



RECHTSANWÄLTE

**Beglaubigte Abschrift**

TCI Partnerschaft von Rechtsanwälten Müller Schmidt mbB  
Fasanenstr. 61 · D - 10719 Berlin

**Vorab per Fax 90188-518**

Landgericht Berlin  
ZK 57

10617 Berlin

<b>Landgericht Berlin</b>		
Eing.: 13. AUG. 2018		
KM / Scheck / Über		
8	Akt.	Anl.

TCI Partnerschaft von  
Rechtsanwälten  
Müller Schmidt mbB

Fasanenstr. 61  
D - 10719 Berlin  
Tel: +49 - (0)30 - 20 05 42-0  
Fax: +49 - (0)30 - 20 05 42-11  
www.tcilaw.de

Norman Müller  
Markus Schmidt  
Carsten Gerlach 1

In Kooperation mit

TCI Rechtsanwälte München  
Ruth Düntsch  
Dr. Truiken J. Heydn  
Dr. Michael Karger 1,2  
Harald Krüger 3  
Dr. Andreas Stadler  
Dr. Thomas Stögmüller 1  
LL.M. (Berkeley)

TCI Rechtsanwälte Mainz

Stephan Breckheimer 3  
LL.M. (Medienrecht)  
Sabine Brumme  
Dr. Olaf Griebenow  
Stephan Schmidt 1  
Christian Welkenbach 1,4

Fachanwalt für

- 1 Informationsrecht
- 2 Verwaltungsrecht
- 3 Arbeitsrecht
- 4 Gewerblichen Rechtsschutz
- 5 Urheber- und Medienrecht

Berlin, den 10. August 2018

**Ansprechpartner**

E-Mail-Adresse:

Aktenzeichen: 172/00123-08/dn

**In dem Rechtsstreit****Patrick Breyer ./. Bundesrepublik Deutschland****- 57 S 87/08 -**

nehmen wir zur Vorbereitung der mündlichen Verhandlung wie folgt Stellung:

1. gerichtliche Auflagen vom 2. Juli 2018

1.1 Zunächst erlauben wir uns noch einmal darauf hinzuweisen, dass die Beklagte im Zweifel Tausende von Telemedienangeboten unterhält. Dabei handelt es sich nicht nur um die originären Webangebote der Institutionen und Behörden der



RECHTSANWÄLTE

Seite 2

Beklagten (z.B. Verfassungsorgane, Bundesministerien und nachgelagerte Behörden, Bundesgerichte), sondern auch um spezielle projekt- oder aufgabenbezogene Webangebote (z.B. [www.endlager-asse.de](http://www.endlager-asse.de), [www.demografie-portal.de](http://www.demografie-portal.de), [www.hilfetelefon.de](http://www.hilfetelefon.de)). Insbesondere letztere Webangebote sind naturgemäß einem stetigen Wandel unterworfen. Eine abschließende Beantwortung der Ziffer (1) der Auflagen ist schon aus diesen Gründen praktisch unmöglich.

Soweit Telemedienangebote der Beklagten von ihr selbst im Informationstechnikzentrum Bund (ITZ Bund) betrieben werden, erfolgt dort eine Verarbeitung (was nach der Legaldefinition der EU Datenschutzgrundverordnung, DS GVO, auch die Speicherung beinhaltet) der IP-Adresse der auf die Webangebote zugreifenden Systeme jedenfalls auf der Infrastrukturebene des ITZ Bund. Dies betrifft derzeit die Webangebote gemäß **Anlage BB 7**.

Privatwirtschaftliche Infrastrukturanbieter, auf deren Infrastruktur gegebenenfalls Telemedien der Beklagten betrieben werden, sind nicht verpflichtet, der Beklagten Auskunft über die von ihnen zum Schutz ihrer Infrastruktur ergriffenen Maßnahmen, zu denen auch die Verarbeitung der IP-Adressen zugreifender Systeme gehört, zu geben. Es handelt sich in diesen Fällen bei der Verarbeitung der IP-Adressen gerade nicht um eine Auftragsdatenverarbeitung für die Beklagte, sondern um eine Datenverarbeitung im Schutzinteresse des Infrastrukturbetreibers, mit denen er auch zum Schutz seiner Kunden beiträgt. Auch aus diesem Grund ist eine vollständige Beantwortung der Auflage nicht möglich. Allgemeine Abfragen bei den Bundesbehörden, ob IP-Adressen gespeichert werden oder nicht, ergeben deshalb keine belastbaren Informationen. Es ist Bundesbehörden - ähnlich wie Mietern eines Hochhauses - nicht bekannt, welche Maßnahmen zum Investitionsschutz der Eigentümer/Betreiber des Hochhauses ergriffen hat und unterhält. Telemedienanbieter, deren Inhalte auf dem Server eines externen Betreibers gehostet werden, können über die Verfahrensweisen zur Sicherung der IT-Systeme des Betreibers und ihren Inhalt keine verlässliche Aus-



RECHTSANWÄLTE

Seite 3

kunft geben. Melden diese Behörden auf eine Abfrage hin, dass keine Verarbeitung der IP-Adressen erfolgt, , gilt dies für ihr Inhalteangebot und Teilsystem, sagt jedoch nichts über die Protokollierung des Gesamtsystems des Betreibers aus.

Die Beklagte hat im Hinblick auf die gerichtliche Auflage auf Basis der seit Mai 2018 neu erstellten Datenschutzerklärungen von Bundesbehörden außerdem die in **Anlage BB 8** aufgeführten Telemedienangebote der Beklagten ermittelt, bei denen jedenfalls durch den Telemedienanbieter keine Verarbeitung der IP-Adressen erfolgt. Eine Aussage über die Verhältnisse auf den von privaten wie öffentlichen (z.B. ITZ Bund) Infrastrukturbetreibern betriebenen Hosts bzw. Servern und den Umfang der dort vorgenommenen Protokollierung können Datenschutzerklärungen aus den oben genannten Gründen allerdings nicht geben.

- 1.2 Hinsichtlich der Ziffer 2 des Auflagenbeschlusses erlauben wir uns zunächst darauf hinzuweisen, dass das Risiko eines Angriffes auf Telemedien der Beklagten nicht alleine auf Basis der Anzahl/Häufigkeit der Angriffe bewertet werden kann. Von ganz wesentlicher, wenn nicht sogar weit überwiegender Bedeutung für die Risikobewertung und damit für die Bewertung der Verhältnismäßigkeit der Verarbeitung von IP-Adressen im Verhältnis zu der auch nach Ansicht des Bundesgerichtshofes geringen Eingriffsintensität in das Recht auf informationelle Selbstbestimmung sind die möglichen Schäden eines Angriffs. Gemäß gängiger Definition ergibt sich das Risiko eines Angriffs als Produkt aus der Schadenshöhe und der Eintrittswahrscheinlichkeit. Neben der Häufigkeit ist deshalb insbesondere auch der für die Beklagte drohende materielle wie immaterielle Schaden bei der Prüfung der Verhältnismäßigkeit zu betrachten.

Ein möglicher Schaden ist dabei nicht nur auf die Funktionsfähigkeit und Erreichbarkeit des angegriffenen Telemediums beschränkt. So nutzen Angreifer



RECHTSANWÄLTE

Seite 4

beispielsweise auf nach dem Stand der Technik gehärteten und überwachten Telemedien bislang unbekannte Schwachstellen, um auf diesem Wege andere Infrastrukturen anzugreifen.

Der entstandene Schaden war z.B. im Falle des sogenannten "Bundeshacks" (Angriff letztendlich auf IT-Infrastrukturen des Auswärtigen Amtes mit der Ausleitung von Daten), der am 28. Februar 2018 presseöffentlich bekannt wurde, erheblich.

Hier wurde Ende 2017 aufgrund eines externen Hinweises bei einem aus dem Internet erreichbaren Webserver einer Bundesbehörde eine Infektion festgestellt, mit der Angreifer den Webserver fernsteuern konnten (Webshell). Für den betroffenen Server waren Logdaten vorhanden. In diesen Logdaten konnte zumindest eine IP-Adresse des Angreifers ermittelt werden, da Zugriffe von dieser Adresse auf die von ihm auf dem Server platzierte Malware enthalten waren.

Mit Kenntnis dieser IP-Adresse konnten weitere durch den Angreifer auf dem Server manipulierte bzw. eingebrachte Dateien durch Analyse der Logdaten entdeckt und der Angriff im Ergebnis auf Basis dieser sowie weiterer daraus abgeleiteter Erkenntnisse unter Kontrolle gebracht und beendet werden. Informationen zu dem Vorfall und zur Rolle der Logdaten sind in einem Bericht des Nationalen Cyber-Abwehrzentrums vom 19. März 2018 enthalten, beigelegt als **Anlage BB 9**.

Aufgrund der Tatsache, dass die Telemedien des Bundes im Übrigen überwiegend von wenigen Anbietern betrieben werden, führen die beobachteten DoS-Angriffe (ca. 2 täglich) gegen ein Telemedium der Beklagten i.d.R. zu einer Gefährdung oder Beeinträchtigung aller dort betriebener Telemedien, da mit diesen Angriffen die zugrunde liegende Infrastruktur insgesamt in ihrer Funktionsfähigkeit beeinträchtigt wird. So erfolgten z.B. am 17. und 18. Mai 2018 wiederholte Low-and-Slow Angriffe durch weltweit verteilte Squid-Proxies auf eine





RECHTSANWÄLTE

Seite 5

Webseite eines Verfassungsorgans der Beklagten, die beim Provider Babel betrieben wird (zu (D)DoS-Attacken [https://de.wikipedia.org/wiki/Denial\\_of\\_Service](https://de.wikipedia.org/wiki/Denial_of_Service), zum Begriff von slow and low Attacken <https://www.cloudflare.com/learning/ddos/ddos-low-and-slow-attack/> und zu Squid-Proxies <https://de.wikipedia.org/wiki/Squid>). Dieser Angriff gefährdete deshalb auch die Funktionsfähigkeit anderer Webangebote der Beklagten, die auf der gleichen Infrastruktur betrieben werden und konnte nur durch die Verarbeitung der IP-Adresse wirksam abgewehrt werden.

**Beweis:** Sachverständigengutachten  
Zeugnis des Herrn Dr. Kai Fuhrberg, b.b.

Im Detail handelte es sich dabei um einen der besonders häufigen sogenannten Wordpress-Pingback Angriffe. Bei solchen Angriffen wird eine unsichere Funktion in Wordpress-Installationen für den Angriff missbraucht. Der Angreifer ist dabei ein Computer, der eine Wordpress-Installation hostet. Werden solche Angriffe erkannt, werden die IP-Adressen des Angreifers erfasst, automatisch in eine Blacklist aufgenommen und in der Folge gesperrt. Weitere Angriffe durch diesen Computer werden infolgedessen später schon am Netzeingang der Infrastruktur des Betreibers erkannt und gesperrt.

Mit derartigen Wordpress-Pingback Angriffen kann jede beliebige Webseite angegriffen werden. Bei dem hier mit dem Betrieb der Telemedienangebote der Beklagten beauftragten Unternehmen, wurden nahezu alle Kunden ein- oder mehrfach angegriffen, dazu zählen u.a. auch die Webseiten der Beklagten [www.bundesregierung.de](http://www.bundesregierung.de), [www.bundestag.de](http://www.bundestag.de), [www.bundeskanzlerin.de](http://www.bundeskanzlerin.de).

Einige derartige Angriffe auf Systeme des BPA:

So wurde beispielhaft am 6. November 2016 von 13:00 bis 13:30 die Webseite [www.bundesregierung.de](http://www.bundesregierung.de) attackiert, ab 13:36 gefolgt von einem Angriff auf



RECHTSANWÄLTE

Seite 6

www.bundestkanzlerin.de durch dieselben Angreifer; am 18. September 2016 erfolgte ein Angriff von 11:28 bis 11:38 auf die Webseite www.bundesregierung.de.

Würden die IP-Adressen der Angreifer nicht gespeichert, könnte man die IP-Adressen in der Folge nicht sperren und die Angriffe würden vermutlich langfristig andauern oder wiederholt, weil sie den Angreifer nichts kosten und eine Entdeckungsgefahr mangels Rückverfolgungsmöglichkeit ausgeschlossen wäre.

Eine technisch andere Angriffsserie auf Systeme des Bundespresseamtes erfolgte ab dem 19. Februar 2016. Es handelte sich um Angriffe unter Verwendung des HIOC-Tools.

Erste Angriffe auf die Webseite www.bundesregierung.de begannen dabei um 17:58 Uhr, die IP-Adressen der Angreifer wurden in eine Blacklist eingetragen. Gegen 20:00 Uhr wurde vermehrt angegriffen, dabei erkannte weitere IP-Adressen wurden der Blacklist hinzugefügt. Die Angriffe wurden bis zum 21. Februar 2016, also über drei Tage, fortgesetzt.

Infolge der Angriffe war die Webseite www.bundesregierung.de aus einigen Netzen anfangs nur schlecht zu erreichen, die Webseite baute sich oft nur mit Verzögerung auf oder wurde gar nicht ausgeliefert. Mit zunehmender Anzahl gesperrter Angreifer-IPs verschwanden die Auswirkungen. Die Angriffe vom 20. und 21. Februar hatten dann dank der Sperrliste, d.h. der Speicherung der IP-Adressen keine Auswirkungen mehr.

Derartige Angriffe können als Seiteneffekt den sogenannten Uplink „verstopfen“, wenn sie besonders breitbandig ausgeführt werden. In der Folge wird dadurch nicht nur die konkret angegriffene Webseite gestört, sondern der Zugriff auf alle auf diesem Uplink liegenden Webseiten (bei privaten Betreibern ggf. auch anderer Kunden).



RECHTSANWÄLTE

Seite 7

Entsprechende Angriffe neueren Datums, die bei der Beklagten tatsächlich zu einer Störung geführt haben, erfolgen derzeit kaum noch, da die Abwehrmaßnahmen die derzeit üblichen Angriffsmuster erkennen und automatisch abwehren. Ohne Speicherung von IP-Adressen wären Störungen in der Verfügbarkeit der Telemedienangebote dagegen nicht zu verhindern.

**Beweis:** Sachverständigengutachten

Weiterhin waren alle in unserem Schriftsatz vom 28. September 2017 unter Ziffer 3.2 genannten Angriffe gegen die bei der Beklagten selbst, nämlich beim ITZ Bund, betriebenen Telemedien gerichtet.

Zur Verdeutlichung übereichen wir als **Anlage BB 10** einen Protokollauszug des ITZ Bund über dort festgestellte Angriffe in einem Zeitraum von ca. 45 Minuten. Die Anzahl der Angriffe ist dabei repräsentativ für jeden anderen Zeitraum gleicher Länge.

**Beweis:** Sachverständigengutachten  
Zeugnis des Herrn Dr. Kai Fuhrberg, b.b.

- 1.3 Zur Beantwortung erlauben wir uns zunächst darauf hinzuweisen, dass dem Bundesministerium für Justiz und Verbraucherschutz für das Telemedienangebot auf seinem Hauptportal [www.bmj.bund.de](http://www.bmj.bund.de) die Speicherung der IP-Adressen durch ein Urteil des Amtsgerichtes Mitte (5 C 314/06) untersagt wurde. Speziell für diese Behörde der Beklagten hat daher die Nicht-Speicherung nichts mit der Sicherheit bzw. Gefährdung des angebotenen Telemediums zu tun.

Die Frage, warum manche Behörden der Beklagten auf eine Speicherung der IP-Adressen verzichten, kann hier nicht beantwortet werden. Nachvollziehbare Gründe hierfür sind nicht erkennbar. Es kann lediglich gemutmaßt werden, dass einige Behörden bzw. die dort für diese Frage verantwortlichen Personen durch



RECHTSANWÄLTE

Seite 8

die (nach hiesiger Einschätzung sachlich falsche) Entscheidung des Amtsgerichtes Mitte irrtümlich davon ausgehen, eine Speicherung der IP-Adressen sei generell unzulässig. Ein weiterer Beweggrund mag darin liegen, dass sich die konkrete Telemedium anbietende Behörde auf die Speicherung des Infrastrukturbetreibers verlässt oder aus schlichter Unkenntnis oder Sorglosigkeit eine Speicherung unterlässt. Aus der möglichen „Unvorsichtigkeit“ einiger Verantwortlicher beim Umgang mit IT-Sicherheit kann allerdings nicht, wie es der Kläger tut, darauf geschlossen werden, dass sich nunmehr die Beklagte insgesamt an diesem unzureichenden Verhalten Einzelner auszurichten hat. Wir weisen in diesem Zusammenhang nochmals darauf hin, dass es schon aus verfassungsrechtlichen Gründen (z.B. Trennung der Staatsgewalten, Ressortverantwortung der Ministerien) beklagtenseitig keine Möglichkeit gibt, eine einheitliche Praxis sämtlicher Behörden vorzuschreiben. Es gibt insoweit schlicht niemanden, der dies verfassungsrechtlich anordnen könnte.

Der Angriffsdruck ergibt sich im Übrigen aus dem potentiellen Angteiferkreis, der Bedeutung des konkreten Telemedienanbieters, aber auch aus der Geeignetheit des Angriffsziels für die Informationsgewinnung. Gerade in nicht professionellen Hackerkreisen werden erfolgreiche Angriffe nachgerade als Trophäen betrachtet. Je prominenter der konkrete Telemedienanbieter desto höher das „Renommée“ des erfolgreichen Hackers. So „zählt“ beispielsweise ein erfolgreicher Angriff auf eine Webseite des Bundeskanzleramtes mehr als ein erfolgreicher Angriff auf die Webseite [www.max-und-flocke-helferland.de](http://www.max-und-flocke-helferland.de).

Da Telemedienangebote aber häufig auch nur als Einstieg für Angriffe auf weitere IT-Infrastrukturen der Beklagten genutzt werden (z.B. beim oben geschilderten Bundeshack), ergibt sich der Angriffsdruck auch aus der Relevanz der eigentlichen Angriffsziele (beim Bundeshack z.B. Daten des Auswärtigen Amtes).



RECHTSANWÄLTE

Seite 9

Wie im Beispiel "Bundeshack" beschrieben, nutzen professionelle (insbesondere auch staatlich gesteuerte) Angreifer, wenn sie das eigentliche Ziel aufgrund von wirksamen Sicherheitsmaßnahmen nicht direkt erreichen können, im Rahmen sogenannter Mehrschrittangriffe zunächst leichter zu erreichende Ziele wie z.B. aus dem Internet zugängliche Telemedienangebote, bei denen sie davon ausgehen, dass das endgültige Ziel diese besucht. Für die Mitarbeiter der Beklagten als Angriffsziel gehören hierzu sicherlich auch die durch die Beklagte betriebenen Telemedienangebote. Es besteht daher nur ein vermeintlich unterschiedlicher Angriffsdruck, als der Täter, sollte er feststellen, dass das endgültige Ziel mehrere Telemedienangebote der Beklagten nutzt, dasjenige Telemedienangebot zunächst angreifen wird, bei welchem ein geringeres Entdeckungsrisiko besteht, weil dort aufgrund der fehlenden Speicherung der IP-Adresse keine Zuordnung seiner verschiedenen Aktivitäten möglich und eine Rückverfolgung bzw. Entdeckung damit unmöglich ist.

Der Angriffsdruck ist daher in Gestalt des Gesamtrisikos für die Beklagte zu bewerten und darf nicht nur auf ein einzelnes Telemedienangebot einer einzelnen Behörde bezogen werden.

Zudem kann nicht geschlussfolgert werden, dass der Angriffsdruck auf ein Telemedienangebot geringer ist, weil dort trotz (oder gerade wegen) der fehlenden IP-Adress-Speicherung scheinbar weniger Angriffe beobachtet wurden. Denn auch wenn keine Angriffe beobachtet wurde, bedeutet dies nicht, dass es diese nicht gab, da die Täter, wie im oben beschriebenen Vorfall, ein großes Interesse haben, möglichst lange unerkannt zu bleiben.

Gerade das oben angeführte Beispiel des „Bundeshacks“ zeigt, dass auch bei eigentlich erst einmal zu erwartendem geringen Angriffsdruck auf eine Protokollierung und Verarbeitung der IP-Adressen nicht verzichtet werden kann: Dort war ein zunächst im Sinne eines klassischen Angriffsdrucks „unverdächtig“ Server bei der Hochschule des Bundes kompromittiert worden und hat in



RECHTSANWÄLTE

Seite 10

der Folge Ausspähung und Datenabflüsse beim Auswärtigen Amt ermöglicht. Auf den ersten Blick unterschiedlicher Angriffsdruk rechtfertigt deshalb keinesfalls unterschiedliche Schutzniveaus.

Um IT-Sicherheitsvorfälle vollumfänglich untersuchen und aufarbeiten zu können (insbesondere das Auffinden des Infektionsweges und von durch den Angreifer manipulierten Dateien), ist die Speicherung der auf eine Anwendung zugreifenden IP-Adressen jedenfalls bei allen Telemedienangeboten zwingend erforderlich.

- 1.4 Die Frage kann seitens der Beklagten nicht beantwortet werden, da sie hierüber keine umfassenden Informationen hat. Die Strafverfolgung liegt mit wenigen Ausnahmen im Aufgabenbereich der Bundesländer, so dass der Beklagten hierzu keinerlei Statistiken vorliegen.

Festzuhalten bleibt aber, dass die IP-Adresse eines Angreifers in den meisten Fällen der einzige Ansatzpunkt zur Ermittlung eines Angreifers ist.

**Beweis:** Sachverständigengutachten

Darüber hinaus ist neben der klassischen Strafverfolgung aber auch zu berücksichtigen, dass die Kenntnis von IP-Adressen, die für Cyber-Angriffe genutzt wurden, nicht allein zur technischen Bewältigung bzw. Gefahrenabwehr bei einem Cyber-Angriff notwendig ist. IP-Adressen sind immer auch ein wesentlicher Teil eines aus technischen und weiteren Indikatoren bestehenden Gesamtbildes, mithilfe dessen eine – je nach Qualität und Quantität der vorliegenden Erkenntnisse – hinreichend sichere politische Bewertung und Zurechnung von Cyber-Angriffen überhaupt erst möglich wird. Im Falle des oben geschilderten Cyber-Angriffs auf das Auswärtige Amt („Bundeshack“) war es auf Grund der vorliegenden Erkenntnisse – was Erkenntnisse über verwendete IP-Adressen



RECHTSANWÄLTE

Seite 11

und die Rekonstruktion des Angriffs einschließt – möglich, für die Bundesregierung eine hinreichend sichere Zurechnung zu treffen.

So wurde seitens des Auswärtigen Amts im Zusammenhang mit der Ausweisung von vier russischen Diplomaten (Fall Skripal) am 26. März 2018 erklärt, dass der Schritt auch vor dem Hintergrund der kürzlichen Cyber-Operation gegen das geschützte IT-System der Bundesregierung erfolgt, die sich nach bisherigen Erkenntnissen mit hoher Wahrscheinlichkeit russischen Quellen zurechnen lässt (<https://www.auswaertiges-amt.de/de/newsroom/bm-skripal-ausweisung-russische-diplomaten/1797546>). Darüber hinaus konnte die Bundesregierung den Cyber-Angriff in parlamentarischen Anfragen auch wie folgt zurechnen: „Modus operandi, technische Merkmale sowie deren Opferflächen sprechen nach bisherigen Erkenntnissen mit hoher Wahrscheinlichkeit für eine Urheberschaft der Angriffskampagne SNAKE“ (BT-Ds 19/1979, S. 15).

Ein Verzicht auf Erkenntnisse aus der Erhebung von IP-Adressen würde regelmäßig die Möglichkeiten der Rekonstruktion und Zurechenbarkeit von Cyber-Angriffen vermindern und damit die Handlungs- und Reaktionsmöglichkeiten der Bundesregierung in Bezug auf Cyber-Angriffe, die sich gegen die Bundesrepublik Deutschland richten, nachhaltig schwächen.

- 1.5 Grundsätzlich sind alle im Rahmen eines Zugriffs auftretenden Logdaten für eine wirkungsvolle Detektion eines Angriffs notwendig oder mindestens nützlich. Dies gilt insbesondere für den Zeitstempel, die Version des verwendeten Protokolls und die Pfade/Daten, auf die zugegriffen wird. Bei allen diesen weiteren Logdaten handelt es sich jedoch nicht um personenbezogene Daten, soweit sie nicht in Verbindung zur IP-Adresse gebracht werden.

Für die vom EuGH angenommene Personenbeziehbarkeit der dynamischen IP-Adresse ist zwingend die Kombination der IP-Adresse mit dem Zeitstempel erforderlich, da nur aus der Kombination beider Daten überhaupt ein Rückschluss





RECHTSANWÄLTE

Seite 12

auf den hinter der dynamischen IP-Adresse stehenden Anschlussinhaber möglich ist. Zudem muss die auskunftsbegehrende Stelle berechtigt i.S.d. 113 TKG sein. Dies ist regelmäßig den Strafverfolgungsbehörden vorbehalten.

- 1.6 Die gefährlichsten, weil professionell ausgeführten Angriffe erstrecken sich in der Regel über einen längeren Zeitraum, da der Angreifer zunächst möglichst unauffällig agiert. Ziel ist die Feststellung weiterer lohnender Ziele und Übernahme der Kontrolle über diese Systeme mit Ziel der Spionage oder Sabotage. Bei nahezu allen derartigen Fällen, die der Beklagten bekannt sind, dauerten diese Aktionen mehrere Monate, so dass der Mindestzeitraum für die Speicherung von Logdaten nicht unter 3 Monaten liegen sollte. § 5 Abs. 2 BSIG sieht deshalb auch eine entsprechende Speicherfrist von drei Monaten vor.

Da z.B. im Falle des oben dargestellten Bundeshacks die Logdaten nicht weit genug in die Vergangenheit reichten, fehlten allerdings wichtige Informationen, um das komplette Vorgehen des Angreifers lückenlos zu rekonstruieren (von ersten Angriffversuchen über die erfolgreiche Infektion des Systems bis zu weiteren Aktionen auf dem System selbst).

Seit Einführung des § 5 BSIG hat sich die Cyber-Sicherheitslage, insbesondere mit Blick auf die Qualität und Professionalisierung von Cyber-Angriffen auf die Regierungsnetze, noch einmal deutlich verschärft. Um die heute existierenden, hochkomplexen und langandauernde Cyber-Angriffsoperationen lückenlos rekonstruieren und aufklären zu können, sind längere Speicherfristen nötig, als bisher in § 5 BSIG geregelt.

## 2. ergänzende Ausführungen zur rechtlichen Würdigung

- 2.1 Soweit sich der Kläger als Anspruchsgrundlage für den von ihm geltend gemachten Unterlassungsanspruch auf §§ 12, 15 TMG beruft, kommen diese als Anspruchsgrundlage nicht mehr in Betracht, da mit Inkrafttreten der DS-GVO





RECHTSANWÄLTE

Seite 13

diese nationales Datenschutzrecht grundsätzlich verdrängt (Anwendungsvorrang der DS-GVO). Eine Ausnahme gilt nur dort, wo nationale Vorschriften aufgrund einer Kollisionsregel, eines Umsetzungsauftrags oder einer Öffnungsklausel in der DS-GVO vorrangig anwendbar sind.

Für den 4. Abschnitt des TMG (§§ 11ff. TMG) kommt keine dieser Ausnahmen in Betracht. Insbesondere ist Art. 95 DS-GVO als Öffnungsklausel nicht einschlägig. Der 4. Abschnitt des TMG stellt gerade keine Umsetzung der ePrivacy-Richtlinie (2002/58/EG) dar, sondern wurde vielmehr in Umsetzung der Datenschutzrichtlinie in das TMG eingeführt. Diese Datenschutzrichtlinie ist nunmehr aber vollständig durch die DS-GVO ersetzt worden. Insoweit gilt daher uneingeschränkt der Anwendungsvorrang der DS-GVO.

- 2.2 Die Befugnis zur Verarbeitung der IP-Adresse als personenbeziehbares Datum ergibt sich für die Beklagte demnach zunächst aus Art. 6 Abs. 1 S. 1 lit. f) DS-GVO, soweit die Beklagte Telemedien außerhalb der Erfüllung ihrer originären Aufgaben betreibt. Im Rahmen ihrer originären Aufgabenerfüllung ergibt sich die Befugnis aus Art. 6 Abs. 1 S. 1 lit. e) DS-GVO i.V.m. Art. 6 Abs. 3 DS-GVO und § 3 BDSG.

Im Erwägungsgrund 49 zur DS-GVO wird herausgestellt, dass für die Verarbeitung personenbezogener Daten, also auch der IP-Adresse, bei Behörden ein berechtigtes Interesse besteht, soweit dadurch die Fähigkeit eines Netzes oder Informationssystems gewährleistet wird, mit einem vorgegebenen Grad der Zuverlässigkeit Störungen oder widerrechtliche oder mutwillige Eingriffe abzuwehren, die die Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit von gespeicherten oder übermittelten personenbezogenen Daten sowie die Sicherheit damit zusammenhängender Dienste, die über diese Netze oder Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen. Beispielsweise erwähnt wird hierzu explizit die Abwehr von DDoS-Angriffen.



RECHTSANWÄLTE

Seite 14

Die Verarbeitung von IP-Adressen ist an dieser Stelle auch notwendig, da gerade im Hinblick auf DDoS-Angriffe andere Abwehrmöglichkeiten nicht bestehen. Denn DDoS Angriffe werden ausschließlich dadurch abgewehrt, indem Zugriffe von durch massenhafte missbräuchliche Zugriffe aufgefallene IP-Nummern bzw. die Server, auf denen diese beheimatet sind, auf Sperrlisten gesetzt und von dort kommende Abrufe blockiert werden.

- 2.3 Nochmals hingewiesen werden muss an dieser Stelle auch darauf, dass jedenfalls die Beklagte in Gestalt des Bundesamtes für Sicherheit in der Informationstechnik (BSI) gemäß § 5 Abs. 1 BSI-Gesetz befugt ist, zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes Protokolldaten, die beim Betrieb von Kommunikationstechnik des Bundes anfallen, zu erheben und automatisiert auszuwerten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern bei der Kommunikationstechnik des Bundes oder von Angriffen auf die Informationstechnik des Bundes erforderlich ist, oder die an den Schnittstellen der Kommunikationstechnik des Bundes anfallenden Daten automatisiert auszuwerten, soweit dies für die Erkennung und Abwehr von Schadprogrammen erforderlich ist. Den Schutzinteressen der Betroffenen hat der Gesetzgeber hier mit den in den Absätzen 2 und 3 des § 5 BSI-Gesetz aufgeführten Bedingungen und Voraussetzungen für die Speicherung angemessen und grundrechtskonform Rechnung getragen.

In der Begründung zu dem Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes, mit dem diese Vorschrift eingeführt wurde, heißt es deshalb auch (BT-Ds 16/11967, S. 14):

*„Absatz 1 gibt dem BSI die Befugnis, zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes die in Absatz 1 aufgezählten Daten automatisiert auszuwerten. Gemäß Nummer 1 kann das BSI Protokolldaten, also sog. Logfiles von Servern, Firewalls usw. erheben und automatisiert auswerten. Dies erfolgt zum einen, um Anzeichen für bevorstehende IT-Angriffe zu finden. Hierzu können die Logfiles automatisiert ausgewertet werden, z. B. hinsichtlich des Datenvolumens oder durch das automatisierte „Absurfen“ von aus dem Bundesnetz heraus aufgerufenen URLs, um sog.*



RECHTSANWÄLTE

Seite 15

*Phishingseiten zu identifizieren. Von besonderer Relevanz für die Erkennung und Abwehr von IT-Angriffen sind die Kopfdaten (sog. Header) der gängigen Kommunikationsprotokolle (IP, ICMP, TCP, UDP, DNS, HTTP und SMTP)....“*

Als Beispiel für die Notwendigkeit der Speicherung der IP-Adresse und die Funktionsweise der Angriffsaufklärung durch das BSI überreichen wir als **Anlage BB 11** einen Auszug aus einer entsprechenden Auswertung von Zugriffen auf Telemedien der Beklagten. In der Spalte E der Tabelle ist die Zugriffsmethode des auf die Telemedien zugreifenden Systems aufgeführt. Diese lautet normalerweise „POST“ oder „GET“. Im vorliegenden Beispiel wurde die ungewöhnliche Zugriffsmethode „PROPFIND“ festgestellt. Anhand der pseudonymisierten IP-Adresse des zugreifenden Systems konnten die nachfolgend in der Auswertung aufgeführten Zugriffe mit der identischen IP-Adresse identifiziert und analysiert werden und dadurch der Erfolg des Angriffs verhindert werden

Die Tatsache, dass der Gesetzgeber für die Bundesverwaltung überhaupt § 5 BSI-Gesetz geschaffen hat zeigt, dass er es für einen sicheren Betrieb von an das Internet angeschlossener Informationstechnik für notwendig hält, IP-Nummern zugreifender Systeme zu speichern. Diese gesetzliche Wertung gilt in gleicher Weise im Übrigen für die Informationstechnik von Privaten, für die § 5 BSI-Gesetz keine Befugnisnorm darstellt und die ihre Berechtigung, zum Investitionsschutz eine Protokollierung einschließlich der IP-Adressen zugreifender System samt zugehörigem Zeitstempel zu betreiben, aus europäischem Datenschutzrecht und damit Art. 6 Abs. 1 S. 1 lit. f) DS-GVO ableiten.

In seiner Entscheidung vom 31. Januar 2013 (LG Berlin, 57 S 87/08) hatte das Landgericht hierzu festgestellt, dass das Betreiben von öffentlichen Internetseiten nach Ansicht des Landgerichtes nicht der Kommunikation zwischen Kläger bzw. anderen Nutzern und der Beklagten bzw. ihren jeweiligen Behörden diene.

Diese Interpretation ist rechtsfehlerhaft und hält einer näheren Prüfung nicht stand. Dazu ist zunächst festzuhalten, dass Internetseiten natürlich auch auf IT-



RECHTSANWÄLTE

Seite 16

Infrastrukturen betrieben werden müssen. Diese Infrastruktur stellt unter Verwendung von Kommunikationstechnik eine Datenverbindung zwischen dem Server mit der Internetseite und dem Nutzer her und tauscht über diese Datenverbindung Daten aus. Es findet also bei jedem Zugriff auf ein Telemedium zweifelsfrei eine Datenkommunikation zwischen dem Server, auf dem sich die Internetseite befindet, und dem Endgerät des Nutzers statt.

3. Der Vollständigkeit halber weisen wir abschließend darauf hin, dass unabhängig von ihrer durchaus fraglichen Richtigkeit die Behauptung des Klägers, der Zeitstempel einer an die Beklagte versandten E-Mail könne mit dem Zeitstempel eines Telemedienzugriffs zusammengeführt werden, so dass dann aufgrund der Daten der E-Mail ein Personenbezug auch für die Telemedienzugriffe hergestellt werden könne, für die Entscheidung des Rechtsstreits keinerlei Relevanz mehr hat. Mit der Entscheidung des EuGH ist der Personenbezug der IP-Adressen in Form der Personenbeziehbarkeit zunächst einmal abschließend gerichtlich geklärt worden. Auf vermeintlich anderweitige Möglichkeiten zur Herstellung des Personenbezugs einer IP-Adresse kommt es daher nicht mehr an.

Beglaubigte und einfache Abschrift anbei

Rechtsanwalt

Behörde (kurz)	Behörde	Ressort	Mandant
ADS	Antidiskriminierungsstelle des Bundes	ADS	antidiskriminierungsstelle.de
ADS	Antidiskriminierungsstelle des Bundes	ADS	eg-check.de
ADS	Antidiskriminierungsstelle des Bundes	ADS	gb-check.de
B4M	Beauftragte der Bundesregierung für die Belange behinderter Menschen	BMAS	behindertenbeauftragte.de
B4M	Beauftragte der Bundesregierung für die Belange behinderter Menschen	BMAS	inklusionslandkarte.de
BKM	Beauftragte der Bundesregierung für Kultur und Medien	BKM	kulturgut-redaktion.doi.de,net
BKM	Beauftragte der Bundesregierung für Kultur und Medien	BKM	kulturgutschutz-deutschland.de
BKM	Beauftragte der Bundesregierung für Kultur und Medien	BKM	kunstsammlung-bund.de
BeschA	Beschaffungsamt des Bundesministeriums des Innern	BMI	besch.a.bund.de
BeschA	Beschaffungsamt des Bundesministeriums des Innern	BMI	b-beschaffung.bund.de
BeschA	Beschaffungsamt des Bundesministeriums des Innern	BMI	evergabe-online.info
BeschA	Beschaffungsamt des Bundesministeriums des Innern	BMI	kqb.bund.de
BeschA	Beschaffungsamt des Bundesministeriums des Innern	BMI	nachhaltige-beschaffung.info
BMF	Bundesministerium der Finanzen	BMF	BFinV Intranet
BMF	Bundesministerium der Finanzen	BMF	BMF Intranet
BrJ	Bundesamt für Justiz	BMJV	bfi.de
BfE	Bundesamt für kerntechnische Entsorgungssicherheit	BMU	bfe.bund.de
BAMF	Bundesamt für Migration und Flüchtlinge	BMI	bamf.de
BAMF	Bundesamt für Migration und Flüchtlinge	BMI	deutsche-islam-konferenz.de
BAMF	Bundesamt für Migration und Flüchtlinge	BMI	wir-sind-bund.de
BAMF	Bundesamt für Migration und Flüchtlinge	BMI	ankommen-app.de
BSI	Bundesamt für Sicherheit in der Informationstechnik	BMI	allianz-fuer-cybersicherheit.de
BSI	Bundesamt für Sicherheit in der Informationstechnik	BMI	bsi.bund.de
BSI	Bundesamt für Sicherheit in der Informationstechnik	BMI	bsi-fuer-buerger.de
BFS	Bundesamt für Strahlenschutz	BMU	asse.bund.de
BFS	Bundesamt für Strahlenschutz	BMU	bfs.de
BFS	Bundesamt für Strahlenschutz	BMU	endlager-konrad.de
BFS	Bundesamt für Strahlenschutz	BMU	endlager-morsleben.de
BFS	Bundesamt für Strahlenschutz	BMU	ssk.de
BVL	Bundesamt für Verbraucherschutz und Lebensmittelsicherheit	BMEL	biosicherheit-bch.de
BVL	Bundesamt für Verbraucherschutz und Lebensmittelsicherheit	BMEL	bvl.bund.de
BVL	Bundesamt für Verbraucherschutz und Lebensmittelsicherheit	BMEL	zkbs-online.de
BfV	Bundesamt für Verfassungsschutz	BMI	wirtschaftsschutz.info
BAFA	Bundesamt für Wirtschaft und Ausfuhrkontrolle	BMWi	BAFA Intranet
BAFA	Bundesamt für Wirtschaft und Ausfuhrkontrolle	BMWi	bafa.de
BAFA	Bundesamt für Wirtschaft und Ausfuhrkontrolle	BMWi	
BAFA	Bundesamt für Wirtschaft und Ausfuhrkontrolle	BMWi	bfae-online.de
BADV	Bundesamt für zentrale Dienste und offene Vermögensfragen	BMI	BADV Intranet
BADV	Bundesamt für zentrale Dienste und offene Vermögensfragen	BMI	badv.bund.de
BADV	Bundesamt für zentrale Dienste und offene Vermögensfragen	BMI	K-PVS Intranet
BADV	Bundesamt für zentrale Dienste und offene Vermögensfragen	BMI	www.k-pvs.bund.de
BDBOS	Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben	BMI	bdbos.bund.de
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht	BMF	baфин.de
BGR	Bundesanstalt für Geowissenschaften und Rohstoffe	BMWi	bgr.bund.de
BGR	Bundesanstalt für Geowissenschaften und Rohstoffe	BMWi	deutsche-rohstoffagentur.de
BGR	Bundesanstalt für Geowissenschaften und Rohstoffe	BMWi	deutscher-rohstoffeffizienz-preis.de
BGR	Bundesanstalt für Geowissenschaften und Rohstoffe	BMWi	genesys-hannover.de
BGR	Bundesanstalt für Geowissenschaften und Rohstoffe	BMWi	geotechnologien-aids.de
BGR	Bundesanstalt für Geowissenschaften und Rohstoffe	BMWi	geozentrum-hannover.de
BGR	Bundesanstalt für Geowissenschaften und Rohstoffe	BMWi	glnet-network.org
BGR	Bundesanstalt für Geowissenschaften und Rohstoffe	BMWi	mags-projekt.de
BGR	Bundesanstalt für Geowissenschaften und Rohstoffe	BMWi	pebs-eu.de
BGR	Bundesanstalt für Geowissenschaften und Rohstoffe	BMWi	roboha.de
BGR	Bundesanstalt für Geowissenschaften und Rohstoffe	BMWi	whymap.org
BLE	Bundesanstalt für Landwirtschaft und Ernährung	BMEL	ble.de
THW	Bundesanstalt Technisches Hilfswerk	BMI	exchangeofexperts.eu
THW	Bundesanstalt Technisches Hilfswerk	BMI	extranet.thw.de
THW	Bundesanstalt Technisches Hilfswerk	BMI	infozentrum.thw.de
THW	Bundesanstalt Technisches Hilfswerk	BMI	lv-bebbst.thw.de
THW	Bundesanstalt Technisches Hilfswerk	BMI	lv-bw.thw.de
THW	Bundesanstalt Technisches Hilfswerk	BMI	lv-by.thw.de
THW	Bundesanstalt Technisches Hilfswerk	BMI	lv-hbni.thw.de
THW	Bundesanstalt Technisches Hilfswerk	BMI	lv-herpsl.thw.de
THW	Bundesanstalt Technisches Hilfswerk	BMI	lv-hhmsh.thw.de
THW	Bundesanstalt Technisches Hilfswerk	BMI	lv-nw.thw.de
THW	Bundesanstalt Technisches Hilfswerk	BMI	lv-snth.thw.de
THW	Bundesanstalt Technisches Hilfswerk	BMI	m.thw.de
THW	Bundesanstalt Technisches Hilfswerk	BMI	reln-ins.thw.de
THW	Bundesanstalt Technisches Hilfswerk	BMI	thw.de
THW	Bundesanstalt Technisches Hilfswerk	BMI	thw-bundesschule.de
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit	BMI	bfdi.bund.de
BEV	Bundeseseisenbahnvermögen		Bundeseseisenbahnvermögen

BGH	Bundesgerichtshof	BGH	bundesgerichtshof.de
BISp	Bundesinstitut für Sportwissenschaft	BMI	bisp.de
BISp	Bundesinstitut für Sportwissenschaft	BMI	bisp-sportpsychologie.de
BISp	Bundesinstitut für Sportwissenschaft	BMI	info.bisp-surf.de
BISp	Bundesinstitut für Sportwissenschaft	BMI	rahnucken.de
BISp	Bundesinstitut für Sportwissenschaft	BMI	bisp-ehf.de
BFARM	Bundesinstitut für Arzneimittel und Medizinprodukte	BMG	bfarm.de
BIB	Bundesinstitut für Bevölkerungsforschung	BMI	bib.bund.de
BIB	Bundesinstitut für Bevölkerungsforschung	BMI	demografie-portal.de
BIB	Bundesinstitut für Bevölkerungsforschung	BMI	jobmob-and-families.eu
BKartA	Bundeskartellamt	BMWi	bundeskartellamt.de
BKartA	Bundeskartellamt	BMWi	ikk2017.de
BKA	Bundeskriminalamt	BMI	bka.de
BKA	Bundeskriminalamt	BMI	project-contra.org
BKA	Bundeskriminalamt	BMI	polizei.de
BKA	Bundeskriminalamt	BMI	innerasichheitsfonds.de
BMJV	Bundesministerium der Justiz und für Verbraucherschutz	BMJV	BMJV Intranet
BMJV	Bundesministerium der Justiz und für Verbraucherschutz	BMJV	bmjv.de
BMJV	Bundesministerium der Justiz und für Verbraucherschutz	BMJV	enorm.bund.de
BMJV	Bundesministerium der Justiz und für Verbraucherschutz	BMJV	fair-im-netz.de
BMJV	Bundesministerium der Justiz und für Verbraucherschutz	BMJV	mietpreisbremse.bund.de
BMJV	Bundesministerium der Justiz und für Verbraucherschutz	BMJV	netzwerk-verbraucherforschung.de
BMJV	Bundesministerium der Justiz und für Verbraucherschutz	BMJV	rosenburg.bmjv.de
BMJV	Bundesministerium der Justiz und für Verbraucherschutz	BMJV	
BMI	Bundesministerium des Innern	BMI	116.de
BMI	Bundesministerium des Innern	BMI	ausgliederbeauftragter.de
BMI	Bundesministerium des Innern	BMI	bmi.bund.de
BMI	Bundesministerium des Innern	BMI	cjo.bund.de
BMI	Bundesministerium des Innern	BMI	imagi.de
BMI	Bundesministerium des Innern	BMI	Intranet des Bundes
BMI	Bundesministerium des Innern	BMI	it-planungsrat.de
BMI	Bundesministerium des Innern	BMI	orghandbuch.de
BMI	Bundesministerium des Innern	BMI	personalausweisportal.de
BMI	Bundesministerium des Innern	BMI	personenstandsrecht.de
BMI	Bundesministerium des Innern	BMI	protokoll-inland.de
BMI	Bundesministerium des Innern	BMI	vereint-gegen-rechtsextratismus.de
BMI	Bundesministerium des Innern	BMI	vertreter-des-bundesinteresses.de
BMI	Bundesministerium des Innern	BMI	verwaltung-innovativ.de
BMAS	Bundesministerium für Arbeit und Soziales	BMAS	blv-lotse.de
BMAS	Bundesministerium für Arbeit und Soziales	BMAS	budget.bmas.de
BMAS	Bundesministerium für Arbeit und Soziales	BMAS	einfach-teilhaben.de
BMAS	Bundesministerium für Arbeit und Soziales	BMAS	esf.de
BMAS	Bundesministerium für Arbeit und Soziales	BMAS	gemeinsam-einfach-machen.de
BMEL	Bundesministerium für Ernährung und Landwirtschaft	BMEL	bmel.de
BND	Bundesnachrichtendienst	BK	bnd.bund.de
BNetzA	Bundesnetzagentur	BMWi	BNetzA Internet
BNetzA	Bundesnetzagentur	BMWi	BNetzA Intranet
BPatG	Bundespatentgericht	BPatG	bundespatentgericht.de
BPOL	Bundespolizei	BMI	bundespolizei.de
BPOL	Bundespolizei	BMI	easypass.de
BPRA	Bundespräsidialamt	BPRA	bundespraesident.de
Bundesrat	Bundesrat	BR	bundesrat.de
Bundesrat	Bundesrat	BR	innenministerkonferenz.de
Bundesrat	Bundesrat	BR	Intranet
Bundesrat	Bundesrat	BR	verkehrsministerkonferenz.de
Bundesrat	Bundesrat	BR	vermittlungsausschuss.de
Bundesrat	Bundesrat	BR	wirtschaftsministerkonferenz.de
BBK	Bundessamt für Bevölkerungsschutz und Katastrophenhilfe	BMI	bbk.bund.de
BBK	Bundessamt für Bevölkerungsschutz und Katastrophenhilfe	BMI	kritik.bund.de
BBK	Bundessamt für Bevölkerungsschutz und Katastrophenhilfe	BMI	max-und-flocka-helferland.de
BBK	Bundessamt für Bevölkerungsschutz und Katastrophenhilfe	BMI	warnung.bund.de
BSG	Bundessozialgericht	BSG	bsg.bund.de
BVA	Bundesverwaltungsamt	BMI	bund.de
BVA	Bundesverwaltungsamt	BMI	bva.bund.de
BVA	Bundesverwaltungsamt	BMI	umfrage.bund.de
BVerfG	Bundesverfassungsgericht	BVerfG	bundesverfassungsgericht.de
BVA	Bundesverwaltungsamt	BMI	Deutschland Online Infrastruktur (im IVBB und IVBV)
BVA	Bundesverwaltungsamt	NDB	Netze des Bundes (Intranet)
BVA	Bundesverwaltungsamt	BMI	Travelmanagement-Portal
BZSt	Bundeszentralamt für Steuern	BMF	bzat.de
BZSt	Bundeszentralamt für Steuern	BMF	www.steuerfachas-info-center.de

BStU	Der Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (BStU)	BKM	bstu.bund.de
BStU	Der Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (BStU)	BKM	demokratie-statt-diktatur.de
BStU	Der Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (BStU)	BKM	untoldstories.de
DNB	Deutsche Nationalbibliothek	BKM	Portal + SubSites
DNB	Deutsche Nationalbibliothek	BKM	Virtuelle Ausstellungen
	Generalbundesanwalt beim BGH		Generalbundesanwalt
GZD	Generalszolldirektion	BMF	BW2 Intranet
GZD	Generalszolldirektion	BMF	kkv.bund.de
GZD	Generalszolldirektion	BMF	zoll.de
ITZBund	Informationstechnikzentrum Bund	BMF	BANU
ITZBund	Informationstechnikzentrum Bund	BMF	GSB Adminmandant
ITZBund	Informationstechnikzentrum Bund	BMF	GSB Dokumentant
ITZBund	Informationstechnikzentrum Bund	BMF	GSB Produktmandant
ITZBund	Informationstechnikzentrum Bund	BMF	GSB Standardlösung
ITZBund	Informationstechnikzentrum Bund	BMF	ITZBund Intranet
ITZBund	Informationstechnikzentrum Bund	BMF	itzbund.de
ITZBund	Informationstechnikzentrum Bund	BMF	PARIS
ITZBund	Informationstechnikzentrum Bund	BMF	RIKO
ITZBund	Informationstechnikzentrum Bund	BMF	
PEI	Paul-Ehrlich-Institut	BMG	pei.de
PEI	Paul-Ehrlich-Institut	BMG	
RKI	Robert Koch Institut	BMG	sbisg.rki.de
RKI	Robert Koch Institut	BMG	efo.rki.de
RKI	Robert Koch Institut	BMG	emerge.rki.eu
RKI	Robert Koch Institut	BMG	esticom.eu
RKI	Robert Koch Institut	BMG	gohj.online
RKI	Robert Koch Institut	BMG	krebsdaten.de
RKI	Robert Koch Institut	BMG	rki.de
RKI	Robert Koch Institut	BMG	tujaemia-network.com
RKI	Robert Koch Institut	BMG	
SRU	Sachverständigenrat für Umweltfragen	BMJ	umweltstat.de
SIBA	Statistisches Bundesamt	StBA	amlich-einfach.de
SIBA	Statistisches Bundesamt	BMJ	destatis.de
SIBA	Statistisches Bundesamt	BMJ	zensus2011.de
SIBA	Statistisches Bundesamt	BMJ	zensus2021.de
UBA	Umweltbundesamt / Deutsche Emissionshandelsstelle	BMU	dahst.de
UBA	Umweltbundesamt / Deutsche Emissionshandelsstelle	BMU	nationales-beleitgramm.de
UBA	Umweltbundesamt / Deutsche Emissionshandelsstelle	BMU	strompreiskompensation.de
ZITIS	Zentrale Stelle für Informationstechnik im Sicherheitsbereich	BMJ	zitis.bund.de

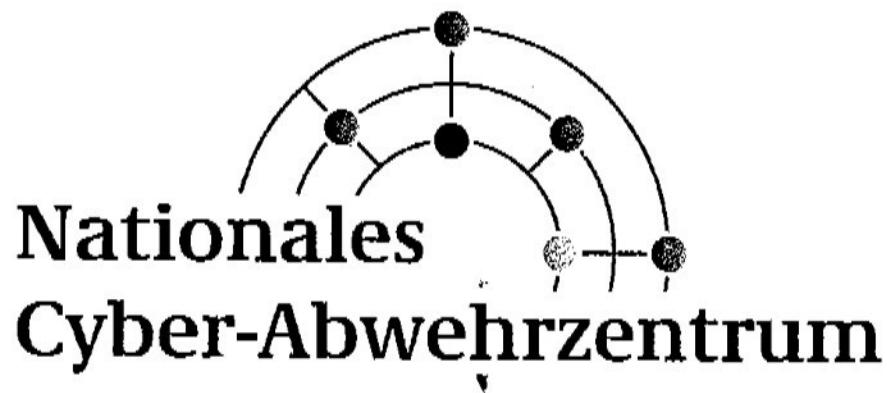


**Telemedien des Bundes, die gem. der angegebenen Datenschutzhinweise keine IP-Adressen  
des Nutzers speichern  
Stand Juli 2018**

[www.auswaertiges-amt.de](http://www.auswaertiges-amt.de)  
[www.antidiskriminierungsstelle.de](http://www.antidiskriminierungsstelle.de)  
[www.bundesausgleichsamt.de](http://www.bundesausgleichsamt.de)  
[www.bafa.de](http://www.bafa.de)  
[bafin.de](http://bafin.de)  
[allianz-fuer-demenz.de](http://allianz-fuer-demenz.de)  
[lokale-allianzen.de](http://lokale-allianzen.de)  
[www.allianz-fuer-demenz.de](http://www.allianz-fuer-demenz.de)  
[www.lokale-allianzen.de](http://www.lokale-allianzen.de)  
[www.pflege-charta-arbeitshilfe.de](http://www.pflege-charta-arbeitshilfe.de)  
[www.pflege-charta.de](http://www.pflege-charta.de)  
[ifos-bund.de](http://ifos-bund.de)  
[www.ifos-bund.de](http://www.ifos-bund.de)  
[www.bakoev.bund.de](http://www.bakoev.bund.de)  
[www.bamf.bund.de](http://www.bamf.bund.de)  
[www.bamf.de](http://www.bamf.de)  
[www.integration-in-deutschland.de](http://www.integration-in-deutschland.de)  
[www.bundesarchiv.de](http://www.bundesarchiv.de)  
[www.bast.de](http://www.bast.de)  
[www.bundesbank.de](http://www.bundesbank.de)  
[ese-initiative.org](http://ese-initiative.org)  
[fis.bbk.bund.de](http://fis.bbk.bund.de)  
[www.bbk-virtuelle-aknz.de](http://www.bbk-virtuelle-aknz.de)  
[www.bbk.bund.de](http://www.bbk.bund.de)  
[www.bevoelkerungsschutz.de](http://www.bevoelkerungsschutz.de)  
[www.kritis.bund.de](http://www.kritis.bund.de)  
[www.max-und-flocke-helferland.de](http://www.max-und-flocke-helferland.de)  
[www.risikomanagement-bau.de](http://www.risikomanagement-bau.de)  
[www.warbung.bund.de](http://www.warbung.bund.de)  
[ecb-culturaldays.eu](http://ecb-culturaldays.eu)  
[www.bbr.bund.de](http://www.bbr.bund.de)  
[www.bdbos.bund.de](http://www.bdbos.bund.de)  
[www.bfarm.de](http://www.bfarm.de)  
[www.behindertenbeauftragte.de](http://www.behindertenbeauftragte.de)  
[www.behindertenbeauftragter.de](http://www.behindertenbeauftragter.de)  
[www.inklusionslandkarte.de](http://www.inklusionslandkarte.de)  
[www.bfd.bund.de](http://www.bfd.bund.de)  
[www.bfdi.bund.de](http://www.bfdi.bund.de)  
[www.bfe-bund.de](http://www.bfe-bund.de)  
[www.bafg.de](http://www.bafg.de)  
[www.bundesjustizamt.de](http://www.bundesjustizamt.de)  
[www.bundeszentralregister.de](http://www.bundeszentralregister.de)  
[www.fuehrungszeugnis.bund.de](http://www.fuehrungszeugnis.bund.de)  
[www.informju.de](http://www.informju.de)  
[www.bfs.de](http://www.bfs.de)  
[www.asse.bund.de](http://www.asse.bund.de)  
[www.endlager-asse.de](http://www.endlager-asse.de)  
[www.endlager-konrad.de](http://www.endlager-konrad.de)

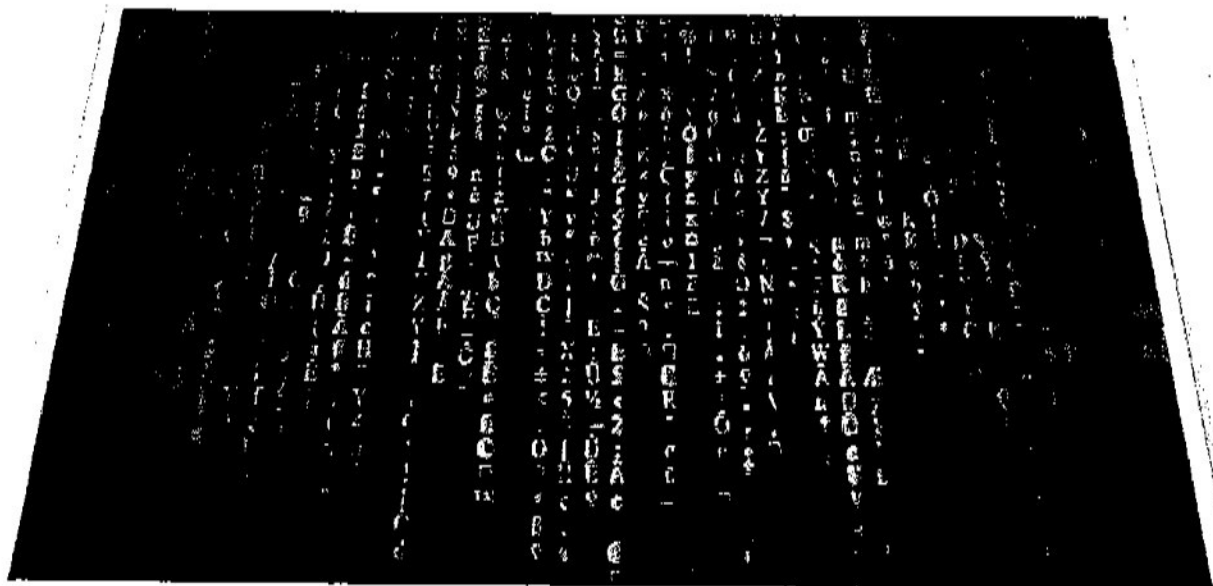


[www.bfu-web.de](http://www.bfu-web.de)  
[www.bfuweb.de](http://www.bfuweb.de)  
[www.bgr.bund.de](http://www.bgr.bund.de)  
[www.bgr.bund.de](http://www.bgr.bund.de)  
[www.deutsche-rohstoffagentur.de](http://www.deutsche-rohstoffagentur.de)  
[www.geotechnologien-aida.de](http://www.geotechnologien-aida.de)  
[www.geozentrum-hannover.de](http://www.geozentrum-hannover.de)  
[www.giraf-network.org](http://www.giraf-network.org)  
[www.mags-projekt.de](http://www.mags-projekt.de)  
[www.bib-demografie.de](http://www.bib-demografie.de)  
[www.bib-demographie.de](http://www.bib-demographie.de)  
[www.demografie-portal.de](http://www.demografie-portal.de)  
[www.bisp-sportpsychologie.de](http://www.bisp-sportpsychologie.de)  
[www.bisp.de](http://www.bisp.de)  
[www.bundeskartellamt.de](http://www.bundeskartellamt.de)  
[www.deutsche-digitale-bibliothek.de](http://www.deutsche-digitale-bibliothek.de)  
[www.kulturgutschutz-deutschland.de](http://www.kulturgutschutz-deutschland.de)  
[www.kunstsammlung-bund.de](http://www.kunstsammlung-bund.de)  
[www.bundeswaldinventur.de](http://www.bundeswaldinventur.de)  
[www.budget.bmas.de](http://www.budget.bmas.de)  
[www.vereinbarkeit-fuer-eltern.de](http://www.vereinbarkeit-fuer-eltern.de)  
[familien-pflege-zeit.de](http://familien-pflege-zeit.de)  
[hilfetelefon.de](http://hilfetelefon.de)  
[jugend-staerken.de](http://jugend-staerken.de)  
[kompetenzagenturen.de](http://kompetenzagenturen.de)  
[wege-zur-pflege.de](http://wege-zur-pflege.de)  
[www.hilfetelefon.de](http://www.hilfetelefon.de)  
[www.jugend-staerken.de](http://www.jugend-staerken.de)  
[www.wege-zur-pflege.de](http://www.wege-zur-pflege.de)  
[www.govdata.de](http://www.govdata.de)  
[www.bmj.bund.de](http://www.bmj.bund.de)  
[www.bmju.bund.de](http://www.bmju.bund.de)  
[www.bmv-registrierung.de](http://www.bmv-registrierung.de)  
[www.kerntechnische-entsorgung.de](http://www.kerntechnische-entsorgung.de)  
[www.bmvbs.de](http://www.bmvbs.de)  
[www.bmz.de](http://www.bmz.de)  
[www.bnd.bund.de](http://www.bnd.bund.de)  
[www.bpb.de](http://www.bpb.de)  
[www.bundespruefstelle.de](http://www.bundespruefstelle.de)  
[www.bundesrechnungshof.de](http://www.bundesrechnungshof.de)  
[www.bsh.de](http://www.bsh.de)  
[www.bund.de](http://www.bund.de)  
[www.bvl.bund.de](http://www.bvl.bund.de)  
[www.dwd.de](http://www.dwd.de)  
[www.geda-studie.de](http://www.geda-studie.de)  
[www.thw.de](http://www.thw.de)



## Informationen des Nationalen Cyber-Abwehrzentrums

Cyber-Angriff auf Ziele im Auswärtigen Amt



## Inhalt

Hintergrund .....	4
Maßnahmen und Erkenntnisse.....	4
BSI .....	4
BfV.....	4
BND .....	5
BAMAD.....	5
Zusammenfassung .....	5

**Beteiligte Behörden:**

BAMAD, BfV, BND, BSI

**Herausgabedatum:**

19.03.2018

**Herausgeber:**

**Nationales Cyber-Abwehrzentrum**  
c/o Bundesamt für Sicherheit in der Informationstechnik  
Godesberger Allee 185-189  
53175 Bonn

E-Mail: [cyber-az@bsi.bund.de](mailto:cyber-az@bsi.bund.de)  
Tel.: 0228 99 9582 6000



## Hintergrund

Gegen Ende des Jahres 2017 wurde das Nationale Cyber-Abwehrzentrum (Cyber-AZ) durch den Bundesnachrichtendienst (BND) – und unmittelbar danach auch durch das Bundesamt für Verfassungsschutz (BfV) – über einen aktuellen, glaubhaften nachrichtendienstlichen Hinweis informiert, demnach IT-Infrastruktur deutscher Bundesbehörden wahrscheinlich durch eine APT<sup>1</sup>-Kampagne kompromittiert sei.

Nach Eingang des Hinweises wurde im Cyber-AZ unter Beteiligung des Bundesamtes für den Militärischen Abschirmdienst (BAMAD), des Bundesamtes für Verfassungsschutz (BfV), des Bundesnachrichtendienstes (BND) und des Bundesamtes für Sicherheit in der Informationstechnik (BSI) eine Arbeitsgruppe eingerichtet, in der seitdem die Bearbeitung des Sachverhaltes koordiniert wird.

## Maßnahmen und Erkenntnisse

### BSI

Das BSI hat in Reaktion auf die nachrichtendienstlichen Hinweise auf den Angriff ein Mobile Incident Response Team (MIRT) zu möglichen Betroffenen entsandt. Dort wurden Daten zur weiteren Analyse im BSI gesichert (forensische Sicherung von Rechnersystemen, Logdaten etc.). Parallel dazu wurden Suchen in den zentralen Protokolldaten des IVBB<sup>2</sup> nach diesen Hinweisen durchgeführt.

Im weiteren Verlauf der Untersuchungen konnten beim Auswärtigen Amt (AA) mutmaßlich mit dem Angriff im Zusammenhang stehende Daten gesichert werden. Diese Daten wurden analysiert, und es wurden Signaturen für das Schadprogrammmerkennungssystem (SES) des BSI erstellt. Das SES dient zur Detektion von Angriffen auf den IVBB.

Bei der forensischen Untersuchung der gesicherten Systeme des AA wurden Schadpro-

gramme festgestellt, die auf einen nachrichtendienstlichen Angriff hinweisen.

In Abstimmung mit dem AA hat das vom BSI entsandte MIRT daher unter strenger Geheimhaltung im AA ein Büro bezogen. Alle Sicherungs-, Analyse- und Gegenmaßnahmen im AA wurden in einer Weise durchgeführt, die es erlaubte, von den Angreifern unentdeckt Informationen über deren Vorgehen zu sammeln.

Das MIRT errichtete unter anderem Sensorik des BSI im Netz des AA, mit deren Hilfe der interne Netzwerkverkehr analysiert werden konnte. Durch die Untersuchungen des MIRT vor Ort, die Detektion der Angreiferkommunikation mit dem SES und der Protokoll Datenanalyse im AA war das BSI schließlich in der Lage, das Vorgehen der Angreifer im AA zu beobachten und seine Aktionen nachzuvollziehen.

Parallel zu Beobachtung und weiteren Analysen wurden – ausgehend von unterschiedlichen Szenarien für die weitere Lageentwicklung – eine Reihe von Sofortmaßnahmen vorbereitet. Nach dem presseöffentlichen Bekanntwerden des Sachverhalts wurden Teile dieser Maßnahmen vorzeitig ergriffen.

Für den Angriff auf das AA wurden Server der Bundesakademie für öffentliche Verwaltung (BAköV) bzw. der Hochschule des Bundes für öffentliche Verwaltung (HS Bund) missbraucht. Deshalb mussten auch hier in Reaktion auf die Offenlegung des Sachverhalts geeignete Sofortmaßnahmen eingeleitet werden. Diese hatten zur Folge, dass seit 02.03.2018 zahlreiche Lernplattformen des Bundes vorübergehend deaktiviert wurden.

### BfV

Das BfV unterstützt die Aufklärung des aktuellen Cyber-Angriffs auf das Auswärtige Amt und die BAKöV/HS Bund durch eigene operative Maßnahmen.

Die im Rahmen der Sachverhaltsaufklärung bekannt gewordenen Erkenntnisse hat das BfV sukzessive in seine operativen Maßnahmen aufgenommen. Taktisches Ziel ist es, darüber weitere Erkenntnisse über Opferrechner, Kommunikationsinhalte, Angriffsversuche und den Angreifer sowie den gewählten Modus Operandi zu gewinnen.

<sup>1</sup> APT: engl. „advanced persistent threat“, dt. „fortgeschrittene andauernde Bedrohung“: komplexer, zielgerichteter, effektiver Cyber-Angriff.

<sup>2</sup> IVBB: „Informationsverbund Berlin-Bonn“, eine Kommunikationsplattform für Stellen des Bundes.



Die nachrichtendienstlichen Erkenntnisse fließen in die Abwehrmaßnahmen zum Schutze des Regierungsnetzes ein und dienen zudem der Zuordnung des Angriffs zu einer Angriffskampagne (Attribution).

### **BND**

Im Anschluss an eine unverzügliche Erstprüfung und Validierung des Ursprungshinweises erfolgte die Meldung des Vorfalls an die zuständigen Behörden im Cyber-AZ (hier: BAMAD, BfV und BSI).

Seitdem arbeitete der BND in der mit dem Sachverhalt betrauten Arbeitsgruppe des Cyber-AZ mit und lieferte mittels SSCD selbst generierte Informationen.

Im Schwerpunkt wird durch den BND zusammen mit internen und externen Partnern der Modus Operandi der Cyber-Kampagne aufgeklärt und analysiert. Hauptaugenmerk wird auf den Einsatz der Datenverkehre zur Kontrolle und Steuerung der eingesetzten Schadsoftware gelegt. Hier gewinnt der BND neue Einblicke in Angriffswege und die sich dynamisch verhaltende Infrastruktur. Diese werden unter anderem an das BSI zum Schutz der Behördennetze übermittelt.

Die hierfür im Schwerpunkt eingesetzten strategischen SIGINT-Fähigkeiten des BND werden durch weitere operative Maßnahmen unterstützt.

### **BAMAD**

Mit der zeitgleichen Informationsüberstellung durch deutsche Sicherheitsbehörden folgte die Aufnahme der Bearbeitung im BAMAD im Dezember 2017. Im Geschäftsbereich des BMVg war zum Zeitpunkt der Erstmeldung von einer Betroffenheit auszugehen. Eine eingehende Prüfung ergab, dass die IT-Systeme des BMVg nicht kompromit-

tiert wurden. Bislang liegen dem BAMAD in diesem Kontext keine Hinweise oder Erkenntnisse vor, dass IT-Systeme der Bundeswehr und des BMVg infiziert sein könnten.

### **Zusammenfassung**

- Das AA war Ziel eines Cyber-Angriffes.
- Für diesen Angriff wurden auch Server der BAKÖV bzw. der HS Bund missbraucht.
- Der IVBB wurde nicht infiziert. Die Netze der einzelnen, über den IVBB verbundenen Behörden sind segmentiert. Der Angreifer hatte daher keine Möglichkeit, sich frei im IVBB zu bewegen.
- Die zuständigen Behörden im Cyber-AZ haben den Angriff nach Kenntnisnahme kontrolliert (und) beobachtet, um weitere Erkenntnisse zu gewinnen.
- Nachdem der Angriff presseöffentlich bekannt geworden war, wurde ein bereits vorab zwischen den Beteiligten abgestimmter, detaillierter Maßnahmenplan umgesetzt und entsprechende Gegenmaßnahmen eingeleitet. Diese führten auch zur Deaktivierung diverser Lernplattformen des Bundes.
- Der Angreifer hat Daten aus dem AA ausgeleitet.
- Die aus dem Angriff gewonnenen Erkenntnisse sind für die weitere Härtung der Netze und Systeme deutscher Bundesbehörden von hohem Wert. Entsprechende Aktivitäten wurden bereits durch das BSI eingeleitet.
- Die Zusammenarbeit zwischen den beteiligten Behörden hat sich als sehr wirkungsvoll zur Abwehr erwiesen.





	A	B	C
1	<i>Zeitstempel wann die Anfrage erfasst wurde</i>	<i>Quell-IP-Adresse des anfragenden Clients</i>	<i>Hostsystem von dem die Logdaten erfasst wurden</i>
2	<b>timestamp</b>	<b>src_ip</b>	<b>host</b>
3	31/Jul/2018:13:43:33 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
4	31/Jul/2018:13:43:34 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
5	31/Jul/2018:13:43:34 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
6	31/Jul/2018:13:43:36 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
7	31/Jul/2018:13:43:39 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
8	31/Jul/2018:13:43:40 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
9	31/Jul/2018:13:43:40 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
10	31/Jul/2018:13:43:41 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
11	31/Jul/2018:13:43:41 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
12	31/Jul/2018:13:43:41 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
13	31/Jul/2018:13:43:43 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
14	31/Jul/2018:13:43:43 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
15	31/Jul/2018:13:43:43 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
16	31/Jul/2018:13:43:44 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
17	31/Jul/2018:13:43:46 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
18	31/Jul/2018:13:43:46 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
19	31/Jul/2018:13:43:47 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
20	31/Jul/2018:13:43:47 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
21	31/Jul/2018:13:43:48 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
22	31/Jul/2018:13:43:48 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
23	31/Jul/2018:13:43:49 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
24	31/Jul/2018:13:43:49 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
25	31/Jul/2018:13:43:49 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
26	31/Jul/2018:13:43:50 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
27	31/Jul/2018:13:43:50 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
28	31/Jul/2018:13:43:51 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
29	31/Jul/2018:13:43:51 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
30	31/Jul/2018:13:43:52 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
31	31/Jul/2018:13:43:53 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
32	31/Jul/2018:13:43:53 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
33	31/Jul/2018:13:43:54 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
34	31/Jul/2018:13:43:54 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
35	31/Jul/2018:13:43:55 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
36	31/Jul/2018:13:43:59 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
37	31/Jul/2018:13:43:59 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
38	31/Jul/2018:13:43:59 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
39	31/Jul/2018:13:44:01 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
40	31/Jul/2018:13:44:01 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
41	31/Jul/2018:13:44:01 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
42	31/Jul/2018:13:44:02 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
43	31/Jul/2018:13:44:02 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
44	31/Jul/2018:13:44:03 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
45	31/Jul/2018:13:44:04 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}
46	31/Jul/2018:13:44:04 +0200	Pseudonymisierte IP-Adresse	{"name": "nginx-server-01"}



example\_attack-1

	D	E
1	HTTP User Agent der vom Client gesendet wurde	HTTP Methode vom Client
2	http.http_user_agent	http.method
3	}	PROPFIND
4	Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/	POST
5	Mozilla/5.0	GET
6	Mozilla/5.0	GET
7	Mozilla/5.0	GET
8	Mozilla/5.0	GET
9	Mozilla/5.0	GET
10	Mozilla/5.0	GET
11	Mozilla/5.0	GET
12	Mozilla/5.0	GET
13	Mozilla/5.0	GET
14	Mozilla/5.0	GET
15	Mozilla/5.0	GET
16	Mozilla/5.0	GET
17	Mozilla/5.0	GET
18	Mozilla/5.0	GET
19	Mozilla/5.0	GET
20	Mozilla/5.0	GET
21	Mozilla/5.0	GET
22	Mozilla/5.0	GET
23	Mozilla/5.0	GET
24	Mozilla/5.0	GET
25	Mozilla/5.0	GET
26	Mozilla/5.0	GET
27	Mozilla/5.0	GET
28	Mozilla/5.0	GET
29	Mozilla/5.0	GET
30	Mozilla/5.0	GET
31	Mozilla/5.0	GET
32	Mozilla/5.0	GET
33	Mozilla/5.0	GET
34	Mozilla/5.0	GET
35	Mozilla/5.0	GET
36	Mozilla/5.0	GET
37	Mozilla/5.0	GET
38	Mozilla/5.0	GET
39	Mozilla/5.0	GET
40	Mozilla/5.0	GET
41	Mozilla/5.0	GET
42	Mozilla/5.0	GET
43	Mozilla/5.0	GET
44	Mozilla/5.0	GET
45	Mozilla/5.0	GET
46	Mozilla/5.0	GET

	F	G	H	I	J
	HTTP Version die zwischen Client und Server eingesetzt wurde	Antwort des Webserver in Bytes	HTTP Statuscode den der Webserver auf die Anfrage geliefert hat	HTTP URL die vom Client angefragt wurde	Sofern aus dem Feld „http.http_user_agent“ extrahierbar, wird hier der verwendete Browser angegeben.
1	http.req_protocol	http.res_size	http.res_status	http.url	http.user_agent.name
3	HTTP/1.1	154	302	/	
4	HTTP/1.1	154	302	/wls-wsat/CoordinatorPortType	Firefox
5	HTTP/1.1	154	302	/index.php	Other
6	HTTP/1.1	154	302	/phpmyadmin/index.php	Other
7	HTTP/1.1	154	302	/phpMyAdmin/index.php	Other
8	HTTP/1.1	154	302	/pmd/index.php	Other
9	HTTP/1.1	154	302	/pma/index.php	Other
10	HTTP/1.1	154	302	/PMA/index.php	Other
11	HTTP/1.1	154	302	/PMA2/index.php	Other
12	HTTP/1.1	154	302	/pmamy/index.php	Other
13	HTTP/1.1	154	302	/pmamy2/index.php	Other
14	HTTP/1.1	154	302	/mysql/index.php	Other
15	HTTP/1.1	154	302	/admin/index.php	Other
16	HTTP/1.1	154	302	/db/index.php	Other
17	HTTP/1.1	154	302	/dbadmin/index.php	Other
18	HTTP/1.1	154	302	/web/phpMyAdmin/index.php	Other
19	HTTP/1.1	154	302	/admin/pma/index.php	Other
20	HTTP/1.1	154	302	/admin/PMA/index.php	Other
21	HTTP/1.1	154	302	/admin/mysql/index.php	Other
22	HTTP/1.1	154	302	/admin/mysql2/index.php	Other
23	HTTP/1.1	154	302	/admin/phpmyadmin/index.php	Other
24	HTTP/1.1	154	302	/admin/phpMyAdmin/index.php	Other
25	HTTP/1.1	154	302	/admin/phpmyadmin2/index.php	Other
26	HTTP/1.1	154	302	/mysqladmin/index.php	Other
27	HTTP/1.1	154	302	/mysql-admin/index.php	Other
28	HTTP/1.1	154	302	/phpadmin/index.php	Other
29	HTTP/1.1	154	302	/phpmyadmin0/index.php	Other
30	HTTP/1.1	154	302	/phpmyadmin1/index.php	Other
31	HTTP/1.1	154	302	/phpmyadmin2/index.php	Other
32	HTTP/1.1	154	302	/myadmin/index.php	Other
33	HTTP/1.1	154	302	/myadmin2/index.php	Other
34	HTTP/1.1	154	302	/xampp/phpmyadmin/index.php	Other
35	HTTP/1.1	154	302	/phpMyadmin_bak/index.php	Other
36	HTTP/1.1	154	302	/www/phpMyAdmin/index.php	Other
37	HTTP/1.1	154	302	/tools/phpMyAdmin/index.php	Other
38	HTTP/1.1	154	302	/phpmyadmin-old/index.php	Other
39	HTTP/1.1	154	302	/phpMyAdminold/index.php	Other
40	HTTP/1.1	154	302	/phpMyAdmin.old/index.php	Other
41	HTTP/1.1	154	302	/pma-old/index.php	Other
42	HTTP/1.1	154	302	/claroline/phpMyAdmin/index.php	Other
43	HTTP/1.1	154	302	/typo3/phpmyadmin/index.php	Other
44	HTTP/1.1	154	302	/phpma/index.php	Other
45	HTTP/1.1	154	302	/phpmyadmin/phpmyadmin/index.php	Other
46	HTTP/1.1	154	302	/phpMyAdmin/phpMyAdmin/index.php	Other

## example\_attack2-1

	K	L	M	N
1	Sofern aus dem Feld „http.user_agent“ extrahierbar, wird hier das verwendete Betriebssystem angegeben.	Quell-Logdatei		
2	http.user_agent.os	source		
3		/var/log/nginx/localhost.access.log		
4	Windows 7	/var/log/nginx/localhost.access.log		
5	Other	/var/log/nginx/localhost.access.log		
6	Other	/var/log/nginx/localhost.access.log		
7	Other	/var/log/nginx/localhost.access.log		
8	Other	/var/log/nginx/localhost.access.log		
9	Other	/var/log/nginx/localhost.access.log		
10	Other	/var/log/nginx/localhost.access.log		
11	Other	/var/log/nginx/localhost.access.log		
12	Other	/var/log/nginx/localhost.access.log		
13	Other	/var/log/nginx/localhost.access.log		
14	Other	/var/log/nginx/localhost.access.log		
15	Other	/var/log/nginx/localhost.access.log		
16	Other	/var/log/nginx/localhost.access.log		
17	Other	/var/log/nginx/localhost.access.log		
18	Other	/var/log/nginx/localhost.access.log		
19	Other	/var/log/nginx/localhost.access.log		
20	Other	/var/log/nginx/localhost.access.log		
21	Other	/var/log/nginx/localhost.access.log		
22	Other	/var/log/nginx/localhost.access.log		
23	Other	/var/log/nginx/localhost.access.log		
24	Other	/var/log/nginx/localhost.access.log		
25	Other	/var/log/nginx/localhost.access.log		
26	Other	/var/log/nginx/localhost.access.log		
27	Other	/var/log/nginx/localhost.access.log		
28	Other	/var/log/nginx/localhost.access.log		
29	Other	/var/log/nginx/localhost.access.log		
30	Other	/var/log/nginx/localhost.access.log		
31	Other	/var/log/nginx/localhost.access.log		
32	Other	/var/log/nginx/localhost.access.log		
33	Other	/var/log/nginx/localhost.access.log		
34	Other	/var/log/nginx/localhost.access.log		
35	Other	/var/log/nginx/localhost.access.log		
36	Other	/var/log/nginx/localhost.access.log		
37	Other	/var/log/nginx/localhost.access.log		
38	Other	/var/log/nginx/localhost.access.log		
39	Other	/var/log/nginx/localhost.access.log		
40	Other	/var/log/nginx/localhost.access.log		
41	Other	/var/log/nginx/localhost.access.log		
42	Other	/var/log/nginx/localhost.access.log		
43	Other	/var/log/nginx/localhost.access.log		
44	Other	/var/log/nginx/localhost.access.log		
45	Other	/var/log/nginx/localhost.access.log		
46	Other	/var/log/nginx/localhost.access.log		