TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Informatik Institut für Systemarchitektur
Professur für Datenschutz und Datensicherheit

Technische Universität Dresden, 01062 Dresden

Dr.-Ing.
Stefan Köpsell

Telefon +49 351 463-[redacted]
Telefax +49 351 463-38255
E-Mail [redacted]

Sekr
E-Mail

Vorab per Fax
Landgericht Berlin
Littenstr. 12-17
10179 Berlin

02. Mai 2012

AZ

Dresden, 30. April 2012

Erläuterungen zum Sachverständigengutachten zu 57 S 87/08

Sehr geehrte Damen und Herren,

haben Sie Dank für Ihren Auftrag vom 4. Januar 2012 der es mir erlaubt, meine im Gutachten vom 29. Juli getroffenen Aussagen bezüglich der Anmerkungen der beiden Partien zu erläutern und zu ergänzen.

Anbei finden Sie eine Vorabversion der gewünschten Erläuterungen und Ergänzungen – die allein gültige finale Version erhalten Sie in wenigen Tagen in schriftlicher Form per Post (wobei eventuell im Rahmen der abschließende Qualitätskontrolle geringfüge Änderungen zur vorliegenden Fassung möglich sind).
Ich habe mich bemüht, zu jeder aufgeworfenen Anmerkung möglichst umfangreich und verständlich zu antworten. Auf der anderen Seite ist es zweifelsfrei so, daß einige der aufgeworfene Thematiken sehr komplex sind und sich nicht in wenigen Seiten unter Berücksichtigung aller Aspekte umfangreich darstellen lassen. Nicht umsonst existiert im Bereich IT-Sicherheit und insbesondere Netzsicherheit eine umfangreiche Menge an Literatur. Sollten also trotz meiner weiteren Erläuterungen nach wie vor Fragen bestehen, so stehe ich für inhaltliche Rückfragen gerne zur Verfügung.

Mit freundlichen Grüßen,

Postadresse (Briefe)
TU Dresden, Fakultät Informatik
Institut für Systemarchitektur
01062 Dresden

Postadresse (Pakete u.ä.)
TU Dresden, Fakultät Informatik
Institut für Systemarchitektur
Helmholtzstraße 10
01069 Dresden

Besucheradresse
Sekretariat
01187 Dresden
Nöthnitzer Straße 46
Zi. 3067

Internet
https://dud.inf.tu-dresden.de/

DRESDEN concept

Allgemeine Anmerkungen

Aus den zum Gutachten getroffen Anmerkungen komme ich zu dem Schluß, daß möglicherweise Gründe für unterschiedliche Auffassungen bezüglich der notwendigen Maßnahmen für den Betrieb eines sicheren IT-System einige grundlegende Diskrepanzen in der Terminologieauslegung und –interpretation sind.
Insofern möchte ich zunächst noch einmal meine Interpretation und Auffassung bezüglich einiger zentraler Begriffe und Verfahren darlegen.
Hier ist sicher zu aller Erst der Begriff „sicherer Betrieb von IT-Systemen" zu nennen. Für mich bedeutet dies, daß ein IT-System so konzipiert, entwickelt, implementiert und betrieben wird, daß das System (quasi „proaktiv") versucht, das Eintreten eines Schadens zu verhindern. Ich bezeichne insbesondere ein IT-System **nicht** als sicher, welches lediglich reaktiv versucht, *nach* dem Eintreten eines Schadens den Schadensverursacher zu ermitteln, um im Zuge des Schadensersatzes den tatsächlich aufgetretenen Gesamtschaden zu minimieren.
Vereinfacht gesagt, muß ein sicheres System also so gebaut sein und betrieben werden, daß erfolgreiche Angriffe weitestgehend ausgeschlossen sind. Ein 100%iger Schutz ist natürlich – egal welches Verfahren angewendet wird – nie möglich.

Nachfolgend wird zunächst auf die Anmerkungen der TCI Rechtsanwälte Berlin (Band 3, Bl. 124 ff) eingegangen. Anschließend erfolgt eine Kommentierung der Anmerkungen des Rechtsanwalts Meinhard Starostik (Band 3 Blatt 116ff). Verkürzend wird dabei die Formulierung „die Beklagte behauptet" bzw. „der Kläger behauptet" verwendet, wenn die entsprechenden Anmerkungen der erwähnten Anwälte referenziert werden.
Abschließend erfolgt eine Beantwortung der im Beschluß vom 20. Mai 2010 in Ziffer 1 genannten Hauptfrage.

Kommentierung der Anmerkungen der TCI Rechtsanwälte Berlin

Erläuterungen zu den Anmerkungen zur Beweisfrage 3

In dem Schreiben der TCI Rechtsanwälte Berlin (Band 3, Bl. 124 ff) wird bezüglich der Beweisfrage 3 festgestellt, daß die Frage „schlicht nicht beantwortet" wurde. Dem ist im Wesentlichen (abzüglich der im Gutachten getroffenen allgemeinen Aussagen) zuzustimmen — insbesondere falls die Erwartungshaltung war, daß im Ergebnis des Gutachtens eine konkrete Zahl im Sinne eines Euro-Betrages genannt werden würde. Richtig ist ferner, daß mir die zur Bestimmung von konkreten Kosten notwendigen Informationen nicht vorliegen und ich auch nicht den Versuch unternommen habe, mir diese Informationen zu beschaffen. Des weiteren wird angemerkt, daß „das Ergebnis aus welchen Gründen auch immer vorgegeben war".
Im folgenden soll daher der Versuch unternommen werden, die Beweggründe für den unterlassen Versuch der konkreten Kostenermittlung darzulegen.

1.) Wie im Gutachten dargelegt (und durch die Anmerkungen auch nicht angezweifelt), läßt sich die Höhe der Kosten nicht pauschal und allgemein bestimmen. Vielmehr ist eine umfangreiche Sicherheitsanalyse notwendige. Diese umfaßt wenigstens eine Ist-Analyse, also die Erfassung sämtlicher eingesetzter IT-Systeme einschließlich der verwendeten Software und der ausgeführten/angebotene Dienste. Ferner ist der Soll-Zustand zu bestimmen. Dies umfaßt wiederum wenigsten die anzubietenden Dienste einschließlich einer vollständigen funktionalen Anforderungsbeschreibung sowie eine Risikoanalyse. Letzteres schließlich umfaßt die Fragestellung, gegen welche Art von Bedrohungen (einschließlich der jeweiligen Schutzziele und Angreifermodelle) man sich schützen will.

2.) Der Klageschrift habe ich entnommen, daß Gegenstand des Gutachtens und insbesondere die Grundlage bezüglich der Beantwortung von Frage 3 die „öffentlich zugänglichen Telemedien der Beklagen im Internet" sind, wobei die Beklagte wiederum die Bundesrepublik Deutschland ist. Es geht also letztlich um (fast) alle öffentlich zugänglichen Telemedien der Bundesrepublik Deutschland im Internet. Allein die vom mir persönlich bisher in Anspruch genommenen öffentlich zugänglichen Telemedien der Bundesrepublik Deutschland haben mich zu dem Schluß kommen lassen, daß es sich hier um ein äußerst umfangreiches Angebot im Sinne der unterschiedlichen Dienste und der damit verbundenen IT-Infrastruktur handelt.

3.) Das zu erstellende Gutachten wurde vom Gericht mit einem Kostenrahmen von ca. 3000 EURO und einer Erstelldauer von ca. 12 Wochen abgeschätzt (siehe Band 3, Bl. 99).

In Kombination von 1.), 2.) und 3.) ergibt sich, daß nach meiner Auffassung eine auch nur irgendwie seriöse Ermittlung der gegebenenfalls anfallenden Kosten im Rahmen des Sachverständigengutachtens nicht – auch nicht ansatzweise – möglich ist. Daher habe ich auch gar nicht erst den ebenfalls Kostenverursachenden Versuch unternommen, dies wider besseren Wissens zu probieren.

Es wird ferner angemerkt, daß der Gutachter „jegliche konkrete Alternative schuldig bleibt, wie die Speicherung von IP-Adressen im Rahmen der erforderlichen Angriffserkennung und –abwehr wirksam ersetzt werden kann". Das keine ganz konkreten und auf die spezifischen IT-Systeme der Beklagten unmittelbar anwendbaren Maßnahmen vorgeschlagen wurden, liegt letztlich an der Tatsache, daß die oben erwähnte, notwendige Ist-/Soll-Analyse aus den ebenfalls dargelegten Gründe unterblieb.
Zusätzlich kann ich auch nicht erkennen, welchen Wert es für ein gerichtliches Sachverständigengutachten (und nicht etwa für ein Lehrbuch über Security Engineering) hätte, wenn das Gutachten mit Aussagen der folgenden Art gefüllt würde:

- Bezüglich des Firewall Systems $\mathcal{F}$ zum Schutze des Dienstes $\mathcal{D}1$ wird empfohlen die INPUT-Regeln:
  - `-p tcp --syn -j LOG`
  - `-p tcp --syn -j REJECT`

zu ersetzen durch:

```
o  -p tcp --syn -j DROP
```

- Bezüglich des beim Dienst $\mathcal{D}2$ verwendeten PHP-Skripts $\mathcal{P}$ wird empfohlen, die einfache Zeichenkettenkonkatenation zur Generierung der SQL-Abfrage aus den Nutzereingaben auf der zugehörigen Web-Seite zu ersetzen durch die Verwendung einer parametrisierten Abfrage, um SQL-Injection-Angriffe zu erschweren.

- Bezüglich des beim Dienstes $\mathcal{D}3$ verwendeten C-Programms $\mathcal{C}$ wird empfohlen die vorhandene statische Reservierung des Speichers für den Puffer `buff` durch eine dynamische Heap-Allokierung zu ersetzen, um Angriffe mittels Pufferüberlauf zu erschweren.

- ...

Im übrigen können die letzten beiden Punkte der Auflistung als Beispiel dafür gelten, wenn im Gutachten zusammenfassend festgestellt wird: „Eine Speicherung von IP-Adressen ist weder zur Angriffserkennung noch zur Angriffsabwehr zwingend erforderlich. Vielmehr existieren eine Reihe von bekannten und in der Praxis angewendeter Verfahren, die ohne Speicherung von IP-Adressen Angriffe erfolgreich abwehren können."
Das diese Verfahren existieren und in jedem Fall notwendig sind, wird im Übrigen auch durch den Vertreter der Beklagten nicht bestritten, denn in seinen Anmerkungen heißt es: „Unstreitig ist dabei, dass die Speicherung von IP-Adressen keinesfalls alleine ausreichend ist, um eine dem Stand der Technik entsprechende Vorsorge zu treffen."
Insofern kann eine der konkret geforderten Ersatzmaßnahmen bezüglich der Speicherung von IP-Adressen schlicht der Verzicht auf die Speicherung sein, da die Speicherung keinen signifikanten Beitrag zur Sicherheit des IT-Systems leistet (siehe erster Anstrich in der obigen Aufzählung). Insofern können hier sogar die Kosten für eine rechtlich und organisatorisch einwandfreie Speicherung gespart werden
So wird beispielsweise am Lehrstuhl des Gutachters seit über 10 Jahren ein Anonymisierungsdienst betrieben, ohne daß IP-Adressen gespeichert werden. Der Dienst wird von geschätzt weltweit mehr als 100 000 Menschen benutzt und ist gleichzeitig permanent Angriffsversuchen aus dem Internet ausgesetzt. Durch sinnvolle Firewallregeln, einem gehärteten Betriebssystem und der möglichst sicherheitsbewußten Programmierung der eingesetzten Softwarekomponenten konnte jedoch ein stabiler Betrieb des Systems erreicht werden bei dem gleichzeitig keine bemerkten Sicherheitsverletzungen auftraten – auch wenn dies natürlich keine Aussagen über den tatsächlichen Sicherheitszustand zuläßt.

In den Anmerkungen zu Beweisfrage 3 wird abschließend ausgeführt, daß es beweiserheblich gewesen wäre, die Aufwendungen für die Überführung der im Gutachten angegeben theoretischen Möglichkeiten zum Schutz eines System ohne Speicherung von IP-Adressen in praxistaugliche und praxiserprobte Produkte anzugeben. Dazu ist wiederum anzumerken, daß zunächst erst einmal zu klären ist, ob die im Gutachten erwähnten eher theoretischen Maßnahmen überhaupt notwendig

sind, um das gewünschte Schutzziel zu erreichen. Wie bereits mehrfach erwähnt bedarf es für den sicheren Betrieb eines IT-System nicht der Speicherung von IP-Adressen. Auch eine ersatzweise durchgeführte Pseudonymisierung, Anonymisierung bzw. Verschlüsselung – also eben die theoretischen Verfahren, um die es hier geht – ist in vielen Fällen nicht notwendig. Insofern sind auch die Kosten, die für eine Überführung der Theorie in die Praxis aufzubringen wären unerheblich – da sie eben nicht anfallen.

Erläuterungen zu den Anmerkungen zur Beweisfrage 2

Nachfolgend Ausführung beziehen sich auf die Anmerkungen der TCI Rechtsanwälte Berlin (Band 3, Bl. 124 ff).
In **Anmerkung 2.1.** heißt es, daß verschwiegen wird, daß auch die Quell-IP-Adresse nicht notwendigerweise die Person des Absenders bestimmt. Zwar wird dies meiner Meinung nach im Gutachten auch nicht behauptet, da hier lediglich allgemein von „Absender" die Rede ist und nicht von irgendwelchen Personen. Nichtsdestotrotz ist die Anmerkung inhaltlich korrekt. Personen sind in der Regel schon deshalb nicht unmittelbar Empfänger oder Absender von IP-Paketen, weil IP-Pakete in der Regel durch technische Systeme übertragen werden.
Im übrigen wird die Behauptung, der Vergleich IP-Adressangaben <-> Postadressangaben (Empfänger, Absender) sei falsch zurückgewiesen. Natürlich sind IP-Adressen und Postadressangaben nicht dasselbe. Aber der Vergleich wurde lediglich bemüht, um klarzustellen, daß insbesondere die Absenderangaben verfälscht werden können. Und dafür hat meiner Meinung nach der Vergleich nach wie vor seine Berechtigung.

In **Anmerkung 2.2** wird behauptet, es wäre falsch, daß der Absender eines IP-Paketes die Absender-IP-Adresse frei festlegen kann. Dem wird widersprochen. Selbstverständlich kann der Absender eines IP-Paketes die Absender-IP-Adresse frei festlegen. Vereinfacht ausgedrückt wird ein IP-Paket mit Hilfe von Software erstellt und dann mittels Hardware verschickt. Der Inhalt des IP-Paketes (inklusive aller Adress- und sonstiger Protokollinformationen) wird also durch die Software bestimmt. Und welche Software zu welchen Zwecken auf der Hardware ausgeführt wird, wird wiederum durch den Nutzer der Hardware bestimmt.
Richtig ist, daß ein Gerät, wenn es mit dem Internet verbunden wird, in der Regel vom Internet-Service-Provider (ISP) eine Empfehlung bezüglich der zu verwendenden, für die Kommunikation relevanten IP-Adressen erhält. Dazu zählt insbesondere die vorgesehene Absender-IP-Adresse, also die IP-Adresse, die das neu verbundene Gerät verwenden sollte. Allerdings gibt es keine technischen Maßnahmen, die dafür sorgen, daß das Gerät der ausgesprochenen Empfehlung auch folgt. Natürlich ist es wie immer im Leben, daß das Nichtbefolgen von Empfehlung Konsequenzen hat.
Konkret ist es hier so, daß bei Verwendung einer anderen als der vorgeschlagenen Absender-IP-Adresse entweder keine oder nur eine eingeschränkte Kommunikation möglich ist.
Dies soll wieder am (offensichtlich ungeliebten) Vergleich mit dem Postverkehr veranschaulicht werden: Enthält ein Brief keine oder falsche Absenderangaben, so

wird der Brief dem Empfänger in der Regel trotzdem korrekt zugestellt. Allerdings ist üblicherweise nur eine unidirektionale Kommunikation möglich, d.h. der Empfänger kann dem Absender nicht antworten bzw. (im Falle einer gefälschten Absenderangabe) die Antwort erreicht einen Dritten.

Es existieren nun aber gerade im Bereich von Angriffen auf IT-Systeme eine ganze Reihe von Angriffsmöglichkeiten (insbesondere im Bereich von Angriffen auf die Verfügbarkeit [Denial of Service][1]) bei denen es überhaupt nicht notwendig ist, eine „Antwort" auf ein versendetes IP-Paket zu erhalten. Ein bekanntes Beispiel für derartige Angriffe ist der Ende der 90er Jahre relevante „Ping of Death"[2]. Dabei war es ausreichend, speziell konstruierte IP-Pakete an das anzugreifende System zu versenden, was (je nach verwendetem Betriebssystem) zu unterschiedlichen ungewünschten Reaktionen führte – in der Regel starteten die angegriffenen Geräte neu bzw. stürzten einfach ab. Hierbei war es insbesondere nicht notwendig, daß das angreifende Gerät selbst IP-Pakete (etwa in Form von Antworten des angegriffenen Systems) erhält. Insofern wurden für die Angriffe oftmals gefälschte Absender-IP-Adressen verwendet. Letzteres wird im übrigen als „Spoofing" bezeichnet und ist ein relevantes Problem bezüglich der Entwicklung sicherer IT-Systeme.

In Anmerkung 2.2 wird weiter ausgeführt, daß dann zunächst nur der Absender die Zuordnung Absender-IP-Adresse <-> Absender kennt. Dies ist mit der Einschränkung korrekt, daß auch der Internet-Service-Provider (ISP) in der Regel die Zuordnung kennt bzw. herstellen kann. Vereinfacht ausgedrückt liegt dies daran, daß der ISP „sieht" auf welcher Leitung/Telekommunikationsverbindung er welches IP-Paket empfängt. Da er nun in der Regel die Leitung/Telekommunikationsverbindung einem Kunden zuordnen kann, erfährt er prinzipiell auch davon, wenn ein Kunde Absender-IP-Adressen verwendet, die von der „Empfehlung" des ISP abweichen.

Im Übrigen wird in der Anmerkung über eine datenschutzrechtliche Einordnung diskutiert, die hier nicht kommentiert wird, da eine datenschutzrechtliche Bewertung der Speicherung von IP-Adressen nicht Gegenstand des Gutachtens war und ist. Ferner ist der Gutachter kein Jurist, womit sich jegliche juristische Wertung von vorn herein verbietet.

In Anmerkung 2.2 wird weiter ausgeführt: „Der Sachverständig führt ... aus, dass deshalb nur ‚dumme' Angreifer über die IP-Adresse identifizierbar seien und daher eine Speicherung der IP-Adresse nicht erforderlich sei." Zunächst ist festzustellen, daß ich bei der Aussage bleibe, daß (etwa im Rahmen möglicher Strafverfolgungsmaßnahmen) an Hand der Absender-IP-Adresse tatsächlich nur „dumme" Angreifer ermittelt werden können. Dies ergibt sich aus der im Gutachten geschilderten – und auch nicht bestrittenen – Möglichkeiten die Absender IP-Adresse zu verfälschen bzw. zu verschleiern.

Zu dem zweiten Teilsatz: „und daher eine Speicherung der IP-Adresse nicht erforderlich sei" ist anzumerken, daß im Gutachten steht, daß „die Speicherung von IP-Adressen höchstens für die Identifizierung von ‚dummen' Angreifern nützlich sein kann". Betont werden soll hier, daß im Gutachten keine Aussage darüber gemacht wurde, ob „Dummenfang" ein hinreichender Grund für das Speichern von IP-Adressen

---

[1] Nachfolgend wird nicht zwischen Denial-of-Service-Angriffen (DoS) und verteilten DoS-Angriffen (dDoS) unterschieden und die allgemeinere Formulierung (DoS) verwendet.

[2] siehe auch: http://insecure.org/sploits/ping-o-death.html

ist. Dies wird wiederum eher als juristische Frage angesehen, die unter Abwägung aller Interessen zu treffen ist und jedenfalls nicht Gegenstand des Gutachtens ist.
Insofern ist eine Kommentierung der weiteren Anmerkungen zu Punkt 2.2 nicht erforderlich. Angemerkt werden soll lediglich, daß ein IT-System, das ein Sicherheitsproblem damit hat, wenn „dumme" Angriffe erfolgen (und daher diesbezüglich eine „Abschreckung" durch IP-Adressen-Speicherung benötigt) generell als unsicher anzusehen und daher schnellstmöglich außer Betrieb zu nehmen ist.

Zu Anmerkung 2.4 ist leider festzustellen, daß die Ausführungen im Gutachten nicht verstanden wurden. Eine Ursache kann sicher darin gesehen werden, daß für das Verständnis des Gutachtens einiges an Fachwissen vorausgesetzt wurde, wobei fehlendes Fachwissen eben zu Unklarheit oder Unverständnis führen kann. Daher soll hier der Versuch unternommen werden die im Gutachten getroffenen Aussagen allgemeinverständlicher darzustellen.
Zunächst zu dem ersten Teil der Anmerkung bezüglich der Speicherung einer konkreten, als ungewollt/verdächtig eingestuften IP-Adresse im Firewallsystem zur Angriffsabwehr. Hier sei als erstes auf die im Gutachten zu findende Fußnote 1 verwiesen, die hier wiederholt wird: „Ist nachfolgend von ‚Speicherung von IP-Adressen' die Rede, so sind zum einen die IP-Adressen des zugreifenden Hostsystems gemeint. Zum anderen wird von einer persistenten und längerfristigen Speicherung ausgegangen. Die für die Gewährleistung der Kommunikation notwendige kurzfristige und flüchtige Speicherung von IP-Adressen etwa im Hauptspeicher von Netzkomponenten ist damit jedenfalls nicht gemeint."
Des weiteren sei die Funktionsweise einer Firewall vereinfachend als Filter beschrieben. Dabei wird ein Vergleich von Merkmalen eintreffender IP-Pakete mit in den Firewall-Regeln gespeicherten Merkmalen getroffen und an Hand der Vergleichsentscheidung dann eine Maßnahme durchgeführt. Üblicherweise handelt es sich bei den Maßnahmen um: Paket passieren lassen bzw. Pakete sperren/verwerfen.
Nehmen wir nun ferner an, daß in der Firewallregel als Merkmal die Absender-IP-Adresse hinterlegt ist. Wie in der Abbildung im Gutachten ebenfalls beispielhaft angenommen soll es sich dabei um die IP-Adresse IP_C handeln. Diese IP-Adresse IP_C ist dann natürlich als Vergleichskriterium in der Firewall gespeichert. Dies ist aber aus logischer Sicht etwas anderes als die Absender-IP-Adresse eines konkret zugreifenden Host-Systems, selbst wenn die Werte inhaltlich übereinstimmen. Daß es sich um zwei unterschiedliche Dinge handelt, sieht man beispielhaft (bezogen auf Abbildung 2 aus dem Gutachten) am besten an IP_A bzw. IP_B von Nutzer A und Nutzer B. Denn diese IP-Adressen werden tatsächlich überhaupt nicht gespeichert.
Ferner ist anzumerken, daß bei der Speicherung von IP_C in der Firewallregel auch keinerlei sonstige Verkehrsdaten bzgl. IP-Adresse C gespeichert werden. In einem üblichen Log-File von Absender-IP-Adressen zugreifender Host-Systeme wird aber genau dies gespeichert, d.h. Informationen darüber wann, wie oft, wie lange etc. der Zugriff erfolgte. Letztlich dürfte es dem Kläger genau um ein Verbot der Speicherung dieser zusätzlichen Informationen gehen – und nicht darum, daß seine IP-Adresse einmalig und ohne jeglichen kontextuellen Bezug zu seinen eigenen Aktivitäten gespeichert ist (wie etwa in einer Firewallregel).

Der nachfolgend Satz in Anmerkung 2.4: „Die Abwehr eines Zugriffs von einer bestimmten IP-Adresse mittels Firewall ist also ohne Speicherung genau dieser IP-Adresse technisch gar nicht möglich." ist schlichtweg falsch und somit zurückzuweisen. Dies ergibt sich schon aus dem trivialen Fakt, daß in Firewallregeln IP-Adressbereiche angegeben werden können, etwa mit Hilfe sogenannter Netzmasken (eng.: netmask). So besagt etwa die nachfolgende Firewallregel (bezüglich des eingehenden Datenverkehrs)

```
-p tcp -s 192.168.178.0/24 -j DROP
```

das alle IP-Pakete mit Absender-IP-Adressen aus dem Bereich 192.168.178.0 bis 192.168.178.255 verworfen werden. Benutzt also ein Angreifer etwa die Absender-IP-Adresse 192.168.178.53, so werden die entsprechenden IP-Pakete verworfen – offensichtlich ohne daß die IP-Adresse 192.168.178.53 irgendwo gespeichert ist.
Anzumerken ist, daß dies natürlich nicht funktioniert, wenn genau eine IP-Adresse gesperrt werden soll. In diesem Fall ist dann in der Tat eben diese eine IP-Adresse in den Firewallregeln zu speichern.
Darüber hinaus soll hier die bereits im Gutachten erwähnte Ersetzung von IP-Adressen nochmals erläutert werden. Dazu ist sich zunächst noch einmal vor Augen zu führen, welche Art der Speicherung von IP-Adressen durch den Kläger beanstandet wird und folglich Gegenstand der Ausführungen im Gutachten ist (siehe die bereits erwähnte Fußnote 1 und die obigen Ausführungen). Es handelt sich hier um die IP-Adresse des zugreifenden Host-System zusammen mit weiteren Kontext-Informationen. Daß die Betrachtung hier nicht losgelöst von den Kontext-Information (also etwa Zeit, Häufigkeit, Dauer der Übertragung etc.) erfolgt, liegt daran, daß eine reine Speicherung der IP-Adresse des zugreifenden Host ohne jegliche weitere Informationen keinen Beitrag für die Sicherheit des IT-Systems liefern kann, da unter anderem die notwendigen Informationen zur Erkennung von Angriffsmustern etwa im Rahmen der Intrusion Detection fehlen. Man wüßte ja noch nicht einmal, wann die IP-Adresse gespeichert wurde und ob somit überhaupt irgendein Bezug zur aktuellen Situation besteht. Insofern ist eine reine Speicherung der IP-Adresse des zugreifenden Host-Systems (ohne jegliche zusätzliche Informationen) jedenfalls nicht zwingend erforderlich für den sicheren Betrieb eines IT-Systems.
Stellt sich somit die Frage, wie es mit der Speicherung der IP-Adresse des zugreifenden Host-System aussieht, wenn diese Speicherung zusammen mit Kontext-Informationen erfolgt und mit Hilfe dieser Kontext-Informationen wiederum eine Anomalieerkennung und somit letztliche eine Angriffserkennung und damit schlußendlich eine Angriffsabwehr durchzuführen.
Hier ist es so – wie im Gutachten bereits dargelegt – daß es regelmäßig nicht auf den konkreten Wert einer IP-Adresse ankommt, sondern lediglich auf Verkettbarkeit von Ereignissen, also beispielsweise das im Rahmen einer Angriffsmustererkennung feststellbar ist, daß zwei IP-Pakete vom selben absendenden Gerät stammen. Und eben dafür reicht es vollkommen aus, wenn vor einer wir auch immer gearteten Speicherung eine eindeutige Ersetzung der IP-Adresse durch einen anderen Wert vorgenommen wird. Dabei ist für die Ersetzung natürlich eine Einwegfunktion zu verwenden, also eine Funktion, die sich leicht berechnen läßt, deren Umkehrfunktion sich aber nicht oder nur mit sehr großem Aufwand berechnen läßt.

Als ein Beispiel für eine praktische Umsetzung wurde im Gutachten hier Verschlüsselung erwähnt. Dabei ist die Verschlüsselung natürlich so zu gestalten, daß die Einwegeigenschaft tatsächlich gegeben ist. Nehmen wir an, es gebe nur die IP-Adressen 1 bis 26, dann ist eine einfache Ersetzung („Verschlüsselung") durch die Buchstaben A bis Z der Form 1 -> A, 2 -> B etc. nicht zielführend, da hier in der Tat aus praktischer Sicht nach wie vor davon gesprochen werden kann, das IP-Adressen gespeichert werden, selbst wenn aus formaler Sicht eben Buchstaben und keine Zahlen gespeichert werden. Verwendet man allerdings für die Abbildung IP-Adresse -> zu speicherndes Kennzeichen ein kryptographisch starkes asymmetrisches Verschlüsselungssystem bei dem zusätzlich der zu Entschlüsselung verwendete geheime Schlüssel nicht erzeugt wird, so erfüllt die Konstruktion die notwendigen Einweganforderung schon wesentlich besser. Zum einen ist eine direkte und unmittelbare Rückgewinnung der IP-Adresse aus einem gespeicherten Kennzeichen nicht möglich, da der dafür notwendige Entschlüsselungsschlüssel nicht existiert (da gar nicht erst erzeugt).
Insofern bleibt als einzige Möglichkeit der Rücküberführung von gespeichertem Kennzeichen in die ursprüngliche IP-Adresse nur das Durchprobieren aller möglichen IP-Adressen. Dazu werden die in Frage kommenden IP-Adressen nacheinander mit dem öffentlichen Schlüssel verschlüsselt und das Ergebnis der Verschlüsselung mit dem gespeicherten Kennzeichen verglichen. Stimmt beides überein, so hat man die ursprüngliche IP-Adresse gefunden. Anzumerken ist, daß hierfür der öffentliche Schlüssel zur Verfügung stehen muß. Dieser braucht für den hier vorliegenden Fall der Anomalieerkennung natürlich nicht wirklich „öffentlich" zu sein. Er braucht noch nicht einmal persistent gespeichert zu werden. Es reicht vollkommen aus, wenn er im flüchtigen Hauptspeicher des Intrusion Detection Systems gespeichert ist. Da ohne den öffentlichen Schlüssel auch kein Durchprobieren möglich ist, wird somit eine Rückführung der gespeicherten Kennzeichen (etwa durch einen außenstehenden Angreifer) weiter erschwert.
Zusätzlich ist zu bedenken, daß das Durchprobieren einiges an Aufwand erfordert. Zwar ist dieser Aufwand unter Berücksichtigung der aktuell kostengünstig zur Verfügung stehenden Rechenleistung bezüglich des Durchsuchens des IPv4-Adressraums durchaus möglich – schlimmstenfalls müßten hier ca. 4 Milliarden Adressen durchprobiert werden.
Glaubt man allerdings der von verschiedenen Experten geäußerten Auffassung, daß die flächendeckende Einführung der neue IP-Generation IPv6 tatsächlich unmittelbar bevorsteht, so ändert sich die Aussage zur Machbarkeit des Durchsuchens.
Prinzipiell existieren ca. 2^{128} IPv6-Adressen. Allerdings ist davon auszugehen, daß ein Angreifer Vorwissen besitzt, welches er nutzen kann, um die Menge in Frage kommender IP-Adressen deutlich zu verkleinern. Er könnte etwa wissen/vermuten, daß ein gespeichertes Kennzeichen aus einer IP-Adresse erzeugt wurde, die wiederum der Deutschen Telekom als ISP gehört. Auf der anderen Seite ist es so, daß gemäß den Regularien des Réseaux IP Européens Network Coordination Centre (RIPE NCC) (http://www.ripe.net/ripe/docs/ripe-545#assignment_size, 5.4.1) einem Endkunden von seinem ISP nicht mehr genau eine IPv6-Adresse vorgeschlagen wird, sondern ein ganzer Adreßbereich, der wenigstens 2^{64} Adressen umfaßt. Es ist dabei dem Endkunden überlassen, welche konkreten Adressen aus diesem Adreßbereich er für seine Endgeräte auswählt.

Legt man diese Zahlen den Überlegungen zu Grunde, so ist eine Rückführung eines gespeicherten Kennzeichens in die zugehörige IPv6-Adresse mit Hilfe des Durchprobierens aller in Frage kommenden IPv6-Adressen jedenfalls nicht mehr praktikabel möglich.
Aus den dargelegten Gründe ist aus meiner Sicht die Speicherung eines Kennzeichens, daß mittels Transformation durch eine Einweg-Funktion aus einer IP-Adresse gewonnen wurde qualitativ nicht das Gleiche wie das unmittelbare Speichern der IP-Adresse. Insofern ist auch etwa bezüglich eines Intrusion Detection Systems die Speicherung von IP-Adressen der zugreifenden Host-Systeme nicht zwingend erforderlich, da hier eben die beschriebene Ersetzung vorgenommen werden kann.
Zusätzlich ist zu bedenken, daß wiederum der Betrieb eines Intrusion Detection Systems bzw. ähnlicher Systeme, die für eine sinnvolle Funktionsweise eine Rückgriff auf gespeicherte Daten benötigen (und nur in diesen Fällen ist die oben erwähnte Ersetzung überhaupt relevant) nicht zwingend notwendig für den sicheren Betrieb eines IT-Systems. Hier ist vielmehr im konkreten Einzelfall zu prüfen, ob durch den zusätzlichen Einsatz eines IDS eine tatsächliche Verbesserung bezüglich der Sicherheit des betreffenden IT-Systems erreicht werden kann.

Zu Anmerkung 2.3: Hier ist zunächst anzumerken, daß eine Rücküberführung eines Ersetzungskennzeichens in die ursprüngliche IP-Adresse, die der Ermittlung des jeweiligen Ersetzungskennzeichens zu Grunde lag, eben nicht in jedem Fall möglich ist. Dies wurde versucht in der Kommentierung zu Anmerkung 2.4 zu erläutern.
Darüber hinaus wird der Aussage widersprochen, Wesensgehalt der Anonymisierung sei es, daß entsprechende Daten (etwa IP-Adressen) völlig willkürlich und nicht nachvollziehbar geändert werden. Die Randomisierung von Daten ist eine Möglichkeit der Anonymisierung. Eine andere Möglichkeit der Anonymisierung besteht in der „Gleichmacherei". Wesensgehalt von Anonymisierung ist nämlich tatsächlich, daß Verkettbarkeit – und damit letztlich Unterscheidbarkeit – beseitigt wird. In Rechnernetzen handelt es sich hier üblicherweise um die Verkettbarkeit von Sendern zu Nachrichten bzw. von Nachrichten und Empfängern oder aber auch von Nachrichten untereinander oder von Sendern und Empfängern etc.
Die oben erwähnte „Gleichmacherei" ist beispielsweise das Grundprinzip hinter den Protokollen und Mechanismen des Anonymisierungsdienstes AN.ON. Idealerweise senden hier alle Sender zu gleichen Zeitpunkten Nachrichten derselben Größe über dieselben Anonymisierungsserver zu den jeweiligen Empfängern. Ausgangsseitig wird dabei von allen Nutzern des Anonymisierungsdienstes dieselbe IP-Adresse verwendet. Erneut soll auch hier ein Beispiel aus der Offline-Welt zum besseren Verständnis herangezogen werden: Bei einer Demonstration wird üblicherweise von der „Anonymität des Einzelnen in der Masse" gesprochen. Diese Anonymität ergibt sich nun aber nicht dadurch, daß alle Teilnehmer willkürlich und nicht nachvollziehbar handeln. Vielmehr ergibt sich die Anonymität hier dadurch, daß alle Teilnehmer möglichst gleich agieren, also etwa in einer Gruppe gleichzeitig denselben Weg ablaufen. Zusätzlich ist zu beobachten, daß sich Teilnehmer gleich oder zumindest ähnlich kleiden.
Die Anmerkung bezüglich der „Rückübersetzbarkeit definierter Regeln" ist in gewisser Weise richtig und falsch zugleich. Zum einen ist es zunächst so, daß es eine definierte Regel geben muß, die für die eindeutige Abbildung der IP-Adressen sorgt. Auf der

anderen Seite ist es so, daß nicht jede „definierte Regel" auch „rückübersetzbar" ist. Der Begriff „definierte Regel" läßt sich im mathematischen Sinne wohl mit dem Begriff der Funktion gleichsetzen. Ist diese nun aber nur surjektiv, so existiert eben keine eindeutige „Rückübersetzbarkeit". Als Beispiel aus der Schulmathematik sei das Quadrieren erwähnt. Hier ist die „Umkehrung", also das Wurzelziehen – zumindest bei Berücksichtigung der ganzen Zahlen – nicht eindeutig.
Allerdings ist üblicherweise für die im Rahmen der Intrusion Detection angestrebte Angriffserkennung tatsächlich eine nicht surjektive Abbildung notwendig. Insofern existiert dann zumindest die theoretische Möglichkeit der Rücküberführung – etwa durch einfaches Durchprobieren aller möglichen Funktionsargumente, d.h. IP-Adressen. Das Durchprobieren wurde bereits in Anmerkung 2.4 (siehe oben) besprochen.
Auf der anderen Seite ist es so, daß allein an Hand des Schlüsseltextes, d.h. ohne Kenntnis der verwendeten kryptographischen Schlüssel eine Rückführung nicht mal theoretisch, d.h. mittels Durchprobieren möglich ist. Man kann sich das vielleicht auch so verdeutlich, daß die verwendeten Schlüssel Teil der mathematischen Funktion, also der „definierten Regel" sind, ohne deren Kenntnis eben keine Rücküberführung möglich ist.
Abschließend sei noch angemerkt, daß der Gutachter nie eine willkürliche Ersetzung von IP-Adressen vorgeschlagen hat. Es wurde lediglich vorgeschlagen, die IP-Adressen mit Hilfe einer Einwegfunktion in eindeutige Ersetzungskennzeichen zu ersetzen, die nicht oder nur mit unrealistisch hohem Aufwand in die der Ersetzung zu Grunde liegenden IP-Adressen zurück überführt werden können.

Zur Anmerkung 2.5: Die hier getroffenen Anmerkungen sind insofern korrekt, als daß auch der Gutachter davon ausgeht, daß bei Benutzung eines Botnetzes regelmäßig die Absender-IP-Adresse nicht manipuliert wird, so daß es sich also um die „echte" IP-Adresse des Rechners handelt.
Die darüber hinausgehenden Anmerkungen sind aber als Wunschdenken bezüglich einer nicht zu Ende gedachten Idee einzustufen. So wird behauptet, man könne die gespeicherten IP-Adressen benutzen, um die Eigentümer der betreffenden Rechner zu informieren. Wie soll das aber praktisch funktionieren? Bei Botnetz-Rechnern handelt es sich zu großen Teilen um Rechner von Privatpersonen, da diese oftmals „ungesichert" betrieben werden und daher besonders leicht durch Angreifer mit entsprechender Botnetz-Schadsoftware verseucht werden können. Will man die betreffenden Personen nun unmittelbar benachrichtigen, so bräuchte man eine Auskunft des jeweiligen ISP, welcher Person die jeweilige IP-Adresse zugeordnet war. Auch wenn der Gutachter kein Jurist ist, so glaubt er doch zu wissen, daß zumindest im deutschen Recht ein derartiger Grund bezüglich eines Auskunftsersuchens an einen Provider nicht vorgesehen ist.
Daß das Informieren von Betroffen tatsächlich nicht so trivial möglich ist, wie in Anmerkung 2.5 glauben gemacht wird, sieht man auch in den jüngsten Bemühungen des BSI, Betroffene eines Botnetzes zu informieren. Dies geschah nämlich nicht durch

eine direkte Kontaktierung der Betroffenen, sondern vielmehr durch eine Pressemitteilung[3].
Zusätzlich ist zu bedenken, daß es sich um ein weltweites Problem handelt. Je nachdem, welcher Studie[4] man glauben mag, so haben Rechner von deutschen Nutzer zwar in der Tat einen nicht zu vernachlässigenden Anteil an allen Botnetz-Rechnern. Auf der anderen Seite würde selbst ein Abschalten aller deutschen Botnetz-Rechner das Angriffspotential nur unwesentlich verringern, so daß in jedem Fall Maßnahmen zu treffen sind, die einen hinreichend guten Schutz gegen Botnetz-Angriffe bieten. Insofern ist auch hier eine zwingende Notwendigkeit der Speicherung von IP-Adressen nicht zu erkennen.
Darüber hinaus gilt, daß selbst wenn man die Betroffene informieren will, eine Speicherung der IP-Adressen des zugreifenden Host-Systems nicht zwingend notwendig ist. Wie oben bereits angedeutet, wäre eine Grundvoraussetzung bezüglich des Informierens von Betroffen, daß entsprechende Regelungen und Prozesse existieren, die ein Informieren ermöglichen. Hier sei vereinfachend angenommen, daß dies durch Zustimmung des jeweiligen Nutzers geschehen ist, d.h. der Nutzer hat mit seinem Provider eine entsprechende Vereinbarung getroffen, daß der Nutzer informiert werden möchte, wenn bezüglich seines Rechners ein Botnetz-Verdacht besteht (oder ggf. sonstigen Befalls durch Schadsoftware). Stellen nun die Sicherheitssysteme der Beklagten fest, daß ein Angriff stattfindet – beispielsweise durch Inhaltsanalyse eines IP-Paketes etwa im Falle des Conficker-Wurms – so kann unmittelbar eine entsprechende Mitteilung an ein dafür vorgesehenes IT-System des Providers des Nutzers erfolgen. Der Provider kann dann (etwa an Hand der Häufigkeit der eintreffenden Warnmeldungen bezüglich eines Nutzer-Rechners) entscheiden, ob der Nutzer zu informieren ist oder nicht. Eine persistente Speicherung der IP-Adresse des zugreifenden Host-Systems durch die IT-Systems der Beklagten ist dabei jedenfalls nicht zwingend notwendig.

Zu Anmerkung 2.6: Hier wird zunächst festgestellt, daß im Gutachten keine konkreten Maßnahmen beschrieben werden, die keine Speicherung von IP-Adressen zwingend erfordern. Dies wird insbesondere bezüglich des Anonymisierungsdienstes AN.ON bemängelt. Zwar wurde im Gutachten bereits angemerkt, daß eine umfangreiche Darstellung aller Möglichkeit des „Security Engineering" den Rahmen des Gutachtens sprengen und vermutlich auch nicht dem intendierten Zwecke dienen würde, dennoch sollen auf Grund der Nachfrage bezüglich des Anonymisierungsdienstes AN.ON hier einige der durchgeführten Maßnahmen näher erläutert werden. Zunächst ist einfach anzumerken, daß im Rahmen von AN.ON schlicht keine IP-Adressen gespeichert werden – auch wenn dies eventuell schier unvorstellbar zu sein scheint. Es existieren im Wesentlichen auch keine dem Speichern von IP-Adressen unmittelbar vergleichbaren Ersetzungsverfahren wie etwa das verschlüsselte Speichern von IP-Adressen. Vielmehr kommen Verfahren und Überlegungen zum Einsatz, die eben ohne Speicherung von IP-Adressen auskommen.

---

[3] https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2012/Hilfe-gegen-Schadsoftware_DNS-Changer_10012012.html

[4] etwa: http://www.mcafee.com/us/resources/white-papers/wp-new-era-of-botnets.pdf

Dies beginnt damit, daß die dem Anonymisierungsdienst zuzurechnenden Server physisch geschützt in Räumlichkeiten betrieben werden, zu denen nur ein begrenzter Personenkreis Zutritt hat. Bezüglich der eigentlichen Anonymisierungsserver ist es so, daß diese auf einer dedizierten Hardware betrieben werden, die ausschließlich durch den Anonymisierungsdienst genutzt wird. Bei Diensten, die nur mittelbar der eigentlichen Anonymisierung dienen, wie etwa der Web-Server zum Betreib der dem Projekt zugehörigen Web-Seite, ist es so, daß hier eine Separierung unterschiedlicher Dienste mit Hilfe von Virtualisierung (konkret: VMWare ESXi 5.0) vorgenommen wird.
Als Betriebssystem für die Anonymisierungsserver wurde Debian Linux gewählt, wobei zum einen der Linux-Kern so übersetzt wurde, daß sämtliche nicht unmittelbar benötigte Funktionalität (etwa Services, Treiber etc.) deaktiviert wurde. Ferner wurden Schnittstellen, die geeignet sind, Manipulationen am System vorzunehmen deaktiviert. Dazu gehört etwa die Möglichkeit, Kode in den Kern des laufenden System mit Hilfe von Modulen nachzuladen, die Möglichkeit mittels `/proc/kcore` den Hauptspeicherinhalt auszulesen oder mittels `kexec` System-Call einen neuen Kern zu starten. Ferner wird der Kern zeitnah zu veröffentlichten Updates des Kern-Kodes aktualisiert, um eventuell im Kern-Kode vorhandene Sicherheitsschwachstellen zu beseitigen.
Bezüglich des verwendeten Debian-Linux Systems wurde zu einem die aktuelle, als „stabil" gekennzeichnete Distribution verwendet, da die innerhalb dieser Distribution veröffentlichte Software besonders bezüglicher Fehler überprüft wird. Ferner erfolgt hier die Bereitstellung von (Sicherheits-)Updates, die entsprechend zeitnahe nach Veröffentlichung eingespielt werden.
Bezüglich der aus der Distribution installierten Software wurde nur installiert, was zwingend für den Betrieb des Anonymisierungsservers benötigt wird. Insbesondere werden auf dem Server keine Dienste ausgeführt, die nicht in unmittelbaren Zusammenhang mit dem Anonymisierungsserver stehen. Konkret laufen hier neben dem eigentlichen Anonymisierungsserver noch ein Cache-Proxy zum Zwischenspeichern der anonym abgerufenen Web-Seiten (Effizienzoptimierung im Falle eines erneuten Abrufes derselben Seiten), ein Dienst zum Synchronisieren der auf dem Server eingestellten Uhrzeit sowie ein Dienst für den Fernzugriff.
Bei letzterem handelt es sich um den Secure Shell Dienst (SSH), also ein Dienst, der mit Hilfe kryptographischer Verfahren (Verschlüsselung etc.) versucht, einfache Angriffe zu verhindern – im Gegensatz etwa zum klassischen Telnet-Dienst, bei dem beispielsweise Login/Paßwort im Klartext übertragen werden. Der SSH-Dienst lauscht nicht auf dem üblichen Port 22. Dies trägt aber nur sehr eingeschränkt zur Sicherheit bei und schützt bestenfalls vor allzu simplen DoS-Angriffsversuchen. Beim SSH-Dienst wird momentan im übrigen auf den Einsatz von Public-Key-Authentifizierung verzichtet. Dessen Einsatz könnte die Sicherheit des Fernzugriffs weiter erhöhen.
Bezüglich des Cache-Proxies ist zu sagen, daß dieser so konfiguriert ist, daß ein Zugriff nur von `localhost` möglich ist. Insbesondere ist eine direkte Verbindungsaufnahme aus dem Internet also nicht möglich, da zur Erbringung des gewünschten Dienstes auch nicht notwendig. Ferner ist der Cache-Proxy so konfiguriert, daß über den Cache-Proxy selbst ein Zugriff auf interne IP-Adressen (insbesondere auch `localhost`) nicht möglich ist. Andernfalls könnte ein Angreifer unter Benutzung des Anonymisierungsdienstes (und des dem Anonymisierungsdienst nachgeschalteten Cache-Proxies) auf `localhost` (und andere interne IP-Adressen) zugreifen, was nicht erwünscht ist und

durch nachfolgend noch näher beschriebene Firewall-Regeln weiter erschwert (hoffentlich verhindert) wird.
Der Anonymisierungsdienst ist so konzipiert, daß zum einen keine Verbindung vom Anonymisierungsdienst zum Nutzer aufgebaut wird, d.h. der Nutzer des Anonymisierungsdienstes muß in seiner Firewall keinen eingangsseitigen Port öffnen[5]. Zum anderen erfolgt sämtliche Kommunikation über genau einen wohldefinierten Port. Dies macht die (Serverseitige) Formulierung von Firewall-Regeln einfacher. Zusätzlich ist es so, daß sämtliche Kommunikation eines Nutzers über genau eine TCP/IP-Verbindung abgewickelt wird. Neben einer verbesserten Effizienz ermöglicht dies unter Sicherheitsaspekten eine klarere Beschreibung der erlaubten / nicht erlaubten Systemzustände.
In der Konsequenz arbeitet die Firewall eingangsseitig nach einem White-List-Konzept. Dies bedeutet, daß zunächst sämtlicher eingehender Datenverkehr verworfen wird, außer es existiert eine Firewall-Regel, die den Datenverkehr explizit erlaubt. Bezüglich des Protokolls UDP werden dabei nur die zur DNS-Auflösung notwendigen UDP-Pakete (Port 53) sowie die zur Zeit-Synchronisation notwendigen UDP-Pakete (Port 123) zugelassen. ICMP wird generell zugelassen – wenngleich man hier unter Sicherheitsaspekten weitere Einschränkungen vornehmen könnte. Daneben wird nur noch das Protokoll TCP zugelassen. Bezüglich TCP wiederum werden zunächst alle Pakete zugelassen, die keine Verbindungsaufbaupakete sind. Ursprünglich wurde hier zwar mit Connection-Tracking gearbeitet, so daß nur Pakete zugelassen wurden, die entweder zu einer bestehenden Verbindung gehören oder einen Verbindungsaufbauwunsch signalisieren. Allerdings hat sich gezeigt, daß diese Art der Analyse vergleichsweise aufwendig ist (im Sinne von Rechenleistung und Hauptspeicherverbrauch). Außerdem erleichtert sie DoS-Angriffe, da nur für eine begrenzte Anzahl von Verbindungen die notwendigen Daten zur Ermittlung der Zugehörigkeit eines neu eintreffenden Datenpaketes zu einer bestehenden Verbindung im Hauptspeicher gehalten werden können. Es kann also bei entsprechend vielen parallel laufenden Verbindungen zu einer Überlastung und damit zu einer Blockierung des Systems kommen.
Ferne werden bezüglich des Protokolls TCP alle Pakete zugelassen, die einen Verbindungsaufbau signalisieren, wobei dabei nur Pakete erlaubt werden, deren Ziel-Portnummer entweder dem Anonymisierungsdienst oder dem Fernwartungsdienst (SSH) zuzurechnen ist.
Darüber hinaus gibt es noch eine weitere Regel, die besagt, daß pro Absender-IP-Adresse lediglich sechs Verbindungsaufbauwünsche pro Minute zulässig sind. Dies ist ebenfalls als eine Maßnahme zur DoS-Abwehr zu werten. Hier ist es im Übrigen nicht notwendig, daß IP-Adressen permanent gespeichert werden. Die entsprechende Analyse erfolgt vielmehr im Hauptspeicher unter Verwendung von Hash-Tabellen. Die Funktionalität zum Speichern von IP-Adressen wurde beim Kompilieren des Linux-Kern deaktiviert.

[5] Als ein Negativbeispiel, wie man es nicht machen sollte, kann hier das ursprüngliche aktive File Transfer Protokoll (FTP) angesehen werden. Diese ist mittlerweile – auch aus Sicherheitsgründen – durch passives FTP ersetzt, das ebenfalls keine Portöffnung durch den auf einen FTP-Server zugreifenden Nutzer mehr erfordert.

Abschließend ist noch anzumerken, daß unerwünschte Pakete einfach verworfen werden (DROP) – es erfolgt also keine Benachrichtigung des Absenders (etwa mittels Reset-Paketen).
Insgesamt ermöglicht der bezüglich Diensten minimalistische Ansatz zusammen mit dem unter Sicherheitsgesichtspunkten vorgenommen Design, daß nur sieben Firewall-Regeln existieren. Diese geringe Anzahl wiederum erleichtert einem Administrator das Verständnis, wodurch wiederum Fehlkonfiguration vermieden wird, was letztlich ebenfalls der Sicherheit zu Gute kommt.
Neben einem Dienste-minimalistischen Ansatz wurde auch ein bezüglich Benutzer minimalistischer Ansatz gewählt. Es existiert aus praktischer Sicht genau ein Benutzer – der Administrator des Systems. Technisch sind dem Administrator unterschiedliche Benutzerkonten zugeordnet, die wiederum unterschiedliche Rechte haben. Somit kann der Administrator für eine konkret anstehend Aufgabe das Benutzerkonto wählen, daß für die durchzuführende Aufgabe gerade ausreichende Rechte hat. Auf diese Weise wird die Möglichkeit eingeschränkt, daß durch Unachtsamkeit bzw. als Folge eines Angriffs vermeidbarer Schaden am Gesamtsystem entsteht. Der Benutzerkonten-minimalistische Ansatz bedeutet auch, daß es sich nicht um eine echte Mehrbenutzerkonfiguration handelt. Damit sollen die Angriffe erschwert werden, bei denen ein berechtigter Nutzer, der nur eingeschränkte Rechte hat, durch Fehler im System(-Kern) erfolgreich eine Rechteausweitung durchführen kann.
Natürlich bleibt der Angriffspunkt „Rechteausweitung" weiterhin insgesamt bestehen, da ein nicht-berechtigter Außenstehender, dem es gelungen ist, sich Zugriff auf ein nicht-privilegiertes Benutzerkonto zu verschaffen, dies nutzen kann, um mit Hilfe von Rechteerweiterung alle für seinen Angriff notwendigen Rechte zu erlangen.
Die auf dem System ausgeführt Software wurde so entwickelt bzw. ausgewählt, daß eine möglichst geringe Wahrscheinlichkeit für einen erfolgreichen Angriff besteht. Bezüglich des Fernwartungsdienstes (SSH) wurde OpenSSH[6] verwendet. Zwar finden sich auch in der OpenSSH-Software immer wieder Fehler, die Angriffe ermöglichen bzw. erleichtern, auf der anderen Seite gibt es eine sehr aktive Gemeinschaft von Entwicklern und Sicherheitsexperten, die ständig an der Verbesserung der Kodequalität arbeiten bzw. bekannte Schwachstellen sehr zeitnah publizieren und beseitigen.
Die Software für den Anonymisierungsdienst selbst wurde unter Berücksichtigung von Sicherheitsaspekten und den bekannten Methoden für sichere Softwareentwicklung entworfen und implementiert. Zunächst wurden die Protokolle so entworfen, daß mit Hilfe kryptographischer Maßnahmen (Verschlüsselung, Integritätssicherung, digitale Signaturen) erfolgreiche Angriffe auf die Schutzziele Vertraulichkeit, Integrität und Zurechenbarkeit von vorne herein erschwert bzw. unterbunden werden. So werden etwa Entschlüsselungsschlüssel nur im Hauptspeicher gehalten und nicht permanent gespeichert.
Die digitale Identität der an der Anonymisierung beteiligen Entitäten wird mit Hilfe von digitalen Signaturen gesichert. Dabei wird auf eine üblicherweise verwendete Public-Key-Infrastructure (PKI) verzichtet. Vielmehr erfolgt der notwendig Austausch von Signaturtestschlüsseln direkt zwischen den beteiligten Parteien (direct trust). Auf diese Weise sollen die mit einer PKI verbundenen Angriffsmöglichkeiten – etwa die jüngst

[6] http://www.openssh.com/

im Web-Umfeld zu beobachtenden Kompromitierungen von Zertifizierungsstellen – vermieden werden.
Darüber hinaus wurden die Protokollabläufe und –details so entworfen, daß DoS-Angriffe nach Möglichkeit erschwert werden. „Least privilege" ist ein weiteres Design-Prinzip, daß bei Entwurf und Betrieb der Anonymisierungsserver angewendet wurde. So kann der Anonymisierungsserver mit den Rechten eines nicht-privilegierten Benutzerkontos ausgeführt werden, um zu verhindern, daß bei einem möglicherweise im Kode enthaltenen Fehler ein Angreifer automatisch privilegierte Rechte auf dem angegriffenen System erhält. Sämtliche Nutzereingaben (im Sinne der über das Internet durch Nutzer als „Eingaben" an den Anonymisierungsdienst verschickten Datenpakete) werden auf Plausibilität einschließlich eines gültigen Wertebereichs überprüft. Wertebereiche wurden ferne so gewählt, daß auch bei Benutzung von Extremwerte keine signifikante Beeinträchtigung des Systems erfolgen kann. Dies betrifft etwa Größenangaben von Datenfeldern. Diese wurden so beschränkt, daß auch bei Ausnutzung der maximal zulässigen Größe (wenige tausend Bytes) eine vollständige Belegung sämtlicher Systemressourcen (Hauptspeicher etc.) durch einen einzelnen Angreifer nur schwer möglich ist. Statische Puffer werden nur verwendet, wenn vorher zugehörige Längenangaben überprüft wurden.. Andernfalls werden dynamisch allokierte Puffer verwendet. Natürlich erfolgt in jedem Fall eine Überprüfung der Längenangaben, so daß kein Pufferüberlauf erfolgen kann.
An Hand der beschriebenen Beispiele wird hoffentlich deutlich, daß beim Anonymisierungsdienst AN.ON sehr wohl eine Reihe konkreter Maßnahmen umgesetzt wurden, die dem sicheren Betrieb des Systems dienen. Eine Speicherung von IP-Adressen findet jedenfalls nicht statt.

In Anmerkung 2.6 wird ferner ausgeführt, daß die bezüglich isharegossip.com beschriebenen Maßnahmen lediglich zur Abwehr von SPAM dienen. Dies ist korrekt und wurde auch nie bestritten. Das Verfahren von isharegossip.com diente im Gutachten lediglich als ein Beispiel für ein in der Praxis tatsächlich angewendetes Ersetzungsverfahren. Natürlich ist dieses Verfahren alleine nicht ausreichend für den sicheren Gesamtbetrieb. Den im betreffenden Anmerkungsabsatz weiter ausgeführten Darlegungen ist ansonsten zuzustimmen – auch wenn sie einer gewissen Logik entbehren. In den Anmerkungen wird zum einen (korrekterweise) bemängelt, daß das erwähnte Verfahren nur gegen SPAM schützt, zum anderen wird dann aber überrascht angemerkt, daß es eben nicht gegen Web-Seiten-Hacking schützt. Der Rückschluß, daß ein Verfahren, daß nur für SPAM-Schutz entwickelt wurde und das bezüglich Web-Seiten-Hacking versagt hat, dann auch bezüglich SAPM-Schutz keine „praktische Wirksamkeit" entfalten kann, kann jedenfalls nicht nachvollzogen werden.

Bezüglich der Dissertation von Ulrich Flegel und der diesbezüglich getroffenen Anmerkung ist es auch nach Wissen des Gutachters so, daß eine praktische Implementierung, die über einen prototypisch/experimentellen Status zur Evaluierung der Machbarkeit des Ansatzes hinausgeht, nicht existiert. Die Intention des Gutachtens war hier in der Tat auch nur, anzumerken, daß es prinzipiell möglich ist. Zumindest kommt Herr Dr. Flegel diesbezüglich in seiner Dissertation zum dem Schluß: „In Sect. 23.3 we show that even for unrealistic settings and during rare pathological situations

the performance of the pseudonymizer is sufficient to cope with the audit volume record of a large site."[7]
In Anmerkung 2.6 wird ferner behauptet: „Kein einziger Hersteller eines gängigen Produktes zum Schutz von IT-Systemen verzichtet auf die Speicherung von IP-Adressen.". Dieser Aussage ist zu wiedersprechen.
Als Gegenbeispiel sie hier zunächst das Betriebssystem Windows 7 der Firma Microsoft erwähnt. Glaubt man den entsprechenden Informationsquellen im Internet[8] so beträgt der Marktanteil von Windows 7 am Gesamtmarkt der Desktop-Betriebssysteme zur Zeit mehr als 45%, wobei im ersten Jahr nach Erscheinen mehr als 240 Millionen Exemplare verkauft wurden. Insofern wird bezüglich Windows 7 durchaus von einem „gängigen Produkt" ausgegangen. Dieses hat zwar nicht primär den Zweck des Schutzes von IT-Systemen zum Ziel, ist aber selbst Bestandteil der IT-Infrastruktur und trägt somit mindestens mittelbar zu deren Schutz bei.
Aus diesem Grund ist bei Windows 7 eine Firewall standardmäßig aktiviert, die unerwünschten Datenverkehr aus dem Internet blockiert und somit zur Abwehr von Angriffen beiträgt.

[7] U. Flegel: „Privacy-Respecting Intrusion Detection", Springer, 2007, S. 193.
[8] http://gs.statcounter.com/#os ww-monthly-201203-201203-bar
http://windowsteamblog.com/windows/b/bloggingwindows/archive/2010/10/21/celebrating-windows-7-at-1-year-more-than-240-million-licenses-sold.aspx

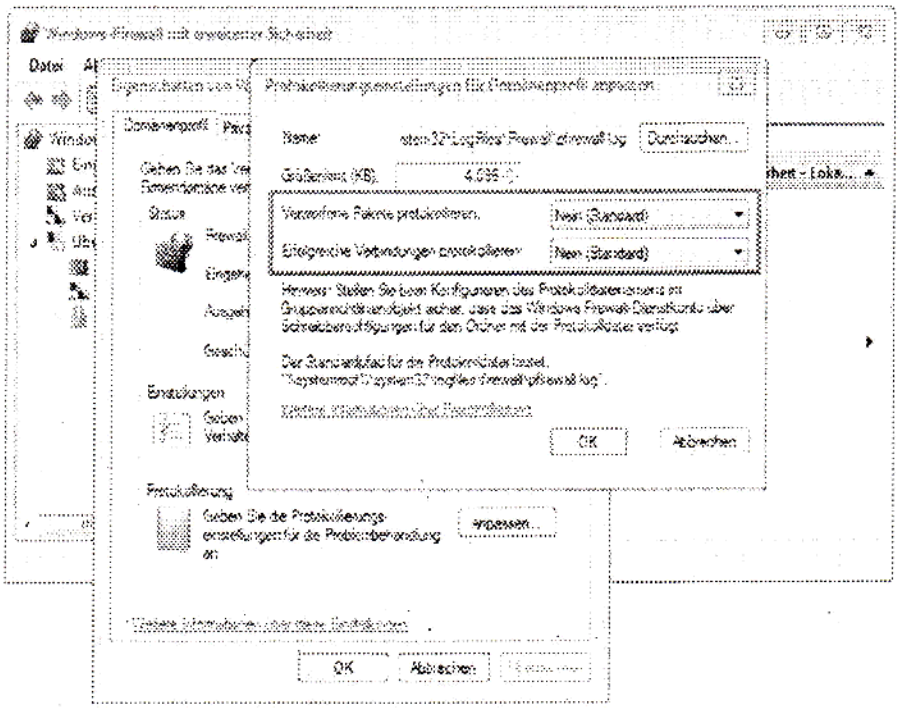

Abbildung 1: Eine Protokollierung von verworfenen Paketen bzw. erfolgreichen Verbindungen – und damit letztlich von IP-Adressen der zugreifenden Host-Systeme – erfolgt bei der in Windows 7 integrierten Firewall standardmäßig nicht.

Wie dem Bildschirmfoto in Abbildung 1 zu entnehmen ist, bietet die Windows-Firewall auch prinzipiell die Möglichkeit, ein Speichern von IP-Adressen zu aktivieren. Interessanterweise ist dies jedoch standardmäßig nicht aktiv – wobei dieser Zustand auch noch als der Standradzustand kenntlich gemacht wird. Es ist davon auszugehen, daß Laien auf dem Gebiet der IT-Sicherheit dies als eine Art Empfehlung interpretieren. Jedenfalls erfolgt bei Deaktivierung der Speicher-Funktion (nachdem sie zuvor manuell aktiviert wurde) keine Warnung bezüglich der nunmehr nicht mehr gewährleisteten Sicherheit. Wie ist dies aber zu interpretieren, wenn für den sicheren Betrieb eines IT-Systems die Speicherung von IP-Adressen tatsächlich zwingend erforderlich wäre? Dies würde bedeuten, daß Microsoft wissentlich seine Kunden in falscher Sicherheit wiegt, da zwar eine Firewall-Funktionalität angeboten wird, die auch scheinbar (standardmäßig) aktiviert ist – die aber keinen Schutz bietet, da ja eben kein (für den Betrieb eines sicheren IT-System angeblich zwingend notwendiges) Speichern von IP-Adressen erfolgt.

Als weiteres Beispiel soll hier der Catalyst 6500 Switch zusammen mit dem Router /Firewall Modul der Cisco 7600 Serie der Firma Cisco Systems, Inc. dienen. Cisco behauptet von sich selbst der „weltweit führende Anbieter von Netzwerk-Lösungen für das Internet" zu sein. Insofern wird davon ausgegangen, daß es sich bei dem erwähnten Produkt um „ein gängiges Produkt zum Schutz von IT-Systemen" handelt.

Im zugehörigen Konfigurationshandbuch[9] finden sich an den verschiedensten Stellen Informationen darüber, wie das Logging – etwa das Speichern von IP-Adressen – ganz oder teilweise deaktiviert werden kann. Hier sei beispielsweise auf die Beschreibung zum vollständigen Deaktivieren des Logging (Seite 25-3) verwiesen. Oder auch auf die auf Seite 13-25 getroffenen Aussagen zum „Access List Logging Overview". Dort heißt es:

„By default, when traffic is denied by an extended ACE, the FWSM generates system log message 106023 for each denied packet, in the following form:

...

If the FWSM is attacked, the number of system log messages for denied packets can be very large. We recommend that you instead enable logging using system log message 106100, which provides statistics for each ACE and lets you limit the number of system log messages produced. Alternatively, you can disable all logging."

Dies ist meiner Meinung nach eine Empfehlung, auf das Speichern einzelner IP-Adressen zu verzichten und statt dessen lediglich eine Statistik zu speichern bzw. das Logging ganz abzuschalten. In jedem Fall findet sich aber an beiden erwähnten Stellen keinerlei Hinweis oder Warnung darauf, daß mit dem Abschalten der Speicherung von IP-Adressen die Sicherheitsfunktionalität nicht mehr gegeben ist. Wenn aber tatsächlich das Speichern von IP-Adressen zwingend erforderlich ist für den sicheren Betrieb eines IT-Systems, dann würde man nicht nur erwarten, daß ein Abschalten dieser unbedingt notwendigen Funktion gar nicht möglich ist, man würde außerdem erwarten, daß es wenigstens entsprechende Warnungen gibt, für den Fall, daß man das Speichern eben doch deaktiviert.

Darüber hinaus seien hier noch die in den Betriebssystemen Linux, FreeBSD, OpenBSD und NetBSD enthaltenen Firewallfunktionalitäten erwähnt. Auch hier ist eine Speicherung der IP-Adressen der zugreifenden Host-Systeme nicht zwingend, ja noch nicht einmal „standardmäßig" vorgesehen. Dabei dient die den erwähnten Betriebssystemen integrierte Firewall nicht nur zum Schutze von Endsystemen, die mit Hilfe dieser Betriebssysteme betrieben werden. Vielmehr werden die erwähnten Betriebssysteme auch in Routern, Switchen und sogenannten Appliances eingesetzt um entweder ausschließlich oder zumindest auch die Funktionalität einer Firewall wahrzunehmen. Auch in diesen Fälle kann das Logging ein oder ausgeschaltet werden.

Die aufgeführte Liste an Beispiele – die sich noch um viele weitere ergänzen läßt – möge ausreichen, um die Behauptung: „Kein einziger Hersteller eines gängigen Produktes zum Schutz von IT-Systemen verzichtet auf die Speicherung von IP-Adressen" zu wiederlegen.

Anmerkung 2.6 schließt mit der Anmerkung: „Mit anderen Worten: In bestimmten Fällen ist eine sinnvolle Ersetzung der Speicherung der IP-Adressen gerade nicht möglich." Dieser Feststellung wird nicht widersprochen, insofern wurde die Aussage des Gutachtens hier richtig interpretiert. Selbstverständlich existieren Fälle, in denen sich die Speicherung von IP-Adressen nicht sinnvoll ersetzen läßt. Dies gilt etwa für den Fall, daß der Betreiber des IT-System genau wissen möchte, welche IP-Adresse

[9] http://www.cisco.com/en/US/docs/security/fwsm/fwsm41/configuration/guide/fwm41cfg.pdf

wann, wie lange etc. bei Zugriff auf das IT-System verwendet wurde. Allerdings hat dies auf der anderen Seite nichts mit der Frage zu tun, ob ein Speichern von IP-Adressen für den sicheren Betreib eines IT-Systems zwingend erforderlich ist.
Die Aussage des Gutachtens, die Grundlage des oben zitierten Satzes aus Anmerkung 2.6 ist, wurde konkret im Zusammenhang mit Intrusion Detection Systemen getroffen. In der Tat kann es hier sein, daß der in einem konkreten Intrusion Detection System implementierte Algorithmus nicht ohne die Speicherung von IP-Adressen auskommt. Allerdings läßt ich daraus nicht schließen, daß damit ein Speicher von IP-Adressen für den sicheren Betrieb eines IT-Systems zwingend erforderlich ist.
Dies ergibt sich schlicht daraus – wie oben bereits geschildert – daß auch der Betrieb eines Intrusion Detection Systems nicht zwingend erforderlich für den sicheren Betrieb eines IT-Systems ist. Was natürlich im Gengenzug nicht bedeutet, daß behauptet wird, Intrusion Detection Systeme seien wirkungslos. Vielmehr ist es so, daß alle dem Gutachter bekannte übliche Funktionalität eines Intrusion Detection Systems auch ohne Speicherung von IP-Adressen erbringbar ist. Dies wiederum ist kein Beweis dafür, daß es nicht doch eine „Spezial-Funktionalität" gibt, die tatsächlich ein Speichern von IP-Adressen erfordert – daher die relativierende Formulierung „in viele Fällen...".
Der Gutachter ist jedoch der Überzeugung, daß – sollte tatsächlich eine derartige „Spezial-Funktionalität" existieren – diese durch andere Sicherheitsmaßnahmen ersetzt werden kann, ohne daß dies zu einer signifikanten Reduktion der Sicherheit des betreffenden IT-Systems führt. Dies gilt zumindest solange, bis nicht eine konkrete technische Maßnahme benannt werden kann, die zwingend das Speichern der IP-Adressen der zugreifenden Host-Systeme erfordert und die sich – unter Beibehaltung des Sicherheitsniveaus – durch keine andere bekannte Sicherheitstechnologie /-maßnahme ersetzen läßt.

Zu Anmerkung 2.7.: Wie im Gutachten bereits dargelegt wird natürlich den am Anfang getroffene Aussagen und Interpretationen zugestimmt, d.h. für eine Angreiferidentifikation kann ein Speichern von IP-Adressen nützlich sein. Der Schluß von „nützlich" auf „erforderlich" ist allerdings gewagt bzw. schlicht falsch. Vielmehr kommt es natürlich auf die Umstände des Angriffs und die in diesem Zuge vorliegenden Informationen an.
Als Beispiel sei hier der Betrug beim Online-Einkauf erwähnt, wobei dann der Betrüger als „Angreifer" gesehen wird. Natürlich kann man versuchen mit Hilfe einer gespeicherten IP-Adresse die Identität eines Betrügers aufzudecken. Genauso kann man aber den Online-Einkauf auch so gestalten, daß man (etwa im Rahmen des Vertragsabschlusses) auf die Online-Identifikationsfunktion des neuen elektronischen Personalausweises zurückgreift. In diesem Fall liegen alle relevanten Informationen unmittelbar vor und es bedarf keines unsicheren, wie ungewissen Rückgriffs auf gespeicherte IP-Adressen.
Im übrigen soll hier nicht weiter diskutiert werden, ob ein Speichern von IP-Adressen zur Angreiferidentifikation nun zwingend erforderlich ist oder nicht. Viel interessanter ist die Feststellung, daß in Anmerkung 2.7 gar kein unmittelbarer Bezug mehr zur Angriffsabwehr bzw. Angriffserkennung erfolgt. Es geht nur noch um Angreifer-identifikation, also eine Sache, die nur noch über zwei Indirektionsstufen etwas mit dem sicheren Betrieb eines IT-Systems zu tun hat. Insofern kann aus der – vom

Gutachter zwar bestrittenen, aber hier trotzdem unterstellten – Notwendigkeit der Speicherung von IP-Adressen zum Zwecke der Identifikation eines Angreifers nicht geschlossen werden, daß demzufolge das Speichern von IP-Adressen für den sicheren Betrieb eines IT-Systems zwingend notwendig ist.
Hier soll wieder ein (vermutlich ungeliebter) Vergleich erfolgen: Die Stahltür eines Banktresors trägt (hoffentlich unbestrittener Weise) zum Schutz des Inhalts des Tresors bei. Sie leiste diese Schutzfunktionalität insbesondere ohne daß sie überhaupt erkennt, daß ein Angriff stattfindet, geschweige denn, daß sie den Angreifer identifiziert. Insofern erfolgt hier eben eine sinnvolle Angriffsabwehr ohne daß Angriffserkennung oder Angreiferidentifikation stattfinden.
In Anmerkung 2.7 wird abschließend ein „Generalpräventions"-Effekt des Speicherns unterstellt und – so wird die getroffene Aussage zumindest interpretiert – implizit behauptet, diese Generalprävention sei notwendig zum sicheren Betrieb der IT-Systeme der Beklagten. Hier bleibt nur zu hoffen, daß diese „Generalprävention durch IP-Adressen-Speicherung" nicht tatsächlich ein signifikanter Baustein im Gesamt-IT-Sicherheitskonzept des Bundes ist. Andernfalls kann einem – auch als Staatsbürger – nur „Angst und Bange" werden. Dies liegt nicht nur daran, daß etwa die Wirksamkeit von Videoüberwachung zur Prävention generell zumindest hinterfragt werden kann[10] es liegt insbesondere daran, daß das Speichern von IP-Adressen überhaupt keine Generalpräventionswirkung entfalten kann.
Für die Präventionswirkung ist es nach Auffassung des Gutachters nämlich nicht nur notwendig, daß der Schuldige identifizierbar ist – es ist mindestens ebenso notwendig, daß der Schuldige mit Bestrafung rechnen muß. Vor welcher Bestrafung soll aber ein staatlich gelenkter Hacker aus Banania oder Citronia Angst haben? Glaubt man den entsprechenden Warnung stattlicher Stellen (etwa: BSI, BKA) so sind derartige Angriffsszenarien Realität. Insofern ist es für den sicheren Betrieb eines IT-Systems zwingend erforderlich, daß Sicherheit auch ohne die (unterstellte) Generalprävention gegeben ist. Ist dies aber wiederum der Fall, so ist das Speichern von IP-Adressen aus Gründen einer Generalprävention für den sicheren Betrieb eines IT-Systems eben nicht mehr zwingend erforderlich.

Erläuterungen zu den Anmerkungen zur Beweisfrage 1

Hier soll zunächst auf die unmittelbar auf 1.) folgenden Anmerkungen eingegangen werden, da die dort geäußerten Anmerkungen als Ursache für die Mißverständlichkeiten angesehen wird. Zu Erinnerung sei nochmal darauf hin gewiesen, daß es um die Frage geht, ob die Speicherung der IP-Adressen der zugreifenden Host-Systeme dem internationalen Stand der Technik dient.

---

[10] So kommt etwa das „Deutsch Forum für Kriminalprävention" in einer Untersuchung (http://www.kriminalpraevention.de/downloads/as/evaluation/Wirksamkeit_Videoueberw.pdf) zum dem Schluß, daß Videoüberwachung zwar als Präventionsmaßnahme in Parkhäusern gut Ergebnisse zeigt – „Hinsichtlich der Verhinderung von Gewalt in Stadtzentren oder in der U-Bahn scheint die Videoüberwachung jedoch weniger geeignet zu sein." Die von der Beklagten selbst zu Grunde gelegten Angriffe auf „hochgefährdete Systeme" scheinen mir eher mit Gewalttaten als mit Autodiebstählen vergleichbar zu sein.

Die Beklagte glaubt nun in den Ausführungen des Gutachtens einen Widerspruch entdeckt zu haben, weil einerseits zwar die Speicherung von IP-Adressen der Erfüllung von nationalen und internationalen Standards, Empfehlungen und Richtlinien dienen kann und trotzdem behauptet wird, das Speichern von IP-Adressen diene nicht dem Stand der Technik. Konkrete Ursache des scheinbaren Widerspruchs liegt in der durch die Beklagte vertretene Ansicht, der Stand der Technik würde durch internationale Empfehlungen, Standards und Regulierungen definiert.
Aber genau dem wird widersprochen. Vielmehr wird behauptet, daß für die Formulierung „dient dem Stand der Technik" keine eindeutige Definition existiert. Nach meiner Interpretation dieser Formulierung können hier Standards, Empfehlungen und Regulierungen bestenfalls als ein Kriterium zur Beantwortung der Frage herangezogen werden – weswegen sie auch im Gutachten thematisiert wurden. Ein mindestens ebenso wichtiges Kriterium ist meiner Meinung nach aber auch die Berücksichtigung der in Praxis existierenden Geräte, Techniken und Technologien und der durch sie definierte Stand der Technik. Und eben der wurde im ersten Teil des Gutachtens bereits beschrieben. Weswegen dann im zweiten Teil des Gutachtens nur noch die Standards als weiteres Kriterium besprochen wurden.
Zusätzlich ist es so, daß selbst wenn man Standards als alleiniges Kriterium für die Beantwortung der Fragestellung heranzieht, sich die Frage stellt, wie damit umzugehen ist, wenn nicht alle Standards eindeutig dieselbe Aussage treffen. Wie ist es zu bewerten, wenn einige Standards aus dem Bereich der IT-Sicherheit das Speichern von IP-Adressen vorschreiben, andere dazu schlicht keine Aussage treffen und wieder andere das Speichern verbieten? Soll man dann die Anzahl der entsprechenden Standards zählen, um so etwa mittels Mehrheiten zu einer Entscheidung zu gelangen? Soll man die Standards zuvor gemäß ihrer Wichtigkeit wichten? Und wenn ja, woran bemißt sich die Wichtigkeit eines Standards?
Letztlich sollte im Rahmen des Gutachtens also nur gezeigt werden, daß sich die Frage nicht eindeutig mit „Ja" bzw. „Nein" beantworten läßt, da weder die zitierten Standards noch der tatsächliche Stand der Technik eindeutig und übereinstimmend eine Speicherung von IP-Adressen vorschreiben bzw. vorsehen. Vielmehr kann man – je nach den der Interpretation der Begrifflichkeit „dient dem Stand der Technik" zugrunde gelegten Kriterien – sowohl ein „Ja" als auch ein „Nein" „beweisen".
Daß die aufgeworfenen Standards – die im Übrigen nur einen kleinen Bruchteil aller im IT-Sicherheitsbereich relevanten Standards darstellen – viel Spielraum für Interpretationen lassen, läßt sich in gewisser Weise auch dem Schriftwechsel der klagenden und beklagten Seite entnehmen.
Insofern handelt es sich nach Auffassung des Gutachters bei Beweisfrage 1 um eine nicht entscheidbare Frage.
Hier ist das ursprüngliche Gutachten tatsächlich ungenügend, da die Kommunikation des zuvor Beschriebenen offensichtlich nicht gelungen ist. Im Übrigen bleibe ich auf Grund der von mir der Interpretation der Begrifflichkeit „dient dem Stand der Technik" zugrunde gelegten Kriterien (Eindeutigkeit von Standards, tatsächlicher Stand der Technik) bei der im Gutachten getroffenen Aussage, daß die Speicherung von IP-Adressen nicht dem nationalen oder internationalen Stand der Technik dient.
Nachfolgend möchte ich noch kurz einige Klarstellung zu den Anmerkung 1.1 bis 1.5 vornehmen. Dies betrifft insbesondere die Punkte, wo neben der Interpretation der

klagenden bzw. beklagten Seite noch mindestens eine dritte existiert, nämlich die des Gutachters.

In Anmerkung 1.1 wird aus der in der Norm erwähnten Speicherung von „Benutzeraktivitäten" hergeleitet, daß hierzu „nur die IP-Adresse als notwendiges Mittel dienen kann." Dem wird widersprochen. Dies ergibt sich schon aus dem Anspruch der Norm: „Die in dieser Internationalen Norm festgelegten Anforderungen sind allgemeiner Natur und auf alle Organisationen anwendbar, unabhängig von Art, Größe und Beschaffenheit." Insbesondere werden mit der Norm also auch solche IT-Systeme adressiert, die – typsicherweise aus Sicherheitsgründen – gar nicht mit dem Internet verbunden sind. Insofern treten bei diesen Systeme gar keine IP-Adressen auf. Vielmehr liegt bei derartigen Systemen in der Regel die durch das System im Rahmen der Anmeldung bestimmte bzw. festgelegte Nutzerkennung (beispielsweise Loginname) den Auditprotokoll zur Benutzeraktivität zu Grunde.
Auch wenn ein IT-System mit dem Internet verbunden ist, so muß nicht zwangsweise die IP-Adresse zur Speicherung von Benutzeraktivitäten herangezogen werden. Auch bei derartigen Systemen ist es nicht unüblich, daß zunächst eine Benutzerauthentifizierung stattfindet, bevor überhaupt relevante Benutzeraktivitäten möglich sind. Insofern kann auch in diesen Fällen die vergebene Benutzerkennung benutzt werden, um die Benutzeraktivitäten in einem Auditprotokoll festzuhalten. Genau genommen wird in Anmerkung 2.1 von der Beklagten selbst eingeräumt, daß die IP-Adresse nicht geeignet ist, Benutzeraktivitäten aufzuzeichnen, denn es wird festgestellt: „Auch hier kennzeichnet die IP-Adresse jedoch nur das Absendergerät und nicht den Absender. ... Die IP-Adresse kennzeichnet, wenn man schon bei dem Vergleich bleiben will, allenfalls das Absender- bzw. Empfängergebäude."
Zu Anmerkung 1.2 ist nicht viel zu sagen, außer, daß im Gutachten ganz bewußt steht, daß die Speicherung von IP-Adressen der Erfüllung der Norm „dienen kann" und nicht „dient". Dies wird damit begründet, daß in der Norm steht, daß Auditprotokoll erstellt werden *sollten* und diese *sollten* dann, „sofern relevant" auch Netzadressen beinhalten. Der Begriff „sollten" wurde dabei – insbesondere in Abgrenzung zum Begriff „müssen" – bei der Erstellung der Norm ganz bewußt gewählt, da in der betreffenden Norm an viele anderen Stellen ganz ausdrücklich von „müssen" die Rede ist. Daraus ergibt sich, daß man die Norm auch erfüllen kann, wenn man keine IP-Adressen aufzeichnet. Ein Zwang zur Aufzeichnung von IP-Adressen kann jedenfalls nicht erkannt werden.

Zu Anmerkung 1.3 ist zu sagen, daß die Interpretation des Wortes „shall" korrekt ist. „Shall" drückt in der Tat eine Verpflichtung aus. Dies ergibt sich unter anderem aus Tabelle H.1 in „ISO/IEC Directives, Part 2". Dieses Dokument legt die allgemeinen Regeln für das Schreiben von internationalen ISO/IEC Standards fest.
Allerdings wurde im Gutachten auch nie anderes behauptet. Im Gutachten heißt es: „Andererseits ist ... lediglich ganz allgemein vorgesehen: ‚The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of the event, subject identity and the outcome ... of the event; ...'". Der Ausdruck „ganz allgemein" bezieht sich dabei unter anderem auf den Term „subject identity". Und mit diesem ist eben nicht zwangsweise eine IP-Adresse gemeint. So wird im betreffenden Standard unter anderem zwischen „user identity", „subject identity" und

„host identity" unterschieden. Wie in dem in Anmerkung 1.3 aufgeführten Beispiel eines Web-Zugriffes sehr richtig festgestellt, kennzeichnet die IP-Adresse (bestenfalls) „das zugreifende System". Und hier scheint es dann eher naheliegend zu sein, von „host identity" und nicht von „subject identity" zu reden.
Der Standard selbst geht an verschiedenen Stellen auf den Begriff des „subject" ein. Zunächst heißt es in Abschnitt 5 „Functional requirements paradigm": „The SFRs [security functional requirements] may define multiple Security Function Policies (SFPs) to represent the rules that the TOE must enforce. Each such SFP must specify its scope of control, by defining the subjects, objects, resources or information, and operations to which it applies." Dies bedeutet, daß sich die konkreten „subjects" erst aus der funktionalen Beschreibung eines gegebenen Systems ergeben.
Jedoch wird zumindest definiert, was ein „subject" sein kann und was nicht. Dazu heißt es:
„Active entities in the TOE that perform operations on objects are referred to as subjects. Several types of subjects may exist within a TOE:
a) those acting on behalf of an authorised user (e.g. UNIX processes);
b) those acting as a specific functional process that may in turn act on behalf of multiple users (e.g. functions as might be found in client/server architectures); or
c) those acting as part of the TOE itself (e.g. processes not acting on behalf of a user).
This part of ISO/IEC 15408 addresses the enforcement of the SFRs over types of subjects as those listed above."

Nimmt man hier als konkretes „subject" den in obiger Definition beispielhaft angesprochenen UNIX-Prozeß, so stellt eine IP-Adresse in diesem Fall jedenfalls keine „subject identity" dar. Unklar bleibt darüber hinaus, ob das zugreifende Host-System – betrachtet hier für den Fall, daß man annimmt eine IP-Adresse dient als identity des zugreifenden Hostsystems – im Sinne des Standards ein „subject" sein kann. Hier ist folgende Formulierung zusätzlich relevant: „Passive entities in the TOE that contain or receive information and upon which subjects perform operations are called objects. In the case where a subject (an active entity) is the target of an operation (e.g. interprocess communication), a subject may also be acted on as an object." Es scheint nicht ganz abwegig, das zugreifende Hostsystem eher als „object" denn als „subject" zu sehen, da es aus sich selbst heraus nicht aktiv ist. Vielmehr sind es die auf einem System laufenden Prozesse, die die Aktivität des Systems bestimmen.

Ferner sei darauf hingewiesen, daß es in der aktuelle Version[11] von ISO/IEC 15408-2 nunmehr heißt:
„7.2.5.2 FAU_GEN.1.2
The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity (**if applicable**), and the outcome (success or failure) of the event; ..."

Bezüglich der „subject identitiy" stellt der Standard also klar, daß es nicht in jedem Fall möglich bzw. notwendig ist, diese zu speichern. Insbesondere ist es also nicht notwendig, krampfhaft nach irgend etwas zu suchen, daß aus dem einen oder anderen

[11] ISO/IEC 15408-2, Third edition 2008-08-15, Corrected version 2011-06-01

Beweggrund heraus als Ersatz für eine sinnvolle „subject identity" herangezogen wird. Man kann dieses Element schlicht weglassen.
Das bereits mehrfach erwähnte Zitat aus Abschnitt 7.2.5.2 ist im Übrigen in Zusammenhang mit Abschnitt 7.2.5.1 zu lesen. Dort heißt es:
„The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the [selection, choose one of: minimum, basic, detailed, not specified] level of audit; and
c) [assignment: other specifically defined auditable events]."

Zunächst fällt auf, daß es heißt: „shall be able to generate" und nicht „shall generate". Darüber hinaus kann der Autor eines konkreten Protection Profiles den Umfang der Erstellung von „audit records" festlegen. Insbesondere wird im Standard selbst auch offen gelassen, was zum „minimum level of audit" zu zählen ist. Dies wird vielmehr ebenfalls durch den Autor eines konkreten Protection Profiles festgelegt. Ob also etwa der Zugriff eines Host-Systems überhaupt zu den „auditable events" zu zählen ist, hängt von einem konkreten Protection Profile ab und ist jedenfalls im Standard nicht definiert.
Aus all den dargelegten Beweggründen bleibt der Gutachter bei der bereits im Gutachten getroffenen Aussage, „daß sich aus ISO 15408 keine Notwendigkeit zur Speicherung von IP-Adressen ergibt".

Zu Anmerkung 1.4 sei nur gesagt, daß es sich beim BSI-Grundschutzhandbuch um ein Sammelwerk handelt, daß viele verschiedene Szenarien und Anwendungsfälle von Informations- und Kommunikationstechnologie behandelt. Wie die Beklagte zu dem Schluß kommt, daß, wenn in einem Szenario (beispielsweise: Betrieb eines Web-Servers) das Speichern von IP-Adressen vorgeschrieben und insofern notwendig ist, dies dann auch für alle anderen damit nicht in Zusammenhang stehenden Szenarien (beispielsweise: Betrieb eines Mail-Servers) gilt, kann nicht nachvollzogen werden. Wollte man dieser Art der Argumentation folgen, so ließe sich auch die in Maßnahme 5.71 in manchen Fällen als notwendig angesehene Pseudonymisierung (von etwa IP-Adressen) verallgemeinern, so daß man dann schließen könnte, daß es immer notwendig ist, das IP-Adressen nur pseudonymisiert gespeichert werden. Der Gutachter hält – wie bereits angedeutet – diese Art der Argumentation für abwegig. Insofern bleibt es bei der bereits im Gutachten getroffenen Feststellung, daß die Frage, ob das Speichern von IP-Adressen für die Erfüllung des BSI-Grundschutzes notwendig ist oder nicht abhängt von dem konkret betriebenen System und insofern jedenfalls nicht allgemein notwendig ist.

Zu Anmerkung 1.5 ist zunächst zu sagen, daß die betreffende technische Richtlinie in der Tat nur das „wie" und nicht das „ob" behandelt. Ob dies wiederum für die Beweisfrage relevant ist, vermag ich als Nichtjurist nicht zu sagen. Die Erwähnung der Norm ist für das Gutachten als solches jedenfalls relevant. Im Gutachten wird nämlich behauptet, daß das unverschlüsselte Speichern von IP-Adressen als veraltet anzusehen ist. Insofern soll die Erwähnung der technischen Richtlinie als ein Beleg für diese Behauptung gelten. Gerade die Beklagte merkt ja in Anmerkung 1. an, daß „der Stand der Technik durch internationale Empfehlungen, Standards und Regulierungen

definiert wird." Insofern ist das unverschlüsselte Speichern von IP-Adressen als veraltetet anzusehen, da nicht mehr – dem durch die technische Richtlinie definierten – Stand der Technik entsprechend.
Auch werden aus Sicht des Gutachters die Fragen des „ob" und „wie" nicht vermischt. Dies wäre nur der Fall, wenn das verschlüsselte Speichern von IP-Adressen eben einfach nur das „wie" beschreiben würde. Vielmehr ist es so, daß die besondere Form des „wie" das „ob" in Frage stellt. Oder anders gesagt: Die Beantwortung der Frage, ob bei geeigneter Verschlüsselung im Ergebnis tatsächlich noch von gespeicherten IP-Adressen geredet werden kann, ist eher philosophischer als technischer Natur – stellt also in jedem Fall etwa qualitativ ganz anderes da. Dies gilt natürlich nur, wenn die Verschlüsselung so erfolgt, daß eine Rückbestimmung der in den Verschlüsselungsalgorithmus eingeflossenen IP-Adressen aus dem Ergebnis der Verschlüsselung nicht oder nur mit unrealistisch hohem Aufwand möglich ist. Wie in der Anmerkung richtig aufgeführt, ist für die Rückgewinnung des Klartextes die Kenntnis von (geheimer) Information notwendig. Steht nun diese Information nicht zur Verfügung – etwa weil sie bei der Initialisierung des kryptographischen Systems nicht erzeugt wurde oder weil sie einen hardwaregeschützten Speicher nicht verlassen kann – so kann jemand, der nur Zugriff auf die verschlüsselten Daten hat, nicht bestimmen, welche IP-Adressen ursprünglich als Eingabe für die Verschlüsselung verwendet wurden. Oder anders gesagt: Bezüglich eines gegebenen Schlüsseltextes und einer beliebig gewählten IP-Adresse läßt sich immer ein Entschlüsselungsschlüssel finden, so daß die Entschlüsselung des Schlüsseltextes eben genau die gewählte IP-Adresse ergibt. Der gespeicherte Schlüsseltext enthält also bei Unkenntnis des Schlüssels gemäß der Shannonschen-Informationstheorie 0 Bit Information über die Klartext-IP-Adressen. Und aus dieser quantitativen Betrachtung („0 Bit") ergibt sich eben ein qualitativer Unterschied bezüglich des „ob".
Dieser qualitative Unterschied – der aus Sicht des Gutachters existiert – ist für das Gutachten wiederum deshalb relevant, weil im Rahmen der Beantwortung von Beweisfrage 2 die Ersetzung von IP-Adressen durch eindeutige Kennzeichen als eine Maßnahme im Rahmen von Intrusion Detection Systemen vorgeschlagen wird, die dann eben – zumindest nach Auffassung des Gutachters – ohne Speicherung von IP-Adressen auskommt.
Was die im weiteren Verlauf der Anmerkung 1.5 getroffenen Erläuterungen zum Thema „Verschlüsselung", „Pseudonymisierung" und „Anonymisierung" mit dem Gutachten konkret zu tun haben ist nicht ersichtlich, weswegen eine Kommentierung hier unterbleiben soll, auch wenn der Gutachter mit den getroffen Ausführungen bezüglich „Verschlüsselung", „Pseudonymisierung" und „Anonymisierung" aus technischer Sicht nicht übereinstimmt.

Aus den insgesamt zur Beweisfrage 1 – hier und im ursprünglichen Gutachten – dargelegten Gründen widerspricht der Sachverständige nach wie vor der Behauptung „dass die Speicherung in vielen aktuellen Empfehlungen, Standards und Regulierungen als erforderliche Maßnahme zum Schutz von IT-Systemen genannt ist." Vielmehr gilt, daß es durchaus Standards gibt, die das fordern und andere, die es eben nicht fordern.

Wie der Gutachter zu der Auffassung kommt, daß die Fragestellung: „dient dem Stand der Technik" nicht entscheidbar ist und das insbesondere hier weder ein klares „ja" noch „nein" möglich ist, wurde oben bereits umfänglich dargelegt.
Hier sein nur angemerkt, daß im Gutachten an keiner Stelle behauptet wurde, daß die erwähnten Standards und Normen veraltet sind. Das Wort „veraltet" kommt im Gutachten an genauer einer Stelle vor – und zwar lediglich in Bezug auf das (unverschlüsselte) Speichern von IP-Adressen.

Kommentierung der Anmerkungen des Rechtsanwalts Meinhard Starostik

Nachfolgend soll die Anmerkungen des Rechtsanwalts Meinhard Starostik (Band 3 Blatt 116ff) kommentiert werden.

Zu Anmerkung 1:
Wie oben bereits ausgeführt, sieht der Gutachter schon einen Unterschied zwischen dem verschlüsselten bzw. nicht-verschlüsselten Speichern von IP-Adressen. Wobei hier zu Grunde gelegt wird, daß die Verschlüsselung so gestaltet wird, daß ein Entschlüsseln nicht mit realistischen Aufwand möglich ist (Details siehe oben).
Insofern besteht damit ganz grundsätzlich auch Schutz gegenüber der Beklagten, da auch sie – vereinfacht ausgedrückt – nicht im Besitz des Entschlüsselungsschlüssels ist. Auf der anderen Seite schützt auch ein komplettes Verbot jeglicher Art der Speicherung von IP-Adressen – inklusiver aller wie auch immer gearteten verschlüsselten Formen – nicht davor, daß ein (böswilliger) Mitarbeiter der Beklagten die Internetnutzung des Klägers ausspioniert. Ein böswilliger Administrator könnte schlicht ohne Wissen der Beklagten eine Speicherung durchführen. Insofern muß der Kläger darauf vertrauen, daß die bei der Beklagten implementierten Prozesse (Mehraugen-Prinzip, Audits etc.) dafür sorgen, daß auch tatsächlich nichts gespeichert wird. Dieses notwendige Vertrauen ist dem Vertrauen vergleichbar, daß der Kläger im Falle der verschlüsselten Speicherung bezüglich der tatsächlichen Nichterzeugung bzw. unmittelbaren Löschung der.Entschlüsselungsschlüssel aufbringen muß.
Will der Kläger sich ohne jegliches Vertrauen in die Beklagte vor der erwähnten Ausspionierung schützen, so bleibt dem Kläger nichts anderes übrig, als einen der erwähnten Anonymisierungsdienste zu verwenden. Nur so kann er verhindern, daß die Beklagte (oder einer ihrer Mitarbeiter) mißbrauchbare Informationen überhaupt erhält.

Zu Anmerkung 2:
Diese Anmerkung verweist auf die Schriftsätze des Klägers vom Juni 2010 (Punkt 4) und vom Oktober 2010 (Punkte 3 und 4).
Zunächst sollen die wiederkehrenden und insofern eher allgemeinen Aussagen dieser Schriftsätze kommentiert und anschließend noch auf einige Details eingegangen werden.
Anzumerken ist zunächst, daß beim Erstellen des Gutachtens nicht nur Web-Server berücksichtigt wurden, sondern allgemein IT-Systeme bzw. Telemedien und Telekommunikationsnetze.
Nach Auffassung des Gutachters werden in den Schriftsätzen unter anderem folgende Behauptungen aufgestellt:
1. IT-Sicherheit bedeute im Wesentlichen, daß Systeme so „fachgerecht eingerichtet und betrieben" werden, daß die Wahrscheinlichkeit eines erfolgreichen Angriffs von vorne herein so gering wie irgend möglich ist und das insofern der zusätzliche Sicherheitsgewinn, der durch das Aufzeichnen von Nutzeraktivitäten möglich sein mag, bestenfalls gering ist.

2. Intrusion Detection Systeme leisten nur einen geringen Beitrag für den sicheren Betrieb eines IT-Systems und können im Extremfall sogar negative Auswirkungen haben.
3. Sperrlisten sind nicht geeignet, um den Schutz des betreffenden IT-Systems signifikant zu verbessern.
Zu 1.) ist festzustellen, daß der Gutachter der gleichen Auffassung ist, was insbesondere in dem hier vorliegenden Dokument im Abschnitt „Allgemeine Anmerkungen" nachzulesen ist.

Zu 2.) Auf der einen Seite hat auch der Gutachter eine durchaus kritische Haltung zur Wirksamkeit von Intrusion Detection Systemen. Jedenfalls treten die angesprochenen Probleme: Schwierigkeit der richtigen Parametrisierung, Erkennung unbekannter Angriffe, Fehlalarme, leichte Vermeidung von Entdeckung durch intelligente Angreifer etc. in Praxis tatsächlich auf und sind bisher nicht wirklich gelöst.
Auf der anderen Seite scheinen die Ausführungen des Klägers in ihrer Tendenz doch zu stark die generelle Unwirksamkeit von Intrusion Detection Systemen herauszustellen. Hier ist der Gutachter anderer Auffassung, d.h. Intrusion Detection Systeme können prinzipiell sehr wohl einen Beitrag zur IT-Sicherheit leisten. Auf Grund der oben erwähnten Unzulänglichkeiten aktueller Intrusion Detection Systeme ist aber zu prüfen, ob nicht andere Maßnahmen existieren, die wesentlich besser geeignet sind, das gewünschte Ziel zu erreichen. Ob der Einsatz eines Intrusion Detection Systems daher zwingend notwendig ist, hängt vom konkreten IT-System ab.
Zusätzlich ist es so, daß auch im Rahmen von Intrusion Detection Systemen nicht zwingend die Speicherung von IP-Adressen der zugreifenden Host-Systeme erforderlich ist.
Konkret wird im Schriftsatz des Klägers vom Juni 2010 die Wirksamkeit eines Intrusion Detection Systems zur Erkennung und somit letztlich zur Abwehr von DoS-Angriffen angesprochen. Hier wird insbesondere angemerkt, daß „die von der Beklagten genutzte Hardware und Software so eingerichtet werden [muß], daß solche Angriffe erfolglos bleiben". Dies könnte zunächst so interpretiert werden, daß die Hardware leistungsfähig genug sein muß, daß auch im Falle eines Angriffs der entsprechende Dienst für berechtigte Nutzer verfügbar bleibt. Anschaffung und Betrieb einer derart dimensionierten Hardware ist aber – legt man etwa die Größe üblicher Botnetze und die durchschnittlich einem Botnetz-Rechner zur Verfügung stehende Upstream-Bandbreite zu grunde – mit enormen Kosten verbunden und wirtschaftlich nicht sinnvoll.
Insofern ist es für eine erfolgreiche Angriffsabwehr notwendig, die Angriffssituation zu erkennen, um dann entsprechende Maßnahmen einzuleiten. Auf der anderen Seite ist es generell nicht in jedem Fall möglich, den Angriff erfolgreich abzuwehren. Dies gilt insbesondere dann, wenn bei einem konkreten DoS-Angriff eine Vielzahl von Rechnern angreift, wobei jeder einzelne Rechner nur Erlaubtes und insofern Unverdächtiges tut – etwa einen üblichen Web-Seiten-Abruf durchführt. Selbst wenn das System eine Überlastsituation prinzipiell feststellt, so kann es nicht entscheiden, welche Anfragen dem Angreifer zuzuordnen sind und bei welchen Anfragen es sich um Anfragen „normaler" Nutzer handelt. Insofern ist auch eine ausschließliche Sperrung der „unberechtigten" Anfragen nicht möglich.

Allerdings existieren andere Arten von DoS-Angriffen, bei denen eine Erkennung und entsprechende Abwehrmaßnahmen sehr wohl sinnvoll möglich sind. Ein typischer Vertreter ist hier das sogenannte „Flooding". Dabei sendet jeder angreifende Rechner soviel Anfrage, wie es die Bandbreite seiner Internet-Anbindung gestattet. Diese Abweichung vom Verhalten eines „normalen" Nutzers des angebotenen Dienstes ist durch ein Intrusion Detection System durchaus feststellbar. Und selbst wenn das Intrusion Detection System fälschlicherweise einem Nutzer „abnormales" Verhalten unterstellt und insofern als Angreifer klassifiziert, so ist dies aus Sicht des Nutzers nicht unbedingt negativ. Als eine Abwehrmaßnahme kann nämlich zunächst die „Anfragehäufigkeit" der „abnormalen" Nutzer auf das statistisch ermittelte „übliche" Maß reduziert werden. Diese Drosselung kann mit Hilfe von Firewalls geschehen. Im Ergebnis bedeutet dies für einen fälschlicherweise „gedrosselten" Nutzer zwar eine Verringerung der von ihm erwarteten Servicequalität des Dienstes, da der Nutzer ja nicht mehr so schnell Anfragen stellen kann, wie er es gern möchte. Wird auf diese Art aber die Überlastung des Systems vermieden, so bekommt er wenigstens überhaupt eine Antwort, was in jedem Fall besser ist, als viele Anfragen zu stellen und keine Antwort zu bekommen.
Insofern kann die Auswertung von Daten im Allgemeinen und die Verwendung eines Intrusion Detection Systems im Besonderen durchaus eine Rolle bei der Erkennung und Abwehr von DoS-Angriffen spielen. Dies bedeutet wiederum nicht, daß im geschilderten Fall das Speichern von IP-Adressen der zugreifenden Host-Systeme notwendig ist. Zur Ermittlung des „üblichen" Nutzer-Verhaltens reicht das Erfassen anonymisierter, statistischer Daten. Für die Erkennung einer (drohenden) Überlastsituation können die in den Anmerkungen erwähnten Testverbindung bzw. andere Indikatoren (Prozessor- sowie Hauptspeicherauslastung etc.) herangezogen werden. Auch für die Identifizierung der „unüblichen" Verbindungen ist eine permanente Speicherung der IP-Adressen der zugreifenden Host-Systeme nicht notwendig. Vielmehr erfolgt die entsprechende Analyse ausschließlich mittels im Hauptspeicher gespeicherter Daten. Auch für die Durchführung entsprechender Gegenmaßnahmen – temporäre Reduktion der erlaubten Zugriffe – ist eine permanente Speicherung der betreffenden IP-Adresse nicht erforderlich. Vielmehr erfolgt auch hier die Speicherung der notwendigen Daten im Hauptspeicher.
Abschließend sei noch angemerkt, daß für Angriffserkennung und Abwehr das bereits mehrfach erwähnte Ersetzungsverfahren angewendet werden kann.

Zu 3.) ist festzustellen, daß auch der Gutachter die Nützlichkeit von Sperrlisten für die Umsetzung von IT-Sicherheit in Frage stellt. Zunächst ist jedoch anzumerken, daß sich auch im Falle des Einsatzes von Sperrlisten pathologische Beispiele konstruieren lassen, in denen die Sperrlisten nützlich sind. So ist vorstellbar, daß ein Angreifer, der über entsprechend große Ressourcen im Sinne von Hardware und Bandbreite verfügt, seine DoS-Angriffe unter Benutzung der immer gleichen, statischen Absender-IP-Adresse ausführt. Gegen einen derartigen Angriff/Angreifer können Sperrlisten durchaus einen wirkungsvollen Abwehrmechanismus darstellen.
Auf der anderen Seite widerspricht dieses Beispiel der im Internet anzutreffenden üblichen Praxis von dynamisch vergebenen IP-Adressen. Der Beklagte bringt in Anmerkung 2.4 das Problem auf den Punkt, indem dort festgestellt wird: „Völlig unklar ist darüber hinaus, wie die Beklagte nach Ansicht des Sachverständigen zu der IP-

Adresse, welche in der Firewall als potentieller Angreifer gespeichert werden soll, kommen soll". Das ist in der Tat völlig unklar – und zwar unabhängig davon, ob IP-Adressen gespeichert werden oder nicht, ob die vom Sachverständigen vorgestellte Ersetzung verwendet wird oder nicht etc.
Ein Teil des Problems beruht auf den oben geschilderten DoS-Angriffen, bei denen jeder zugreifende Rechner nur Erlaubtes in üblicher und unverdächtiger Art und Weise tut. Insofern kann nicht zwischen angreifenden und „normalen" Rechnern unterschieden werden. In der Konsequenz bleibt nur, alle IP-Adressen in die Sperrliste aufzunehmen, was letztlich bedeutet, daß der Dienst für niemanden mehr erreichbar ist und insofern der DoS-Angriff erfolgreich war, was ja gerade verhindert werden sollte.
Selbst wenn es gelingt, bezüglich des aktuellen Zeitpunktes festzustellen, daß von einer konkreten IP-Adresse ein Angriff ausgeht, so kann diese IP-Adresse nicht einfach in eine Sperrliste aufgenommen werden. Zum einen kann der Angreifer leicht eine andere IP-Adresse verwenden – im einfachsten Fall, indem er seine Verbindung zum Internet trennt und neu aufbaut und im Rahmen dessen eine neue dynamische IP-Adresse erhält. Zum anderen kann die ursprünglich vom Angreifer verwendete dynamische IP-Adresse mittlerweile einem „ehrlichen" Nutzer zugewiesen worden sein, so daß dieser dann fälschlicherweise nicht mehr auf das Angebot zugreifen kann. Insofern wird auch durch den Gutachter die Nützlichkeit eine Sperrliste, die auf IP-Adressen von zugreifenden Host-Systemen basiert, stark angezweifelt.

Neben diesen eher allgemeinen Betrachtungen sollen nun noch einige konkrete Anmerkungen zu einzelnen Punkten des Schriftsatzes des Klägers vom Juni bzw. Oktober 2010 besprochen werden, wobei hier nur Punkte aufgegriffen werden, wo der Gutachter eine andere Meinung vertritt als im jeweiligen Schriftsatz enthalten.

Zu c) Drittmeldungen (aus Schriftsatz vom Juni 2010)
Zwar sind die beschriebenen Maßnahmen korrekt, d.h. Sicherheitslücken müssen unabhängig von deren Ausnutzung geschlossen werden, Schadprogramme müssen beseitigt werden und eine Sperrung von IP-Adressen ist ohne eigene Protokollierung möglich.
Auf der anderen Seite kann eine Protokollierung der Zugriffe hilfreich sein, um besser bewerten zu können, ob aus einer Sicherheitslücke ein Schaden entstanden ist und ggf. welcher.
Prinzipiell lassen sich Sicherheitslücken nicht 100%ig vermeiden. Sie lassen sich typsicherweise erst dann schließen, wenn der Hersteller ein entsprechendes Sicherheitsupdate bereitstellt (was in manchen Fällen Jahre dauern kann) oder wenn wenigstens allgemein auf ein Sicherheitsproblem in einem gegebenen Produkt hingewiesen wird, so daß ein Alternativprodukt verwendet werden kann.
Erfährt der Betreiber eines IT-Systems also, daß das von ihm betriebene System (zeitweise) eine Sicherheitslücke hatte, die prinzipiell von einem Angreifer hätte ausgenutzt werden können, so stellt sich für den Betreiber die Frage, wie er darauf reagieren soll.
Am einfachsten läßt sich die Frage für den Fall beantworten, in dem das betroffene System selbst nicht primär für die Datenspeicherung verantwortlich ist. Handelt es sich beispielsweise um einen Web-Server, bezüglich dessen der primäre Speicher der

auszuliefernden Web-Seiten ein getrennt arbeitendes (Datenbank-)System ist, so kann der betreffende Web-Server einfach komplett neu installiert werden. Es ist insofern unerheblich, ob der Web-Server tatsächlich angegriffen wurde oder nicht. Protokollierung ist hier tatsächlich nicht erforderlich.
Ist allerdings der primäre Informationsspeicher selbst betroffen, so ist die Situation ungleich schwieriger. Insbesondere löst ein Backup das Problem nicht, da sich im Backup letztlich nur eine Kopie der Manipulationen befindet. Ist beispielsweise ein Datenbanksystem betroffen, so muß versucht werden die „erlaubten" Transaktionen von den Manipulationen zu unterscheiden und es muß versucht werden, die Manipulationen rückgängig zu machen. Letzteres kann aber sehr Kostenintensiv sein – insbesondere wenn „erlaubte" Transaktionen auf zuvor manipulierten Daten basieren. Letztlich wird man vielfach auch nicht mit Sicherheit sagen können, ob eine Manipulation vorliegt oder nicht. Vielmehr geht es eher um Wahrscheinlichkeiten, d.h. Indizien die dafür oder dagegen sprechen. Gegeben die mit einer tatsächlich stattgefundenen Manipulation verbundenen Kosten kommt es darauf an, die Wahrscheinlichkeit einer Fehleinschätzung zu minimieren. Für all dies können (Zugriffs-)protokolle hilfreich sein.
Inwiefern die Speicherung der IP-Adressen der zugreifenden Host-Systeme hier relevant ist oder nicht muß ein Einzelfall geprüft werden. Sie kann aber in manchen Fällen dafür durchaus nützlich sein.

Zu e) Schadprogramme (aus Schriftsatz vom Juni 2010)
Hier sei nur angemerkt, daß das Verfahren der „regelmäßigen Integritätsprüfung" sicher geeignet ist, wenn es einen adäquaten Vergleichswert gibt – wie etwa bei einem Web-Server, der selbst keiner Veränderung unterliegt und dessen Daten in Form der auszuliefernden Web-Seiten auf einem anderen System (zusätzlich) gespeichert sind.
Das Verfahren läßt sich jedoch nicht zur Erkennung von Manipulationen an sich üblicherweise verändernden Daten – wie etwa im Falle eines Datenbanksystems – anwenden. Dies wurde entsprechend gerade diskutiert.

Zu Punkt 3 aus dem Schriftsatz vom Oktober 2010 ist nach Ansicht des Gutachters alles Relevante bereits im Gutachten bzw. in den hier vorliegenden Erläuterungen gesagt.

Zu **Punkt 4 aus dem Schriftsatz vom Oktober 2010** ist zunächst anzumerken, daß nachfolgend nur kommentiert wird, was nicht eh schon auf Grund des bisher gesagten klar ist.
Bezüglich des ersten Absatzes ist anzumerken, daß es aus Sicherheitssicht durchaus empfehlenswert ist, den eigentlichen Web-Server und die Datenbank auf getrennten Systemen zu betreiben, die wiederum beide abgeschottet vom internen Netz zu betreiben sind. Sinnvoll scheint es hier zu sein, sowohl Web- als auch Datenbank-Server in einer DMZ[12] zu betreiben, wobei diese ggf. zweistufig auszurichten ist, da davon auszugehen ist, daß der Datenbank-Server dem internen Netz „näher" steht als

[12] DeMilitarized Zone, eine bildliche Beschreibung der Tatsache, daß ein System sowohl vom öffentlichen Netz als auch vom internen Netz abgeschottet betrieben wird.

der Web-Server, da die auf dem Datenbank-Server hinterlegten Daten in der Regel durch Mitarbeiter – die sich wiederum im internen Netz befinden – bereitgestellt wird. Im übrigen hält auch der Gutachter das Prinzip „nur das Notwendig" – im Sinne der installierten bzw. aktivierten Dienste, Programme, Prozesse und Protokolle – für ein allgemein anerkanntes Prinzip der IT-Sicherheit. Die Idee von „Nur das Notwendige" findet sich auch im verwandten Prinzip der „least privileges" wieder – also des Prinzips, daß Nutzer nur diejenigen Rechte (aus technischer Sicht) im System haben sollten, die zur Erfüllung ihrer Aufgaben unbedingt notwendig sind. Beide Prinzipien wurden durch den Gutachter etwa im Rahmen des Anonymisierungsdienstes AN.ON umgesetzt.
Bezüglich des dritten Absatzes und der darin aus einer Studie übernommene Zahl, daß „nur 20% den Vorfall an Strafverfolgungsbehörden zu Weiterverfolgung meldeten" wird bestritten – sofern dies durch den Kläger mit der Nennung der Zahl zum Ausdruck gebracht werden sollte – daß die verbleibenden 80% eine Meldung aus IT-Sicherheitsbezogenen Vernunftserwägungen heraus unterließen. Die Interpretation des Gutachters ist hier vielmehr, daß die erwähnten 80% schlicht vermeiden wollten, daß der Name des jeweiligen Unternehmens in Zusammenhang mit IT-Sicherheitsproblemen (öffentlich) erwähnt wird (etwa durch ein entsprechendes Informationsleck bei den Strafverfolgungsbehörden).
Zur „regelmäßigen Integritätsprüfung" wurde bereits einiges gesagt. Wie bereits erwähnt kann diese Maßnahme in einigen Szenarien sinnvoll sein – in andere scheint eine sinnvolle Anwendbarkeit jedoch nicht gegeben. Im entsprechend Grundschutzbaustein sind selbst eine Reihe von Einschränkungen und Abwägungen genannt, etwa: „Im normalen Betrieb jedes größeren IT-Systems ergeben sich ständig kleinere und größere Änderungen an Systemdateien. Generell ist es daher empfehlenswert, das Integritätsprüfungsprogramm so zu konfigurieren, dass nur Veränderungen an relevanten Dateien erfasst werden." Auf diese Weise lassen sich also Manipulationen an „relevanten Daten" erkennen, auf der anderen Seite werden Systemdateien ausgenommen, die wiederum im Fall eines Befalls durch Schadsoftware besonders häufig betroffen sind. Insofern bleiben die Daten zwar „geschützt", das System als Ganzes ist aber kompromittiert.
Im übrigen wurde oben bereits bezweifelt, daß im Falle von Datenbanken der Baustein „regelmäßige Integritätsprüfung" sinnvoll angewendet werden kann.

Abschließend soll noch angemerkt werden, daß der Aussage widersprochen wird, „dieses Risiko [die Abschottung des Webserver zu durchbrechen] kann durch eine physische Trennung von sonstigen Systemen ausgeschlossen werden." Konkret wird die Formulierung „kann ausgeschlossen werden" als Ausdruck der Unmöglichkeit interpretiert. Und dem wird widersprochen.
Zwar ist eine physische Trennung unzweifelhaft geeignet, das Durchbrechen der Abschottung des Web-Servers für einen Angreifer deutlich zu erschweren. Auf der anderen Seite impliziert eine physische Trennung in den seltensten Fällen auch eine logische Trennung. Typischerweise finden bidirektionale Informationsflüsse zwischen dem Web-Server und Rechnern von Mitarbeitern statt. So wäre es nicht untypisch, daß ein Mitarbeiter die Web-Seiten an seinem Rechner erstellt und dann in die Datenbank bzw. auf den Web-Server überträgt. Im Falle einer Netzseitigen physischen Trennung könnte dazu beispielsweise ein USB-Stick benutzt werden. Umgekehrt

treffen auf einen Web-Server Daten und Dokumente eine, die durch Mitarbeiter zu bearbeiten sind – etwa wenn auf der Web-Seite ein Kontaktformular angeboten wird oder – im Falle der Beklagten sicher nicht unüblich – wenn Bürger ausgefüllt Formulare in Form von beispielsweise Word- oder PDF-Dokumenten auf den Web-Server „hochladen" (speichern). Auch diese Dokumente müssen in geeigneter (elektronischer) Form vom Web-Server auf die Rechner der Mitarbeiter transportiert werden.
Angriffsmöglichkeiten bieten sich hier zum einen durch den Transport selbst – etwa wenn sich eine auf dem Web-Server im Rahmen eines Angriffs hinterlegte Schadsoftware auf den USB-Stick aus obigem Beispiel kopiert. Wird der USB-Stick nun an den Rechner eines Mitarbeiters eingesteckt, so kann sich die Schadsoftware hier ggf. weiterverbreiten. Natürlich existieren auch in diesem Szenario mögliche Gegenmaßnahmen – so könnte der USB-Stick zuvor auf Befall durch Schadsoftware untersucht werden. Letztendlich gibt es aber keinen 100%ig Schutz – insbesondere, wenn es sich um eine bisher unbekannte Schadsoftware handelt.
Als weiterer Angriffspunkt bleiben die Daten und Dokumente selbst. Handelt es sich um Word- oder PDF-Dokumente, so stellen sie durchaus ein Risiko dar. Natürlich kann auch hier versucht werden, die Dokumente zuvor auf Befall durch Schadsoftware zu untersuchen. Wie bereits erläutert gelingt dies nicht immer.

Zu Anmerkung 3:
Es ist zutreffend, daß in ISO/IEC 27002 – wie im Übrigen in einer ganzen Reihe weiterer Standards aus dem Bereich der IT-Sicherheit – auf einschlägige gesetzliche Bestimmungen verwiesen wird, die – etwa im Rahmen der Aufzeichnung von Audit- oder sonstigen Protokollen – zu beachten sind.
Allerdings wurden derartige, in den Standards und Normen enthaltene juristische Bezüge bei der Bewertung der Frage, ob ein konkreter Standard nun die Speicherung von IP-Adressen vorschreibe, empfehle, verbiete etc. nicht berücksichtigt. Zum einen ist der Gutachter wie bereits mehrfach erwähnt kein Jurist und kann schon aus diesem Grunde die entsprechende juristischen Bemerkungen nicht sinnvoll bewerten und einschätzen. Zum anderen ist der Gutachter davon ausgegangen, daß im Rahmen des Verfahrens ja gerade untersucht werden soll, ob ein Speichern von IP-Adressen der zugreifenden Host-Systeme zulässig ist oder nicht und insofern im Einklang mit geltenden rechtlichen Regelungen steht. Daher wäre eine Argumentationskette der Art: Im Standard wird auf die Einhaltung rechtlicher Regelungen verweisen; deshalb verbietet der Standard das Speichern von IP-Adressen; und dies ist wiederum der Grund, warum das Gericht zu der Entscheidung kommen soll, daß damit aus rechtlicher Sicht ein Speichern von IP-Adressen nicht zulässig ist. Bei einer derartigen Argumentation würde es sich letztlich um einen Zirkelschluß handeln – was durch den Klagenden selbst in Anmerkung 6 entsprechend thematisiert wird. Insofern wurde versucht, bezüglich der Standards und Normen ausschließlich unter Benutzung der technischen Informationen und Details zu argumentieren.

Zu Anmerkung 4:
Zunächst wird behauptet, „Telemedien der Beklagten, die der Information der Öffentlichkeit dienen und damit jedermann zur Verfügung stehen [können] nicht ‚unberechtigt' genutzt werden." Hier soll zunächst nochmal an den oben erwähnten „Ping-of-Death" erinnert werden. Dem „Ping-of-Death" liegt dabei ein nützliches

Protokoll, nämlich das Ping-Protokoll zu Grunde. Nutzfunktion ist dabei, aus der Ferne zu prüfen, ob ein gegebener Rechner aus dem Netz erreichbar ist. Dazu wird ein IP-Paket (das sogenannte Echo-Request-Paket) an den zu überprüfenden Rechner gesendet. Dieser antwortet darauf Protokollgemäß ebenfalls mit einem IP-Paket (Echo-Response-Paket), was schlußendlich zu der Annahme führt, daß der betreffende Rechner erreichbar ist. Das zugehörige Ping-Programm ist dabei unter anderem im Dokument RFC-2151[13] beschrieben und das dem Ping-Protokoll zugrundeliegende ICMP-Protokoll in RFC-792[14].

Beim „Ping-of-Death" ist es nun so, daß ein Angreifer ein gemäß den erwähnten Standards korrektes Ping-Paket an den angegriffenen Rechner sendet. Durch Implementierungsfehler kam es allerdings in der Regel dazu, daß der angegriffene Rechner abstürzte oder anderweitige Fehlfunktionen ausführte. Hier stellt sich also – vermutlich eher aus juristischer denn aus technischer Sicht – die Frage, ob ein (technisch) korrektes Benutzen einer öffentlich zugänglichen Funktion nicht doch im Ergebnis zu einer „unberechtigten" Nutzung führen kann. Was also im konkreten Beispiel bedeutet, daß das Ausführen eines „Ping-of-Death" als unerlaubter Angriff und nicht als erlaubtes Benutzen der Ping-Funktionalität gewertet wird.

Darüber hinaus haben auch viele der Denial-of-Service- (DoS-)Angriffe die Eigenart, daß sie „Erlaubtes" derartig ausführen, daß im Ergebnis etwas „Ungewünschtes", wenn nicht gar „Unerlaubtes" entsteht. Konkret ist es oftmals so, daß bei einem DoS-Angriff „lediglich" öffentlich zugängliche Telemedien genutzt werden. Dies geschieht aber durch eine Vielzahl parallel zugreifender Systeme, die noch dazu typsicherweise „unüblich" (wenn auch aus technischer Sicht durchaus nicht Regelverletzend) auf die angebotenen Telemedien zugreifen. Das Ziel dabei ist eine Überlastung der angegriffenen Systems zu erreichen, was oftmals auch gelingt.

Legt man hier zwecks Bewertung die etwa im Umfeld der Gruppe „Anonymous" durchgeführten DoS-Angriffe[15] und die damit in Zusammenhang stehenden polizeilichen und juristischen Maßnahmen[16] zu Grunde, so scheint es so zu sein, daß auch eine aus technischer Sicht „korrekte" Nutzung von öffentlich zur Verfügung gestellten Telemedien letztlich als „unberechtigte" Nutzung eingestuft wird oder zumindest werden kann.[17]

Insofern – und auch unter Berücksichtigung der üblichen Einschränkung, daß der Gutachter kein Jurist ist und sich daher juristische Einschätzungen eigentlich verbieten – wird der Aussage widersprochen, „Telemedien der Beklagten, die der Information der Öffentlichkeit dienen und damit jedermann zur Verfügung stehen [können] nicht ‚unberechtigt' genutzt werden."

---

[13] ftp://ftp.rfc-editor.org/in-notes/rfc2151.txt

[14] ftp://ftp.rfc-editor.org/in-notes/rfc792.txt

[15] etwa im Rahmen der „Operation Payback" (http://www.heise.de/ct/artikel/Operation-Payback-Proteste-per-Mausklick-1150151.html)

[16] http://www.heise.de/newsticker/meldung/Festnahme-wegen-Attacken-von-Wikileaks-Unterstuetzern-3-Update-1150835.html
http://www.heise.de/newsticker/meldung/Auch-FBI-gegen-Anonymous-1180017.html

[17] Anderslautende Meinung siehe etwa hier: http://www.heise.de/tp/artikel/33/33843/1.html

Die weiteren Erläuterungen im Rahmen von Anmerkung 4 beziehen sich im Wesentlichen wieder auf juristische Bezüge, weswegen – wie oben bereits allgemein erläutert – hier keine Kommentierung erfolgt.

Zu den Anmerkungen 5 und 6 gibt es aus der technischen Sicht des Gutachters und über das was in diesem Dokument betreffend der ETSI-Richtlinie bereits gesagt wurde, nichts zusätzlich zu kommentieren. Die Problematik des Zirkelschlusses wurde im Übrigen bereits in der Kommentierung von Anmerkung 2 aufgegriffen.

Die in **Anmerkung 7** erwähnten technischen Aspekte soll hier nur insofern kommentiert werden, als daß der Gutachter an verschiedenen Stellen des ursprünglichen Gutachtens und der hier vorliegenden Erläuterung in der Tat betont hat, daß für den sicheren Betrieb eines IT-Systems die Speicherung der IP-Adressen der zugreifenden Host-Systeme nicht zwingend erforderlich ist.

Zur Hauptfrage

Abschließend soll eine Beantwortung der im Beschluß vom 20. Mai 2010 in Ziffer 1 genannten Hauptfrage erfolgen, da eine derartige Antwort im ursprünglichen Gutachten nicht vorhanden ist. Dies liegt wiederum daran, daß die Hauptfrage nicht als Frage, sondern eher als einleitend erläuternde Motivation interpretiert wurde.
Konkret wird in der Hauptfrage gefragt, ob zur Gewährleistung und Aufrechterhaltung der IT-Sicherheit und der Funktionalität der von der Beklagten betriebenen und verwendeten Telemedien und Telekommunikationsnetze die Speicherung und spätere Verwendung von IP-Adressen des zugreifenden Hostsystem ihrer Nutzer erforderlich ist.
Bezüglich der in der Frage angesprochenen Aspekte der IT-Sicherheit läßt sich die Frage klar mit „Nein, eine Speicherung ist nicht erforderlich" beantworten. Erklärende Erläuterungen und Begründen lassen sich hier sowohl im ursprünglichen Gutachten als auch in den hier vorliegenden Erläuterungen insbesondere den Informationen bezüglich der Beantwortung von Beweisfrage 2 entnehmen.
Bezüglich der in der Frage angesprochenen Aspekte der „Funktionsfähigkeit" der Telemedien ist die Beantwortung nicht so eindeutig, d.h. es kann insbesondere nicht einfach mit „Nein" geantwortet werden. Begründet wird dies damit, daß hier nicht nur Sicherheitsaspekte relevant sind, d.h. daß das System so gebaut und betrieben wird, daß eine gewünschte Funktionalität auch im Falle eines Angriffes aufrecht erhalten werden kann, sondern daß auch die gewünschte Funktionalität selbst unter dem Begriff der „Funktionsfähigkeit" subsummiert wird. Insofern hängt es von der konkret gewünschten bzw. angebotenen Funktionalität ab, ob das Speichern von IP-Adressen erforderlich ist oder nicht. Gehört es etwa zum Funktionsumfang eines betriebenen oder verwendeten Telemediums, daß das Telemedium detailliert Auskunft über die IP-Adressen der in der Vergangenheit zugreifenden Host-Systeme gibt (inklusive Informationen wie etwa Zeit und Dauer), so ist ein Speichern von IP-Adressen für die Funktionsfähigkeit zwingend erforderlich.
Natürlich mag als Einwand hier gelten, daß es sich um ein konstruiert pathologisches Beispiel für die Notwendigkeit der Speicherung von IP-Adressen aus Gründen der

Funktionsfähigkeit handelt. Tatsächlich muß eingeräumt werden, daß bezüglich der durch den Gutachter in Augenschein genommen öffentlich zugänglichen Telemedien der Beklagten – dabei handelt es sich konkret um die Web-Seiten unterschiedlicher Ministerien, des Bundeskanzleramts, der Bundeskanzlerin, des Bundespräsidenten und des Bundestages – keine Funktionalität gefunden werden konnte, für die ein Speichern von IP-Adressen zwingend erforderlich wäre.