Von der Industrie- und Handelskammer zu Koblenz
öffentlich bestellter und vereidigter Sachverständiger
für Systeme der Informationsverarbeitung

Dipl.-Ing. Wolfgang Lehnigk-Emden

Auf dem Hürter 21
D-56299 Ochtendung

Tel: +49 (0) 26 25 / 96 69 0
Fax: +49 (0) 26 25 / 96 69 31

www.svlehnigk.de
wle@svlehnigk.de

13.01.2025

Gutachten 5315G22

im Auftrag des

Landgericht Berlin vom 28.01.2022

30 S 5/21

in dem

Rechtsstreit

Patrick Breyer **- Kläger -**

Prozessbevollmächtigte: Rechtsanwaltskanzlei Jonas Breyer
Schiersteiner Str. 37a
65187 Wiesbaden

gegen

Bundesrepublik Deutschland **- Beklagte -**

Prozessbevollmächtigte: TCI Partnerschaft von Rechtsanwälten Müller Schmidt mbH
Fasanenstraße 61
10719 Berlin
Gz.: 172/00123-08/ms

Inhalt

1. Auftrag 3
2. Grundlage des Gutachtens 5
3. Backend-Infrastruktur öffentlich zugänglicher Telemedien und Risiken, denen sie ausgesetzt sind 6
4. Angriffsanalysen und die Rolle der IP-Adresse an zwei Beispielen 8
5. Beweisfragen (1) 10
5.1. Grundlagen 10
5.2. Zu Beweisfrage (1) a) 12
5.3. Zu Beweisfrage (1) b) 13
5.4. Zu Beweisfrage (1) c) 14
5.5. Zu Beweisfrage (1) d) 15
5.6. Zu Beweisfrage (1) e) 15
6. Beweisfragen (2) 17
6.1. Zu den Beweisfragen 2) a) und b) 17
6.2. Zu Beweisfrage (2) c) 19
7. Beweisfragen (3) 20
7.1. Zu Beweisfrage (3) a) 20
7.2. Zu Beweisfrage (3) b) 20
7.3. Zu Beweisfrage (3) c) 22
7.4. Zu Beweisfrage (3) d) 23
8. Gutachterliche Auseinandersetzung mit den Privatgutachten 24
8.1. Zur 2. Frage 24
8.2. Zur 3. Frage 25
9. Gutachtenergebnis 26

1. Auftrag

Mit Beweisbeschluss des Landgericht Berlin vom 19.09.2018 soll Beweis erhoben werden über die folgenden Fragen:

(1)

a) Welchen sicherheitstechnischen Zwecken dient die Protokollierung und Speicherung dynamischer IP-Adressen von zugreifenden Host-Systemen über die Dauer des konkreten Nutzungsvorgangs hinaus im Rahmen des Betriebs von öffentlich zugänglichen Telemedien, wie sie die Beklagte betreibt?

b) Was konkret bewirkt / verhindert / ermöglicht bzw. welche Funktion erfüllt die Speicherung der dynamischen IP-Adressen von zugreifenden Telemedien dabei jeweils und

c) an welchem Ort werden die Adressen dabei jeweils gespeichert?

d) Wer kann dabei jeweils auf die gespeicherten Adressen zugreifen?

e) Welche weiteren Log-Daten müssen jeweils mit der IP-Adresse gemeinsam gespeichert werden, um die jeweiligen Zwecke zu erreichen?

(2)

a) Ist die Protokollierung und Speicherung der vollständigen, nicht-anonymisierten dynamischen IP-Adressen über den konkreten Nutzungsvorgang hinaus zwingend erforderlich, um die einzelnen zu Ziffer (1) gegebenenfalls vom Sachverständigen festgestellten Zwecke jeweils erreichen?

b) oder können die zu Ziffer (1) genannten Zwecke jeweils auch durch andere gleich geeignete Mittel /Maßnahmen (beispielsweise moderne, regelmäßig aktualisierte Software, Systemtrennung etc.) erreicht werden und wenn ja, welche?

c) Sind diese etwaigen alternativen Mittel / Maßnahmen besonders aufwendig und /oder kostspielig und wenn ja, in welcher Größenordnung ungefähr?

(3) Sollte der Sachverständige die zwingende Erforderlichkeit gemäß Ziffer (2) bejahen:

a) Warum gibt es dann von der Beklagten betriebene öffentlich zugängliche Telemedien, die ohne die Speicherung der vollständigen, nicht-anonymisierten dynamischen IP-Adressen über den konkreten Nutzungsvorgang hinaus auskommen?

b) Wie häufig treten die zu Ziffer (1) vom Sachverständigen gegebenenfalls festgestellten sicherheitsrelevanten Angriffe / Bedrohungen bei den von der Beklagten betriebenen öffentlich zugänglichen Telemedien auf bzw. wie wahrscheinlich sind diese Angriffe/Bedrohungen und welche Schäden mit welchen Folgen und welchem Ausmaß können dadurch verursacht werden?

c) Gibt es statistische Erhebungen / Erkenntnisse darüber, ob und gegebenenfalls, wie häufig Angreifer auf Telemedien aufgrund bzw. infolge einer Speicherung von dynamischen IP-Adressen persönlich tatsächlich identifiziert wurden? Wenn nicht, was ist Ihre Einschätzung?

d) Bedarf es zwingend zusätzlicher Log-Daten wie beispielsweise eines Zeitstempels, und wenn ja, welcher, um den Nutzer einer dynamischen IP-Adresse identifizieren zu

können oder ist die Identifizierung in bestimmten Fällen auch ohne weitere Log-Daten möglich, beispielsweise bei entsprechend langer Nutzungsdauer einer dynamischen IP-Adresse aufgrund einer „always-on"-Einstellung des genutzten Routers in Verbindung mit dem Nutzerverhalten?

Bei der Beantwortung der Fragen soll sich der Sachverständige auch mit dem Gutachten des Herr Dr.-Ing. Stefan Köpsell vom 29.07.2011 (Bl. 104 ff. Bd. III d.A.) nebst ergänzender Erläuterungen vom 07.05.2012 (Bl. 152 ff. Bd. III d.A.), dem von der Beklagten vorgelegten Privatgutachten des Herrn Prof. Dr. Peter Martini vom 20.11.2012 (Anlage BB 5 zum Schriftsatz der Beklagten vom 30.11.2012, Bl. 26 ff. Bd. IV d.A.) und dem Vortrag der Parteien auseinander setzen.

2. Grundlage des Gutachtens

Grundlage des Gutachtens sind:

- Gerichtsakte des Amtsgericht Tiergarten 6 Bände (nummeriert bis Bd. 7)
- Gerichtsakte Bundesgerichtshof bis Bl. 207 (Bd. Nr. 5)

Zur Konkretisierung der Beweisfragen stellte das Gericht auf Anfrage des Sachverständigen wie folgt klar:

1. Schriftsatz des Landgericht Berlin vom 28.06.2022 mit der Antwort auf die Frage des Sachverständigen vom 30.05.2022.

   Demnach sollen die Ziele „Strafverfolgungspraxis" und „Abschreckung aufgrund der Strafverfolgungspraxis" nicht unter die „sicherheitstechnischen Zwecke" im Sinne der Frage (1) fallen und es deshalb dazu keinerlei Ausführungen bedarf.

2. Schriftsatz des Landgericht Berlin vom 10.02.2023 mit der Antwort auf die Frage des Sachverständigen vom 27.01.2023. Darin gibt das Gericht vor,

   „...dass auch die von Ihnen (Sachverständiger) dort beschriebenen Ziele (insbesondere: Hilfeleistung zu der Unschädlichmachung von Botnets, deren Zweck ein Angriff auf von der Beklagten betriebene, öffentlich zugängliche Telemedien ist) vorsorglich als von dem Begriff des „sicherheitstechnischen Zweckes" abgedeckt zu behandeln sind und die Berücksichtigung dieser Ziele innerhalb Ihrer Bearbeitung das Beweisthema demgemäß nicht überdehnt."

3. Schriftsatz des Landgericht Berlin vom 20.11.2023 mit der Antwort auf die Frage des Sachverständigen vom 04.08.2023 mit dem Schriftsatz der klagenden Partei vom 04.09.2023 sowie dem Schriftsatz der beklagten Partei vom 25.09.2023. Darin gibt das Gericht vor:

   „Unter (1) ist allein Ihre (des Sachverständigen) fachliche Einschätzung zu den sicherheitstechnischen Zwecken im Zusammenhang der Protokollierung und Speicherung dynamischer IP-Adressen von zugreifenden Host-Systemen über die Dauer des konkreten Nutzungsvorgangs hinaus im Rahmen des Betriebs von öffentlich zugänglichen Telemedien gefragt. Dieser Punkt (1) hat eine generelle Stoßrichtung, es geht nicht um einzelne Telemedien der Beklagten.

   Gleichermaßen sollen Sie (der Sachverständige) unter (2) - neben weiterem ("Kosten etwaiger alternativer Mittel /Maßnahmen" ...) - in einem generellen Maßstab bewerten, ob die zuvor zu (1) ggf. festgestellten sicherheitstechnischen Zwecke alternativ auch durch andere - im Beweisbeschluss exemplarisch näher benannte - gleich geeignete Mittel bzw. Maßnahmen erreicht werden können.

   Auch die Beweisfrage (3a) zielt allenfalls mittelbar, jedenfalls nicht konkret den einzelnen Telemedien nach auf die Ihrerseits (sachverständigenseits) aufgeworfenen „individualisierten Sicherheitsbedürfnisse" der Beklagten ab."

3. Backend-Infrastruktur öffentlich zugänglicher Telemedien und Risiken, denen sie ausgesetzt sind

Die von der Beklagten betriebenen, öffentlich zugänglichen Telemedien umfassen eine Vielzahl von Systemen zum Betrieb allgemein zugänglicher Internetseiten und -portale[1]. Diese Systeme ermöglichen Bundesbehörden, sonstigen Bundesorganen und Bundeseinrichtungen, aktuelle Informationen öffentlich und zum Abruf für jedermann bereitzustellen. Einige dieser Internetseiten sind dialogfähig.

Die Internetseiten, die ein Web-Anwender mit seinem Browser von einem Client-Gerät (PC, mobile Geräte usw.) abrufen kann, werden auf einem Backend-System zusammengestellt und an den Client über das Internet übertragen.

Allgemein bestehen solche Backend-Systeme aus Servern mit unterschiedlichen Funktionen sowie anderen Geräten wie z.B. Firewalls. Auf diesen Geräten laufen Programme (=Dienste) zur Kommunikation mit dem Web-Client sowie zur Zusammenstellung der jeweilig abgefragten Internetseiten, ggf. mit individuell zusammengestellten Daten entsprechend der Anfrage des Nutzers (z.B. Registrierungsseiten)[2].

Abb. 1 zeigt eine typische Infrastruktur eines solchen Backend-Systems.

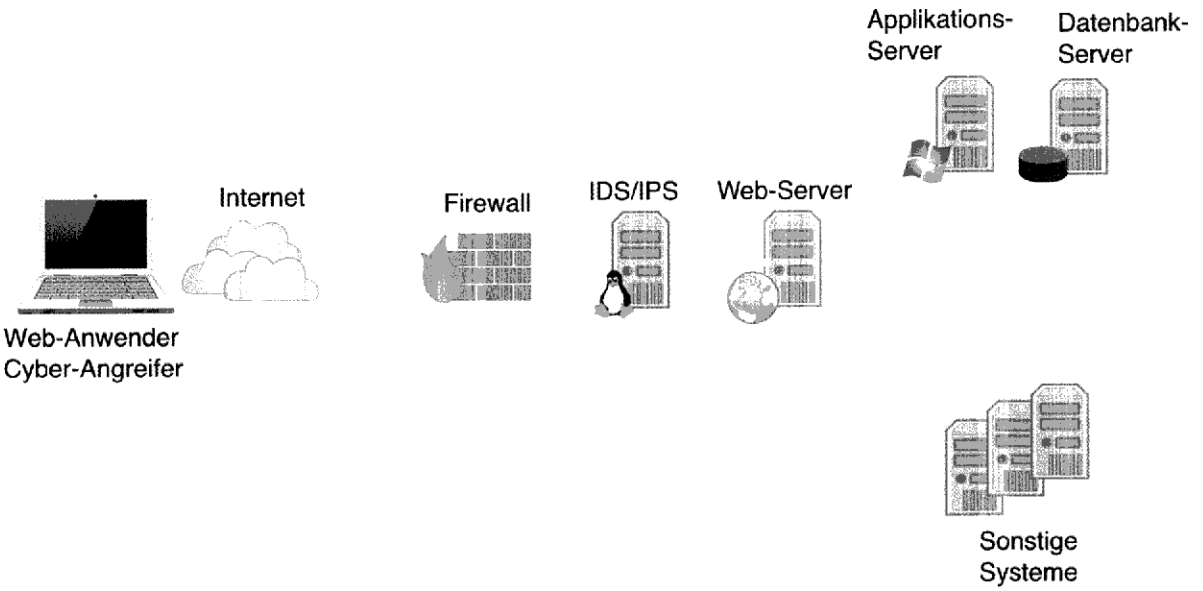

Abb. 1

Die Funktionen der einzelnen Server inklusive der darauf betriebenen Dienste beschreiben sich wie folgt:

---

[1] Z.B. Auflistung in der Anlage BB12 (Bl. 112 f d.A. Bd. VI) zum Schriftsatz der beklagten Partei vom 10.08.2018

[2] Siehe auch Seite 4 Privatgutachten Prof. Dr. Martini vom 20.11.2012 (Anlage BB 5 zum Schriftsatz der Beklagten vom 30.11.2012, Bl. 26 ff. Bd. IV d.A.)

- **Firewall:** Überwacht den Datenverkehr zwischen verschiedenen Netzwerken. Sie dient dazu, unerwünschten oder schädlichen Datenverkehr zu blockieren und berechtigten Datenverkehr zuzulassen, basierend auf vordefinierten Regeln. Firewalls arbeiten regelbasiert und kennen somit nur bekannte Muster von Bedrohungen.
- **IDS (Intrusion Detection System) und IPS (Intrusion Prevention System):** Sicherheitstechnologien, die Netzwerke, Systeme und Anwendungen vor Cyberangriffen schützen sollen. IDS bezeichnet Überwachungssysteme, die den Netzwerkverkehr oder Aktivitäten in einem System analysieren und verdächtige Vorgänge erkennen. IPS erweitert die Funktionalitäten von IDS um die Möglichkeit, erkannte Angriffe direkt zu stoppen.
- **Security Information and Event Management Systeme (SIEM):** Software zur Protokollierung und Analyse sicherheitsrelevanter Ereignisse. Damit können Cyberbedrohungen erkannt und im besten Fall hinreichend schnell darauf reagiert werden.
- **Webserver:** Liefert statische Webinhalte in Form von HTML-Seiten, Dateien, Bildern, Videos an anfragende Host-Systeme, die dort im Webbrowser angezeigt und ggf. auch mit Daten bedient werden können. Webserver stellen dazu die angefragten Inhalte zur Auslieferung zusammen und betreiben die technische Kommunikation mit den zugreifenden Host-Systemen.
- **Applikations-Server:** Betreibt die eigentliche Anwendung (z.B. Prüffunktionen, die beim Versuch der Anmeldung eines registrierten Nutzers ablaufen).
- **Datenbank-Server:** Dient als Datenquelle (z.B. Datenbank der registrierten Nutzer).
- **Load Balancer:** Verteilt die Last bei Einsatz mehrerer nachgeschalteter Webserver.
- **Verzeichnisdienste:** Verwalten Ressourcen, Benutzer, Geräte oder Dienste innerhalb eines Netzwerks und machen sie leicht auffindbar.
- **Personalisierungsdienste:** Passen Inhalte, Funktionen oder Erlebnisse an die individuellen Bedürfnisse, Vorlieben oder das Verhalten von Nutzern an. Sie sind ein wesentlicher Bestandteil moderner Web- und App-Systeme und tragen dazu bei, Nutzerinteraktionen effektiver und attraktiver zu gestalten.
- **Authentifizierungsdienste:** Eine wesentliche Komponente zur Web-Sicherheit als Grundlage für den Schutz von Benutzerdaten, Systemressourcen und Anwendungen. Dabei handelt es sich um Systeme oder Protokolle zur Prüfung, ob eine Person oder ein System tatsächlich diejenige Entität ist, die sie vorgibt zu sein.

Solche Backend-Systeme stellen Webseiten zur Verfügung, die von darauf zugreifenden Host-Systemen mittels Software, typischerweise Web-Browser, bedient werden. Die Dienste und Systeme der Backend-Infrastruktur sind damit für den „normalen" Nutzer, der Internetseiten mit den technischen Mitteln üblicher Browser bedient, intransparent. Insbesondere hat der „normale" Nutzer keine Möglichkeit, den Aufbau von Backend-Systemen zu eruieren oder darauf zuzugreifen.

Die so oder ähnlich ausgestatteten Backend-Systeme sind allerdings oftmals mit Schwachstellen behaftet, auch bei Einsatz aller zur Verfügung stehenden sicherheitstechnischen Maßnahmen. Diese Schwachstellen können als Einfallstor für Cyberangriffe genutzt werden.

Solche Schwachstellen ermöglichen es dem Angreifer, Attacken mit Zielen wie z.B. der Manipulation von Authentifizierungsdaten, dem Abgreifen von Authentifizierungsdaten, sensibler Daten oder Nutzerdaten, der Kompromittierung von Webseiten oder dem Auslesen von Daten/Dokumenten aus Datenbankservern auszuführen. Darüber hinaus können über diesen Weg weitere Netzwerke des Webseitenbetreibers entsprechend angegriffen werden.

Die von Angreifern am häufigsten genutzten Schwachstellen sind z.B. in der jährlich aktualisierten OWASP Top10 Liste[3] veröffentlicht.

4. Angriffsanalysen und die Rolle der IP-Adresse an zwei Beispielen

Um gegebenenfalls davon verursachte Schäden zu erkennen, deren Auswirkung einzuschätzen und solche Angriffe künftig zu verhindern, müssen die Verläufe von Angriffen detailliert rückverfolgt und analysiert werden.

Die Vorgehensweise dazu beschreibt sich an den folgenden beiden Beispiel-Cyberangriffen, welche die drei Schwachstellen A04-Insecure Design, A05-Security Misconfiguration und A5-Vulnerable und Outdated Components der OWASP Top10 2021 in einer alltäglichen Art und Weise ausnutzten.

Beispiel 1: Konstruiertes Beispiel zur Isolation einer IP-Adresse und der daraus aufbauenden Analyse eines Cyberangriffs

Ein detailliertes Beispiel zur Isolation einer IP-Adresse und der daraus resultierenden Analyse eines Cyberangriffs wird in folgendem Artikel „Using Logs to Investigate a Web Application Attack“ beschrieben:

https://www.acunetix.com/blog/articles/using-logs-to-investigate-a-web-application-attack/

Beispiel 2: Dokumentation eines realen Cyberangriffs und dessen Nachbearbeitung aus der Praxis von IT-Sicherheitsverantwortlichen

Der im Folgenden beschriebene Fall dokumentiert einen realen Cyberangriff und dessen Nachbearbeitung.

Ein Konzern mit zahlreichen Webservern wurde Opfer eines Cyberangriffs. Der Angriff begann mit dem Ausnutzen einer Schwachstelle in einer veralteten WordPress-Installation4 eines Webservers, die durch nicht aktualisierte Plugins entstanden war. Der Angreifer verschaffte

---

[3] **Open Worldwide Application Security Project (OWASP)** ist eine Non-Profit-Organisation mit dem Ziel, die Sicherheit von Software zu verbessern. U.A. stellt die OWASP eine jährlich aktualisierte Top10 Liste der kritischsten Web-Services-Schwachstellen frei zugänglich über ihr Internetportal zur Verfügung s. https://owasp.org/Top10/

[4] WordPress ist eine Content-Management-Plattform, die es auch dem unbedarften Programmierer ermöglicht, Webseiten zu erstellen und zu verwalten. Mit Hilfe von Plugins kann WordPress um diverse Funktionen erweitert werden. Derzeit existieren über 60.000 Plugins, die der Nutzer aus dem Internet herunterladen und seiner WordPress-Konfiguration hinzufügen kann. Derartige Plugins beinhalten oftmals technische Schwachstellen, die von Angreifer ausgenutzt werden. Darüber hinaus lassen sich die Quellcodes von Plugins mittels Code-Editor bearbeiten und anpassen, so dass dadurch die Gefahr von Schwachstellen (ungewollt) weiter verschärft werden kann.

sich darüber den Zugang auf diesen Server, lud eine Web-Shell5 hoch und nutzte diese, um Befehle auszuführen.

Dies gab ihm die Möglichkeit, im weiteren Angriffsverlauf andere Server im internen Netzwerk mit Malware zu infizierten. Dies führte zu Serverausfällen, Produktionsstillständen, Datenverlusten und Manipulationen an Webseiten.

Nach der Entdeckung des Angriffs wurde eine IT-forensische Analyse durchgeführt, um Schadensbild und -umfang zu erfassen, kompromittierte Systeme zu identifizieren und die Infrastruktur zu bereinigen. Ein zentraler Bestandteil der Analyse war die Identifikation von Kompromittierungsindikatoren (IoCs) 6.

Als Kompromittierungsindikatoren konnte dabei die vom Angreifer genutzte, dynamische IP-Adresse herausgefunden werden, die in den Zugriffs-Logdateien eines betroffenen Webservers protokolliert wurde. Alternative Kompromittierungsindikatoren konnten im Analyseverlauf nicht ermittelt werden, so dass die IP-Adresse der einzige, zielführende Kompromitierungsindikator war.

Könnte der Angreifer aber löschen.

Diese dynamische IP-Adresse ermöglichte es, alle Server nach verdächtigen Zugriffen zu durchsuchen, die Vorgehensweise des Angreifers nachzuvollziehen und das Einfallstor – ein veraltetes WordPress-Plug-In – zu identifizieren.

Ohne die gespeicherte dynamische IP-Adresse wären die Angriffswege und betroffenen Systeme nicht rekonstruierbar gewesen.

Je nach IP-Adr., z.B. DDOS.

---

[5] Benutzerschnittstelle zur Eingabe und Ausführung von Befehlen zur Fernsteuerung von Webservern.

[6] **Indicator of Compromise (IoC)** ist in der Computerforensik ein Artefakt, das in einem Netzwerk oder Betriebssystem beobachtet wird und mit hoher Wahrscheinlichkeit auf einen Computerangriff hinweist. Typische IoCs sind Virensignaturen und IP-Adressen, MD5-Hashes von Malware-Dateien oder URLs bzw. Domänennamen von Botnet-Befehls- und Kontrollservern.

5. Beweisfragen (1)

5.1. Grundlagen

Während oder nach erfolgten Cyberangriffen ist es in der Regel notwendig, diese mit folgenden Zwecken zu analysieren:

- Erkennung der Angriffsart: Identifikation, ob es sich beispielsweise um SQL-Injections, Cross-Site-Scripting (XSS), Distributed-Denial-of-Service-Angriffe (DDoS) usw. handelt.
- Feststellung der Einfallstore und Angriffswege: Feststellung, welche Schwachstellen ausgenutzt wurden und über welche Infrastrukturteile die Angreifer Zugang erlangt haben.
- Ermittlung angegriffener Systeme, Dienste, Datenbanken, Accounts und verursachter Schäden: Z.B. Datenexfiltration, Malware-Infiltration oder Manipulation von Daten.
- Verbesserung der Systemsicherheit: Die Auswertung gespeicherter dynamischen IP-Adressen kann Hinweise auf sicherheitsrelevante Muster (z. B. wiederholte Zugriffe von verdächtigen IP-Bereichen) liefern. Die daraus gewonnenen Erkenntnisse ermöglichen das Aufsetzen möglichst geeigneter Sicherheitsmaßnahmen gegen künftige, gleichgeartete Cyberangriffe.
- Auswertung für forensische Zwecke: Vorbereitung einer Nachvollziehbarkeit für interne Sicherheitsbewertungen oder als Hilfeleistung zu der Unschädlichmachung von Botnets, deren Zweck ein Angriff auf von der Beklagten betriebene, öffentlich zugängliche Telemedien ist.

Die Grundlagen, aus denen die relevanten Erkenntnisse gewonnen werden, hängen von der Art des konkret ausgeführten Cyberangriffs ab.

Die Beweisfrage (1) reduziert die relevanten Cyberangriffsarten auf solche, die von zugreifenden Host-Systemen im Rahmen des Betriebs von öffentlich zugänglichen Telemedien, wie sie die Beklagte betreibt, ausgehen und geführt werden.

Solche Angriffe nutzen typischerweise die von Webseitenbetreibern über das Internet angebotenen Web-Dienste als Einfallstore. Angreifer durchsuchen die dazu betriebenen Backend-Infrastrukturen gezielt nach Schwachstellen, die Einfallstore auf deren Systeme und Dienste liefern. Oftmals sind dies:

1. Nutzung von Komponenten mit bekannten Schwachstellen:

   Fündig werden Angreifer in der Regel bei veralteten oder schlecht gepflegten Content-Management-Systemen (CMS) wie Joomla, TYPO3, WordPress, Drupal..., die bekannte Sicherheitslücken aufweisen.

   Insbesondere deren Möglichkeit der Verwendung von Plugins zur Erweiterung der Funktionalität von Webseiten bietet Einfallstore für Cyberangriffe.

   So bietet z.B. WordPress derzeit ca. 58.000 kostenlos verfügbare, von Dritten erstellten Plugins an, die jedoch den größten Anteil (>90%) der gemeldeten WordPress Sicherheitslücken verursachten.

2. Sicherheitsrelevante Fehlkonfigurationen: Z.B. unsichere Standardkonfigurationen, ungeschützte Cloud-Speicher, fehlerhafte HTTP-Header oder ausführliche Fehlerausgaben, die vertrauliche Informationen preisgeben.
3. Injection-Angriffe: Angriffsgegenstand sind Datenbanken und Web-Dienste unter Ausnutzung gezielter Eingaben, um Serverfunktionen zu manipulieren (z. B. SQL-, LDAP- oder Command-Injection).

Datenbasis und Grundlage für die Analyse solcher Cyberangriffe sind Logdateien, die von den einzelnen Servern/Diensten der betroffenen Backend-Infrastruktur geführt werden. Bei den hier relevanten Angriffsarten werden dazu in erster Linie die in Webservern geführten Zugriffslogdateien (Access Logs) herangezogen. Andere in solchen Backend-Infrastrukturen geführte Logdateien wie z.B. der IDS/IPS-Dienste, der Firewalls, Autorisierungsdienste, Datenbankserver, RDP-Logs, usw. können dazu Informationen sein.

Zugriffslogdateien von Webservern können detaillierte Informationen zu jeder Anfrage, die Clients (Browser, Skript, Bot usw.) an die Backend-Infrastruktur stellen, protokollieren. Welche Daten zu jeder Anfrage darin abgelegt werden, kann aus einer festgelegten Menge an Datenfeldern ausgewählt werden. Die Konfiguration, welche dieser Felder gespeichert werden, obliegt den Administratoren und hängt von den betrieblichen Anforderungen der jeweiligen Backend-Infrastruktur ab. Dabei wird z.B. auch festgelegt, ob die IP-Adresse des zugreifenden Hosts gespeichert und ob die IP-Adresse anonymisiert wird oder nicht.

Allgemein dienen diese protokollierten Daten der Fehlerdiagnose und Fehlerbehebung von Webanwendungen, statistischen Auswertungen z.B. zu Besucherzahlen, Nutzungsmustern und Geolokalisierung der Nutzer, Leistungsoptimierung der Backend-Infrastruktur usw. Für solche Nutzungen ist eine Protokollierung und Speicherung der vollständigen, nicht-anonymisierten dynamischen IP-Adresse über den konkreten Nutzungsvorgang hinaus nicht erforderlich.

Die sehr umfangreichen Datenbestände in den Zugriffslogdateien eignen sich aber insbesondere auch für die Analysen von Cyberangriffen der vorgenannten Arten.

Gespeicherte dynamische IP-Adressen der zugreifenden Host-Systeme dienen dabei z.B. als Datenpool, um daraus u.U. die für die weiteren Analysen und Ermittlungen notwendigen und oftmals zielführenden Kompromittierungsindikatoren zu isolieren.

Der Kompromittierungsindikator ist ein wesentliches Merkmal von Cyberangriffen. Er dient als Grundlage zur Festlegung und Durchführung weiterer Analyseschritte, um z.B. damit Angriffskorrelationen von Cyberattacken aufzudecken. Ein oftmals für die weiteren Analysen initialer und einziger Kompromittierungsindikator ist eine in den Zugriffprotokollen gespeicherte, immer wiederkehrende und/oder in ihren Benutzungskontexten auffällige IP-Adresse zugreifender Host-Systeme.

Basierend auf diesen Grundlagen beantworten sich die Beweisfragen unter (1) wie folgt:

5.2. Zu Beweisfrage (1) a)

Die Protokollierung und Speicherung dynamischer IP-Adressen von zugreifenden Host-Systemen über die Dauer des konkreten Nutzungsvorgangs hinaus im Rahmen des Betriebs von öffentlich zugänglichen Telemedien, wie sie die Beklagte betreibt, dient zumindest den folgenden sicherheitstechnischen Zwecken:

1. **Ermittlung von Angriffsstrategien**
    - **Korrelation von Ereignissen:** Die IP-Adresse dient zur Identifikation von Kompromittierungsindikatoren und Angriffsmustern. Damit können z.B. Angriffe aus verschiedenen Logs (z.B. Webserver-Logs, IDS/IPS-Logs) miteinander verknüpft werden.
    - **Zielgerichtetheit:** Mit der IP-Adresse lässt sich feststellen, ob ein Angriff gezielt gegen einen bestimmten Server/Dienst in der gesamten Backend-Infrastruktur sowie ggf. in allen damit verbundenen Netzwerken durchgeführt wurde.
    - **Häufigkeit**: Mit der IP-Adresse kann festgestellt werden, ob von dem zugreifenden Host-System aus über einen längeren Zeitraum Angriffsvorbereitungen getroffen und Angriffsversuche durchgeführt wurden.
    - **Verbindung zu früheren oder koordinierten Angriffen:** Angreifer nutzen häufig wiederholt bestimmte IP-Adressen oder Adressräume. Eine vollständige Adresse hilft, Muster und Zusammenhänge zu früheren oder zu koordinierten Angriffen zu erkennen.
2. **Aufdecken von Schwachstellen in der Backend-Infrastruktur**

    Mit der IP-Adresse können die ausgenutzten Schwachstellen in der Backend-Infrastruktur wie z.B. veraltete CMS Plugins ermittelt werden Zudem können sie auf die Verwendung von Exploit-Tools[7] hinweisen, die spezifisch für bestimmte Netzwerke oder Systeme eingesetzt werden. Die Erkenntnisse daraus liefern die Grundlagen dazu, die Backend-Infrastruktur gegen diese konkreten Angriffsarten abzuhärten.
3. **Blockierung**: z.B. Blacklisting[8] auffälliger IP-Adressen z.B. in Firewalls.
4. **Unterstützung forensischer Analysen**: Bereitstellung von Daten zur technischen und auch rechtlichen Nachvollziehbarkeit. Die Erkenntnisse daraus liefern z.B. die technischen Grundlagen der Hilfeleistungen zu der Unschädlichmachung von Botnets.

---

[7] **Exploit-Tools**: Programme zum Ausnutzen von Schwachstellen in Computersystemen, Netzwerken oder Anwendungen

[8] **Blacklisting:** Liste, in der bestimmte Elemente, wie Benutzer, IP-Adressen, Dateien, Programme oder Inhalte, explizit als unerwünscht oder verboten markiert werden.

5. **Identifikation der Quelle der Attacke**
    - **Geolokalisierung:** Die vollständige IP-Adresse erlaubt es, den geografischen Ursprung der Attacke zu bestimmen, z. B. das Land oder die Region, aus der der Angriff stammt.
    - **Zuordnung zu einem Netzwerk:** Sie ermöglicht die Identifikation des zugehörigen Internetdienstanbieters (ISP) oder Netzwerks. Dies liefert z.B. die technische Grundlage, um verdächtige Aktivität aus bestimmten autonomen Systemen (AS) zu erkennen und ggf. zu verhindern.

5.3. Zu Beweisfrage (1) b)

Die Speicherung der dynamischen IP-Adressen von zugreifenden Host-Systemen über die Dauer eines Nutzungsvorgangs bewirkt und ermöglicht verschiedene sicherheits-, rechts- und betriebsrelevante Funktionen. Diese gruppieren sich wie folgt:

1. Feststellung, ob und in welchem Umfang unbemerkte Cyberangriffe für den Angreifer erfolgreich waren:
    - Ohne gespeicherte Daten wäre es unmöglich, unautorisierte Zugriffe nachzuvollziehen, die z. B. zu einem späteren Zeitpunkt entdeckt werden.
    - Beispiel: (s. die oben genannten, beiden Beispiele).
2. Rückverfolgbarkeit von Interaktionen:
    - Die IP-Adresse ermöglicht es, Zugriffe einem spezifischen Gerät oder Netzwerk zuzuordnen. Dies ist besonders wichtig für die Rekonstruktion von Ereignissen im Nachhinein.
    - Beispiel: Bei einem Datendiebstahl kann die protokollierte IP-Adresse helfen, den Zugriffspunkt und Zeitpunkt des Angriffs zu identifizieren.
3. Ermittlung der Korrelationen von Angriffsmustern:
    - Gespeicherte IP-Adressen dienen als Ausgangspunkt, um wiederkehrende Angriffsversuche von einer oder mehreren Adressen zu erkennen.
    - Beispiel: Mehrere SQL-Injections aus denselben oder ähnlichen IP-Bereichen können auf ein gezieltes Angriffsszenario hinweisen.
4. Identifikation von Anomalien:
    - Abweichungen vom normalen Zugriffsmuster können erkannt werden. Dadurch wird z.B. ein rechtzeitiges Blacklisting solcher IP-Adressen ermöglicht. Damit können weitere Aktionen, die von solchen IP-Adressen ausgehen, verhindert werden.
    - Beispiel: Eine ungewöhnlich hohe Anzahl von Anfragen von einer IP-Adresse innerhalb kurzer Zeit (z. B. ein Brute-Force-Angriff).
5. Forensische Untersuchungen:
    - Die IP-Adresse bildet einen essenziellen Teil der Beweiskette, die für die Untersuchung von Cybervorfällen notwendig ist.

- Beispiel: Bei der Untersuchung eines Distributed-Denial-of-Service-Angriffs (DDoS) helfen gespeicherte IP-Adressen, die beteiligten Botnetz-Knoten zu identifizieren und durch deren Internetdienstanbieter (ISP) unschädlich machen zu lassen.

6. Geobasierte Zugriffsanalysen:
   - Analysen der Herkunft von Anfragen können regionale Angriffsmuster erkennen oder unerwünschte Zugriffe aus bestimmten Regionen blockieren, z.B. bei Angriffsversuchen ausländischer, hacktivistisch aggierender Cybergruppierungen.

5.4. Zu Beweisfrage (1) c)

Die Speicherung von IP-Adressen zugreifender Host-Systeme über die Dauer des Nutzungsvorgangs hinaus erfolgt in der Regel abhängig von der Konfiguration und Funktionsweise der konkreten Backend-Infrastruktur an spezifischen Speicherorten.

Typischerweise sind dies Speicherorte, die von folgenden Servern/Diensten geführt werden:

1. **Webserver:** Bei Webservern wie z.B. Apache HTTP Server oder NGINX[9] kann die dynamische IP-Adresse des zugreifenden Hosts im konfigurierbaren „access log“[10] über die Dauer des konkreten Nutzungsvorganges hinaus gespeichert werden.
2. **Intrusion Detection/Prevention Systeme (IDS/IPS) und Security Information and Event Management Systeme (SIEM)** protokollieren und speichern IP-Adressen. Sie sammeln dazu auch Logs aus verschiedenen Quellen (z. B. Firewalls, Webserver, Netzwerksensoren) und speichern sie in zentralisierten Logdatenbanken oder auf dedizierten Analyseplattformen.
3. **Firewalls und Router**: Protokollieren eingehende und ausgehende Verbindungen und speichern diese Daten lokal oder auf zentralen Servern.
4. **Datenbanken zur Langzeitspeicherung:** IP-Adressen können für Langzeitanalysen in Datenbanken abgelegt werden. Die Daten werden in relationalen oder NoSQL-Datenbanken gespeichert und ggf. mit weiteren Informationen angereichert.

Umfang und Speicherorte hängen von individuellen technischen und organisatorischen Gegebenheiten sowie dem individuellen Schutzbedarf und jeweiligen Backend-Infrastruktur ab.

[9] Beide Webserversysteme haben zusammen derzeit einen Marktanteil von ca. 50 %. Quelle: https://maxcluster.de/blog/webserver-vergleich-apache-nginx-caddy

[10] Quelle z.B.: https://httpd.apache.org/docs/2.4/logs.html#accesslog

5.5. Zu Beweisfrage (1) d)

Wer Zugriff auf gespeicherte IP-Adressen hat, hängt maßgeblich von den organisatorischen und technischen Gegebenheiten der jeweiligen Backend-Infrastruktur ab. In der Regel ist der Zugriff auf die Nutzergruppen beschränkt, die zur sachgerechten Erledigung ihrer Aufgaben auf den Zugriff angewiesen sind. Dies sind im Wesentlichen:

1. **Systemadministratoren** von Servern/Diensten der Backend-Infrastruktur haben immer direkten Zugriff auf solche Logdateien zur Überwachung, Fehlerbehebung und Verwaltung der Backend-Infrastruktur.
2. **Sicherheitsverantwortliche** (IT-Security-Teams) insbesondere zur Untersuchung von Sicherheitsvorfällen.
3. **Datenschutzbeauftragte** greifen auf Access-Logdateien zu, z.B. um Verstöße gegen den Datenschutz zu bewerten.
4. **Entwickler/Support-Teams** können in seltenen Fällen begrenzten Zugriff auf Logdateien benötigen, z.B. bei der Fehleranalyse (Debugging) oder der Behebung von Problemen oder Ausfällen in Bereichen der Backend-Infrastruktur.

5.6. Zu Beweisfrage (1) e)

Um die unter 5.2 beschriebenen, sicherheitstechnischen Zwecke zu erreichen, müssen zu jeder Anfrage gemeinsam mit der IP-Adresse weitere Log-Daten gespeichert werden. Die folgende Auflistung gruppiert nach dem Zweck der Speicherung:

1. **Ermittlung von Angriffsstrategien**
    - **Zeitstempel:** Uhrzeit, um Ereignisse chronologisch zu analysieren und Korrelationen zwischen Logs zu erkennen.
    - **Protokolltyp:** Angabe des verwendeten Protokolls (z. B. HTTP, HTTPS, SMTP, SSH, FTP).
    - **Angeforderte Ressource/URL:** Die spezifische angefragte Ressource (Web-Seite), die Rückschlüsse auf den Angriffsvektor ermöglicht (z. B. /wp-login.php).
    - **HTTP-Methoden:** GET, POST, PUT, DELETE liefern die Grundlage, um potenziell bösartige Aktivitäten zu identifizieren.
    - **Antwortstatus:** HTTP-Statuscodes (z. B. 404, 500), um zu erkennen, ob die Anfragen erfolgreich waren oder Fehlermeldungen zurückgegeben wurden.
    - **Benutzeragent:** Informationen über das Gerät oder den Browser, die auf automatisierte Tools hinweisen können.
    - **Verbindungsquelle:** Informationen wie Portnummern oder verwendete Netzwerkprotokolle.
    - **Signatur oder Regel-ID**, die den Angriff beschreibt.
    - **Schweregrad** (Severity) des Ereignisses.

- **Zieladresse/Zielport:** Die Adresse (IP-Adresse) des angegriffenen Systems und Nummer des genutzten Ports.

2. **Aufdecken von Schwachstellen in der Backend-Infrastruktur**
   - **Exploit-Indikatoren:** Hinweise auf die verwendeten Schwachstellen (z. B. bestimmte Anfrageparameter oder URLs).
   - **Betroffene Systeme/Dienste:** Logs, die die Zielkomponenten der Angriffe angeben (z. B. Datenbankserver, Webserver, CMS-Plugins).
   - **Fehlermeldungen:** System- oder Anwendungsmeldungen, die durch den Angriff ausgelöst wurden und auf Schwachstellen hinweisen.
   - **Authentifizierungsversuche:** Daten zu erfolgreichen oder fehlgeschlagenen Login-Versuchen, um Brute-Force-Angriffe zu erkennen.
   - **Blockierung:** Dazu werden keine über die zu blockierende IP-Adresse hinausgehende Daten benötigt.
3. **Unterstützung forensischer Analysen**
   - **Kompletter Netzwerkverkehr:** (z. B. durch Packet Capture Tools wie Wireshark).
   - **IDS/IPS-Warnungen:** Details zu erkannten Angriffen.
   - **Systemprotokolle:** Fehler- oder Ereignisprotokolle von betroffenen Servern oder Anwendungen.
   - **Authentifizierungsprotokolle:** Informationen über die Nutzung von Benutzerkonten, einschließlich von Passwortversuchen.
   - **DNS-Logs:** Informationen zu DNS-Anfragen, die auf C2-Kommunikation (Command and Control) hinweisen können. → also URLs.
   - **Identifikation der Quelle der Attacke:** Dazu werden keine über die zu blockierende IP-Adresse hinausgehende Daten benötigt.

Bemerkung:

Die o.g. Auflistungen beinhaltet u.a. auch die Log-Daten, die zur Konfiguration des Apache „access log“ zur Verfügung stehen11.

[11] Siehe: https://httpd.apache.org/docs/2.4/logs.html

6. Beweisfragen (2)

6.1. Zu den Beweisfragen 2) a) und b)

Als Grundlage für die zur Ermittlung von Angriffsstrategien erforderlichen Analysen der Korrelation von Ereignissen, der Zielgerichtetheit, der Häufigkeit und der Verbindung zu früheren oder koordinierten Angriffen ist die vollständige, nicht anonymisierte IP-Adresse das effektivste und oftmals einzige Mittel. Dies gilt ebenso für die Tätigkeiten zum Aufdecken ausgenutzter Schwachstellen in der Backend-Infrastruktur. Auf die beiden in Kap. 4 aufgeführten Beispiele dazu wird verwiesen.

Alternativ werden folgende Mittel/Maßnahmen genannt, die sich zusammen mit ihrer Brauchbarkeit zum Erreichen der vorgenannten Zwecke wie folgt beschreiben:

1. **Pseudonymisierung:** Der Austausch der IP-Adresse in den Logfiles gegen ein Pseudonym (wie z.B. Client 1, Client 2, Client 3, usw.) erlaubt zwar die Unterscheidung einzelner zugreifender Hosts. Jedoch gehen dabei sämtliche aus der IP-Adresse erkennbaren Muster verloren, beispielsweise dass die Clients 1, 2 und 3 vom Provider XYZ aus dem Land ABC stammen. Zudem besteht die Gefahr, dass unterschiedliche Clients fehlerhaft auf dasselbe Pseudonym zugeordnet werden, wodurch die Unterscheidbarkeit eingeschränkt oder aufgehoben werden kann.
2. **Hashing**[12]**:** Das Ersetzen der IP-Adressen in den Logfiles durch eine Zahl mittels Hashing ermöglicht zwar die Ermittlung von Angriffsstrategien. Jedoch gewährleistet dieses Verfahren keinen Datenschutz. Z.B. können mit einer leicht zu programmierenden Software etwa alle 2 hoch 32 existierenden IPv4-Adressen in ihre jeweiligen Hashwerte umrechnen und diese in einer Tabelle abspeichern werden. Bei Bedarf könnte der pseudonymisierende Hashwert als Schlüssel zur Abfrage der zugehörigen IP-Adresse aus dieser Tabelle genutzt werden.
3. **Netzwerküberwachungstools:** Systeme wie SIEM (Security Information and Event Management) können Angriffsmuster oft, aber nicht immer korrelieren, ohne auf vollständige IP-Adressen angewiesen zu sein. Sie ersetzen daher nicht die vollständige, nicht-anonymisierte IP-Adresse zum Erreichen der vorgenannten sicherheitstechnischen Zwecke.
4. **Moderne, regelmäßig aktualisierte Software:** Diese Maßnahme ist grundsätzlich notwendig, da sie die Basis für eine gesicherte Backend-Infrastruktur bildet. Dabei ist jedoch folgendes zu berücksichtigen:

   Häufig sind aktuelle Schwachstellen, etwa in Plugins in den jeweils verfügbaren Softwareupdates nicht berücksichtigt. Beispielhaft wird auf die oben genannte Problematik der Plugins von Content-Management-Systemen verwiesen.

[12] **Hashing** ist ein mathematisches Verfahren (z.B. SHA256), mit dem Daten beliebiger Größe in einen fixen Zahlenwert umgewandelt werden.

Aktuell gewinnen diesbezüglich die Möglichkeiten der Sprachmodelle der „Künstlichen Intelligenz" zunehmend an Bedeutung. Diese ermöglichen das automatische Erstellen oder zumindest die Unterstützung bei der Erstellung von Quellcodes umfangreicher und komplexer Softwaresysteme.

Angreifern stehen dadurch im beschleunigten Maße immer neue oder weiterentwickelte Angriffstechniken und -methoden auf Server/Dienste zur Verfügung. Darüber hinaus können auch softwaretechnisch unbedarfte Angreifer die KI zur Erstellung von Software für Cyberattacken nutzen.

Dadurch wird sich nicht nur das Repertoire der Angriffstools, sondern auch die Anzahl von Angreifern vergrößern[13].

Dies führt zwangsläufig zu einer Zunahme und dem Auftreten neuer Angriffsmethoden in zunehmend kürzeren Zeitabständen. Da diese erst nach den ersten damit ausgeführten Cyberangriffen bekannt werden, können Verantwortliche sie erst danach in die Software der davon betroffenen Server oder Dienste integrieren. Die aktualisierten Sicherheitsmaßnahmen lassen sich dann erst in den Backend-Infrastrukturen anwenden. Regelmäßige Softwareaktualisierungen der Server/Dienste in Backend-Infrastrukturen bleiben dennoch wirksam, wenn auch in reduzierter Form.

Ferner ist zu beachten, dass Entwickler von Web-Services und deren Updates ebenfalls die Möglichkeiten der KI zur Softwareerstellung nutzen. Die Ergebnisse dieser KI-unterstützten Programmierung sind derzeit aus verschiedenen Gründen oft fehlerbehafteter als die der klassischen Programmierung. Bereits jetzt ist eine Zunahme fehlerhafter Softwareupdates, die Schwachstellen aufweisen, erkennbar[14].

Zusammenfassend ist die regelmäßig und zeitnah durchgeführte Softwareaktualisierung ein notwendiger, aber nicht hinreichender Bestandteil von Maßnahmen zur Erhaltung einer möglichst hoch gegen Cyberangriffe gehärteten Backend-Infrastruktur.

5. Systemtrennung: Damit werden verschiedene Dienste, Anwendungen oder Funktionen auf unterschiedliche physische oder virtuelle Server so verteilt, dass sie möglichst nicht in einem Netzwerk mit der Backend-Infrastruktur zusammenliegen. Diese Dienste sind damit nicht für Cyberangriffe, die von zugreifenden Host-Systemen geführt werden, erreichbar. Dadurch wird die Angriffsfläche insgesamt eingeschränkt.

   Allerdings wird auch mit dieser Maßnahme kein vollständiger Schutz gegen Cyberangriffe von zugreifenden Host-Systemen erreicht. So wirken z.B. Cross-Site-Scripting (XSS) auf die Webanwendungsebene (insbesondere Webserver), die nicht aus der Backend-Infrastruktur herausgenommen werden können.

---

[13] vgl. Cybercrime Bundeslagebild 2023 des BKA zum Download unter: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2023/CC_2023.html

[14] Quelle z.B.: https://www.wordfence.com/blog/2023/02/the-wordpress-ecosystem-is-becoming-more-secure-with-responsible-disclosure-becoming-more-common/

Darüber hinaus steht eine Vielzahl weiterer möglichen Mittel und Maßnahmen wie z.B. die Nutzung von IDS (Intrusion Detection System) und IPS (Intrusion Prevention System), Security Information and Event Management Systeme (SIEM), regelmäßige Überprüfungen z.B. mittels Penetrationstests usw. zur Verfügung, die insgesamt zwar zusammen mit den hier genannten Mitteln und Maßnahmen die Sicherheit von Backend-Infrastrukturen auf ein hohes Niveau bringen können. Einen vollständigen Schutz bieten diese jedoch auch in kombinierter und der jeweiligen, individuellen Konfiguration der Backend-Infrastrukturen angepassten Anwendung nicht.

Zusammenfassend ist die Protokollierung und Speicherung der vollständigen, nicht-anonymisierten dynamischen IP-Adresse über den konkreten Nutzungsvorgang hinaus zwingend erforderlich, um die einzelnen zu Ziffer (1) beschriebenen Zwecke jeweils erreichen.

Die zu Ziffer (1) genannten Zwecke können nicht durch andere gleich geeignete Mittel /Maßnahmen erreicht werden.

Bemerkung:

Aufgrund dieser Tatsachen wird in der Praxis neben dem technisch Notwendigen und Machbaren auch das Kriterium des Schutzbedarfes bei der Entscheidung über den Einsatz solcher Sicherheitssysteme berücksichtigt. Allgemein wird der Schutzbedarf in Schutzbedarfskategorien unterteilt.

Das BSI hat dazu beispielsweise die Definition der Schutzbedarfskategorien der Recplast GmbH veröffentlicht[15]. Diese definiert die drei Schutzbedarfskategorien „normal", „hoch" und „sehr hoch".

6.2. Zu Beweisfrage (2) c)

Da die zu Ziffer (1) genannten Zwecke nicht durch andere gleich geeignete Mittel/Maßnahmen erreicht werden können, entfällt eine Beantwortung der Beweisfrage (2) c).

Bemerkung:

Eine ungefähre Schätzung, in welcher Kostengrößenordnung der Einsatz möglicherweise gleich gearteter Mittel/Maßnahmen liegen könnte, ist bezogen auf die Gegebenheiten der Beklagten nicht belastbar möglich. Die Basis, auf der eine solche Schätzung aufbauen könnte, wäre z.B. eine grobe Übersicht darüber, wie allgemein die Infrastruktur der betriebenen Backends ausgestattet ist und ob und wie sie gepflegt wird. Wegen der Vielzahl möglicher auch sehr unterschiedlichen Konfigurationen der betriebenen Backend-Infrastrukturen, dürfte dies jedoch nach der derzeitigen Einschätzung des Sachverständigen kaum zielführend möglich sein.

---

[15] Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Recplast/A21_Definition_Schutzbedarfskategorien.pdf?__blob=publicationFile&v=5

7. Beweisfragen (3)

7.1. Zu Beweisfrage (3) a)

Die Frage, warum die von der Beklagten betriebenen öffentlich zugänglichen Telemedien ohne die Speicherung der vollständigen, nicht-anonymisierten dynamischen IP-Adressen über den konkreten Nutzungsvorgang hinaus auskommen, lässt sich nicht allgemein beantworten. Mögliche Gründe führt die Beklagte in ihrer Replik vom 10.08.2018 an.

Darüber hinaus sind nach der Einschätzung des Sachverständigen folgende Gründe denkbar:

1. **Backend-Infrastruktur und Kosten-Nutzen-Abwägung**
2. **Einfachheit der Infrastruktur**: Systeme, die nur statische Inhalte bereitstellen (z. B. reine Informationswebseiten ohne Nutzerinteraktion), benötigen keine komplexen Backend-Infrastrukturen mit Datenbankserver, Anwendungsserver, Verzeichnisdienste, Personalisierungsdienste, Authentifizierungsdienste und andere Netzwerke, die spezifische Nutzerdaten verarbeiten. In solchen Fällen könnte das Interesse an aufwendigen Analysen sicherheitsrelevanten Cyberangriffen gering sein.
3. **Ersatz vs. Bereinigung**: Backend-Infrastrukturen können so ausgelegt sein, dass bei einem Angriff oder Schadensfall die betroffenen Systeme schnell neu aufgesetzt werden können. Die Wiederherstellung erfolgt über gesicherte Images, Snapshots oder Containerlösungen, was eine detaillierte Analyse entbehrlich machen kann.
4. **Einschätzung des Schutzbedarfs**: Das BSI unterscheidet zwischen den Schutzbedarfskategorien **"Normal"**, **"Hoch"** und **"Sehr Hoch"** (s.o.), basierend auf möglichen Schäden durch Cyberangriffe. Für die Beklagte könnten Reputationsschäden, Verletzungen der Vertraulichkeit, Abgriff geheimer Daten usw. diesbezüglich relevante Kriterien für die Einschätzung des Schutzbedarfes der jeweiligen Backend-Infrastruktur sein.

   Wird der Schutzbedarf als "Normal" eingestuft, können die Sicherheitsvorkehrungen u.U. im geringeren Niveau angelegt werden. Die Speicherung von vollständigen, nicht anonymisierten dynamischen IP-Adressen könnte bei diesen Backend-Infrastrukturen u.U. überflüssig sein. Dies wäre aber in jedem konkreten Fall einzeln zu bewerten.

Aha. Also IP unnötig. Beweislast bei Bekl.

7.2. Zu Beweisfrage (3) b)

Die Beweisfrage, wie häufig sicherheitsrelevante Angriffe oder Bedrohungen auf den von der Beklagten betriebenen öffentlich zugänglichen Telemedien auftreten bzw. wie wahrscheinlich sie sind, lässt sich nur auf der Grundlage belastbarer Statistiken beantworten. Statistiken über Angriffe auf die Telemedien der Beklagten sind allerdings öffentlich nicht zugänglich[16].

Man muss jedoch davon ausgehen, dass die Wahrscheinlichkeit für das Auftreten solcher sicherheitsrelevanten Angriffe oder Bedrohungen auf die vom Bund betriebenen Telemedien

[16] Der Sachverständige hat beim BSI nach derartigen Daten angefragt. Die Antwort ist noch offen und kann ggf. nachgereicht werden.

hoch ist. Dabei stellen nicht nur Angriffe von "üblichen Hacker" signifikante Bedrohungen dar. Von besonderer Bedeutung sind vorliegend auch die Aktivitäten ausländischer hacktivistischer Cybergruppierungen, die oft von Geheimdiensten gesteuert werden[17].

Von den zugreifenden Host-Systemen dieser Angreifergruppen ausgehenden, relevanten Angriffe/Bedrohungen, denen die Backend-Infrastrukturen der Beklagten ausgesetzt sind, listen sich zusammen mit den davon verursachten Schäden, Folgenden und Ausmaßen wie folgt:

1. **Datenverlust und Datenmissbrauch**

   Schäden: Unbefugter Zugriff auf sensible oder persönliche Daten, wie Bürgerdaten, Finanzinformationen oder vertrauliche Regierungsinformationen.

   Folgen: Verlust des öffentlichen Vertrauens, rechtliche Konsequenzen, finanzielle Verluste und mögliche politische Instabilität.

   Ausmaß: Abhängig von der Art und Menge der kompromittierten Daten, können die Auswirkungen von individuellen Datenschutzverletzungen bis hin zu nationalen Sicherheitsrisiken reichen.

2. **Dienstausfall** (Denial of Service, DoS)

   Schäden: Unterbrechung oder Beeinträchtigung der Verfügbarkeit von Online-Diensten, wie Websites, E-Government-Portalen oder Kommunikationssystemen.

   Folgen: Störung des öffentlichen Dienstes, Verzögerungen bei der Bereitstellung wichtiger Informationen und Dienstleistungen, wirtschaftliche Verluste.

   Ausmaß: Kann von kurzfristigen Unterbrechungen bis hin zu langfristigen Ausfällen reichen, die die Funktionsfähigkeit der Regierung beeinträchtigen.

5. **Datenmanipulation**

   Schäden: Unbefugte Änderung oder Manipulation von Daten, wie Finanzdaten, Bürgerdaten oder Regierungsinformationen.

   Folgen: Fehlinformationen, falsche Entscheidungen, finanzielle Verluste, rechtliche Konsequenzen.

   Ausmaß: Kann von kleineren Fehlern bis hin zu groß angelegten Manipulationen reichen, die das Vertrauen in die Regierung und ihre Dienste untergraben.

6. **Ransomware-Angriffe**

   Schäden: Verschlüsselung von Daten und Systemen, gefolgt von Lösegeldforderungen.

   Folgen: Datenverlust, Dienstausfall, finanzielle Verluste, rechtliche Konsequenzen.

---

17 Siehe z.B. https://www.verfassungsschutz.de/DE/themen/cyberabwehr/akteure-und-angriffsmethoden/akteure-und-angriffsmethoden_node.html#doc714088bodyText2

Ausmaß: Kann von einzelnen Systemen bis hin zu großen Netzwerken reichen, die die Funktionsfähigkeit der Regierung beeinträchtigen.

7. **Cyber-Spionage**

   Schäden: Abgreifen vertraulicher Informationen, wie strategische Pläne, diplomatische Korrespondenz, militärische Geheimnisse usw.

   Folgen: Verlust von strategischen Vorteilen, politische Instabilität, nationale Sicherheitsrisiken.

   Ausmaß: Kann von kleineren Informationslecks bis hin zu groß angelegten Spionageoperationen reichen, die die nationale Sicherheit gefährden.

8. **Reputationsschäden**

   Schäden: Verlust des öffentlichen Vertrauens in die Fähigkeit der Regierung, ihre Bürger und Daten zu schützen.

   Folgen: Politische Instabilität, wirtschaftliche Verluste, rechtliche Konsequenzen.

   Ausmaß: Kann von kurzfristigen Imageproblemen bis hin zu langfristigen Vertrauensverlusten reichen, die die Legitimität von Regierungen und deren Organisationen untergraben.

7.3. Zu Beweisfrage (3) c)

Die nach den Recherchen des Sachverständigen einzigen, öffentlich zugänglichen statistischen Erhebungen / Erkenntnisse darüber, ob und wie häufig Angreifer auf Telemedien aufgrund oder infolge einer Speicherung von dynamischen IP-Adressen persönlich tatsächlich identifiziert wurden, sind im „Positionspapier des Bundeskriminalamtes zu erforderlichen Speicherfristen von IP-Adressen“ vom 21. Juli 2023 veröffentlicht[18]. Diese beziehen sich jedoch ausschließlich auf den Bereich des sexuellen Missbrauchs von Kindern.

Demnach wurden dem BKA im Zeitraum von Ende 2021 bis Anfang August 2022 984 IP-Adressen übermittelt. Bei 41% der Vorgänge konnte die IP-Adresse einem Nutzeranschluss als Grundlage der Täteridentifizierung zugeordnet werden.

Hierbei dürfte es sich nach Einschätzung des Sachverständigen um eine Obergrenze erreichbarer Erfolgsquoten handeln.

Darüber hinaus gilt, dass hinter diesen IP-Adressen inländische Privatpersonen stehen. Bei den Angreifern auf die Backend-Infrastruktur der Beklagten handelt es sich jedoch nur zu einem geringen Teil um Täter aus diesem Privatpersonenkreis. Überwiegend agieren hier professionell organisierte Angreifer und Organisationen. Diese verwenden oft gefälschte IP-Adressen unter Benutzung von Proxys und Anonymitätsnetzwerken.

---

18 https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/230623_Mindestspeicherfristen_IP-Adressen.html

Der Sachverständige schätzt daher, dass die Erfolgsquote zur Identifizierung der Angreifer aufgrund oder infolge der Speicherung von dynamischen IP-Adressen in den Backend-Infrastrukturen der Beklagten bei unter 10 % der für die Cyberangriffe verantwortlichen IP-Adressen liegt.

Bei Brute-Force-Angriffen, die von Botnetzen unter Beteiligung zivil oder privat genutzter Webclients ausgehen, dürfte diese Erfolgsquote höher sein.

7.4. Zu Beweisfrage (3) d)

Die Identifikation von Nutzern dynamischer IP-Adressen kann nur von zugeordneten Internet Service Provider (ISP) geleistet werden, da nur dort diese Zusammenhänge entstehen und bekannt sind. Zur Zuordnung ist neben der IP-Adresse auch der Zeitstempel zur Nutzeridentifikation notwendig, denn:

1. **Dynamische IP-Adressen wechseln regelmäßig**: ISPs teilen dynamische IP-Adressen aus einem Pool zu und ändern sie regelmäßig, z. B. alle 24 Stunden. Ohne den Zeitstempel kann der ISP nicht nachvollziehen, welchem Nutzer die IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war.
2. **Nutzung mehrerer Geräte**: Wenn mehrere Geräte dieselbe IP-Adresse nutzen (z. B. in einem Netzwerk hinter einem NAT-Router), kann der genaue Zeitpunkt der Aktivität helfen, den verantwortlichen Nutzer oder das Gerät einzugrenzen.

Darüber hinaus werden oftmals die folgenden Daten benötigt:

1. **Portnummern**: Diese helfen insbesondere bei Carrier-Grade NAT (CGNAT)-Infrastrukturen, wo mehrere Nutzer (z.B. Mehrfamilienhäuser) eine öffentliche IP-Adresse teilen. Das damit gekennzeichnete Host-System und in der Folge dessen Nutzer kann in solchen Konstellationen über die IP-Adresse zusammen mit der Port-Nr. identifiziert werden.
   → nein, wird nämlich Standardmäßig nicht protokolliert.
2. **Protokolldetails**: Informationen zu den verwendeten Protokollen (z. B. TCP oder UDP) und spezifische Zieladressen können ebenfalls zur Identifizierung beitragen. Daher IP wurlos.

Bei Betrieb von "always-on"-Routern bleiben die Host-Systeme kontinuierlich mit dem Internet verbunden. Solche Router kommen besonders häufig im privaten oder unternehmerischen Umfeld zum Einsatz. Diese Konfigurationen ermöglichen es, dass die dynamische IP-Adresse länger konstant bleibt, da der Router durchgehend verbunden ist. Daher erfolgt keine regelmäßige, sondern nur sporadische Zuweisung neuer IP-Adressen durch den Internetdienstanbieter.

Auch bei diesen Konfigurationen wechseln die dynamischen IP-Adressen, wenn auch nicht regelmäßig. Deshalb bedarf es auch der Protokollierung der genannten Daten zusätzlich zur dynamischen IP-Adresse.

8. Gutachterliche Auseinandersetzung mit den Privatgutachten

Die von den Parteien vorgelegten Gutachten/Privatgutachten behandeln die folgenden Fragen[19]:

1. Dient die Speicherung der IP-Adressen dem nationalen und internationalen Stand der Technik?
2. Ist eine Speicherung von IP-Adressen nach dem derzeitigen Stand der Technik zwingend erforderlich oder bestehen andere Möglichkeiten, um die von der Beklagten betriebenen Webseiten vor schadhaften Angriff zu schützen oder die Gefahr von Sicherheitsverletzungen zu mindern?
3. Welche Kosten wären gegebenenfalls für andere Maßnahmen aufzuwenden?

Die 1. Frage an die Parteigutachter ist in den Fragen des Beweisbeschlusses vom 19.09.2018 nicht aufgeworfen. Eine Auseinandersetzung dazu entfällt daher.

8.1. Zur 2. Frage

Die 2. Frage an die Parteigutachter entspricht im Wesentlichen den Fragen (2) a) und (2) b) des Beweisbeschlusses vom 19.09.2018.

Ausführungen des Dr. Ing. Köpsell in seinem Gutachten vom 29.07.2028 sowie ergänzenden Erläuterungen vom 07.05.2012 bearbeiten diesbezüglich die:

- Identifizierung von Angreifern (Gutachten S. 5f)
- Erkennung und Abwehr von Cyberangriffen (Gutachten S. 7f)

Dr. Köpsells Feststellungen zur Angreiferidentifizierung auf Basis der IPAdresse, insbesondere die Erwähnung des „dummen" Angreifers, sind inhaltlich korrekt. Sie werden im Wesentlichen durch die Antwort zur gerichtlichen Beweisfrage 3 d) in Kapitel 7.3 des gegenwärtigen Gutachtens gestützt.

Bezüglich Brute-Force-Angriffen, die von Botnetzen unter Beteiligung zivil oder privat genutzter Webclients ausgehen, erklärt Dr. Köpsell, dass keine Rückschlüsse auf die eigentlichen Täter möglich seien. Diese Einschätzung ist im Wesentlichen korrekt.

Bzgl. Brute-Force-Angriffen, die von Botnetzen unter Beteiligung zivil oder privat genutzter Webclients ausgehen ist die Feststellung Dr. Köpsell, dass dadurch auf die eigentlichen Täter keine Rückschlüsse gezogen werden können, zwar im Wesentlichen korrekt. Die Tatsache, dass die IP-Adressen zugreifen Host-Systeme zur Austrocknung von Botnetzen, bei denen zivil oder privat genutzte Webclients integriert sind, genutzt werden können, bleibt im Gutachten Dr. Köpsell unberücksichtigt.

Sie wird aber in seinen ergänzenden Erläuterungen S. 12 (Zu Anmerkung 2.5) behandelt. Die darin aufgeführten Möglichkeiten z.B. in Zusammenarbeit mit dem ISP könnten möglicherweise ergriffen werden. Ob sie im Verlauf der Zeit seit den Ausführungen Dr. Köpsell so ergriffen wurden, entzieht sich den Kenntnissen des Sachverständigen. Die Speicherung der

---

[19] Quelle: Anschreiben Dr. Köpsell vom 29.07.2022 zu seinem Gutachten (Bl. 103 Bd. III d.A.) sowie Seite 2 Privatgutachten Prof. Dr. Martini

dynamischen IP-Adressen ist liefert aktuell zumindest in einem geringen Umfang die Möglichkeit zum Austrocknen von Botnetzen unter Mithilfe des jeweiligen ISP.

Prof. Dr. Martini erläutert in seinem Privatgutachten auf S. 18 die Verwendung der IP-Adressen bei Angriffen per Botnetzen. Die unter „Ein (leider sehr reales) Beispiel" beschriebene Verwendung der protokollierten IP-Adressen entspricht den im vorliegenden gerichtlich beauftragten Gutachten unter Kap. 5.2 gelisteten Zwecken der „Häufigkeit" und **„Verbindung zu früheren oder koordinierten Angriffen"**.

Dr. Köpsell behandelt in seinem Gutachten und den ergänzenden Stellungnahmen das Thema der Erkennung und Abwehr von Cyberangriffen überwiegend aus der Perspektive proaktiver Maßnahmen.

Im Kontext reaktiver Maßnahmen, wie sie im gerichtlich beauftragten Gutachten unter Kapitel 6.1 aufgelistet sind, hält Dr. Köpsell die Speicherung von IP-Adressen für nicht notwendig. Eine Ersetzung der IP-Adresse durch eine Zufallszahl wäre seiner Ansicht nach ausreichend (siehe Gutachten Dr. Köpsell S. 7, unten, sowie seine Stellungnahme S. 11, unten).

Auf Grundlage dieser Argumentation bietet das Gutachten keine weiteren Ausführungen zur Notwendigkeit der Protokollierung und Speicherung der vollständigen, nicht-anonymisierten dynamischen IP-Adresse über den konkreten Nutzungsvorgang hinaus an. Prof. Dr. Martini bewertet diese Darstellung als fehlerhaft und liefert eine nachvollziehbare Begründung hierfür in Kapitel 3.3 seines Privatgutachtens.

In diesem Zusammenhang wird auch auf die beiden praxisnahen Beispiel in Kap. 4 des vorliegenden gerichtlich Gutachtens verwiesen.

Die Ausarbeitungen beider Privatgutachter beinhalten keine Hinweise dazu, dass bei der Entscheidung über die Protokollierung und Speicherung der vollständigen, nicht-anonymisierten dynamischen IP-Adresse über den konkreten Nutzungsvorgang hinaus auch das Kriterium des Schutzbedarfes der jeweiligen Backend-Infrastruktur berücksichtigen ist.

8.2. Zur 3. Frage

Die 3. Frage an die Parteigutachter entspricht im Wesentlichen der Frage (2) c) des Beweisbeschlusses vom 19.09.2018.

Die Feststellungen der beiden Privatgutachter dazu sind entsprechend.

Bemerkung:

Der Vortrag der Parteien beinhaltet keine über die in den Privatgutachten hinausgehenden Einlassungen, die mit den Beweisfragen zu dem vorliegenden, gerichtlichen Gutachten in Bezug zu bringen wären. Daher hat der Sachverständige diesbezüglich hier nicht weiter ausgeführt.

Sollte eine weitere Ausarbeitung in diesem Zusammenhang erforderlich sein, müssten dafür spezifische Beweisfragen gestellt werden.

9. Gutachtenergebnis

Die im Beweisbeschluss zu diesem Gutachten gestellten Fragen beantworten sich zusammenfassend wie folgt:

Zu (1) a):

Die Protokollierung und Speicherung dynamischer IP-Adressen von zugreifenden Host-Systemen über die Dauer des konkreten Nutzungsvorgangs hinaus im Rahmen des Betriebs von öffentlich zugänglichen Telemedien, wie sie die Beklagte betreibt, dient zumindest folgenden sicherheitstechnischen Zwecken:

1. Ermittlung von Angriffsstrategien
    - Korrelation von Ereignissen
    - Zielgerichtetheit
    - Häufigkeit
    - Verbindung zu früheren oder koordinierten
2. Aufdecken von Schwachstellen in der Backend-Infrastruktur
3. Blockierung
4. Unterstützung forensischer Analysen
5. Identifikation der Quelle der Attacke
    - Geolokalisierung
    - Zuordnung zu einem Netzwerk.

Zu (1) b)

Die Speicherung der dynamischen IP-Adressen von zugreifenden Host-Systemen über die Dauer eines Nutzungsvorgangs hinaus bewirkt und ermöglicht verschiedene sicherheits-, rechts- und betriebsrelevante Funktionen. Diese sind:

1. Feststellung, ob und in welchem Umfang unbemerkte Cyberangriffe für den Angreifer erfolgreich waren.
2. Rückverfolgbarkeit von Interaktionen.
3. Ermittlung der Korrelationen von Angriffsmustern.
4. Identifikation von Anomalien.
5. Forensische Untersuchungen.
6. Geobasierte Zugriffsanalysen.

Zu (1) c)

Die Speicherung von IP-Adressen zugreifender Host-Systeme über die Dauer des Nutzungsvorgangs hinaus erfolgt in der Regel abhängig von der Konfiguration und Funktionsweise der konkreten Backend-Infrastruktur an spezifischen Speicherorten.

Typischerweise sind dies Speicherorte, die von folgenden Servern/Diensten geführt werden:

1. Webserver

2. Intrusion Detection/Prevention Systeme (IDS/IPS) und Security Information and Event Management Systeme (SIEM).
3. Firewalls und Router.
1. Datenbanken zur Langzeitspeicherung.

Umfang und Speicherorte hängen von individuellen technischen und organisatorischen Gegebenheiten sowie dem individuellen Schutzbedarf und jeweiligen Backend-Infrastruktur ab.

Zu (1) d)

Wer Zugriff auf gespeicherte, dynamische IP-Adressen hat, hängt maßgeblich von den organisatorischen und technischen Gegebenheiten der jeweiligen Backend-Infrastruktur ab. In der Regel ist der Zugriff auf die Nutzergruppen beschränkt, die zur sachgerechten Erledigung ihrer Aufgaben auf den Zugriff angewiesen sind. Dies sind im Wesentlichen:

1. Systemadministratoren
2. Sicherheitsverantwortliche (IT-Security-Teams)
3. Datenschutzbeauftragte
4. Entwickler/Support-Teams.

Zu (1) e)

Um die unter 5.2 beschriebenen, sicherheitstechnischen Zwecke zu erreichen, müssen zu jeder Anfrage gemeinsam mit der IP-Adresse weitere Log-Daten gespeichert werden. Die folgende Auflistung gruppiert nach dem Zweck der Speicherung:

1. Ermittlung von Angriffsstrategien
    - Zeitstempel
    - Protokolltyp
    - Angeforderte Ressource/URL
    - HTTP-Methoden
    - Antwortstatus
    - Benutzeragent
    - Verbindungsquelle
    - Signatur oder Regel-ID
    - Schweregrad
    - Zieladresse/Zielport.
2. Aufdecken von Schwachstellen in der Backend-Infrastruktur
    - Exploit-Indikatoren
    - Betroffene Systeme/Dienste
    - Fehlermeldungen
    - Authentifizierungsversuche
    - Blockierung

3. Unterstützung forensischer Analysen
    - Kompletter Netzwerkverkehr
    - IDS/IPS-Warnungen
    - Systemprotokolle
    - Authentifizierungsprotokolle
    - DNS-Logs
    - Identifikation der Quelle der Attacke

Zu (2) a)

Die Protokollierung und Speicherung der vollständigen, nicht-anonymisierten dynamischen IP-Adresse über den konkreten Nutzungsvorgang hinaus ist zwingend erforderlich, um die einzelnen zu Ziffer (1) beschriebenen Zwecke jeweils erreichen.

Zu (2) b)

Die zu Ziffer (1) genannten Zwecke können nicht durch andere gleich geeignete Mittel /Maßnahmen erreicht werden.

Zu (2) c)

Da die zu Ziffer (1) genannten Zwecke nicht durch andere gleich geeignete Mittel /Maßnahmen erreicht werden können, entfällt eine Beantwortung der Beweisfrage (2) c).

Zu (3) a)

Die Frage, warum die von der Beklagten betriebenen öffentlich zugänglichen Telemedien ohne die Speicherung der vollständigen, nicht-anonymisierten dynamischen IP-Adressen über den konkreten Nutzungsvorgang hinaus auskommen, lässt sich nicht allgemein beantworten. Mögliche Gründe führt die Beklagte in ihrer Replik vom 10.08.2018 an.

Darüber hinaus sind nach der Einschätzung des Sachverständigen folgende Gründe denkbar:

1. Backend-Infrastruktur und Kosten-Nutzen-Abwägung
2. Einfachheit der Infrastruktur
3. Ersatz vs. Bereinigung
4. Einschätzung des Schutzbedarfs der betroffenen Backend-Infrastruktur

Wird der Schutzbedarf als "Normal" eingestuft, können die Sicherheitsvorkehrungen u.U. im geringeren Niveau angelegt werden. Die Speicherung von vollständigen, nicht anonymisierten dynamischen IP-Adressen könnte bei diesen Backend-Infrastrukturen u.U. überflüssig sein. Dies wäre aber in jedem konkreten Fall einzeln zu bewerten.

Zu (3) b)

Die Beweisfrage, wie häufig sicherheitsrelevante Angriffe oder Bedrohungen auf den von der Beklagten betriebenen öffentlich zugänglichen Telemedien auftreten bzw. wie wahrscheinlich sie sind, lässt sich nur auf der Grundlage belastbarer Statistiken beantworten. Statistiken über Angriffe auf die Telemedien der Beklagten sind allerdings öffentlich nicht zugänglich.

Von den zugreifenden Host-Systemen dieser Angreifergruppen ausgehenden, relevanten Angriffe/Bedrohungen, denen die Backend-Infrastrukturen der Beklagten ausgesetzt sind, listen sich wie folgt:

1. Datenverlust und Datenmissbrauch
2. Dienstausfall (Denial of Service, DoS)
3. Datenmanipulation
4. Ransomware-Angriffe
5. Cyber-Spionage
6. Reputationsschäden

Zu den Schäden, Folgen und Ausmaßen, die davon verursacht werden können, wird auf Kap. 7.3 dieses Gutachtens verwiesen.

Zu (3) c)

Der Sachverständige schätzt daher, dass die Erfolgsquote zur Identifizierung der Angreifer aufgrund oder infolge der Speicherung von dynamischen IP-Adressen in den Backend-Infrastrukturen der Beklagten bei unter 10 % der für die Cyberangriffe verantwortlichen dynamische IP-Adressen liegt.

Bei Brute-Force-Angriffen, die von Botnetzen unter Beteiligung zivil oder privat genutzter Webclients ausgehen, dürfte diese Erfolgsquote höher sein.

Zu (3) d)

Um den Nutzer einer dynamischen IP-Adresse identifizieren zu können, bedarf es folgende zusätzliche Log-Daten:

1. Zeitstempel
2. Portnummern
3. Protokolldetails.

Auch bei diesen Konfigurationen der Router der zugreifenden Host-Systeme wechseln die dynamischen IP-Adressen, wenn auch nicht regelmäßig. Deshalb bedarf es auch der Protokollierung der genannten Daten zusätzlich zur dynamischen IP-Adresse.

[redacted]

Dipl.-Ing. W. Lehnigk-Emden

öbuv. Sachverständiger

Das Gutachten wurde in 4 Ausfertigungen erstellt, davon eine zur Akte des Sachverständigen. Es hat einen Umfang von 29 Seiten (58.901 Anschläge) und ist ohne Anlagen.