszuschließen. In Betracht kommt aber eine Wertung des Angebots als Nebenangebot, es sei denn, der Auftraggeber hat Nebenangebote nicht zugelassen (§ 25 Nr. 5 VOB/A).

In seinem Urteil vom 16.04.2002 (X ZR 67/00, FSt 84/2003) entschied der Bundesgerichtshof, daß das Angebot eines Bieters, in dem dieser die Aufnahme der Arbeiten von der Erteilung gültiger Arbeitserlaubnisse für ausländische Arbeitnehmer abhängig machte, als Hauptangebot auszuschließen war. Eine Wertung als Nebenangebot ließ der Bundesgerichtshof zu. Wegen der zum Zeitpunkt der Vergabe offenen Frage, ob die beantragten Arbeitserlaubnisse erteilt würden, erachtete er das Nebenangebot aber als den geforderten (Haupt-)Angeboten nicht gleichwertig und billigte die Entscheidung des Bauherrn, einem anderen, teuereren Bieter den Auftrag auf dessen Hauptangebot zu erteilen.

In einem vom Bayerischen Obersten Landesgericht am 16.09.2002 entschiedenen Fall (Az.: Verg 19/02, Vergaberechts-Report 2/2003, Seite 2) enthielten die Verdingungsunterlagen bei einer öffentlichen Ausschreibung detaillierte Regelungen zu den Ausführungsfristen, insbesondere Regelungen zum Beginn und zur Fertigstellung der Arbeiten. Ein Bieter vermerkte in einem Begleitschreiben zu seinem Angebot: „Die Angabe eines Ausführungstermins erfolgt nach Verhandlung und Klärung aller technischer Einzelheiten bei Auftragserteilung.“ Das Bayerische Oberste Landesgericht führte aus, daß ein Angebot mit abweichenden oder einschränkenden

Erklärungen (hier einem Vorbehalt zur Leistungszeit) als Nebenangebot gewertet werden könne. Vorliegend komme jedoch eine Wertung als Nebenangebot wegen der Unbestimmtheit der Leistungszeit nicht in Betracht. Eine diesbezügliche Nachverhandlung mit dem Bieter sei unzulässig und verstieße gegen § 24 Nr. 1 VOB/A.

9. Zuschlag, Annehmbarkeit, Gleichwertigkeit

Der Zuschlag ist nach § 25 Nr. 3 Abs. 3 VOB/A auf das Angebot zu erteilen, das unter Berücksichtigung aller Gesichtspunkte, wie z.B. Preis, Ausführungsfrist, Betriebs- und Folgekosten, Gestaltung, Rentabilität oder technischer Wert, als das wirtschaftlichste erscheint (vgl. BGH, NZBau 2000, 35). Ein Nebenangebot muß grundsätzlich annehmbarer sein als der Auftraggebervorschlag. Annehmbarer heißt, daß der Bietervorschlag entweder eine bessere Lösung und nicht teuerer ist, oder eine gleichwertige Lösung und preislich günstiger ist (vgl. Heiermann/Riedl/Rusam, VOB, 8. Auflage, A § 25 Rdn. 93).

Will der Auftraggeber ausnahmsweise aus Gründen der Wirtschaftlichkeit einen Bietervorschlag in die Wertung einbeziehen, der keine qualitativ (z.B. Lagerhalle in Holzbauweise anstatt der ausgeschriebenen Stahlbetonbauweise) oder quantitativ (z.B. dreilagige anstatt vierlagige Dachabdeckung) gleichwertige Lösung der Bauaufgabe ist, ist dies nur möglich, wenn eine Wettbewerbsverzerrung mit Sicherheit ausgeschlossen werden kann. Ansonsten können in berechtigten Einzelfällen nur die Aufhebung der Ausschreibung und eine erneute Ausschreibung in Betracht kommen (vgl. Heiermann/Riedl/Rusam, VOB, 8. Auflage, A § 25 Rdn. 94 bis 96).

10. Sonderfälle: Pauschalpreisnebenangebote, Pauschalierung von Angeboten, bedingte Nebenangebote

Da Nebenangebote oft als Pauschalpreisangebote abgegeben werden, ist besonderes Augenmerk darauf zu legen, ob der Preis angemessen ist. Dies kann insbesondere bei im Leistungsverzeichnis enthaltenen „großzügigen“ Mengenansätzen relevant werden. Hauptangebote mit Einheitspreisen sind dann für einen Preisvergleich nicht mehr geeignet (vgl. Heiermann/Riedl/Rusam, VOB, 8. Auflage, A § 25 Rdn. 99 und den oben dargestellten Fall des OLG Frankfurt a.M., NZBau 2002, 692).

In Fällen ungenauer Mengenansätze im Leistungsverzeichnis bietet der Auftragnehmer bei oder nach Vertragsabschluß häufig eine Pauschalpreisvereinbarung an. Dies steht nicht im Widerspruch zu § 24 Nr. 3 VOB/A. Voraussetzung ist in solchen Fällen, daß sich der Auftraggeber ein Bild über die Mengenreserven verschafft, daß der Auftragnehmer die volle Verantwortung für die erstellten Unterlagen übernimmt und daß, abgesehen von Eingriffen des Bauherrn, eine Preisanpassung im Sinne des § 2 Nr. 7 Abs. 1 VOB/B vertraglich ausgeschlossen wird (vgl. Heiermann/Riedl/Rusam, VOB, 8. Auflage, A § 25 Rdn. 98 und OLG Frankfurt a.M., NZBau 2002, 692).

Bei bedingten Nebenangeboten (z.B. Lieferung von Kies aus firmeneigener Grube, falls Abbaugenehmigung erteilt wird) ist Vorsicht geboten. Eine Wertung ist nicht möglich, wenn der Eintritt der Bedingung offen und die Bauausführung damit fraglich ist. Die Wertung ist unzulässig, wenn der Eintritt der Bedingung vom Bieter abhängt, da er sonst nach Angebotseröffnung entscheiden könnte, ob er im Wettbewerb bleibt oder nicht, und damit eine echte Wettbewerbssituation nicht mehr gegeben wäre (vgl. Heiermann/Riedl/Rusam, VOB, 8. Auflage, A § 25 Rdn. 100).

Aufgaben und Organisation einer Innenrevision im kommunalen Krankenhaus

Verfasser: Wolfgang **Diller**

Inhaltsübersicht Seite

1. Einführung

Eine Innenrevision als eigenständige Stelle oder Funktionseinheit ist bisher nur in wenigen kommunalen Krankenhäusern in Bayern eingerichtet. Die Gründe hierfür liegen zum einen sicherlich darin, daß Krankenhäuser allgemein im Vergleich zu anderen Unternehmen erst spät ein Erkenntnisobjekt der Betriebswirtschaft wurden und damit die Beschäftigung mit Fragen der Innenrevision noch nicht so ausgeprägt ist wie in anderen Branchen. Zum anderen waren die kommunalen Krankenhäuser in Bayern durch die Kommunalgesetze ausnahmslos der örtlichen und überörtlichen Rechnungsprüfung unterworfen, so daß man aus diesem Grund nicht unbedingt die Notwendigkeit zur Einrichtung einer weiteren Kontrollinstanz sah.

Mit der Änderung der kommunalrechtlichen Vorschriften in den Jahren 1992 und 1995 wurde den Krankenhausträgern die Möglichkeit eröffnet, ihre Krankenhäuser in Rechtsformen mit eigener Rechtspersönlichkeit (GmbH und Kommunalunternehmen) zu überführen, für die eine örtliche und überörtliche Rechnungsprüfung gesetzlich nicht mehr vorgeschrieben ist. Diese Krankenhäuser unterliegen der jährlichen Abschlußprüfung nach § 316 HGB oder Art. 91 GO und sind damit im Hinblick auf die Prüfungspflichten sonstigen Unternehmen im nichtkommunalen Bereich gleichgestellt.

Wie für diese Unternehmen auch, stellt sich damit insbesondere für die kommunalen Krankenhäuser mit eigener Rechtspersönlichkeit die Frage nach Notwendigkeit und Organisation einer Innenrevision. Aber auch die Krankenhäuser, die weiterhin der kommunalen Rechnungsprüfung unterliegen, werden sich die Frage stellen müssen, ob die der Krankenhausleitung obliegende Kontrollfunktion, die mit der zunehmenden Komplexität des Krankenhausbetriebs ständig steigenden Anforderungen gerecht werden muß, noch ohne eine eigene innerbetriebliche Funktionseinheit erfüllt werden kann.

Hingewiesen sei in diesem Zusammenhang auch auf die durch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) in § 91 Abs. 2 AktG aufgenommene Verpflichtung des Vorstands, geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden. Aus der Gesetzesbegründung für das KonTraG ergibt sich eine Ausstrahlungswirkung auf andere Rechtsformen, so daß eine entsprechende Verpflichtung der Geschäftsführung generell gegeben ist.

2. Definition und Aufgaben der Innenrevision im Krankenhaus

2.1 Allgemeine Definition und Aufgabenstellung der Innenrevision

Die Betriebswirtschaftslehre definiert die Innenrevision als eine prozeßunabhängige Überwachungsfunktion, die im Auftrag der Geschäftsleitung Prüfungen in allen Unternehmensbereichen durchführt.[1] Der Begriff „prozeßunabhängig“ bedeutet dabei, daß die Überwachungsmaßnahme von einer Person durchgeführt wird, die vom zu überwachenden Prozeß oder Verantwortungsbereich weder direkt noch indirekt abhängig ist. Im Gegensatz dazu wird der Begriff

[1] Rolf Hofmann: Prüfungshandbuch, Praxisorientierter Leitfaden einer umfassenden Revisionskonzeption, Berlin 1990, S. 15

Kontrolle verwendet, wenn die Überwachung der mit der Ausführung der Aufgabe befaßten Person obliegt. Eine typische Kontrollfunktion ist zum Beispiel die Kontenabstimmung durch die Finanzbuchhaltung.

Grundsätzlich besteht die Aufgabe der Innenrevision darin, für die Geschäftsführung deren Verpflichtung zu übernehmen, die Ordnungsmäßigkeit des gesamten Geschäftsablaufs durch zweckentsprechende Kontrollen sicherzustellen; sie ist somit eine aus der Gesamtverantwortung der Geschäftsführung abgeleitete Teilfunktion, für deren zuverlässige Arbeit diese die Verantwortung trägt.[2]

Allgemein lassen sich die Aufgaben der Innenrevision im einzelnen wie folgt benennen:

- Schutz des Unternehmensvermögens vor Verlusten und Schäden aller Art
- Überwachung der Beachtung von Gesetzen, internen Richtlinien und Anweisungen
- Prüfung der formellen und materiellen Ordnungsmäßigkeit von Buchführung, Bilanzierung, Berichterstattung und Dokumentation
- Überprüfung des internen Kontrollsystems
- Durchführung von Rentabilitäts- und Wirtschaftlichkeitsprüfungen

2.2 Aufgaben der Innenrevision im Krankenhaus

2.2.1 Vorbemerkung

Abgeleitet von der allgemeinen Funktion werden im folgenden Aufgabengebiete der Innenrevision im Krankenhaus angesprochen. Dabei soll es nicht Ziel dieses Beitrags sein, die Inhalte der einzelnen Prüfungsgebiete im Detail aufzuzeigen. Die Prüfungsbereiche werden nur allgemein beleuchtet; einzelne Fragestellungen zu den Prüfungsgebieten können jedoch aus der angegebenen Literatur ersehen werden.

2.2.2 Prüfung des Verwaltungsbereichs

In der Regel denkt man im Zusammenhang mit der Innenrevision zunächst an die Aufgaben im kaufmännischen Bereich. Im Krankenhaus ergeben sich für die Innenrevision hier die Schwerpunkte

- Patientenverwaltung,
- Finanz- und Rechnungswesen,
- Materialwirtschaft,
- Personalwesen,
- sonstige Erlösbereiche und
- EDV-Anwendung.

[2] vgl. Joachim S. Tanski: Interne Revision im Krankenhaus, Stuttgart, Berlin, Köln 2001, S. 10

Prüfungsinhalte im Bereich der **Patientenverwaltung** sind insbesondere die korrekte und zeitnahe Erfassung der im Zusammenhang mit der Patientenbehandlung anfallenden Daten, um eine vollständige Abrechnung der erbrachten Leistungen zu gewährleisten. Dies betrifft nicht nur die allgemeinen Krankenhausleistungen, sondern auch die Wahlleistungen und ambulanten Leistungen des Krankenhauses.

Das **Finanz- und Rechnungswesen** bildet einen Schwerpunkt der externen Prüfung (Jahresabschlußprüfung oder örtliche und überörtliche Rechnungsprüfung). Die Innenrevision wird besonders in diesem Bereich ihre Prüfungshandlungen auf die Prüfungstätigkeit der externen Prüfung abstellen. Ansatzpunkte für die Innenrevision ergeben sich im Hinblick auf den wirtschaftlichen Einsatz der Vermögensgegenstände und Schulden. In diesem Zusammenhang stehen z.B. Fragen der wirtschaftlichen Beschaffung des Anlagevermögens sowie der ordnungsgemäßen Anforderung und Verwendung von Fördermitteln im Mittelpunkt. Daneben ist insbesondere das interne Rechnungswesen (Kosten- und Leistungsrechnung) ein Gegenstand der Prüfungstätigkeit der Innenrevision.

Im Bereich der **Materialwirtschaft** sind der Einkaufsvorgang, die Lagerwirtschaft und die Zahlungsabwicklung mit den Lieferanten Prüfungsschwerpunkte der Innenrevision.

Beim **Personalwesen** sind neben der Überprüfung der tarif- bzw. vertragsgerechten Vergütung der wirtschaftliche Personaleinsatz und die Personalentwicklung Prüfungsgegenstand der Innenrevision.

Weiterhin sind die **sonstigen Erlösbereiche** ein umfangreiches Aufgabengebiet der Innenrevision. Zu überprüfen sind hierbei insbesondere die Erstattungen aus dem Nebentätigkeitsbereich der Ärzte, die Leistungsbeziehungen der Nebenbetriebe des Krankenhauses (z.B. Essenslieferungen) oder der Vollzug von eventuellen Kooperationsvereinbarungen.[3]

Ein an Bedeutung zunehmendes Prüfungsgebiet ist die Informationstechnologie im Krankenhaus. Die Schlüsselstellung der EDV ergibt sich daraus, daß das gesamte Leistungsgeschehen des Krankenhauses unter Einsatz der Informationstechnologie dokumentiert wird und die Betriebsabläufe mehr und mehr von einer funktionierenden EDV-Technik abhängig werden. Ebenso wie in anderen Unternehmensbereichen können damit auch im Krankenhaus Fehlfunktionen in der Informationstechnik zu einer Gefahr für den Bestand des Unternehmens werden.

Die Prüfung bezieht sich auf die Sicherheit der EDV-Hardware, die Organisation des EDV-Einsatzes und die Prüfung der Software. Hinweise zu einzelnen Prüfungsinhalten und -fragestellungen finden sich z.B. im Prüfungsstandard 330 des Instituts der Wirtschaftsprüfer[4].

2.2.3 Prüfung des internen Kontrollsystems

Auf das interne Kontrollsystem als Prüfungsobjekt der Innenrevision im kommunalen Krankenhaus soll an dieser Stelle gesondert eingegangen werden. Das interne Kontrollsystem umfaßt sämtliche aufeinander abgestimmte Methoden und Maßnahmen in einem Unternehmen, die

---

[3] zu einzelnen Fragestellungen der Innenrevision im Zusammenhang mit den genannten Prüfungsgebieten vgl. Joachim S. Tanski, a.a.O., S. 49 ff.

[4] vgl. Prüfungsstandard 330: Abschlußprüfung bei Einsatz von Informationstechnologie, in: IDW Prüfungsstandards (IDW PS), IDW Stellungnahmen zur Rechnungslegung (IDW RS), IDW Standards (IDW S), Düsseldorf 2002

dazu dienen, sein Vermögen zu sichern, die Genauigkeit und Zuverlässigkeit der Abrechnungsdaten zu gewährleisten und die Einhaltung der vorgeschriebenen Geschäftspolitik zu unterstützen.[5] Zum internen Kontrollsystem gehören unter anderem Organisationspläne, Geschäftsverteilungspläne, Arbeitsanweisungen, Stellenbeschreibungen, Arbeitsablaufpläne, Formularwesen. Die Innenrevision selbst kann als Teil des internen Kontrollsystems gesehen werden.

Für die kommunalen Einrichtungen in Bayern sind umfangreiche Regelungen zur Organisation des Finanz- und Kassenwesens durch die Kommunalhaushaltsverordnung (KommHV) vorgegeben. Insoweit mußten die kommunalen Krankenhäuser für diesen Bereich keine eigenen Grundlagen erarbeiten. Kommunale Krankenhäuser mit eigener Rechtspersönlichkeit sind jedoch vom Geltungsbereich der KommHV ausgenommen. Nach unseren Beobachtungen sind für diese Krankenhäuser vielfach noch nicht in ausreichendem Umfang Ersatzregelungen für die Vorschriften der KommHV getroffen worden. Allgemein sind auch Arbeitsanweisungen, Stellenbeschreibungen und Arbeitsablaufpläne in den kommunalen Krankenhäusern noch nicht umfänglich erarbeitet.

Die Untersuchung des internen Kontrollsystems ist eine wesentliche Aufgabe der Innenrevision. Im Rahmen dieser Tätigkeit sind der Aufbau und die Funktion des internen Kontrollsystems zu prüfen. Die Untersuchung der Vollständigkeit erforderlicher Regelungen gehört zur Aufbauprüfung. Die Funktionsfähigkeit des internen Kontrollsystems läßt sich durch den Nachvollzug von Verarbeitungs- und Kontrollvorgängen, Befragung und Beobachtung sowie durch Einzelprüfung von Geschäftsvorfällen feststellen. Nähere Hinweise zur Prüfung des internen Kontrollsystems können z.B. dem Prüfungsstandard 260 des Instituts der Wirtschaftsprüfer[6] entnommen werden.

2.2.4 Prüfung sonstiger Krankenhausbereiche

Um ihrer grundsätzlichen Aufgabe gerecht zu werden, das Unternehmensvermögen vor Verlusten und Schäden aller Art zu schützen, kann sich die Tätigkeit der Innenrevision nicht allein auf den Verwaltungsbereich beschränken, sondern muß alle mit der Leistungserstellung im Krankenhaus befaßten Bereiche einbeziehen. Im Rahmen der Risikovorsorge obliegt der Innenrevision die Früherkennung von Gefahrenzuständen in allen Bereichen des Krankenhauses durch systematische Fehlersuche.

Als besonders risikobehaftet im Krankenhaus sind die ärztliche und pflegerische Tätigkeit, aber auch die betriebs- und medizintechnische Infrastruktur zu sehen. Zum Schutz vor Haftungsrisiken gehören zu den Aufgabenbereichen der Innenrevision z.B.

- Medizin-Geräteverordnung,
- Patientenaufklärung,
- Dokumentation und Archivierung,
- Krankenhaushygiene,
- Strahlenschutz,
- Datenschutz und
- Unfallverhütung.

---

[5] vgl. Rolf Hofmann, a.a.O., S. 147

[6] in: IDW Prüfungsstandards (IDW PS), IDW Stellungnahmen zur Rechnungslegung (IDW RS), IDW Standards (IDW S), a.a.O.

Zuweilen wird die Meinung vertreten, die zumeist kaufmännisch ausgebildete Innenrevision sei mit einer Revisionstätigkeit auf diesen Gebieten überfordert. Im Rahmen der Risikovorsorge untersucht die Innenrevision aber insbesondere, ob für die genannten Risikofelder geeignete Vorschriften und Dienstanweisungen im Krankenhaus vorliegen und inwieweit deren Einhaltung gewährleistet ist. Diese Aufgabenstellung setzt insoweit keine fachspezifische Ausbildung z.B. in der Medizin oder der Technik voraus.

Wertvolle Ansatzpunkte für die Tätigkeit der Innenrevision auf diesem Gebiet ergeben sich aus Risikoanalysen, die von Versicherungsgesellschaften bzw. deren Beauftragten für Krankenhäuser erstellt werden.[7]

3. Wahrnehmung der Revisionsaufgaben im kommunalen Krankenhaus

3.1 Krankenhausinterne Wahrnehmung von Revisionsaufgaben

Wenn auch - wie bereits einleitend erwähnt - in vielen kommunalen Krankenhäusern keine Innenrevision als eigenständige Organisationseinheit vorhanden ist, kann man daraus nicht schließen, daß Revisionsaufgaben in den Krankenhäusern überhaupt nicht wahrgenommen werden.

So findet eine Stichprobenprüfung durch die Geschäftsleitung mehr oder weniger in jedem Krankenhaus statt. Der Umfang der Überwachung durch die Geschäftsleitung wird von der Größe des Krankenhauses abhängen, wobei in kleineren Krankenhäusern die Geschäftsleitung naturgemäß eine größere Kontrollfunktion wahrnehmen kann.

Weiterhin nehmen gesondert beauftragte Mitarbeiter, die in jedem Krankenhaus benannt sind, Revisionsaufgaben wahr. Zu denken ist dabei z.B. an die Tätigkeit von Datenschutz-, Sicherheits-, Strahlenschutz-, Hygiene- und Qualitätsbeauftragten. Im Rahmen ihrer Funktion überwachen diese Mitarbeiter die Beachtung von Gesetzen und Richtlinien und tragen zum Schutz des Unternehmensvermögens vor Verlusten und Schäden bei; sie erfüllen damit grundsätzliche Aufgaben der Innenrevision.

Im Verwaltungsbereich werden vielfach Revisionsaufgaben durch das Controlling wahrgenommen, beispielsweise dadurch, daß der Controller die ihm gelieferten Daten auf ihre Richtigkeit hin überprüft. Zum Teil werden dem Controlling auch Rentabilitäts- und Wirtschaftlichkeitsprüfungen übertragen, ein Aufgabenbereich, der grundsätzlich auch der Innenrevision obliegt.

An dieser Stelle sei aber darauf hingewiesen, daß sich das Controlling und die Kontrolle durch die Innenrevision deutlich voneinander unterscheiden. Das Controlling übt eine Lenkungsfunktion aus, die auf die Zukunft ausgerichtet ist. Die Prüfung durch die Innenrevision hat die Recht- und Ordnungsmäßigkeit als Schwerpunkt und ist eher vergangenheitsorientiert. Die Aufgabenabgrenzung zwischen Innenrevision und Controlling läßt sich stark vereinfacht so erklären, daß die Innenrevision die Richtigkeit des Zahlenwerks überprüft, das dem Controlling als Grundlage dient.

---

[7] Weitere Hinweise zur Prüfung der sonstigen Krankenhausbereiche können dem Buch von Joachim S. Tanski, a.a.O., S. 96 ff., entnommen werden.

3.2 Prüfungen durch externe Einrichtungen

Kommunale Krankenhäuser mit eigener Rechtspersönlichkeit unterliegen der jährlichen Abschlußprüfung nach § 316 HGB oder Art. 91 GO. Im Rahmen dieser Prüfung hat der Abschlußprüfer die Einhaltung der für die Rechnungslegung geltenden gesetzlichen Vorschriften zu prüfen und zu untersuchen, ob der Jahresabschluß unter Beachtung der Grundsätze ordnungsmäßiger Buchführung ein den tatsächlichen Verhältnissen entsprechendes Bild der Vermögens-, Finanz- und Ertragslage vermittelt. Die Prüfung der Einhaltung anderer gesetzlicher Vorschriften gehört nur insoweit zu den Aufgaben der Abschlußprüfung, als sich aus diesen anderen Vorschriften üblicherweise Rückwirkungen auf den Jahresabschluß oder den Lagebericht ergeben oder als die Nichtbeachtung solcher Gesetze erfahrungsgemäß Risiken zur Folge haben kann, denen im Lagebericht Rechnung zu tragen ist.[8]

Durch die Kommunalgesetze (Art. 94 Abs. 1 Satz 1 Nr. 2 GO in Verbindung mit § 53 des Haushaltsgrundsätzegesetzes für die GmbH und Art. 107 Abs. 3 Satz 2 GO für das Kommunalunternehmen) wird der in § 317 HGB geregelte Prüfungsumfang zwar erweitert um die Prüfung

– der Ordnungsmäßigkeit der Geschäftsführung,

– der Entwicklung der Vermögens- und Ertragslage sowie der Liquidität und Rentabilität,

– der verlustbringenden Geschäfte und der Ursachen der Verluste, wenn diese Geschäfte und die Ursachen für die Vermögens- und Ertragslage von Bedeutung waren,

– der Ursachen eines in der Gewinn- und Verlustrechnung ausgewiesenen Jahresfehlbetrags.

Der Schwerpunkt der Jahresabschlußprüfung liegt allerdings in einer umfassenden Prüfung der Rechnungslegung. Aufgrund ihrer Ausrichtung wird sie damit insbesondere die außerhalb der Verwaltung liegenden Prüfungsthemen der Innenrevision nur kurz beleuchten können.

Soweit die kommunalen Krankenhäuser der örtlichen und überörtlichen Rechnungsprüfung unterliegen, stellt sich die Situation etwas anders dar. Die Rechnungsprüfung erstreckt sich nach Art. 106 GO insbesondere darauf, ob

– die Haushaltssatzung und der Haushaltsplan (bei Krankenhäusern der Wirtschaftsplan) eingehalten worden sind,

– die Einnahmen und Ausgaben begründet und belegt sowie die Jahresrechnung und die Vermögensnachweise (bei Krankenhäusern der Jahresabschluß) ordnungsgemäß aufgestellt sind,

– wirtschaftlich und sparsam verfahren wird,

– die Aufgaben mit geringerem Personal- oder Sachaufwand oder auf andere Weise wirksamer erfüllt werden können.

[8] vgl. IDW Prüfungsstandards (IDW PS), IDW Stellungnahmen zur Rechnungslegung (IDW RS), IDW Standards (IDW S), a.a.O.

Damit wird deutlich, daß die Rechnungsprüfung über die Prüfung der Rechnungslegung hinausgeht und von ihrer Ausrichtung her mehr Überschneidungen mit den Aufgaben der Innenrevision aufweist als die Jahresabschlußprüfung nach § 316 HGB. Jedoch hat auch die Rechnungsprüfung ihren Schwerpunkt im Verwaltungsbereich, so daß sich insbesondere im Hinblick auf die darüber hinaus genannten Prüfungsthemen auch für die Krankenhäuser, die der Rechnungsprüfung unterliegen, die Frage stellt, ob eine Innenrevision erforderlich ist.

Neben der jährlichen Abschlußprüfung bzw. der Rechnungs- und Kassenprüfung finden noch sonstige Prüfungen durch externe Institutionen in den kommunalen Krankenhäusern statt, die sich mit dem Aufgabengebiet der Innenrevision überschneiden. Zu denken ist dabei z.B. an Prüfungen durch die Finanzbehörden und die Sozialversicherungsträger. Diese Prüfungen beziehen sich aber zumeist auf ein relativ enges Prüfungsgebiet.

Revisionsaufgaben werden auch in den Fällen wahrgenommen, in denen externe Gutachter fallweise für die Untersuchung von bestimmten Einzelbereichen herangezogen werden. In der Regel werden sich diese Begutachtungen jedoch ebenfalls auf ein enges Untersuchungsgebiet beziehen.

3.3 Folgerungen für das Erfordernis einer Innenrevision

Wie dargestellt, führen verschiedene interne und externe Stellen Prüfungen in den kommunalen Krankenhäusern durch; Kontrollfunktionen, die dem Aufgabenbereich der Innenrevision zuzuordnen sind, werden damit auch wahrgenommen, wenn keine Innenrevision als eigene Funktionseinheit eingerichtet ist.

Es bleibt aber festzustellen, daß, wenn eine eigene Innenrevision fehlt, die Revision durch die internen Stellen in der Regel nur fallweise durchgeführt wird und der Prüfungstätigkeit keine umfassende Planung vorausgeht. Die Revisionsaufgaben sind außerdem zumeist auf mehrere Stellen verteilt, was letztlich die Zuordnung der Verantwortung für eine umfassende Wahrnehmung der Prüfungsfunktion erschwert. Außerdem ist häufig keine systematische Dokumentation der Prüfungshandlungen über die verschiedenen Bereiche hinweg gegeben.

Die externe Prüfung hat neben der überwiegenden Konzentration auf den Verwaltungsbereich aus der Sicht der Krankenhausführung den Nachteil, daß sie keinen Einfluß auf die Prüfungstätigkeit nehmen kann. Wenn die Geschäftsführung ihre Verpflichtung, die Ordnungsmäßigkeit des gesamten Geschäftsablaufs zu überwachen, anderen Personen überträgt, muß sie auch Einfluß auf die Prüfungsinhalte nehmen können. Dieser Einfluß entfällt aber bei einer externen Prüfung. Externe Prüfungen können deshalb die Innenrevision in der Funktion als Überwachungsbeauftragte der Geschäftsführung nicht ersetzen. Hinzu kommt die zeitliche Dimension der Prüfungstätigkeit. In der Regel kann die Innenrevision leichter eine zeitnahe Prüfung gewährleisten als eine externe Prüfung.

Eine systematisch organisierte Prüfungstätigkeit als Funktion der Geschäftsführung kann damit letztlich nur durch eine Innenrevision gewährleistet werden.

4. Organisation der Innenrevision im Krankenhaus

4.1 Vorbemerkung

Obwohl die Funktion der Innenrevision grundsätzlich als sinnvoll anerkannt wird, stößt deren Einrichtung doch auf Vorbehalte. Diese leiten sich zum einen daraus ab, daß eine Innenrevision als eigenständige Stelle erst ab einer gewissen Krankenhausgröße ausgelastet werden kann. Viele kommunale Krankenhäuser in Bayern erreichen von ihrer Bettenzahl her nicht die Größenordnung, ab der die Vorhaltung von eigenem Personal für die Innenrevision gerechtfertigt ist.

Bei Krankenhäusern, die groß genug wären, eigene Mitarbeiter für die Innenrevision sinnvoll auszulasten, wird die Schaffung einer neuen Stelle unter den derzeitigen gesundheitspolitischen Vorgaben für die Krankenhäuser aus finanziellen Gründen als problematisch gesehen. Zwar läßt sich argumentieren, daß sich die Innenrevision bei entsprechend erfolgreicher Tätigkeit durch die Abwendung von Schaden und die Verbesserung der Wirtschaftlichkeit zumindest selbst finanzieren müßte. Es fehlt jedoch grundsätzlich die Möglichkeit, einen unmittelbaren Zusammenhang zwischen den Kosten einer Innenrevision und den durch sie erzielbaren Einsparungen herzustellen und damit eine rechnerisch nachvollziehbare Begründung für die Beschäftigung zusätzlichen Personals zu liefern.

Im Hinblick auf die vielfältigen Überwachungsaufgaben, die nur zum Teil von internen und externen Einrichtungen erfüllt werden, kann aber trotzdem nicht auf die Funktion einer Innenrevision verzichtet werden. Es soll deshalb im folgenden insbesondere auch auf die Frage eingegangen werden, wie die Funktion einer Innenrevision wahrgenommen werden kann, auch wenn es nicht möglich ist, eine eigenständige Stelle hierfür einzurichten.

4.2 Organisatorische Eingliederung der Innenrevision

Gemäß ihrer Funktion als prozeßunabhängige Überwachungseinheit muß die Innenrevision als Stabsstelle eingerichtet oder einer Stabsstelle zugeordnet werden. Eine Übertragung von Aufgaben der Innenrevision auf eine Stelle, die selbst in der Linienfunktion tätig ist, widerspricht der anzustrebenden unabhängigen Kontrolltätigkeit.

Sofern eine eigene Stelle für die Innenrevision vorgehalten werden kann, ist die organisatorische Eingliederung als Stabsstelle problemlos. Aussagen, ab welcher Krankenhausgröße eine eigene Stelle für die Innenrevision zu empfehlen ist, lassen sich nicht allgemein treffen. Neben der Bettenzahl des Krankenhauses hängt der Personalbedarf für die Innenrevision von der Komplexität der Aufgabenstellung ab. Außerdem ist zu berücksichtigen, in welchem Umfang andere interne oder externe Stellen Revisionsaufgaben wahrnehmen. Die Voraussetzungen werden damit für jedes Krankenhaus unterschiedlich sein. Grundsätzlich wird die Schaffung einer eigenen Stelle für die Innenrevision aber eine Krankenhausgröße von mindestens 400 bis 500 Betten erfordern.

Sofern eine eigene Stelle für die Innenrevision nicht eingerichtet werden kann, bietet sich die Zuordnung der Funktion der Innenrevision zu einer anderen Stabsstelle an. Zu denken ist hier insbesondere z.B. an das Controlling oder die Qualitätskontrolle. Allerdings besteht bei einer

derartigen Lösung immer die Gefahr, daß die Aufgaben der Innenrevision gegenüber dem Tagesgeschäft in den Hintergrund treten und nicht im erforderlichen Umfang wahrgenommen werden.

Eine weitere Möglichkeit besteht in der Zusammenarbeit mehrerer Krankenhäuser. Zumindest bei Krankenhäusern des gleichen Trägers dürfte die Einrichtung einer übergeordneten Innenrevision für mehrere Krankenhäuser keine organisatorischen Probleme bereiten. Aber auch für Krankenhäuser verschiedener Träger bietet sich eine Kooperation auf dem Gebiet einer gemeinsamen Innenrevision an. Voraussetzung hierfür ist jedoch, daß jedes Krankenhaus entsprechenden Einfluß auf die Tätigkeit der gemeinsamen Innenrevision ausüben kann, damit die Funktion als Dienstleister für die jeweilige Krankenhausführung gewährleistet ist.

4.3 Mindestanforderungen an eine Innenrevision

Unabhängig davon, ob für die Innenrevision eine eigene Stelle geschaffen wird oder ob die Aufgaben der Innenrevision einer anderen Stelle als zusätzliche Funktion übertragen werden, sollten aus unserer Sicht zumindest folgende Anforderungen erfüllt werden, um die Funktion der Innenrevision zu gewährleisten:

– Zunächst sollte eine **Dienstanweisung** für die Innenrevision erarbeitet werden. Darin wären vor allem Aufgaben, Stellung sowie Richtlinien über die Prüfungsdurchführung und Berichterstattung der Innenrevision festzulegen. Beispiele für derartige grundlegende Bestimmungen über die Innenrevision sind im Internet zu finden.[9]

– Weiterhin wäre ein jährlicher **Prüfungsplan** für die Innenrevision zu erstellen. Eine entsprechende Aufgabenplanung ist vor allem auch dann wichtig, wenn die Innenrevision nicht als eigenständige Stelle eingerichtet ist, sondern als zusätzliche Funktion wahrgenommen wird. Durch die Einhaltung des Prüfungsplans wäre sicherzustellen, daß die Aufgaben der Innenrevision neben den sonstigen Aufgaben nicht vernachlässigt werden.

– Über die Prüfungshandlungen und Prüfungsergebnisse der Innenrevision wäre eine **schriftliche Dokumentation** zu erstellen. Eine Berichterstattung ist nicht nur für die Geschäftsführung, für die die Innenrevision die Aufgabe der Überwachung übernimmt, wichtig; sie dient auch als Tätigkeitsnachweis zur Abstimmung der Prüfungshandlungen mit externen Prüfungen (z.B. Abschlußprüfung).

– Außerdem sollte die **Umsetzung der Prüfungsfeststellungen und -empfehlungen** nachgewiesen werden. Eine entsprechende Dokumentation erlaubt internen und externen Stellen eine Beurteilung der Wirksamkeit der Überwachungsfunktion der Innenrevision und trägt damit ebenfalls dazu bei, die Prüfungshandlungen anderer Stellen mit denen der Innenrevision abzustimmen.

[9] z.B. unter: http.//www.verwaltung.uni-halle.de/KANZLER/ZGST/ABL/1994/94'3'06.htm

5. Zusammenfassung

Eine Innenrevision ist bisher nur in wenigen kommunalen Krankenhäusern in Bayern eingerichtet. Mit der zunehmenden Umwandlung der Krankenhäuser in Rechtsformen mit eigener Rechtspersönlichkeit sowie der steigenden Komplexität des Krankenhausbetriebs wird jedoch das Erfordernis dringender, eine unternehmenseigene, prozeßunabhängige Überwachungsfunktion zu schaffen, die die Geschäftsführung bei der Erfüllung der Pflicht zur Kontrolle des Betriebsgeschehens unterstützt. Die Überwachungsfunktion schließt dabei nicht nur die Arbeitsabläufe des Verwaltungsbereichs, sondern auch des medizinischen und technischen Leistungsbereichs des Krankenhauses ein.

Obwohl verschiedene interne und externe Stellen in den kommunalen Krankenhäusern Prüfungen durchführen, die sich mit den Aufgaben der Innenrevision überschneiden, kann auf Dauer nicht auf die Einrichtung einer krankenhausinternen Kontrollinstanz verzichtet werden. Viele kommunale Krankenhäuser in Bayern weisen aber nicht die Mindestbetriebsgröße auf, die eine gesonderte Vorhaltung von Personal für die Innenrevision rechtfertigen würde. Soweit alternative Lösungen, wie z.B. die Kooperation mit anderen Krankenhäusern, nicht zu verwirklichen sind, muß das Aufgabengebiet der Innenrevision dann von einer anderen Stelle mit wahrgenommen werden. Um die Funktion der Innenrevision auch unter diesen organisatorischen Voraussetzungen zu gewährleisten, müssen folgende Mindestanforderungen erfüllt werden:

– Erlaß einer Dienstanweisung für die Innenrevision

– Erstellung eines Prüfungsplans

– schriftliche Dokumentation der Prüfungsergebnisse

– Berichterstattung über die Umsetzung der Prüfungshinweise

E. Veröffentlichungen

1. BKPV-Mitteilungen

RdNr.	Titel
1	Cross-Border-Leasing Struktur und Risiken eines modernen Finanzierungsinstruments
2	Geldanlagen von Gemeinden bei anderen Gemeinden
3	Privatwirtschaftliche Betätigung von Kommunen als unlauterer Wettbewerb im Sinn des UWG?
4	Zulässigkeit der Koppelung des Verkaufs gemeindlicher Grundstücke mit dem Bezug von Fernwärme
5	Änderung der Eigenbetriebsverordnung und der Verordnung über Kommunalunternehmen durch Verordnung vom 12.10.2001
6	Eintragung des gesetzlichen Vertreters eines Eigenbetriebs in das Handelsregister
7	Gesetz zur Eindämmung illegaler Betätigung im Baugewerbe - Auswirkungen auf kommunale Gebietskörperschaften und ihre Betriebe
8	Ausschreibungsfreie In-House-Geschäfte
9	Neuregelung des Schadensersatzrechts
10	Änderung der Kommunalhaushaltsverordnung und der Verwaltungsvorschriften
11	Änderung der Kommunalhaushaltsverordnung und der Verwaltungsvorschriften: Sonderrücklagen
12	Änderung der Kommunalhaushaltsverordnung und der Verwaltungsvorschriften: Unterscheidung zwischen rentierlicher und nichtrentierlicher Verschuldung
13	Änderung der Kommunalhaushaltsverordnung und der Verwaltungsvorschriften: Anhebung der Wertgrenze für Bestandsverzeichnisse
14	Untersuchungen der Wirtschaftlichkeit der Müllabfuhr in kreisfreien Städten
15	Wirtschaftlichkeit und Sicherheit in der Informationstechnik
16	Kartellrechtliche Zulässigkeit kommunaler Sammelbestellungen
Bau 1	Die Neuregelungen der VOB 2000 und des Vergabehandbuchs Hochbau, Ausgabe Bayern, zu Skonto-, Nachlaß- und Nebenangeboten
Bau 2	Auswirkung der Euro-Einführung auf die Lohngleitklausel
Bau 3	Ausgleich für Mengenänderungen nach § 2 Nr. 3 VOB/B
Bau 4	Anträge auf Zuwendungen nach RZWas 2000 Vergütung des Ingenieurs für die Vorbereitung der Anträge auf Finanzierung
Bau 5	Unwirksame Bürgschaften „auf erstes Anfordern“ können für bestehende Verträge nun doch als einfache Bürgschaften aufrechterhalten werden

RdNr.	Titel
Bau 6	Änderungen der VOB/B durch die Fassung 2002
Bau 7	Ausschluß neuer Unternehmen vom Vergabeverfahren wegen fehlender Sachkunde
Bau 8	Schuldrechtsmodernisierungsgesetz und VOB/B 2002
Bau 9	Umgang mit Angeboten, die Spekulationspreise enthalten

2. Beratungsdienst für kommunale Unternehmen Nr. 1/2002