Kommunikation & Recht

Betriebs-Berater für
● Medien ● Telekommunikation ● Multimedia

4
K&R

21. Jahrgang April 2018 Seiten 217 – 288

dfv Mediengruppe · Frankfurt am Main

3. Sammelklage gegen Google in Großbritannien

In Großbritannien muss sich Google dagegen in einer Sammelklage gegen den Vorwurf verteidigen, in den Jahren 2011 und 2012 auf dem iPhone Datenschutzeinstellungen umgangen und auf diese Weise rechtswidrig das Surfverhalten der Internetnutzer überwacht zu haben.[85] Das Verfahren ist noch in einem sehr frühen Stadium, so dass der weitere Verlauf abzuwarten ist.

4. GMail als Telekommunikationsdienst

Inzwischen hat sich das OVG Münster mit dem Streit zwischen der Bundesnetzagentur und Google über die Einstufung von Google Mail als Telekommunikationsdienst beschäftigt. Das VG Köln als Vorinstanz hatte entschieden, dass Google Mail gem. § 6 TKG bei der Bundesnetzagentur meldepflichtig sei.[86]

Mit Entscheidung vom 26. 2. 2018 hat das OVG Münster das Berufungsverfahren ausgesetzt und die Sache dem EuGH zur Vorabentscheidung vorgelegt.[87] Der EuGH muss nun klären, ob Webmail-Dienste unter die Definition des Telekommunikationsdienstes im Sinne der RL 2002/21/EG fallen können.[88]

85 *Wieduwilt*, FAZ v. 30. 11. 2017.
86 VG Köln, 11. 11. 2015 – 21 K 450/15, K&R 2016, 141 ff. = MMR 2016, 141.
87 OVG Münster, 26. 2. 2018 – 13 A 17/16, Pressemitteilung vom 26. 2. 2018.
88 *Grünwald/Nüßing*, MMR 2016, 91 zur grundsätzlichen Fragestellung.

RA Dr. Florian Deusch, Ravensburg, und Prof. Dr. Tobias Eggendorfer, Weingarten*

Penetrationstest bei Auftragsverarbeitung

Stand der Technik und damit Pflicht bei Web-Anwendungen

Nach der DSGVO und dem – noch geltenden – Bundesdatenschutzgesetz 2003[1] (BDSG 2003) muss der Auftraggeber einer Auftragsverarbeitung seinen Auftragnehmer sorgfältig bezüglich der technischen und organisatorischen Datenschutz- und IT-Sicherheitsmaßnahmen auswählen. Er muss die Umsetzung der Maßnahmen prüfen oder sich geeignet nachweisen lassen. Die aktuelle Praxis beschränkt sich dabei im Wesentlichen auf die Prüfung der Netzwerksicherheit sowie der organisatorischen Maßnahmen. Die Anlage 1 zu § 9 BDSG 2003 ist dabei – soweit ersichtlich – das typische Prüfraster. Doch erscheint dies unzureichend: Ein weitaus größerer Teil der Datenverluste geschieht aktuell über fehlerhafte Anwendungssoftware, insbesondere bei Web-Anwendungen. Der Beitrag diskutiert deshalb, ob ein Penetrationstest zu der obligatorischen Prüfung gehört, weil er gezielt nach Sicherheitslücken sucht, die zu einer Datenexfiltration führen könnten.

I. Einleitung

Wer IT-Dienste auslagert (E-Mail-Verwaltung, Nutzung von „Cloud"-Diensten oder andere Web-Anwendungen), lässt Daten durch einen Dritten weisungsgebunden verarbeiten. Bei personenbezogenen Daten gelten die Regelungen der Auftragsverarbeitung. Den Auftraggeber treffen nach BDSG 2003 und DSGVO umfangreiche Prüfpflichten, die die Datensicherheit beim Auftragnehmer gewährleisten sollen, insbesondere zu den „technischen und organisatorischen Maßnahmen" (TOM). Sofern der Auftraggeber in der Praxis überhaupt Prüfungen vornimmt, legt er in der Regel die 8 TOMs der Anlage zu § 9 BDSG 2003 zugrunde.[2] Ab dem 25. 5. 2018 gelten mit der DSGVO zwar neue Regeln für die Auftragsverarbeitung, eine inhaltliche Erweiterung der Prüfpflichten wird der DSGVO jedenfalls bislang nicht zugeschrieben.[3]

Bei der „TOM-Prüfung" hat sich in der Praxis eine Reduzierung auf die Sicherheit des Rechenzentrums und der Netzwerkinfrastruktur durchgesetzt, ohne die Sicherheit der Web-Anwendung des Auftragnehmers zu berücksichtigen.[4] Doch reicht das aus?

Datenexfiltration erfolgt heute weniger durch Angriffe auf Netze, sondern hauptsächlich durch Angriffe wie Code-Injections auf die Anwendung selbst, und über Angriffe auf Nebenwegen wie Social Engineering.[5] Kaum ein Datenschutzbeauftragter fordert jedoch im Rahmen einer TOM-Prüfung die Ergebnisse eines halbwegs aktuellen Penetrationstests[6] der Anwendung oder führt ihn gar selbst durch.

* Mehr über die Autoren erfahren Sie auf S. XII. Der Autor *Deusch* ist als Rechtsanwalt, FA für Informationstechnologierecht und externer zertifizierter Datenschutzbeauftragter in der Anwaltskanzlei Dr. Gretter tätig; der Autor *Eggendorfer* ist Professor für IT-Sicherheit an der Hochschule Weingarten, freiberuflicher IT-Berater und ebenso zertifizierter externer Datenschutzbeauftragter. Alle angegebenen Links wurden zuletzt abgerufen am: 9. 3. 2018, soweit nicht anders vermerkt.

1 DSGVO: Datenschutz-Grundverordnung = VO (EU) des Europäischen Parlaments und des Rates vom 27. 4. 2016, ABl. Nr. L 119, S. 1 ff.; Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. 1. 2003 (BGBl. I S. 66), das zuletzt durch Art. 10 Abs. 2 des Gesetzes vom 31. 10. 2017 (BGBl. I S. 3618) geändert worden ist.

2 Infoblatt „Auftragsdatenverarbeitung" des bayerischen Landesamts für Datenschutzaufsicht, Stand März 2016, online unter https://www.lda.bayern.de/media/info_adv.pdf., 23. 11. 2017; *Gola/Schomerus*, BDSG, Kommentar, 12. Aufl. 2015, § 11 Rn. 20; *Schneider*, Handbuch des EDV-Rechts, 5. Aufl. 2017, Kap. A Rn. 232.

3 *Härting*, ITRB 2016, 137; *Schneider* (Fn. 2), Kap. A Rn. 628 ff.; *Lissner*, in: Taeger (Hrsg.), Smart World – Smart Law, weltweite Netze mit regionaler Regulierung, 2016, S. 401, 408; *von Holleben/Knaut*, CR 2017, 299, 302.

4 Die Vermeidung und gegebenenfalls Behebung von Sicherheitslücken ist jedenfalls kein Prüfungspunkt in der ansonsten vorbildlichen und ausführlichen Prüfliste von *Müller*, in: Koreng/Lachenmann, Formularhandbuch Datenschutzrecht, 2015, S. 513 ff. ebenso die Folgeauflage, siehe *Müller*, in: Koreng/Lachenmann, Formularhandbuch Datenschutzrecht, 2. Aufl. 2018, S. 459 ff., 627 ff. sowie *Witt*, S. 675 ff.

5 Vgl. den Bericht „Die Lage der IT-Sicherheit in Deutschland 2016" des Bundesamts für Sicherheit in der Informationstechnik, unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2016.pdf?__blob=publicationFile&v=5; zu IT-Sicherheitslücken in Anwendungsprogrammen siehe auch *Deusch/Eggendorfer*, K&R 2016, 152, 153. Oftmals sind sogar die eher oberflächlichen TOMs so allgemein, dass sie auf die konkrete Datenverarbeitung nicht anwendbar sind, doch das kann vorliegend außen vor bleiben.

6 In der IT-Sicherheit spricht man oft kurz von einem „Pen-Test". Der Begriff wird im Folgenden verwendet.

Damit ergibt sich die Frage: Kann bzw. muss der Auftraggeber einer Auftragsverarbeitung vom Auftragnehmer verlangen, einen solchen Test nachzuweisen oder diesen beim Auftragnehmer sogar selbst durchführen?

Zur Untersuchung dieser Frage vergleicht Abschnitt II die Rechtslage zur Auftragsverarbeitung nach dem BDSG 2003 und der DSGVO. Nach einer technischen Betrachtung zur IT-Sicherheit bei Webanwendungen (Abschnitt III) stellt Abschnitt IV dar, ob und, falls ja, in welchem Umfang Pentests zum „Pflichtprogramm" einer „TOM-Prüfung" nach der DSGVO gehören.

II. Auftragsdatenverarbeitung nach dem BDSG 2003 und nach der DSGVO

Der Vergleich der Regelungen zur Auftragsdatenverarbeitung gemäß § 11 BDSG 2003 mit Art. 28 und 29 DSGVO liefert erste Erkenntnisse für eine Verpflichtung zu einem Pentest.

1. Auftragsdatenverarbeitung gem. § 11 BDSG 2003

§ 11 Abs. 1 BDSG 2003 weist dem Auftraggeber die Verantwortung für den Datenschutz zu. Der „Clou" daran ist: Der Auftraggeber kann dem Auftragnehmer personenbezogene Daten zur Verarbeitung überlassen, ohne dass hierfür gemäß § 4 Abs. 1 BDSG 2003 die Einwilligung der Betroffenen oder eine sonstige Rechtsgrundlage erforderlich wäre.[7]

Tatbestandsvoraussetzung für eine Auftragsdatenverarbeitung ist das Weisungsrecht des Auftraggebers, andernfalls liegt eine eigenverantwortliche Datenverarbeitung des Auftragnehmers vor (sogenannte „Funktionsübertragung").[8]

Gemäß § 11 Abs. 2 S. 1 BDSG 2003 ist der Auftragnehmer sorgfältig und unter „besonderer Berücksichtigung der von ihm getroffenen technischen und organisatorischen Maßnahmen" auszuwählen.[9]

Die Sicherstellung angemessener TOMs durch den Auftragnehmer ist ein Kernpunkt des § 11 BDSG 2003. Nach den Vorstellungen des Gesetzgebers legt der Auftraggeber selbst die TOMs fest, delegiert sie an den Auftragnehmer und überprüft sie sodann.[10]

Der Auftraggeber hat sich von der Einhaltung der beim Auftragnehmer getroffenen TOMs zu überzeugen, und zwar *vor* Beginn der Datenverarbeitung und sodann regelmäßig danach (§ 11 Abs. 2 S. 4 BDSG 2003). Er muss diese Kontrolle dokumentieren (§ 11 Abs. 2 S. 5 BDSG 2003). Für den Ablauf der TOM-Prüfung gemäß § 11 Abs. 2 S. 4 BDSG 2003 gibt es wenig Vorgaben: Eine Vor-Ort-Kontrolle beim Auftragnehmer wird nicht als zwingend angesehen. Stattdessen sind Beurteilungen von sachverständigen Dritten, die Vorlage von Zertifikaten oder Prüfungsergebnissen und sogar Selbstauskünfte der Auftragnehmer als ausreichend anerkannt.[11] In Bezug auf den Prüfungsinhalt behandeln die für die Praxis vorgeschlagenen Prüflisten bislang nicht die Sicherheit von Software- bzw. Webanwendungen.[12]

2. Auftragsverarbeitung nach der DSGVO

a) Begriff der Auftragsverarbeitung

Im Gegensatz zum BDSG 2003 verwendet die DSGVO nicht den Begriff „Auftragsdatenverarbeitung", sondern „Auftragsverarbeitung" (Art. 4 Nr. 8, 28 DSGVO). Ob eine Datenverarbeitung „nach Weisung" des Auftraggebers ein zwingendes Tatbestandsmerkmal der Auftragsverarbeitung ist oder eine Verpflichtung der Parteien, Weisungsbefugnisse zu vereinbaren, ist unter der DSGVO strittig.[13]

b) Gesetzliche Pflichten des Auftragsverarbeiters, Beauftragung und Sanktionen

Im Gegensatz zum BDSG 2003 statuiert die DSGVO *originäre Gesetzespflichten des Auftragnehmers*, zum Beispiel zur Sicherheit der Verarbeitung (Art. 32 DSGVO) oder zur Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 Abs. 2 DSGVO).[14]

Abweichend von § 11 Abs. 2 S. 4 BDSG 2003 fehlt in der DSGVO eine ausdrückliche Regelung, wonach sich der Auftraggeber vor Beginn der Datenverarbeitung und regelmäßig danach von den TOMs des Auftragnehmers zu überzeugen und dies zu dokumentieren hat.

Allerdings darf ein Auftragsverarbeiter nur beauftragt werden, wenn er ausreichende Garantien und Nachweise zur Durchführung der TOMs bietet (Art. 28 Abs. 1 DSGVO). Deshalb sind die bisherigen TOM-Prüfungen *vor* der Auftragsvergabe gemäß § 11 Abs. 2 S. 4 BDSG 2003 auch nach Maßgabe der DSGVO nötig. Es empfiehlt sich für den Auftraggeber aufgrund Art. 5 Abs. 2 DSGVO, die TOMs beim Auftragnehmer zu prüfen und dies zu dokumentieren.[15] Die aus § 9 BDSG 2003 bzw. der Anlage dazu bekannten „TOMs" sind nunmehr in Art. 32 DSGVO geregelt.[16]

Anders als nach dem BDSG 2003 haftet der Auftragsverarbeiter nicht nur aufgrund des Auftrags gemäß Art. 28 Abs. 4 S. 2 DSGVO gegenüber seinem Auftraggeber, sondern auch unmittelbar gegenüber der betroffenen Person gemäß Art. 82 DSGVO.[17] Drastisch erhöht hat die DSGVO den Bußgeldrahmen für die Datenschutzbehörden, und zwar gemäß Art. 83 DSGVO bis zu € 20,0 Mio. oder 4 % des Jahresumsatzes, je nachdem, welcher der Beträge höher ist. Das Bußgeld droht dem Verantwortlichen/Auftraggeber bei einem Datenschutzverstoß „seines" Auftragsverarbeiters, aber auch unmittelbar dem Auftragsverarbeiter.[18]

---

7 Zur Verantwortung und „Privilegierung" der Auftragsdatenverarbeitung, siehe *Schneider* (Fn. 2), Kap. A Rn. 226, 444, 477; *Plath*, Kommentar BDSG/DSGVO, 2. Aufl. 2016, § 11 BDSG Rn. 1, 2, 7; *Gola/Schomerus* (Fn. 2), § 11 Rn. 3 f.

8 Zur Abgrenzung siehe *Plath* (Fn. 7), § 11 BDSG Rn. 27; die DSGVO sieht diese Unterscheidung nicht mehr vor, auch bei einer „Funktionsübertragung" kann eine Auftragsverarbeitung vorliegen, siehe *Schneider* (Fn. 2), Kap. A Rn. 630.

9 *Schneider* (Fn. 2), Kap. A Rn. 473.

10 *Auer-Reinsdorff/Conrad*, Handbuch IT- und Datenschutzrecht, 2. Aufl. 2016, § 33 Rn. 205; ähnlich *Gola/Schomerus* (Fn. 2), § 11 Rn. 20: Der Auftragnehmer muss die Vorkehrungen treffen, die auch der Auftraggeber treffen würde.

11 *Gola/Schomerus* (Fn. 2), § 11 Rn. 21; *Plath* (Fn. 7), § 11 BDSG Rn. 92; *Bergt*, in: Taeger (Hrsg.), Law as a Service (LaaS) – Recht im Internet- und Cloud-Zeitalter, 2013, S. 37, 46, 47, zur Auffassung der Aufsichtsbehörden siehe exemplarisch das bayerische Landesamt für Datenschutzaufsicht: https://www.lda.bayern.de/media/info_adv.pdf.

12 Die Vermeidung und gegebenenfalls Behebung von Sicherheitslücken ist jedenfalls kein Prüfungspunkt in der ansonsten vorbildlichen und ausführlichen Prüfliste von *Müller*, in: Koreng/Lachenmann (Fn. 4), S. 513 ff. auch nicht in der Folgeauflage, siehe *Müller*, in: Koreng/Lachenmann (Fn. 4), S. 459 ff.

13 *Härting*, Datenschutzgrundverordnung, 2016, Rn. 579; *Schneider* (Fn. 2), Kap. A Rn. 628 - 630; *Gola*, DSGVO, 2017, Art. 4 Rn. 57; von *Holleben/Knaut*, CR 2017, 299, 300.

14 *Schneider* (Fn. 2), Kap. A Rn. 633; *Bierekoven*, ITRB 2017, 282, 283.

15 Auch *Lissner*, in: Taeger (Hrsg.) (Fn. 3), S. 401, 408; *Härting*, ITRB 2016, 137, *Gola* (Fn. 13), Art. 28 Rn. 6; *Witt*, in: Koreng/Lachenmann (Fn. 4), S. 675 ff.

16 *Plath* (Fn. 7), Art. 32 DSGVO Rn. 1.

17 *Gola* (Fn. 13), Art. 82 Rn. 3.

18 *Gola* (Fn. 13), Art. 83 Rn. 12.

III. Webanwendung und Sicherheit

1. Herkömmlich: Schutz der Infrastruktur

Vielfach wird Auftragsverarbeitung mit Hilfe von Webanwendungen durchgeführt, vom Bewerbermanagementsystem bis hin zur Veranstaltungsplanung gibt es zahlreiche Dienste. Dabei sind die Systeme üblicherweise in Rechenzentren von Drittanbietern gehostet. Von technisch angemessen umgesetzten Sicherheitsmaßnahmen des Rechenzentrums kann dabei meist ausgegangen werden, so dass zumindest der physische Zugriff auf die Hardware abgesichert ist.

Kritisch in solchen Hostingfällen können allerdings Remote-Management-Konsolen sein, die einen Zugriff auf Bildschirm und Monitor des Rechners über das Internet ermöglichen.[19]

Auch sind die relativ einfachen, quasi-mechanischen Maßnahmen, wie Firewalls, in der Regel vorhanden und mittlerweile meist sachgerecht implementiert. Seltener sind indes Intrusion Detection Systeme der verschiedenen Ausprägungen vorhanden, doch arbeiten diese kaum präventiv, sondern ermöglichen es im Wesentlichen nur, im Falle eines Angriffes, diesen früher zu erkennen und zu ermitteln, welche Daten der Angreifer wie exfiltriert hat.

2. Gefahren für die IT-Sicherheit von Webanwendungen und Gegenmaßnahmen

Verschiedene Indikatoren verdeutlichen, dass nicht die IT-Infrastruktur (Hardware und Netzwerke), sondern die Webanwendungen angegriffen werden. Obgleich Gegenmaßnahmen bekannt und verfügbar sind, werden diese noch immer nicht konsequent durchgeführt.

a) CVE-Einträge

Mit CVE-Einträgen („Common Vulnerabilities and Exposures“) dokumentiert die IT-Sicherheit üblicher Weise Sicherheitsprobleme, deren Zahl ist ein Gradmesser für die Gefahrenlage.[20]

Die meisten CVE-gelisteten Angriffe zielen nicht (mehr) auf die IT-Infrastruktur ab, sondern auf die Webanwendung. Zum Beispiel gibt es allein für das Blog-System Wordpress im Jahr 2017 170 CVE-Einträge, das heißt im Schnitt jeden zweiten Tag eine relevante Sicherheitslücke. 804 Einträge beschreiben nur sogenannte Cross-Site-Scripting-Angriffe, eine typische Sicherheitslücke in Webanwendungen. Dies sind mehr als zwei Meldungen pro Tag.

Die CVE-Einträge sind dabei nur die Spitze des Eisbergs, denn die gibt es nur, sobald der sicherheitsrelevante Programmierfehler dort gemeldet ist und eine gewisse Relevanz erreicht. Bei vielen proprietären Anwendungen werden Sicherheitsprobleme auf dem kleinen Dienstweg behoben und nicht öffentlich dokumentiert.[21]

b) OWASP

Einen anderen Anhalt für gängige Sicherheitslücken liefern die jährlichen OWASP Top 10, eine Auflistung der Top 10 der *„Most Critical Web Application Security Risks“*. Seit 2013 finden sich dort beständig, teils mit wechselnden Rängen, insbesondere folgende Angriffe:[22]

- Von Bash- über LDAP- bis hin zur SQL-Injection: Bei einer „Injection“ schleusen Angreifer einen Code so in die Anwendung ein, dass diese den eingefügten Code wie ihre eigenen Instruktionen ausführt. Das Programm erhält also durch den Angriff neue Funktionen, zum Beispiel um einen Rechner fernzusteuern (Shell-Injection, PHP-Injection etc.). Etwas spezifischer können Angreifer auch Datenbanken über „SQL-Injections“ auslesen.[23] Lightweight Directory Access Protocol (LDAP) ist ein Netzwerkprotokoll zur Abfrage und Änderung von Informationen verteilter Verzeichnisdienste.[24]
- Authentifizierungsprobleme und Session-Management-Angriffe: Hier versucht der Angreifer, durch vorgetäuschte Identifikationen auf die Kommunikation zwischen den beteiligten Computern zuzugreifen.[25]
- Cross-Site-Scripting (XXS): Als hervorgehobener Sonderfall von Injection-Angriffen: Beim Cross-Site-Scripting schleusen die Angreifer JavaScript-Schadcode in den Webbrowser des Anwenders.[26]
- Fehlkonfiguration von Sicherheitseinstellungen: Fehlerhafte Konfigurationen von Sicherheitseinstellungen begünstigen die Angriffe oder lassen schützenswerte Daten ohne besonderes Know-how von außen lesbar werden.
- Ausgabe von vertraulichen Daten, wie Kreditkartennummern: Angreifer fangen vertrauliche Daten ab, die die Nutzer bedenkenlos über unverschlüsselte und nicht zertifizierte Kommunikationskanäle freigeben.
- Kontrolle bei Zugriff auf bestimmte Funktionen.
- Cross Site Request Forgery: Der Angreifer veranlasst den Nutzer einer Webanwendung, eine manipulierte URL aufzurufen.[27]
- Nutzung bekannt unsicherer Komponenten von Drittanbietern: Aus Effizienzgründen nutzen Entwickler oft fertige Bibliotheken und Frameworks für bestimmte Funktionen. Sind diese nicht aktuell, können Lücken darin Angriffe leicht ermöglichen.
- Ungeprüfte Weiterleitung oder Umleitung auf Webseiten.

Alle diese Lücken sind geeignet, um Zugriff auf datenschutzrelevante Nutzerdaten zu erlangen. Datenschutzrechtliche Relevanz erlangen sie, wenn Webanwendungen Teil der Auftragsverarbeitung sind.

c) Sicherheitsmaßnahmen

Gegenmaßnahmen gegen solche Sicherheitslücken knüpfen an zwei Aspekten an:

19 *Eggendorfer*, Fernsteuerung mit Bild. Server vollständig remote steuern mit Raritan Eric Express. Linux Magazin, S. 76 ff., 10/2006.

20 http://cve.mitre.org/about/.

21 CVE-Einträge: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Wordpress%202017; Web: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=2017+XSS. Allein im Jahr 2017 sind 8 000 Sicherheitsfehler außerhalb der CVE-Einträge dokumentiert, https://www.bleepingcomputer.com/news/security/nearly-8-000-security-flaws-did-not-receive-a-cve-id-in-2017/.

22 OWASP: Open Web Application Security Project; siehe https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project; zu den OWASP Top Ten: https://www.owasp.org/index.php/Top_Ten.

23 Ein prominentes Beispiel war der Sony-Playstation-Network-Hack.

24 https://blog.javan.de/it-sicherheit-code-injection-grundsaetzliches-prinzip-und-beispiele-fuer-sql-und-html/; https://de.wikipedia.org/wiki/Bash_(Shell); https://de.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol.

25 https://www.securify.nl/advisory/SFY20170404/authentication_bypass_vulnerability_in_western_digital_my_cloud_allows_escalation_to_admin_privileges.html.

26 https://www.heise.de/security/artikel/Cross-Site-Scripting-Datenklau-ueber-Bande-270244.html; https://www.vulnerability-lab.com/get_content.php?id=1737, https://www.osisecurity.com.au/smartjobboard-cross-site-scripting-personal-information-disclosure-and-phpmailer-package.html sowie https://www.osisecurity.com.au/acoracms-browser-redirect-and-cross-site-scripting-vulnerabilities.html.

27 https://www.acunetix.com/websitesecurity/csrf-attacks/.

Einerseits muss von Anfang an durch Qualitätsmanagement in der Softwareentwicklung, defensives Programmieren, automatisierte Tests und gezielte Penetrationtests begleitend zur Entwicklung ein hohes Sicherheitsniveau erreicht werden, alternativ können sogenannte „Web Application Firewalls", also Proxy-Lösungen, kritische Zugriffe filtern. Allerdings helfen diese allenfalls symptomatisch gegen Injection-Angriffe, und auch das nur mit Einschränkungen, wie z. B. die XSS-Cheat-Sheets zeigen.[28] Gegen grundlegende Probleme, wie z. B. falsch konfigurierte Sicherheitseinstellungen, mangelhafte Zugriffskontrollmechanismen, vorhersagbare Session-IDs und sonstige Logikfehler helfen solche Schutz-Proxies naturgemäß nicht.[29]

d) Web-Pentest

Genau diese Fehler kann ein sorgfältig durchgeführter Pentest aufdecken, indem gezielte Angriffsversuche Sicherheitslücken in der Anwendung zu Tage fördern. Dabei werden systematisch mögliche Sicherheitslücken getestet. Unterstützend kann „Fuzzing" eingesetzt werden, dabei werden „zufällig" Daten über Eingabeschnittstellen eingespielt, um so möglicherweise Fehler auszulösen.

Solche Pentests lassen sich mit geringem Aufwand mit teilweise automatisierten Tools durchführen, zum Beispiel mit Werkzeugen wie OWASP/OWTF oder dem Metasploit-Framework. Allerdings empfehlen sich automatisierte Tests nur, um einen ersten Eindruck zu gewinnen, bevor manuell nachgearbeitet wird.[30]

Für einen Pentest ist zu definieren, welches Prüfobjekt untersucht wird (zum Beispiel die Web-Anwendung oder die IT-Infrastruktur eines Rechenzentrums) und welche Prüftiefe der Test haben soll.

In technischer Hinsicht lassen sich Pentests nach dem Wissen des Angreifers über das System unterscheiden: Hat er nur das Wissen von einem externen Dritten, spricht man von einem „Black-Box-Test", liegen dem Tester Programmcode und alle Unterlagen vor, handelt es sich um einen „White-Box-Test". Während letzterer wahrscheinlicher mehr Lücken aufzeigt, wird zugunsten von ersterem häufig vorgebracht, dass er dem entspräche, was real passieren könne.

Viele Anbieter solcher Tests bieten in der Praxis auch verschiedene Intensitäten an: Von einem einfachen, vollautomatischen Test, den jedes Script-Kiddie[31] sich mit fertigen Tools zusammenklicken kann, bis hin zu gründlichen, manuellen Tests.

Einige Anbieter, wie z. B. Google und Facebook, bieten zusätzlich „Bug-Bounties" an: Belohnungen für Sicherheitsforscher, die eine Lücke außerhalb eines beauftragten Pentests finden.

e) Pentest bei Software as a Service

Web-Anwendungen sind heutzutage der typische Anwendungsfall der Cloud-Dienst-Variante „Software as a Service". Hierbei nutzt der Anwender neben der IT-Infrastruktur und der Plattform des Anbieters auch dessen Anwendungssoftware. Sobald hier personenbezogene Daten verarbeitet werden, handelt es sich um eine Auftragsverarbeitung, so dass hier eine Sicherheitsprüfung durchzuführen ist.[32]

Da die Anwendung beim SaaS dem Nutzer in der Regel über eine Web-Applikation bereitgestellt wird, sind die vorgenannten Risiken beim SaaS vorhanden. Pentests können die Risiken herabsetzen, indem sie Sicherheitslücken offenbaren und so gezielte Gegenmaßnahmen ermöglichen.

IV. Pentest bei Web-Anwendungen und Datenschutz

Aus den Abschnitten II und III ergibt sich folgender Befund:

- Es existieren internet-spezifische Risiken für web-basierte Verarbeitungen. Hiergegen sind konkrete IT-Sicherheitsmaßnahmen erforderlich und verfügbar, insbesondere ein Pentest zur Ermittlung (und anschließenden Schließung) von Sicherheitslücken.
- Dennoch haben weder die internet-spezifischen Risiken noch die vorhandenen Gegenmaßnahmen Eingang gefunden in die vielfach standardisierten TOM-Prüfungen bei Auftragsverarbeitungen.

Damit ergeben sich für die Auftragsverarbeitung die Fragen,

- ob und für wen ein Pentest für web-basierte Vorgänge verpflichtend ist (siehe unten Ziff. 1) und,
- falls ja, ob und wie der Verantwortliche einen Pentest gegen den Auftragsverarbeiter durchsetzen kann (Ziff. 2).

1. Verpflichtung zum Pentest bei der Auftragsverarbeitung

Für eine Verpflichtung zum Pentest sind einerseits der Art. 32 DSGVO und andererseits die Art. 28 Abs. 10, 25 DSGVO relevant.

a) Pentest als „Stand der Technik" gemäß Art. 32 DSGVO?

Gemäß Art. 32 Abs. 1, 1. Hs. DSGVO treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten unter Berücksichtigung des *Stands der Technik*, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen.

Der (unbestimmte Rechts-) Begriff „Stand der Technik" wird im deutschen Recht wie folgt abgegrenzt:

28 Zu den Sicherheitslücken im Rahmen der Softwareprogrammierung, deren rechtliche Konsequenzen und Gegenmaßnahmen: https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet; zu den weiteren Alternativen: *Deusch/Eggendorfer*, K&R 2015, 152, 513.

29 *Eggendorfer*, Seltener Zufall. Gute Vorhersagbarkeit bedeutet schlechte Sicherheit. Linux Magazin, 01 2012; *Eggendorfer*, Schöne Bescherung. Wie DHL Kundendaten preisgibt. Linux Magazin, S. 778 ff., 12 2008; *Bauer/Magnus*: Angriff auf Pakete. Weitere Paketdienste mit Datenlecks. Linux Magazin, 01 2010.

30 https://www.owasp.org/index.php/OWASP_OWTF, https://www.metasploit.com/, https://www.rapid7.com/products/nexpose/download/.

31 Script-Kiddies sind (häufig) Anfänger im Bereich der IT-Sicherheit, die ohne die Funktionsweise zu verstehen fertige Tools einsetzen, die automatisch Sicherheitslücken entdecken und ausnutzen. Lücken, die solche Tools finden, sind daher besonders kritisch.

32 Vgl. die Orientierungshilfe Cloud Computing der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und des Düsseldorfer Kreises, S. 7, 36 unter https://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf.

aa) Allgemein anerkannte Regeln der Technik

Dies sind alle technischen Regeln, die

- sich in der Wissenschaft als (theoretisch) richtig durchgesetzt haben *und*
- in der Praxis erprobt und bewährt und damit „allgemein anerkannt" sind.

Die Rechtsprechung vermutet dies bei allen kodifizierten technischen Normen (DIN, VDI, VDE usw.).[33]

bb) Stand der Technik

Maßgeblich sind die neuesten technischen Erkenntnisse, unabhängig von einer „allgemeinen" Anerkennung durch Wissenschaft oder Praxis. Gleichwohl ist eine gewisse Bewährung in der Praxis nötig.[34]

cc) Stand von Wissenschaft und Technik

Relevant sind die neusten technischen und wissenschaftlichen Erkenntnisse, unabhängig davon, ob eine bestimmte Lösung in der Praxis bereits umgesetzt wurde oder nicht.[35]

dd) Autonome Auslegung von „Stand der Technik" in Art. 32 DSGVO

Der „Stand der Technik" i. S. d. Art. 32 DSGVO ist jedoch nicht unmittelbar durch einen Rückgriff auf das deutsche Recht zu ermitteln. Denn Rechtsbegriffe aus EU-Normen sind autonom (anhand des EU-Rechts) auszulegen, wobei jedoch mitgliedstaatliche Vorstellungen auch gewisse Relevanz entwickeln können.[36]

Zur Definition des Stands der Technik nach der DSGVO gibt es bislang verschiedene Ansätze:

- Auf den Zweck des Rechtsbegriffs abstellend, hält *Knopp* den Stand der Technik für eingehalten, wenn durch die konkrete Maßnahme die Schutzziele der DSGVO erreicht würden. Darüber hinaus sei der Verweis auf den Stand der Technik lediglich als Aufforderung zu verstehen, die Eignung der Maßnahmen regelmäßig zu überprüfen.[37]

  Diese Definition wird dem Gesetzeswortlaut aber nicht gerecht. Der Stand der Technik soll der *Maßstab* sein, ob eine Maßnahme zur Erreichung der gesetzlichen Ziele geeignet ist. Wenn man in den Schutzzielen den Maßstab sieht, blendet man den Stand der Technik aus.
- Andere Autoren stellen auf die Verfügbarkeit technologischer Werkzeuge ab und beziehen die Gegebenheiten des Marktes ein.[38] Das Abstellen auf Marktgegebenheiten kann jedoch problematisch sein, da insoweit der wirtschaftliche Erfolg einer bestimmten IT-Sicherheitslösung über ihre technische Eignung entscheiden würde.
- Wieder andere Stimmen sehen im Stand der Technik einen Verweis auf außerjuristische Normen wie etwa die ISO 27001-Normenreihe.[39] Dies würde dem deutschen Begriff „anerkannte Regeln der Technik" entsprechen (siehe oben lit. aa) und Rechtssicherheit vermitteln, aber fortschrittliche Techniken vernachlässigen, die noch keinen Eingang in technische Regelwerke gefunden haben. Für Pentests gibt es, soweit ersichtlich, bislang keinen technischen Standard in der Qualität der ISO,[40] allenfalls aus den Anforderungen des Qualitätsmanagements und der Produktsicherheit lassen sich auf der Ebene der ISO-Normen vergleichbare Regeln finden, die als Quelle herhalten könnten.
- *Eigene Betrachtungen:* Der „Stand der Technik" ist im EU-Recht nicht neu. Bereits Art. 17 der Datenschutzrichtlinie (RL 95/46/EG) stellt auf diesen Begriff ab, ebenso die Art. 14 und 16 der NIS-Richtlinie (RL 2016/1148/EU). Soweit die NIS-Richtlinie durch § 8 a BSIG und § 13 Abs. 7 TMG umgesetzt wird, ist es auch hier geboten, den dort geregelten „Stand der Technik" unter Beachtung des EU-Rechts (richtlinienkonform) auszulegen. Der Stand der Technik wird dabei wie unter lit. aa bis cc abgegrenzt zum allgemeinen Stand der Technik und dem Stand von Wissenschaft und Technik. Maßgeblich ist hiernach der Entwicklungsstand fortschrittlicher Verfahren, der nach herrschender Auffassung führender Fachleute das Erreichen des gesetzlichen Zieles als gesichert erscheinen lässt, was gleichgesetzt wird mit dem europäischen Rechtsbegriff der „besten verfügbaren Techniken".[41]

  Anknüpfend an den englischen Begriff „state of the art" aus der NIS-Richtlinie hat die Europäische Agentur für Netz- und Informationssicherheit (enisa) durch die „Working Group 3" der NIS-Plattform Techniken und Verfahren zusammengetragen zu „state-of-the-art of Secure ITC Landscape". Hierbei ging es um das Aufzeigen der derzeit eingesetzten und vorhandenen Technologien zur IT-Sicherheit und zum Datenschutz (*map current and existing technologies in the field of cybersecurity and privacy*).[42]

Auf dieser Grundlage ergeben sich zwei Merkmale für den Stand der Technik:

- Das Vorhandensein einer bestimmten Technologie und
- eine gewisse Bewährung in der Praxis, wenngleich eine allgemeine Anerkennung nicht erforderlich ist.

Dies entspricht im Wesentlichen dem Stand der Technik nach Maßgabe des deutschen Rechts (siehe oben lit. bb).

Bestätigt wird dieser Befund durch die Rechtsprechung des EuGH, der (allerdings im Kontext der Produkthaftung) den „Stand von Wissenschaft und Technik" als den „höchsten Stand" einstuft.[43] Dies legt nahe, dass auch der EuGH von einer Abgrenzung verschiedener Standards ausgeht, die mit dem deutschen Recht (siehe oben lit. aa bis cc) vergleichbar ist.

ee) Konsequenzen für das Pentesting als Sicherheitsmaßnahme

Aufgrund des vorstehenden Befunds verlangt der Stand der Technik einen Pentest, wenn

- hierfür eine bestimmte Technologie existiert und
- diese in der Praxis angewendet wird bzw. nachweislich positive Effekte für die IT-Sicherheit hat.

33 Z. B. OLG Brandenburg, 18. 6. 2009 – 12 U 164/08, NJW-RR 2009, 1468.
34 BVerfG, 8. 8. 1978 – 2 BvL 8/77, NJW 1979, 359, 362.
35 *Seibel*, NJW 2013, 3000 ff.
36 EuGH, 27. 4. 1999 – C-99/96, Slg. 1999-I, S. 2277, 2310; *Frenz*, Handbuch Europarecht, Band 5, 2010, § 2 Rn. 356; *Gola* (Fn. 13) Art. 32 Rn. 15.
37 *Knopp*, DuD 2016, 663, 666.
38 *Gola* (Fn. 13), Art. 32 Rn. 16 - 19; *Plath* (Fn. 7), Art. 25 DSGVO Rn. 5.
39 *Schantz/Wolff*, Das neue Datenschutzrecht, 2017, Rn. 852.
40 Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet zwar Pentests für Behörden an sowie Zertifizierungen für externe Pentest-Unternehmen, hat aber keinen inhaltlichen Standard für Pentests definiert, siehe https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Dienstleistungen/ISPentest_ISWebcheck/ispentest_iswebcheck.html.
41 *Gehrmann/Klett*, K&R 2017, 372, 375, abstellend auf das Handbuch der Rechtsförmlichkeit des Bundesjustizministeriums.
42 https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/state-of-the-art-of-the-secure-ict-landscape/view, dort S. 9.
43 EuGH, 29. 5. 1997 – C-300/95, dort Rn. 26.

Die Ausführungen unter Abschnitt III haben gezeigt, dass es Bedrohungen für die IT-Sicherheit einer Web-Anwendung gibt, denen mit Pentests begegnet werden kann (vorausgesetzt, die Ergebnisse eines Pentests werden auch umgesetzt, insbesondere ermittelte Sicherheitslücken beseitigt).

Dass Pentests in der Praxis zur Erhöhung der IT-Sicherheit von Web-Anwendungen durchgeführt werden, ergibt sich zum Beispiel aus den Publikationen des Bundesamts für Sicherheit in der Informationstechnik (BSI). Das BSI bietet Pentests für Behörden an und empfiehlt in seinem „Anforderungskatalog Cloud Computing" (C 5) mindestens einen Pentest pro Jahr.[44] Für dieses Erfordernis referenziert das BSI auf verschiedene technische Normen wie etwa A 13.1.1 ISO 27001:2013 und M 5.150 BSI-Grundschutz.[45]

Auffallend ist dabei, dass das BSI den Pentest ausdrücklich „*unabhängig vom Anwendungskontext*" für alle Cloud-Lösungen verlangt.[46] Dementsprechend verlangt das BSI bei jeder cloud-bezogenen Web-Anwendung einen jährlichen Pentest aufgrund des „Stands der Technik". Damit überwiegt in Bezug auf den Pentest der Stand der Technik stets die übrigen Kriterien in Art. 32 Abs. 1 DSGVO, nämlich die Kosten, Eintrittswahrscheinlichkeit und Schwere des Risikos und die Art der Verarbeitung. Insofern deckt sich die Auffassung des BSI mit dem Befund in Abschnitt III oben.

Somit steht fest: Für Web-Anwendungen, in denen personenbezogene Daten verarbeitet werden, ist ein regelmäßiger Pentest gemäß Art. 32 Abs. 1 DSGVO verpflichtend.

b) Adressaten der Pentest-Pflicht gemäß Art. 32 DSGVO

Art. 17 der Datenschutzrichtlinie (RL 95/46/EG) hat lediglich den Verantwortlichen (nicht den Auftragsverarbeiter) zu TOMs verpflichtet (abweichend von § 9 BDSG 2003, wonach auch der Auftragsverarbeiter verpflichtet ist).

Gemäß Art. 32 Abs. 1 DSGVO sind der Verantwortliche *und* der Auftragsverarbeiter jeweils unabhängig voneinander zu den TOMs verpflichtet. Wenn der Verantwortliche einen Verarbeitungsvorgang ganz oder teilweise an einen Auftragsverarbeiter ausgelagert hat, kann er TOMs an den Auftragnehmer delegieren, bleibt aber für alle TOMs der gesamten Verarbeitung Pflichtadressat aus Art. 32 DSGVO.[47]

Für die Pflicht zum Pentest bei der Auftragsverarbeitung bedeutet dies:

Obwohl der Auftraggeber in der Praxis mangels Zugriffsmöglichkeiten auf das IT-System des Auftragsverarbeiters meist keine Möglichkeit hat, den Pentest selbst durchzuführen, darf er dennoch keine personenbezogenen Daten durch eine Web-Anwendung ohne Pentest verarbeiten lassen. Der Verantwortliche darf Auftragsverarbeiter gemäß Art. 28 Abs. 1 DSGVO nur beauftragen, wenn sie hinreichende Garantien für die TOMs bieten.

In der Konsequenz kann die Beauftragung eines Auftragsverarbeiters ohne ausreichenden Pentest ein Bußgeld zu Lasten des Verantwortlichen (vgl. Art. 28 Abs. 1, 83 Abs. 4 lit. a DSGVO) sowie Schadensersatzpflichten (Art. 82 DSGVO) nach sich ziehen.

c) Art. 28 Abs. 10, 25 DSGVO

Die Realität weicht leider oftmals vom Wortlaut des Gesetzes ab. Verantwortliche, die zum Beispiel Cloud-Computing-Anbieter beauftragen möchten, sehen sich oftmals mit einem schwer auffindbaren Katalog an Kleingedrucktem konfrontiert. Dort ist entweder überhaupt kein Pentest geregelt oder es gibt keine effektive Möglichkeit für den Auftraggeber, die Durchführung des Tests zu prüfen.

Dies gibt Anlass zu folgenden Thesen:

- Einerseits könnte bereits in derartigen Angeboten des Anbieters ein Verstoß gegen Art. 32 Abs. 1 DSGVO gesehen werden. Allerdings verpflichtet Art. 32 Abs. 1 DSGVO den Auftragsverarbeiter zu den TOMs nur für den Vorgang der Verarbeitung, während Art. 25 DSGVO bereits an einen Zeitpunkt vor der Verarbeitung anknüpft, und zwar dann, wenn die Mittel der Verarbeitung bestimmt werden (Art. 25 DSGVO gilt aber nur für Verantwortliche und nicht für Auftragsverarbeiter).[48] Folglich dürfte in dem bloßen Angebot des Anbieters zur Auftragsverarbeitung ohne Pentest noch kein Verstoß gegen Art. 32 DSGVO liegen.
- Andererseits verdeutlicht der Anbieter durch sein standardisiertes Angebot, dass er (jedenfalls in Bezug auf den Pentest) dem Verantwortlichen weder eine Weisungs- noch eine Kontrollmöglichkeit einräumen will. Unter der DSGVO ist strittig, ob die Weisungsabhängigkeit des Auftragsverarbeiters ein Tatbestandsmerkmal oder eine Rechtspflicht ist.[49] Unabhängig hiervon ist unter den dargestellten Voraussetzungen mit dem Anbieter kein Vertragsschluss zu den Anforderungen des Art. 28 Abs. 3 DSGVO möglich. Dies lässt entweder den Tatbestand einer Auftragsverarbeitung entfallen oder es steht bereits fest, dass die Pflichten einer Auftragsverarbeitung nicht erfüllt werden können. In derartigen Fällen entscheidet nicht der Auftraggeber, sondern der Anbieter über die Mittel der Verarbeitung. Der Anbieter wird damit gemäß Art. 28 Abs. 10 DSGVO selbst zum Verantwortlichen.
- Ob standardisierte Cloud-Angebote als Auftragsverarbeitung gewertet werden können, hängt somit davon ab, ob dem Kunden effektive Weisungs- und Kontrollmöglichkeiten verbleiben. In Bezug auf den Pentest dürfte es ausreichend sein, wenn der Anbieter gemäß den BSI-Empfehlungen (siehe oben lit. a) zumindest jährlich einen Pentest nachweist (zu den Inhalten siehe unten Ziff. 2). Ohne einen ordnungsgemäßen Pentest-Nachweis wird der Anbieter jedoch zum Verantwortlichen und er ist gemäß Art. 25 Abs. 1 DSGVO zum Datenschutz durch Technikgestaltung verpflichtet („Privacy by Design"). Da der Pentest bei Web-Anwendungen zum Stand der Technik gehört (siehe oben lit. a), muss bereits das Angebot des Auftragnehmers den ordnungsgemäßen Nachweis jährlicher Pentests umfassen.

44 Zum Pentest für Behörden siehe den Link in Fn. 43; zum jährlichen Pentest im Anforderungskatalog Cloud-Computing siehe https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/Anforderungskatalog.pdf;jsessionid=657AF09 E 4EB210 B 753 F 67EE 3 F 4A76545.1_cid341?__blob=publicationFile&v=7, dort S. 50.

45 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/Anforderungskatalog_Referenzierung.pdf?__blob=publicationFile&v=4; der Verweis wird hergestellt durch die Kennziffer RB-18 auf Seite 50 des BSI-Anforderungskatalogs C 5 (Fn. 44), die in der Tabelle unter dem Link in dieser Fußnote 45 den oben genannten Normen zugeordnet wird.

46 https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Anforderungskatalog/FAQ/Faq_Anforderungen_node.html;jsessionid=657AF09 E 4EB210 B 753 F 67EE3 F 4A76545.1_cid341.

47 *Schneider* (Fn. 2), Kap. A Rn. 633; *Gola* (Fn. 13), Art. 32 Rn. 8.

48 *Plath* (Fn. 7), Art. 25 DSGVO Rn. 4; *Gola* (Fn. 13), Art. 25 Rn. 12.

49 Nachweise siehe oben Abschnitt II Ziffer 2 lit. a.

2. Kann der Verantwortliche vom Auftragsverarbeiter einen Pentest verlangen?

Für das (Innen-)Verhältnis zwischen dem Verantwortlichen und dem Auftragsverarbeiter lässt sich aus der DSGVO kein gesetzlicher Anspruch des Verantwortlichen auf Durchführung oder gar Duldung eines Pentests ableiten (lit. a). Vielmehr ist eine vertragliche Vereinbarung mit entsprechend qualifiziertem Inhalt erforderlich (lit. b). Ohne behördliches Einschreiten hat ein Verantwortlicher keine Möglichkeit, einen Pentest vom Auftragsverarbeiter zu erzwingen (lit. c).

a) Aussagen der DSGVO zum Verhältnis zwischen Verantwortlichem und Auftragsverarbeiter

Im Gegensatz zu Art. 17 der Datenschutzrichtlinie (RL 95/46/EG) verpflichtet Art. 32 Abs. 1 DSGVO den Verantwortlichen und den Auftragsverarbeiter im Rahmen ihrer TOMs zum Pentesting. Allerdings hat der Verordnungsgeber damit keine Aussage zum Verhältnis zwischen dem Verantwortlichen und dem Auftragsverarbeiter getroffen. Der Auftragsverarbeiter ist gemäß Art. 32 DSGVO zwar zu einem Pentest verpflichtet – ob der Verantwortliche einen Nachweis hierüber verlangen (oder gar den Pentest selbst durchführen) kann, ist gesetzlich nicht geregelt.

Bereits nach dem BDSG 2003 kann der Auftraggeber einer Auftragsdatenverarbeitung von seiner Pflicht zur Kontrolle des Auftragnehmers keine Rechte gegenüber dem Auftragnehmer herleiten. Vielmehr sind entsprechende Zutritts-, Kontroll- und Weisungsrechte mit dem Auftragnehmer vertraglich zu vereinbaren. Dies hat sich durch die DSGVO nicht geändert. Auch hier hat sich der Verantwortliche entsprechende Weisungs- und Kontrollbefugnisse vertraglich auszubedingen.[50]

Auch Ansprüche im Zusammenhang mit anderen Normen scheitern: Auskunfts- oder Besichtigungsansprüche aus den §§ 242, 259, 260 oder 809 BGB setzen stets einen zugrundeliegenden (Haupt-)Anspruch des Anspruchstellers voraus.[51] Dies könnte zum Beispiel vorliegen, wenn der Verantwortliche von einem Betroffenen gemäß Art. 82 DSGVO aufgrund eines Datenschutzverstoßes aus der Sphäre des Auftragsverarbeiters in Anspruch genommen wird. Solange jedoch keine derartigen Ansprüche konkret drohen, gibt es für einen Auskunftsanspruch des Verantwortlichen gegen den Auftragsverarbeiter keine Rechtsgrundlage.

Somit hat der Verantwortliche ohne vertragliche Vereinbarung keinen Anspruch gegen den Auftragsverarbeiter auf Nachweis oder gar Duldung eines Pentests, weder vor noch nach der Beauftragung.

b) Vertragliche Vereinbarungen zu ordnungsgemäßem Pentest

Es ist nicht zwingend erforderlich, dass der Verantwortliche den Pentest beim Auftragsverarbeiter selbst durchführt. Wenngleich dies in Einzelfällen erforderlich sein mag und auftraggeberseitige Pentests die Entdeckung von Sicherheitslücken steigern, ist zu berücksichtigen, dass ein Pentest das IT-System des Auftragsverarbeiters auch beschädigen könnte. Zum Beispiel könnte er Betriebsstörungen verursachen, versehentlich Daten anderer Kunden exfiltrieren oder beschädigen. Dies würde den Verantwortlichen gegenüber dem Auftragsverarbeiter haftbar machen.[52]

Anstelle persönlicher Vor-Ort-Kontrollen ist deshalb in der Regel ein aussagekräftiger Nachweis durch den Auftragsverarbeiter ausreichend, zum Beispiel durch Testate, Bestätigungen von Sachverständigen oder sogar durch Selbstauskünfte. Jedoch müssen derartige Nachweise nach ihrem Inhalt den Verantwortlichen eine zutreffende Beurteilung zu den TOMs des Auftragsverarbeiters ermöglichen.[53]

Solange kein technischer Standard an den inhaltlichen Nachweis über einen ordnungsgemäßen Pentest vorliegt, empfiehlt sich aus Sicht des Verantwortlichen, auf Aussagen mindestens zu folgenden Punkten zu bestehen und diese vertraglich zu vereinbaren:

- Prüfungsobjekt: welches System und welche Funktionen wurden geprüft?
- Prüfungszeitraum und Abschluss der Prüfung,
- Prüfungsmittel: womit wurde geprüft, zum Beispiel durch welche Tools oder durch welche manuellen Maßnahmen?
- Prüftiefe und Intensität (siehe oben Abschnitt II. Ziff. 2 lit. d),
- Identität und Qualifikation der Prüfungsorganisation/des Prüfers,
- Prüfungsergebnis,
- abgeleitete Maßnahmen aufgrund des Prüfungsergebnisses,
- Nachprüfungen nach Behebung etwaiger festgestellter Sicherheitslücken,
- mindestens unaufgeforderter jährlicher Nachweis des Pentests mit obigen Inhalten.

c) Konsequenzen einer Auftragsverarbeitung ohne vereinbarten Pentest

Ein Auftragsverarbeiter, der für seine Web-Anwendung keinen ordnungsgemäßen Pentest-Nachweis anbietet, bietet nicht die erforderlichen Garantien gemäß Art. 28 Abs. 1 DSGVO. Der Auftraggeber darf ihn nicht beauftragen.

Ohne vertragliche Regelung gibt es weder vor noch nach Auftragserteilung einen Anspruch des Verantwortlichen gegen den Auftragsverarbeiter auf Durchführung, Duldung oder Nachweis eines Pentests.

Dies führt zu der misslichen Situation, dass die DSGVO den Verantwortlichen, der für seine Verarbeitung auf standardisierte Web-Anwendungen großer Anbieter angewiesen ist (etwa in der Cloud), zu Pentests zwingt, ihm aber keinen Anspruch gegen einen Anbieter auf Durchführung oder Nachweis hierfür vermittelt. Dies, obgleich der Auftragsverarbeiter gemäß Art. 32 DSGVO unabhängig vom Verantwortlichen zu regelmäßigen Pentests verpflichtet ist (siehe oben Ziff. 1 lit. a, ee und lit. b).

Der Grund hierfür ist, dass ein Verstoß gegen die gesetzlichen Pflichten aus Art. 32 DSGVO für den Auftragsverarbeiter lediglich im Schadensfall (gemäß Art. 82 Abs. 1 DSGVO) Haftungspflichten gegenüber dem Betroffenen vermittelt. Der Verantwortliche kann allenfalls gemäß Art. 82 Abs. 5 DSGVO beim Auftragsverarbeiter Regress nehmen, nachdem er den Betroffenen entschädigt hat.

50 Für das BDSG 2003: *Gola/Schomerus* (Fn. 2), § 11 BDSG Rn. 21; zur DSGVO: *Gola* (Fn. 13), Art. 28 Rn. 9.

51 *Palandt*, Kommentar zum BGB, 77. Aufl. 2018, § 259 Rn. 9, 260 Rn. 1, 2, 809 Rn. 4; auch wenn man die Auftragsverarbeitung als „Auftrag" gemäß den §§ 662, 675 BGB versteht, sind dem Auskunftsanspruch nach § 666 die Grenzen des § 242 BGB gesetzt, siehe *Palandt* (Fn. 51), § 666 Rn. 1.

52 Zur Kontraindikation durch massenweise Vor-Ort-Kontrollen siehe *Schneider* (Fn. 2), Kap. A Rn. 232.

53 *Gola* (Fn. 13), Art. 28 Rn. 11; *Schneider* (Fn. 2), Kap. A Rn. 631 mit Verweis auf Rn. 232.

Zudem kann ein unterlassener Pentest für den Auftragsverarbeiter gemäß den Art. 32, 83 Abs. 4 lit. a DSGVO ein Bußgeld nach sich ziehen. Zuständig hierfür ist jedoch die Aufsichtsbehörde und nicht der Verantwortliche.

Mangels ausreichender gesetzlicher Möglichkeiten für den Verantwortlichen, Anbieter von Auftragsverarbeitungen zur Erfüllung datenschutzrechtlicher Erfordernisse zu veranlassen, sind die datenschutzrechtlichen Aufsichtsbehörden aufgerufen, auf DSGVO-konforme Angebote hinzuwirken, etwa durch Hinweise oder die Nutzung der aufsichtsrechtlichen Instrumente des Art. 58 Abs. 1 und 2 DSGVO. Andernfalls bleiben die Verantwortlichen gegenüber marktbeherrschenden Anbietern von Auftragsverarbeitungen „im Regen stehen".

V. Fazit

1. Auftragsverarbeiter treffen nach der DSGVO eigenständige Pflichten zur Erfüllung datenschutzrechtlicher Vorgaben.

2. Web-basierte Verarbeitungen personenbezogener Daten sind mit internet-spezifischen Risiken verbunden. Diese Risiken sind von der herkömmlichen „TOM-Prüfung" nicht erfasst.

3. Ein ordnungsgemäß durchgeführter Pentest ist ein geeignetes Mittel, um die internet-spezifischen Gefahren web-bezogener Verarbeitungen zu erfassen und anschließend zu eliminieren.

4. Pentests gehören deshalb zum Stand der Technik und sind bei allen web-bezogenen Verarbeitungen personenbezogener Daten gemäß Art. 32 Abs. 1 DSGVO zwingend.

5. Im Verhältnis zwischen dem Verantwortlichen und dem Auftragsverarbeiter gibt es keinen gesetzlichen Anspruch auf Durchführung oder Nachweis eines Pentests. Deshalb sind die datenschutzrechtlichen Aufsichtsbehörden aufgerufen, auf datenschutzkonforme Angebote der Auftragsverarbeiter hinzuwirken.

RA Sebastian Louven, Oldenburg*

Datenzugangsverhältnis, FRAND und Wettbewerbsrecht

Daten sind eine wesentliche Grundlage wirtschaftlichen Wachstums in der Europäischen Union geworden. Nicht nur dass die Digitalbranche selbst neue Entwicklungen mit sich gebracht hat, auch herkömmliche Wirtschaftszweige werden zunehmend digitalisiert. Dabei zeigt sich zunehmend die wirtschaftliche Bedeutung von Daten, sei es als Ressource für neue Geschäftsmodelle, wettbewerbswesentliche Information oder auch im negativen Sinn als Möglichkeit zur Wettbewerbsbeschränkung, indem Unternehmen Daten nicht teilen. Doch können nach bereits bestehenden wettbewerbsrechtlichen Regelungen Unternehmen gezwungen werden, anderen Unternehmen bestimmte Daten bereitzustellen? Wie könnte ein derartiges Datenzugangsverhältnis aussehen und welche Rahmenbedingungen könnten gelten?

I. Einleitung – „Building a European Data Economy"

Am 10. 1. 2017 hat die EU-Kommission eine Mitteilung mit dem Titel „Building a European Data Economy" veröffentlicht, mit der verschiedene Ideen und Vorschläge für rechtliche Rahmenbedingungen im Zusammenhang mit der europäischen Datenwirtschaft unterbreitet werden.[1] Neben einem europaweiten grenzüberschreitenden Datenfluss, Haftungsaspekten bei autonomen Systemen und Internet-of-Things-Anwendungen sowie Portabilität und Interoperabilität von nicht-personenbezogenen Daten und Standards wird dort auch der Zugang und die Übertragung von Daten diskutiert. Ergänzt wird diese Mitteilung durch ein Arbeitspapier.[2] Der Veröffentlichung ist ein Konsultationsprozess vorangegangen.

II. Möglichkeiten für bestehende Datenzugangsverhältnisse

Ein Datenzugangsverhältnis lässt sich als eine konkrete rechtliche Beziehung zwischen einem Anbieter und einem Nachfrager über den Zugang zu Daten beschreiben.[3] Losgelöst von einer freiwilligen Zugangsgewährung und vertraglichen Ausgestaltung dieser Beziehung stellt sich im Zusammenhang mit der Mitteilung der Kommission die Frage nach einem Zugangsanspruch zu Daten unter wettbewerblichen Gesichtspunkten, also als Vorleistungsprodukt. Hierbei könnte das grundsätzliche Bestehen eines Datenzugangsverhältnisses zwar bereits unter verschiedenen einfachgesetzlichen Bestimmungen diskutiert werden. Eine einheitliche Regelung über das „Ob" eines allgemeinen Zugangsanspruchs zu Daten lässt sich bislang aber nur unter kartellrechtlichen Gesichtspunkten annehmen.[4]

1. Verschiedene Typen von Daten

Unabhängig von zivilprozessualen Bestimmtheitsvoraussetzungen stellt sich im Zusammenhang mit dem Zugang

* Der Beitrag basiert auf einem Vortrag, gehalten auf der DSRI-Herbstakademie 2017, erschienen im Tagungsband der Herbstakademie 2017: *Telle*, Daten und FRAND – Regulatorische Bedingungen von Datenzugangsverhältnissen, in: Taeger (Hrsg.), Recht 4.0 – Innovationen aus den rechtswissenschaftlichen Laboren, 2017, S. 421 ff. Sämtliche zitierten Internetquellen wurden zuletzt abgerufen am: 8. 3. 2018. Mehr über den Autor erfahren Sie auf S. XII.

1 Commission, COM(2017) 9 final.

2 Commission, SWD(2017) 2 final.

3 Übersicht dazu: Commission, COM(2017) 9 final, S. 11 ff.

4 Commission, SWD(2017) 2 final, S. 21; dazu *Telle*, in: Hennemann/Sattler (Hrsg.), Immaterialgüter und Digitalisierung, 2017, S. 73 ff.; *König*, in: Hennemann/Sattler (Fn. 4), S. 89 ff.