TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Informatik Institut für Systemarchitektur
Professur für Datenschutz und Datensicherheit

Technische Universität Dresden, 01062 Dresden

EINGEGANGEN
25. Aug. 2011
Erl.....

Landgericht Berlin
Littenstr. 12-17
10179 Berlin

Gemeinsame Briefannahme
Justizbehörden Mitte
Eing. 18.08.11 00-24
7 ..... Scheck ..... Abschr.
..... KM ..... Akt. ..... Anl.

Dr.-Ing.
Stefan Köpsell

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

Sekr.:
E-Mail:

AZ:

Dresden, 29. Juli 2011

Sachverständigengutachten zu 57 S 87/08

Sehr geehrte Damen und Herren,

haben Sie Dank für Ihren Auftrag vom 25. März 2011 zur Erstellung eines Sachverständigengutachtens. Der Beweisbeschluß vom 20. Mai 2010 lautet:

„Es soll durch Einholung eines schriftlichen Sachverständigengutachtens Beweis erhoben werden über die Behauptung des Beklagten, zur Gewährleistung und Aufrechterhaltung der IT-Sicherheit und der Funktionsfähigkeit der von ihr betriebenen und verwendeten Telemedien und Telekommunikationsnetze sei die Speicherung und spätere Verwendung von IP-Adressen des zugreifenden Hostsystems ihrer Nutzer erforderlich.

Der Sachverständige soll insbesondere dazu Stellung nehmen,

- ob die Speicherung dieser IP-Adressen dem nationalen und internationalem Stand der Technik dient,
- ob nach dem derzeitigen technischen Stand eine Speicherung von IP-Adressen zwingend erforderlich ist oder ob andere Möglichkeiten bestehen, um die von der Beklagten betriebenen Webseiten vor schadhaften Angriffen zu schützen oder die Gefahr von Sicherheitsverletzungen zu mindern,
- welche Kosten gegebenenfalls für andere Maßnahmen aufzuwenden wären."

Anbei finden Sie das gewünschte Gutachten. Für inhaltliche Rückfragen stehe ich Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen,

[redacted]

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/

Zusammenfassung der Ergebnisse

Kurz zusammengefaßt lassen sich die gestellten Fragen wie folgt beantworten:

1.) zur Frage, *ob die Speicherung*[1] *dieser IP-Adressen dem nationalen und internationalem Stand der Technik dient:*

- Aus meiner Sicht **dient** die Speicherung von IP-Adressen **nicht dem** nationalen oder internationalen **Stand der Technik**. Die Speicherung von IP-Adressen **steht bestenfalls im Einklang mit einigen nationalen und internationalen Standards und Empfehlungen**. **Gleichzeitig existieren** andere nationale und internationale **Standards und Empfehlungen, die eine Speicherung** von IP-Adressen **nicht fordern** bzw. sich klar gegen eine (unverschlüsselte) Speicherung von IP-Adressen aussprechen.

2.) zur Frage, *ob nach dem derzeitigen technischen Stand eine Speicherung von IP-Adressen zwingend erforderlich ist oder ob andere Möglichkeiten bestehen, um die von der Beklagten betriebenen Webseiten vor schadhaften Angriffen zu schützen oder die Gefahr von Sicherheitsverletzungen zu mindern:*

- Eine **Speicherung** von IP-Adressen **ist weder zur Angriffserkennung noch zur Angriffsabwehr zwingend erforderlich.** Vielmehr existiert eine Reihe von bekannten und in der Praxis angewendeter Verfahren, die ohne eine Speicherung von IP-Adressen Angriffe erfolgreich erkennen und abwehren können. Darüber hinaus ist ein **IT-System, für dessen Sicherheit die Speicherung von IP-Adressen notwendig ist, generell** als **unsicher** anzusehen. **Für** eine **verläßliche Angreiferidentifizierung** ist eine **Speicherung** von IP-Adressen nicht ausreichend sondern **bestenfalls nützlich**.

3.) zur Frage, *welche Kosten gegebenenfalls für andere Maßnahmen aufzuwenden wären:*

- Die **Höhe der Kosten** für andere Maßnahmen **läßt sich nicht allgemein beziffern**, da dies stark von der aktuell vorhandenen Netzinfrastruktur (Hard- und Software), dem Schutzbedarf für die angebotenen Dienste und dem Ausbildungsstand des verfügbaren Personals abhängt. Es treten jedoch im Wesentlichen **keine zusätzlichen Kosten** (durch den Verzicht auf die IP-Adressen-Speicherung) auf, da (wie unter 2. erwähnt) diese anderen Sicherheitsmaßnahmen in jedem Fall zwingend erforderlich für den sicheren Betrieb des IT-Systems sind.

---

[1] 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.

Detaillierte Ausführungen zur Beantwortung der gestellten Fragen

Anmerkung: Frage 1 und 2 wurden in der Reihenfolge vertauscht.

2.) zur Frage, ob nach dem derzeitigen technischen Stand eine Speicherung von IP-Adressen zwingend erforderlich ist oder ob andere Möglichkeiten bestehen, um die von der Beklagten betriebenen Webseiten vor schadhaften Angriffen zu schützen oder die Gefahr von Sicherheitsverletzungen zu mindern

Einführend soll zunächst kurz die Bedeutung von IP-Adressen für die Kommunikation im Internet erläutert werden. Anschließend wird die Frage diskutiert, ob die Speicherung von IP-Adressen für den sicheren Betrieb eines IT-Systems zwingend erforderlich ist. Dabei wird insbesondere zwischen Angreiferidentifizierung, Angriffserkennung und Angriffsabwehr unterschieden. Abschließend wird erläutert, welche Alternativen existieren, um Webseiten vor schadhaften Angriffen zu schützen, ohne IP-Adressen zu speichern.

Datenübertragungen im Internet finden grundsätzlich Paket-basiert statt, d. h. es wird nicht, wie etwa im klassischen Telefonnetz, eine Verbindung (physisch) geschaltet. Vielmehr wird der zu übertragende Datenstrom in IP[2]-Pakete aufgeteilt, die einzeln und unabhängig voneinander zum Empfänger übertragen werden. Die sogenannte Ziel-IP-Adresse bestimmt dabei für jedes IP-Paket, für welchen Empfänger (genauer: welches Endgerät) das entsprechende IP-Paket bestimmt ist. Die sogenannte Quell-IP-Adresse eines IP-Paketes dient dazu, den Absender eines IP-Paketes zu bestimmen. Sie ist insbesondere dann wichtig, wenn der Empfänger Daten zurück an den ursprünglichen Sender übermitteln möchte, es sich also um eine bidirektionale Kommunikation handelt.
Die Angabe von Quell- und Ziel-IP-Adresse ist bezüglich Funktionalität und Sicherheitseigenschaften gut mit der Angabe von Absender- und Empfängeradresse im Postverkehr vergleichbar. Insbesondere ist in beiden Fällen die Absenderangabe durch den Absender frei festlegbar[3]. Dies hat unmittelbar Auswirkungen auf die Nützlichkeit der IP-Adressen-Speicherung für die **Identifizierung von Angreifern:** Natürlich läßt sich nicht ausschließen, daß ein Angreifer eine korrekte Absenderangabe vornimmt und insofern identifizierbar ist. Auf Grund der leichten Fälschbarkeit einer Quell-IP-Adresse ist jedoch in der Regel an Hand der IP-Adresse **keine verläßliche Identifikation des Absenders durchführbar.** Letzteres ergibt sich insbesondere aus der Tatsache, daß im Internet eine Vielzahl frei verfügbarer Anonymisierungsdienste angeboten wird. Sinn dieser Anonymisierungsdienste ist gerade die Änderung der Quell-IP-Adresse, so daß der eigentliche Absender durch den Anonymisierungsdienst verborgen wird. Zu den bekannten Anonymisierungsdiensten gehören etwa Tor[4], AN.ON[5] und einfache

---

[2] „IP" steht für „Internet Protocol".
[3] Einschränkend ist lediglich anzumerken, daß technisch bedingt die Quell-IP-Adresse nicht komplett weggelassen werden kann und daß die Menge möglicher Quell-IP-Adressen endlich ist.
[4] https://www.torproject.org/

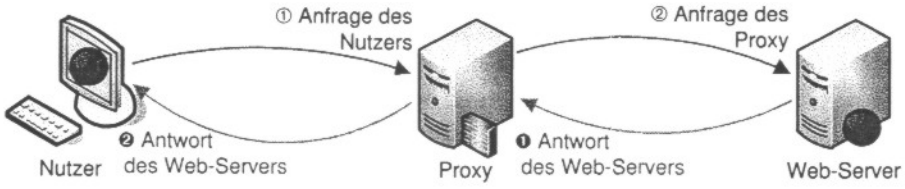

Abbildung 1: Anonymisierung durch Verwendung einfacher Proxies

Proxies (siehe Abbildung 1). Bezüglich letzterem existieren im Internet zugängliche Listen, die die notwendigen Zugangsdaten für die Nutzung dieser Proxies enthalten[6].

Während die erwähnten Anonymisierungsdienste für den „normalen" Internetnutzer gedacht sind, stehen für Kriminelle mit den sogenannten Botnetzen weitere sehr gute Möglichkeiten zur Verfügung, die eigene Identität bei der Durchführung von Angriffen zu verschleiern. Bei einem Botnetz handelt es sich um eine Menge von Rechnern, auf die Kriminelle unerlaubterweise Zugriff haben. Meist handelt es sich dabei um Rechner von Privatpersonen, die mit Schadsoftware „verseucht" sind, so daß Kriminelle die Rechner aus der Ferne steuern können. Botnetze werden wiederum anderen Kriminellen zum Kauf oder zur Miete angeboten. Eine häufige Anwendung ist dabei das Versenden von SPAM-E-Mails mit Hilfe der Botnetz-Rechner. Genauso ist es aber auch möglich, daß die Botnetz-Rechner benutzt werden, um Angriffe auf IT-Systeme zu initiieren. Insofern wird dann die IP-Adresse der Botnetz-Rechner gespeichert, was wiederum keinen Rückschluß auf die eigentlichen Täter ermöglicht.
Zusammenfassend läßt sich also feststellen, daß die Speicherung von IP-Adressen höchstens für die Identifizierung von „dummen" Angreifern nützlich sein kann. Halbwegs intelligenten Angreifern stehen auf einfachste Art und Weise Mittel zur Verfügung, um sich einer Identifizierung an Hand der IP-Adresse zu entziehen.
Sollte dennoch (auf Grund einer eventuell möglichen Identifizierung) auf die Speicherung von IP-Adressen nicht verzichtet werden, so gebietet es der Stand der Technik zumindest, die **IP-Adressen lediglich verschlüsselt** zu **speichern**. Damit läßt sich erreichen, daß Unberechtigte keine Kenntnis von den gespeicherten IP-Adressen erlangen. Insbesondere lassen sich leicht Zugriffsregeln auf die gespeicherten IP-Adressen umsetzen, etwa im Sinne des Mehr-Augen-Prinzips.

Zur **Angriffserkennung** ist die Speicherung von IP-Adressen ebenfalls nicht zwingend erforderlich. Allgemein sei dazu zunächst gesagt, daß die Mehrzahl sinnvoller IT-Sicherheitsmaßnahmen gänzlich ohne eine Analyse der Absender-IP-Adressen auskommt, da eine Angriffserkennung (und entsprechend eine Angriffsabwehr) ausschließlich an Hand der transportierten Inhalte erfolgt. Insofern beziehen sich die nachfolgenden Ausführungen lediglich auf die verbleibende Restmenge an Fällen, für die zur Angriffserkennung (oder –abwehr) eine Auswertung der Absender-IP-Adresse sinnvoll ist. Auch in diesen Fällen ist eine (unverschlüsselte) Speicherung der Absender-IP-Adressen jedoch nicht zwingend erforderlich.

---

[5] https://anon.inf.tu-dresden.de/
[6] als kleine Auswahl etwa: http://proxy4free.com/, http://nntime.com/, http://multiproxy.org/

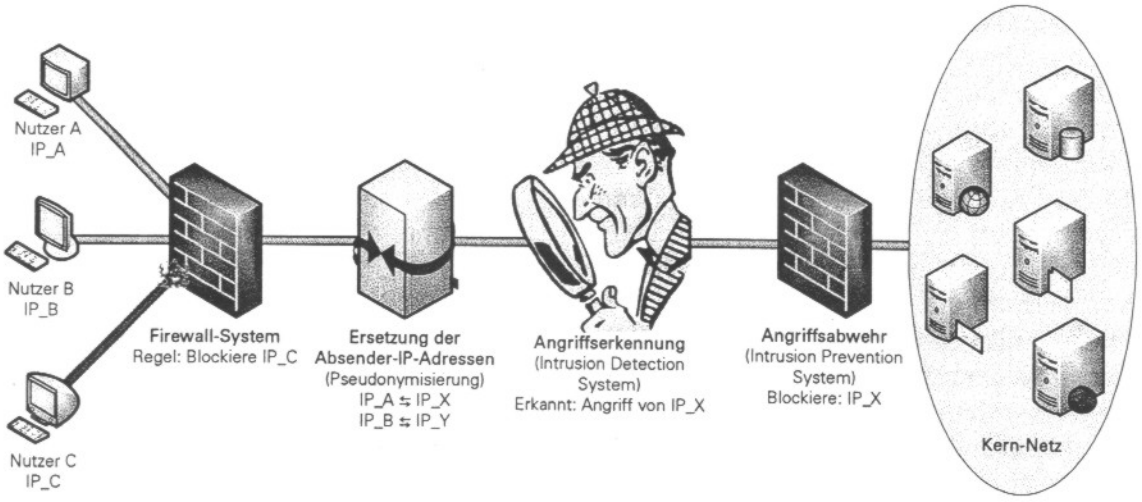

Abbildung 2: Vereinfachte Darstellung von Angriffserkennung und -abwehr ohne Speicherung von Absender-IP-Adressen

Dies ist zunächst offensichtlich bezüglich trivialer Angriffserkennungsregeln, die im Wesentlichen von den Absender-IP-Adressen abhängen, also etwa: „Die Absender-IP-Adresse 1.2.3.4 gehört einem Angreifer. Alle IP-Pakete von dieser IP-Adresse sind daher als Angriffsversuch zu werten." Hier ist eine Speicherung der IP-Adresse nicht notwendig. Vielmehr kann ein derartiger Angriffsversuch unmittelbar durch die Firewalls des zu schützenden IT-Systems abgewehrt werden, indem dort vermerkt wird, daß alle IP-Pakete von der Absender-IP-Adresse 1.2.3.4 verworfen und nicht in das eigentliche Kernnetz des IT-Systems weitergeleitet werden.
Allerdings ist es so, daß nicht immer an Hand eines einzigen IP-Pakets entschieden werden kann, ob es sich um einen Angriffsversuch handelt oder nicht. Vielmehr kann sich erst aus der Summe mehrerer einzelner (durchaus für sich genommen „harmloser") Aktivitäten ergeben, daß es sich um einen Angriff handelt. Um dies zu entdecken, werten Angriffserkennungssysteme (Intrusion Detection Systeme) den gesamten Datenverkehr aus, um Angriffsmuster zu erkennen (Signaturanalyse) bzw. Abweichungen von dem als „normal" definierten Datenverkehr festzustellen (Anomalieerkennung).
Der Absender-IP-Adresse kommt dabei üblicherweise die Rolle zu, Zusammengehörigkeiten festzustellen. Also etwa zu ermitteln, daß eine Menge von IP-Paketen einen zusammengehörigen Datenstrom bildet oder bei zeitlich entkoppelten Aktivitäten festzustellen, daß sie vermutlich vom selben Verursacher stammen. Zur Bestimmung derartiger Zusammengehörigkeiten ist allerdings eine **Speicherung der IP-Adresse nicht erforderlich**. Vielmehr reicht es aus, wenn eine Ersetzung der IP-Adresse beispielsweise durch eine Zufallszahl vorgenommen wird. Die Ersetzung muß dann in der Regel eineindeutig sein und darf keine Rückschlüsse auf die ursprüngliche IP-Adresse zulassen. Beides läßt sich technisch sehr leicht durch Verschlüsselung der IP-Adresse erreichen. Anzumerken ist, daß das Ersetzungskennzeichen selbst wieder aus der Menge gültiger IP-Adressen stammen kann. Auf diese Weise lassen sich vorhandene Systeme zur Angriffserkennung und –abwehr prinzipiell weiter verwenden, da sich das Datenformat eines IP-Paketes nicht ändert (siehe Abbildung 2).

Allerdings kommt es hier auf die konkrete Arbeitsweise insbesondere der vorhandenen Angriffserkennungssysteme an, da diese aus der Absender-IP-Adresse eventuell noch weitere Informationen ableiten, etwa die Zugehörigkeit zu einem Absender-Land oder die Zusammengehörigkeit bezüglich eines (bestimmten) Teilnetzes. In vielen Fällen sollte sich allerdings eine sinnvolle Ersetzung ohne relevanten Informationsverlust vornehmen lassen.
In der Praxis werden derartige Verfahren etwa bei dem durch den Autor am Lehrstuhl Datenschutz & Datensicherheit der TU Dresden betriebenen Anonymisierungsdienst AN.ON[7] oder der (zur Zeit nicht mehr verfügbaren) Website isharegossip.com[8] vorgenommen.
Neben der oben beispielhaft skizzierten Ersetzung von IP-Adressen sind in der Dissertationsschrift[9] von Dr. Ulrich Flegel weitere Verfahren beschrieben, die eine Angriffserkennung (und -abwehr) ermöglichen, ohne das IP-Adressen oder andere identifizierende Merkmale im Klartext gespeichert werden müssen.
Zusätzlich sei angemerkt, daß ein Angreifer mit Hilfe der oben erwähnten Verfahren zur Anonymisierung erreichen kann, daß er ständig wechselnde Absender-IP-Adressen verwendet. Insofern ist die Herstellung eines Zusammenhangs zwischen verschiedenen Aktivitäten eines Angreifers an Hand der Absender-IP-Adresse äußerst unzuverlässig und daher für die Angriffserkennung nur bedingt geeignet. Dabei kommt erschwerend hinzu, daß auch viele „normale" Internetnutzer mit häufig (in der Regel täglich) wechselnden IP-Adressen (sogenannten „dynamischen IP-Adressen) im Internet auftreten.

Zur **Angriffsabwehr** ist eine **Speicherung der IP-Adresse** ebenfalls **nicht erforderlich.** Für den trivialen Fall, daß die Abwehr von Angriffen lediglich an Hand der Absender-IP-Adresse erfolgt, wurde bereits oben erwähnt, daß eine Abwehr durch eine Firewall leicht möglich ist, wofür eine Speicherung der IP-Adresse jedenfalls nicht erforderlich ist.
Auch für die Abwehr eines Angriffs, der durch ein Intrusion Detection System (siehe oben) erkannt wurde, ist eine Speicherung von IP-Adressen nicht erforderlich. Vielmehr wird durch die Abwehrsysteme (Firewalls bzw. Intrusion Prevention Systeme) dieselbe Ersetzung vorgenommen, wie sie auch durch das Angriffserkennungssystem vorgenommen wurde. Auf diese Weise kann das Abwehrsystem IP-Pakete verwerfen, in deren Absenderangabe nun ein Kennzeichen steht, für welches das Erkennungssystem festgestellt hat, daß von dieser Quelle Angriffe ausgehen.

Zusammenfassend läßt sich somit feststellen, daß weder zur Angriffserkennung noch zur Angriffsabwehr eine Speicherung von IP-Adressen erforderlich ist.

---

[7] Der Anonymisierungsdienst wird aktuell von etwa 150000 Nutzern weltweit benutzt. Die zugehörige Infrastruktur (Anonymisierungs- und Web-Server, Softwareverwaltungssystem etc. stehen unter ständigen Angriffsversuchen, insbesondere Angriffen auf die Verfügbarkeit (Denial-of-Service-Angriffe).
[8] In Anhang A befindet sich ein Auszug aus der iShareGossip Web-Seite vom 3. Mai 2011, der das Vorgehen zur Erkennung von Angriffen trotz verschlüsselter Speicherung der IP-Adresse beschreibt.
[9] U. Flegel: „Privacy-Respecting Intrusion Detection", Springer, 2007.

Aus der fehlenden Verläßlichkeit bezüglich der Authentizität von Absender-IP-Adressen ergibt sich ferner, daß die Speicherung von IP-Adressen zur Angreiferidentifizierung bestenfalls nützlich sein kann und andere Maßnahmen (als die Speicherung der IP-Adressen) zum Schutz der betriebenen IT-Systeme zwingend erforderlich sind. Anders gesagt: eine Speicherung von IP-Adressen kann bestenfalls einen marginalen Sicherheitsgewinn bringen, der für sich genommen nicht ausreichend für den sicheren Betrieb von IT-Systemen ist.
Ein Beispiel aus der „offline Welt" mag dies verdeutlichen: Üblicherweise werden zum Zutrittsschutz bei Wohnungen, Häusern oder Autos verschlossene Türen verwendet. Wohingegen der Vorschlag, einfach die Türen offen stehen zu lassen und statt dessen ausschließlich Überwachungskameras zu installieren, wohl auf wenig Akzeptanz stoßen dürfte. Bezogen auf ein IT-System kann man die „verschlossenen Türen" als die vorzunehmenden „anderen Maßnahmen" verstehen und die Überwachungskameras sind das Gleichnis für das Speichern von IP-Adressen.
Im allgemeinen existieren viele „andere Maßnahmen" die möglich und auch notwendig für den sicheren Betrieb eines vernetzten IT-Systems sind. Eine umfassende Darstellung würde an dieser Stelle sicher zu weit führen[10], da beispielsweise eine Vielzahl umfangreicher Bücher im Bereich des „Security Engineering" existiert, welche beispielsweise entsprechende kryptographische Verfahren und Protokolle beschreiben. Darüber hinaus existieren eine Vielzahl von Standards, Empfehlungen und Richtlinien zum sicheren Betreiben eines IT-Systems. In Deutschland sind hier insbesondere die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebenen Maßnahmen zum IT-Grundschutz zu erwähnen.[11] Eine Vielzahl der dort vorgeschlagenen Maßnahmen steht in keinem Zusammenhang mit dem Speichern von IP-Adressen, d. h. zur Umsetzung der Maßnahmen ist eine Speicherung nicht erforderlich.
Aus den vom Gericht zur Verfügung gestellten Unterlagen geht allerdings hervor, daß der Beklagte einige Beispiele[12] vorgetragen hat, für die aus seiner Sicht eine Speicherung von IP-Adressen zwingend erforderlich ist. An Hand dieser Beispiele soll nachfolgend erläutert werden, wie Schutz auch ohne Speicherung von IP-Adressen erreicht werden kann.

- E 1 a) *Anomalieerkennung im Rahmen eines Intrusion Detection Systems*
  - Wie ein Verzicht auf die Speicherung von IP-Adressen möglich ist, wurde bereits oben erläutert.

- E 1 b) *Sperrung von IP-Adressen nach Anomalieerkennung (Angriffsabwehr)*
  - Wie ein Verzicht auf die Speicherung von IP-Adressen möglich ist, wurde bereits oben erläutert.

---

[10] Sollte das Gericht hier anderer Meinung sein, so bin ich gerne bereit, entsprechende Ausführungen nachzureichen.
[11] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html
[12] etwa zu finden unter Punkt E (S. 26ff) im Schriftsatz von den Rechtsanwälten Wendler / Tremml vom 22. März 2010.

- (Anmerkung: Das geschilderte Angriffsszenario erscheint insgesamt wenig plausibel. Es wird argumentiert, daß ein Angreifer einen Angriff unter Benutzung einer bestimmten Absender-IP-Adresse *x* durchführt. Die Analyse des Angriffs dauere Wochen und erst dann wird die IP-Adresse *x* in eine Sperrliste aufgenommen. Klarerweise verwendet der Angreifer zu diesem Zeitpunkt bereits eine völlig neue Absender-IP-Adresse (siehe Ausführungen oben) und die Sperrung trägt insofern nichts zum Schutz bei.)

- E 1 c) *Analyse der eigenen Logs auf bekannte Angreifer-IP-Adressen*
  - Auch in diesem Fall ist es ausreichend, wenn an Stelle der IP-Adressen die oben erwähnten Ersetzungskennzeichen gespeichert werden. Für die neu in Erfahrung gebrachten Angreifer-IP-Adressen wird dann ebenfalls eine Ersetzung durchgeführt. Anschließend werden die Log-Dateien auf die so erhaltenen Ersetzungskennzeichen des Angreifers durchsucht.

- E 1 d) *Angriffserkennung und Abwehr an Hand komplexer Angriffsmuster*
  - Auch hier wird im Wesentlichen auf eine Verkettung von Aktivitäten mit Hilfe der IP-Adresse abgezielt. Wie oben bereits ausgeführt, ist zum einen für die Ermittlung der Zusammengehörigkeit keine Speicherung der IP-Adresse notwendig. Zum anderen werden bei derartigen Angriffen regelmäßig unterschiedliche Absender-IP-Adressen verwendet, so daß die Erkennungswahrscheinlichkeit bei Angriffen halbwegs intelligenter Angreifer als gering einzuschätzen ist.

- E 1 e) ist inhaltlich zu E 1 d) vergleichbar, insofern gilt das zu E 1 d ausgeführte.

- E 2) *Speicherung für Täteridentifizierung und Strafverfolgung*
  - Hier wird als neuer Aspekt die Möglichkeit zur Täteridentifizierung und Strafverfolgung erwähnt. Allerdings wurde oben bereits ausgeführt, daß eine IP-Adresse eben nicht verläßlich geeignet ist, den Verursacher zu ermitteln — insbesondere wenn es sich um einen Täter handelt, der sich der oben erwähnten Methoden zur Verschleierung seiner Identität bedient.

1.) zur Frage, ob die Speicherung dieser IP-Adressen dem nationalen und internationalem Stand der Technik dient

Meiner Meinung nach **dient** die Speicherung **nicht dem nationalen oder internationalem Stand der Technik** in Hinblick auf die Absicherung von IT-Systemen. Dies ergibt sich zum einen aus der Tatsache, daß sich IP-Adressen leicht fälschen lassen und insofern deren Speicherung und Auswertung bestenfalls einen geringen Beitrag zum Schutz eines IT-Systems leisten kann. Zum anderen existiert für die Absicherung von IT-Systemen eine Vielzahl von anderen, wesentlich effektiveren Mitteln und Methoden.

Insofern sehe ich letzteres als den Stand der Technik und entsprechend das Speichern von IP-Adressen als „veraltet" an. Dies gilt insbesondere, wenn die Speicherung der IP-Adressen unverschlüsselt erfolgt.
Gleichwohl **kann** das Speichern von IP-Adressen **der Erfüllung von nationalen und internationalen Empfehlungen, Standards und Regulierungen dienen**. In der Tat existiert eine Vielzahl von relevanten und bedeutenden Standards, die das Speichern von IP-Adressen vorsehen. Dies geschieht dabei üblicherweise, um eine Auditierbarkeit des Systems zu gewährleisten.
Allerdings hängt es von dem konkreten Standard ab, da sowohl Standards existieren, die das Speichern von IP-Adressen empfehlen bzw. vorschreiben als auch Standards[13], die das (unverschlüsselte) Speichern von IP-Adressen nicht empfehlen oder vorschreiben bzw. sogar „verbieten".
Dies soll exemplarisch an Hand der vom Beklagten vorgebrachten Standards (ISO 27001, ISO 27002, ISO/IEC 15408, BSI Grundschutz) als auch an einem weiteren Beispiel erläutert werden.

- *DIN ISO/IEC 27001:2008-09*[14]: Diese Norm beschäftigt sich ganz allgemein mit der Einrichtung eines Informationssicherheits-Managementsystems. Relevant sind hier insbesondere die in Abschnitt A.10.10 „Überwachung" genannten Maßnahmen und hier wiederum die Maßnahmen A.10.10.1 „Auditprotokolle" und A.10.10.3 „Schutz von Protokollinformationen". In ersterem heißt es lediglich ganz allgemein: *„Es müssen Auditprotokolle erstellt werden, in denen Benutzeraktivitäten, Fehler und Informationssicherheitsvorfälle festgehalten werden. Sie müssen für einen vereinbarten Zeitraum verwahrt werden, um in zukünftigen Untersuchungen und Überwachungen der Zugriffskontrolle behilflich zu sein."*. In letzterem steht: *„Protokollierungseinrichtungen und Informationen aus Protokollen sollten vor Verfälschung und unbefugtem Zugang geschützt werden."* Aus beidem läßt sich **keine Notwendigkeit zur Speicherung von IP-Adressen** ableiten. Darüber hinaus ist zweifelhaft, ob eine Speicherung von IP-Adressen im Klartext der Erfüllung des Standards dient.

- *DIN ISO/IEC 27002:2008-09*: Bei dieser Norm handelt es sich im Wesentlichen um vertiefende Ausführungen zu ISO 27001. Als Konkretisierung der bereits in ISO 27001 (siehe oben) erwähnten „Auditprotokolle" wird in Abschnitt 10.10.1 eine **Speicherung von IP-Adressen empfohlen**: *„Auditprotokolle sollten, sofern relevant, die folgenden Elemente beinhalten: ... j) Netzadressen und Protokolle; ... Die Auditprotokolle dürfen private und vertrauliche persönliche Daten enthalten. Angemessene Maßnahmen zur Einhaltung des Datenschutzes sollten getroffen werden (siehe 15.1.4)."* In Konkretisierung des oben ebenfalls

[13] Hier wird natürlich auf Standards Bezug genommen, die sich offensichtlich mit der Thematik des (sicheren) Betriebs von IT-Systemen beschäftigen.
[14] Da aus den Unterlagen nicht ersichtlich ist, auf welche Version der Standards ISO 27001 und ISO 27002 Bezug genommen wird, wird hier die entsprechende deutsche Adaption vom Deutschen Institut für Normung e.V. (DIN) herangezogen.

erwähnten „Schutz von Protokollinformationen" wird lediglich auf die unerlaubte Modifikation der Protokolldaten abgehoben, Maßnahmen für Vertraulichkeit (etwa Verschlüsselung) sind jedenfalls nicht explizit gefordert.
Auch im referenzierten Abschnitt 15.1.4 „Datenschutz und Vertraulichkeit von personenbezogenen Informationen" wird lediglich sehr allgemein von der Notwendigkeit der Einhaltung von *„einschlägigen Gesetzen, Vorschriften und gegebenenfalls Vertragsklauseln"* geredet. Am relevantesten ist dabei noch die Formulierung *„Angemessene technische und organisatorische Maßnahmen zum Schutz personenbezogener Informationen sollten umgesetzt werden."*
Zusammenfassend läßt sich also feststellen, daß eine Speicherung von IP-Adressen der Erfüllung von ISO 27002 dienen kann. Interpretationsspielraum besteht hauptsächlich bezüglich der Frage, ob eine Speicherung im Klartext zulässig ist oder die Speicherung verschlüsselt erfolgen muß.

- *DIN ISO/IEC 15408-1...3*: Zunächst ist anzumerken, daß kein unmittelbarer Zusammenhang zwischen dem ISO-Standard 15408 und der zu untersuchenden Fragestellung besteht. Bei ISO 15408 (den sogenannten „Common Criteria for Information Technology Security Evaluation") handelt es sich um eine Norm, die beschreibt, wie die Sicherheit von IT-Systemen evaluiert werden kann. Ausgangspunkt ist dabei ein zu erstellendes „Protection Profile", das für ein konkretes IT-System beschreibt, was zu schützen ist. Evaluiert wird dann, ob durch eine konkrete Umsetzung des IT-Systems ausreichender Schutz durch entsprechend aus der Norm und dem Protection Profile zu entnehmender Maßnahmen (Sicherheitsbausteine) besteht.
  Für die Beantwortung der Frage, ob eine Speicherung von IP-Adressen der Erfüllung von ISO 15408 dient, ist es also zunächst notwendig, die entsprechenden Protection Profiles für die betriebenen IT-Systeme zu benennen.
  Andererseits ist im einzig relevanten Sicherheitsbaustein (aus ISO 15408-2) „7.2. Security audit data generation" lediglich ganz allgemein vorgesehen: *„The TSF[15] shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; ... "*. Außerdem sei angemerkt, daß im Katalog der Sicherheitsbausteine auch welche für Datenschutz (insbesondere Anonymisierung und Pseudonymisierung) vorgesehen sind.
  Zusammenfassend läßt sich feststellen, daß sich aus ISO 15408 **keine Notwendigkeit zur Speicherung von IP-Adressen** ergibt.

- *BSI-Grundschutz(kataloge)*: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet mit seinem „IT-Grundschutz" umfangreiche

[15] Die Abkürzung „TSF" kann hier übersetzt werden als: „Die Sicherheitskomponenten des IT-Systems".

Informationen und Handlungsanweisungen in Form von Standards und Empfehlungen für den sicheren Betrieb von IT-Systemen. Dabei sind insbesondere die in den IT-Grundschutz-Katalogen aufgeführten Sicherheitsmaßnahmen sehr konkret bezüglich des praktischen Betriebs von IT-Systemen. Allerdings sind vorgeschlagene Maßnahmen in Bezug auf die Speicherung von IP-Adressen nicht widerspruchsfrei bzw. konsistent.
In Maßnahme M4.182 „Überwachen des IIS-Systems", eine Maßnahme, die sich mit der Absicherung der Internet Information Services (IIS), des Webservers der Firma Microsoft, beschäftigt, heißt es: *„Eine minimale Protokollierung sollte folgende Informationen beinhalten: ..., Client IP-Adresse, ...* ". Hier ist also eine **Speicherung von IP-Adressen gefordert**.
Allerdings ist in den Maßnahmen (M4.193 – M4.196) zum Apache-Webserver[16], dem Webserver der Apache Software Foundation, sowie in den allgemeinen Maßnahmen zum Betrieb eines Webservers (M2.174) bzw. zum Betrieb eines E-Mail-Servers (M5.56) eine **Speicherung von IP-Adressen nicht** explizit **vorgesehen**. Insofern kann man argumentieren, daß sich die Speicherung von IP-Adressen durch den Austausch des IIS-Webservers durch ein anderes Produkt vermeiden läßt.
Die **Speicherung von IP-Adressen** ist allerdings auch ganz allgemein in Maßnahme M4.47 „Protokollierung der Sicherheitsgateway-Aktivitäten" **vorgesehen**. In der allgemeineren Maßnahme M4.81 „Audit und Protokollierung der Aktivitäten im Netz" ist eine **Speicherung von IP-Adressen** wiederum **nicht** explizit **gefordert**.
Abschließend sei noch auf die Maßnahme M5.71 „Intrusion Detection und Intrusion Response Systeme" hingewiesen, die ebenfalls keine Speicherung von IP-Adressen explizit vorsieht und ferner folgenden Passus enthält: *„Da auch bei der automatischen Auswertung von Protokollinformationen die Datenschutzbestimmungen oder Personalvereinbarungen beachtet werden müssen, kann es unter Umständen notwendig werden, diese Daten pseudonymisiert abzulegen."*
Zusammenfassend läßt sich also feststellen, daß sich die Notwendigkeit der Speicherung von IP-Adressen zur Erfüllung der IT-Grundschutz-Kataloge bestenfalls aus einigen wenigen Maßnahmen ergibt.

- *ETSI TR 102 661 V1.2.1 (2009-11)*: Dieser technische Bericht des European Telecommunications Standards Institute (ETSI) enthält Empfehlungen bezüglich der Art und Weise der Speicherung von Daten, die im Rahmen der Vorratsdatenspeicherung bzw. der Strafverfolgung anfallen. Insofern lassen sich hier gewisse Parallelen ziehen zu der Begründung für die Speicherung von IP-Adressen durch den Beklagten (nämlich die Aufklärung von Angriffen und Mißbrauchsfällen). In ETSI TR 102 661 ist in Abschnitt 7.6.1 „Confidentiality of stored data" vorgeschrieben: *„DR[17] data that are stored within storing devices, require high protection in terms of confidentiality.*

[16] Beim Apache-Webserver handelt es sich um den vermutlich meistgenutzten Webserver im Internet (http://news.netcraft.com/archives/category/web-server-survey/).
[17] „DR" steht für „Data retention".

Hence, the DR retained telecommunication data, the DR session execution data and the DR-related log data that the CSP network produces and stores, is recommended to be kept encrypted during their entire retention period within storage devices." Es wird also empfohlen, die Daten ausschließlich verschlüsselt zu speichern. Auf Grund der Aktualität der Vorratsdatenspeicherung und der damit verbundenen technischen Regelungen kann ein verschlüsseltes Speichern von Log-Daten gleichzeitig als Stand der Technik angesehen werden.

3.) zur Frage, welche Kosten gegebenenfalls für andere Maßnahmen aufzuwenden wären

Welche Kosten konkret für andere Maßnahmen aufzuwenden wären, läßt sich nicht allgemein beantworten. Die Kosten hängen insbesondere stark von der vorhandenen Hard- und Softwareinfrastruktur, von der Art der betriebenen und entsprechend für die Öffentlichkeit angebotenen Dienste und deren Schutzbedürftigkeit sowie dem Ausbildungsstand des verfügbaren Personals ab. Auch lassen sich die Kosten schwer eingrenzen, da hier von einigen Tausend bis mehreren Hunderttausend Euro alles möglich ist.
Anzumerken ist allerdings, daß die Kosten für die „anderen Maßnahmen" in jedem Fall aufgewendet werden müssen, d. h. unabhängig davon, ob IP-Adressen gespeichert werden oder nicht. Dies ergibt sich schlicht aus der Tatsache, daß eine Speicherung von IP-Adressen bestenfalls geringfügig zum Schutz eines IT-Systems beitragen kann. Somit entstehen durch den Verzicht auf IP-Adressen-Speicherung zusätzliche Kosten dann, wenn die oben erwähnten Verfahren zur Ersetzung von IP-Adressen durch zufällige Kennzeichen nicht durch die vorhandenen Systeme zur Angriffserkennung und Angriffsabwehr unterstützt werden. Es ist allerdings davon auszugehen, daß viele der marktüblichen Systeme eine derartige Ersetzung nicht oder nur eingeschränkt unterstützen. Hier hängt es wiederum von den konkret vorhandenen Systemen ab, wie leicht oder schwer eine Erweiterung möglich ist, was entsprechend mit geringen oder hohen Kosten verbunden ist.