Maxime Veit / Dirk Müllmann / Melanie Volkamer

Technische und datenschutzrechtliche Einordnung von Weiterleitungs-URLs in E-Mails**

Was bei Weiterleitungs-URLs in E-Mails aus Marketinggründen zu beachten ist

*Häufig sind Links in E-Mails eingebunden, um Empfänger*innen einfacher auf Webseiten oder Webseiteninhalte hinweisen zu können. Dazu wird hinter einem Linktext die entsprechende URL (auch Webadresse genannt) hinterlegt, die bei einem Klick geöffnet wird. Zunehmend ist zu beobachten, dass es sich bei der hinterlegten URL jedoch nicht um die sog. Ziel-URL, d.h. die eigentliche Adresse der Webseite, handelt, sondern eine sog. Weiterleitungs-URL hinterlegt wurde. Anders als die Ziel-URL leitet die Weiterleitungs-URL zunächst auf eine andere URL weiter. Sie tritt in zwei unterschiedlichen Formen auf, die auch kombiniert werden können: Einerseits als Weiterleitungs-URLs, die der Mailserver der Empfänger*innen aus Security-Gründen integriert, und anderseits in Form von Weiterleitungs-URL, die von Absender*innen aus Marketinggründen verwendet werden. Der Beitrag untersucht die Weiterleitungs-URL aus Marketingründen unter technischen und datenschutzrechtlichen Gesichtspunkten und leitet aus den Ergebnissen Empfehlungen für ihren Einsatz ab.*

Keywords: Tracking-URL, E-Mail, IT-Sicherheit, Datenschutz, Weiterleitungs-URL

I. Beschreibung

Die Möglichkeit, Links in E-Mails einzubetten, birgt den grundsätzlichen Vorteil der schnellen Auffindbarkeit konkreter Webseiten. Entsprechend enthält heute ein Großteil der E-Mails Links. Hierbei ist eine URL hinterlegt, die mit einem Klick jene Webseite öffnet, die der URL zugeordnet ist. Links in E-Mails einzubetten hat aber auch Nachteile: Angreifer*innen, häufig

** Dieser Aufsatz ist erschienen in CR 12/2023, 810. Es handelt sich um eine Zweitveröffentlichung des Akzeptierten Manuskripts. Der Beitrag wurde unterstützt durch KASTEL - Institut für Informationssicherheit und Verlässlichkeit Security Research Labs und des Topics Engineering Secure Systems (ESS) der Helmholtz Gemeinschaft (HGF) am KIT.

als Phisher*innen bezeichnet, verschicken authentisch wirkende E-Mails, bei denen der Link nicht mit der eigentlich gewünschten Webseite, sondern mit einer Phishing-URL hinterlegt ist.

1. Phishing-Problematik durch Links in E-Mails und Gegenmaßnahmen

Klicken Empfänger*innen auf den Linktext eines Angreifers, werden sie zu einer Phishing-Webseite geleitet. Diese versucht entweder Schadsoftware auf das Gerät der Empfänger*innen zu laden oder die Login-Seite eines Dritten möglichst authentisch zu imitieren, damit Empfänger*innen dort ihre sensiblen Informationen, wie z.B. die Login-Daten, eingeben. Diese Form des Cyber-Angriffs stellt eine zunehmende Gefahr für Unternehmen und Privatpersonen dar.[5] Dies liegt unter anderem daran, dass Angreifer*innen die E-Mails immer authentischer gestalten und Phishing-E-Mails häufig allenfalls noch an den Phishing-URLs hinter dem Link als solche entlarvt werden können.

Als wirksames Mittel zur Erkennung solcher Links wird daher die Prüfung der registrierten Domain in der URL im Rahmen von Anti-Phishing-Awareness-Maßnahmen[6] geschult. Bei der registrierten Domain handelt es sich um den Teil der URL, der dem Inhaber der Webseite zugeordnet werden kann auf den der Link verweist (z.B. ist die registrierte Domain der URL https://secuso.aifb.kit.edu/1047.php kit.edu).

2. Formen von Weiterleitungs-URLs

Zunehmend ist zu beobachten, dass es sich bei der URL hinter einem Link in E-Mails nicht um die sog. Ziel-URL, d.h. die eigentliche Adresse der Webseite, handelt, sondern eine sog. Weiterleitungs-URL hinterlegt wurde. Über die Weiterleitungs-URL wird zunächst ein Dienst der in der Weiterleitungs-URL definierten registrierten Domain aufgerufen. Dort ist definiert, wohin die Anfrage weitergeleitet wird, u.a. zu welcher Ziel-URL weitergeleitet werden soll.

Weiterleitungs-URLs treten in zwei unterschiedlichen Formen auf, die auch kombiniert werden können:

---

[5] Wirtschaftsschutz 2021. (2021). bitkom. https://www.bitkom.org/sites/default/files/2021-08/bitkom-slides-wirtschaftsschutz-cybercrime-05-08-2021.pdf. Alle Links wurden zuletzt am 23.06.2023 abgerufen.

[6] vgl. Betrügerische Nachrichten. (2020). SecUSo. https://secuso.aifb.kit.edu/downloads/Flyer/NoPhish_betr.Nachrichten/KIT-Faltblatt-BN-DE_08.11.2020.pdf.

- Einerseits in Form von Weiterleitungs-URLs, die der Mailserver der Empfänger*innen aus *Security-Gründen* integriert;
- Anderseits als Weiterleitung, die von den von Absender*innen aus *Marketinggründen* verwendet werden.

URL-Weiterleitungen aus Security- und aus Marketinggründen unterscheiden sich in ihren Funktionsweisen und ihrem Zweck. Bei der URL-Weiterleitung aus Security-Gründen wird zunächst eine Zwischeninstanz aufgerufen, um die Ziel-URL zu prüfen, bevor auf diese weitergeleitet wird. Dies geschieht zwar auch bei URL-Weiterleitungen aus Marketinggründen, hierbei werden jedoch anstatt der Durchführung einer Sicherheitsprüfung der Ziel-URL regelmäßig Informationen über den Nutzer*innen aus Marketinggründen (z.B. ungefährer Standort, Browser und Sprache) erfasst, um etwa Inhalte der E-Mail (z.B. des Newsletters) zu optimieren oder zu evaluieren, welche Angebote für Nutzer*innen oder speziell den Empfänger*innen besonders attraktiv sind. Die Zwischeninstanz bei Weiterleitungs-URLs aus Marketingründen wird von den Absender*innen bestimmt und kann nicht nur je nach Absender bzw. Absenderin, sondern sogar von Empfänger*innen zu Empfänger*innen der gleichen E-Mail unterschiedlich sein. Durch individualisierte Weiterleitungs-URLs ist es möglich zu erfassen, welche Empfänger*innen auf den Link geklickt haben.

In diesem Aufsatz wird die Weiterleitungs-URL aus Marketinggründen aus technischer und datenschutzrechtlicher Sicht untersucht und Empfehlungen für ihren Einsatz abgeleitet[7].

3. Weiterleitungs-URLs aus Marketinggründen

Die Zwischeninstanz, über die definiert wird, wohin die Anfrage für eine konkrete Weiterleitungs-URL weitergeleitet wird, kann von verschiedenen Institutionen bereitgestellt werden. Einerseits können die Absender*innen den Dienst selbst betreiben und die Informationen zum Klickverhalten durch ihren *eigenen Server*[8] erheben. Alternativ können die Absender*innen aber auch den Service eines *externen Dienstleisters* nutzen, der die

[7] Für eine Analyse von Weiterleitungs-URLs aus Security-Gründen sei verwiesen auf: Müllmann/Veit/Volkamer, Technische und Rechtliche Auseinandersetzung mit Weiterleitungs-URLs in E-Mails aus Security-Gründen, in: Demmler/Krupka/Federrath (Hrsg.), 52. Jahrestagung der Gesellschaft für Informatik, INFORMATIK 2022, Informatik in den Naturwissenschaften, Hamburg, 2022, S. 601 - 615.

[8] Hinweis: Hierbei können grundsätzlich auch Kurz-URL-Dienste, sog. URL Shortener, für die Umsetzung eingesetzt werden. Deren primäre Aufgabe ist es, einen langen Link zu verkürzen, damit man ihn sich z.B. einfacher notieren kann oder er weniger Platz in Social-Media-Beiträgen einnimmt.

entsprechenden Informationen erhebt, gegebenenfalls aufbereitet und den Absender*innen die aufbereiteten Informationen als Statistiken zur Verfügung stellt.

Für Empfänger*innen erscheint in der E-Mail als Link-Ziel lediglich die Weiterleitungs-URL (je nach E-Mail-Client in der Statusleiste und/oder Tooltip, wenn der Link mit der Maus berührt wird). Informationen über die Ziel-URL sind auch nicht im HTML-Code der E-Mail einsehbar[9]. Darüber hinaus bekommen Empfänger*innen von der Weiterleitung visuell bzw. in der Nutzungserfahrung des Webseitenaufrufs nichts mit. Im Webbrowser wird direkt die Webseite der Ziel-URL angezeigt.

II. Technische Bewertung

Bei der Untersuchung, inwieweit die Verwendung der Marketing-Weiterleitungs-URLs ein Security-Risiko darstellen, ist die Frage zu beantworten, ob diese Technik genutzt werden kann, um Phishing E-Mails nicht von echten E-Mails unterscheidbar zu machen.

Eine wesentliche Anti-Phishing-Awareness-Maßnahme ist der Hinweis, dass viele Phishing-E-Mails an der Plausibilität von Absender*innen und Inhalt erkannt werden können. Ferner können insbesondere gut gemachte Phishing-E-Mails durch Überprüfung der registrierten Domain in der URL hinter dem Link erkennen werden.[10]

1. Verwendung eigener Server

Verwenden die Absender*innen einen *eigenen Server* für die Weiterleitungs-URL steigt das Security-Risiko grundsätzlich nicht. Die Zwischeninstanz[11] ist in diesen Fällen auf dem eigenen Server gehostet und verwendet somit die eigene (registrierte) Domain. Die Empfänger*innen können demnach die registrierte Domain der Weiterleitungs-URL den Absender*innen zuordnen. So verwendet z.B. das KIT in Newslettern den internen Dienst „s.kit.edu“ für Weiterleitungs-URLs. Weiterleitungs-URLs würden daher immer die registrierte Domain „kit.edu“ enthalten. Somit wird z.B. die URL *https://secuso.aifb.kit.edu/betruegerische*

[9] Entsprechend ist es nicht einfach möglich, E-Mail-Clients zu erweitern, damit die Ziel-URL angezeigt wird.
[10] Vgl. z. B. Betrügerische Nachrichten. (2020). SECUSO. https://secuso.aifb.kit.edu/downloads/Flyer/KIT_Faltblatt_BN_DE_DinL_Entwurf01.pdf.; Vgl. What You Spot Phishing Emails (Today). (2015). What You Need To Know. https://www.youtube.com/watch?v=U7tbJVSInvo.
[11] Einige Content-Management-Systeme (CMS) bieten bereits die Möglichkeit an, Weiterleitungs-URLs für den eigenen Server zu erstellen. Alternativ gibt es auch - zum Teil sogar kostenlose - Tools, die dies ermöglichen.

_nachrichten_erkennen.php zu *https://s.kit.eu/nophish* umgewandelt. Ein solcher Link kann daher weiterhin überprüft werden.

Bei diesem Ansatz müssen diese Dienste jedoch richtig konfiguriert sein. Andernfalls steigt das Security Risiko signifikant an, da es auch für Angreifer*innen möglich ist, ebenfalls die URL, mit vertrauenswürdiger registrierter Domain, zu verwenden, um die Nutzer*innen auf gefährliche Schadwebseiten umzuleiten.[12]

2. Verwendung externer Dienstleister

Alternativ zur selbst gehosteten Lösung auf dem eigenen Server, kann die Zwischeninstanz auch auf den Servern externer Dienstleister liegen. Bei der Verwendung *externer Dienstleister* und dabei URLs mit einer registrierten Domain, die nicht der Organisation des Absendenden zugeordnet werden kann, besteht das Problem, dass die registrierte Domain der URL nicht mit den Absender*innen verknüpft werden kann. Hierdurch steigt das Security-Risiko. Es werden grundsätzlich zwei Umsetzungsformen unterschieden: Die Weiterleitungs-URLs können entweder im Pfad der URL die Ziel URL enthalten oder keinerlei Informationen über die Ziel URL bereitstellen. Die Höhe des Risikos hängt dabei davon ab, welche der beiden Umsetzungsformen genutzt wird.

a) Ziel-URL nicht erkennbar

Ist die *Ziel-URL nicht im hinteren Teil der Weiterleitungs-URL* erkennbar enthalten, können Empfänger*innen die URL nicht ohne Weiteres überprüfen. Würden Empfänger*innen eine E-Mail erhalten, die vermeintlich von der Forschungsgruppe SECUSO des KIT kommt und würden dort hinter einem Link die Weiterleitungs-URL https://bit.ly/3nvBA6p vorfinden, ist nicht ersichtlich, dass diese zu der Website https://secuso.aifb.kit.edu/ führt .

Grundsätzlich können aber auch Angreifer*innen externe Weiterleitungs-URL-Dienste nutzen, um Phishing URLs zu verschleiern. Viele externe Dienste zur Generierung von Weiterleitungs-URLs können ohne Anmeldung und somit anonym verwendet werden. Das macht sie für Angreifer*innen attraktiv. Die Einbettung von Weiterleitungs-URL in eine legitime E-Mail (z.B. einen internen Firmen-Newsletter) führt also dazu, dass (ohne weitere Vorkehrungen wie

[12] URL-Redirects – eine gut gemeinte Schwachstelle: https://web-inspection.de/url-redirects-eine-gut-gemeinte-schwachstelle/.

das digitale Signieren von E-Mails) legitime E-Mails nicht von Phishing E-Mails[13] unterschieden werden können. Darüber hinaus könnte dieses Vorgehen bei Empfänger*innen dazu führen, dass die Empfehlung der Anti-Phishing-Awareness-Maßnahme, nicht auf Links, bei denen die Ziel-URL nicht bekannt ist, zu klicken, als unwichtig wahrgenommen wird. Auf diese Weise würde die Verwendung externer Weiterleitungs-Dienste eine weitreichende negative Auswirkung auf die Sicherheit der Empfänger*innen haben.

b) Ziel-URL erkennbar

Ist die Ziel-URL im hinteren Teil der Weiterleitungs-URL erkennbar enthalten, so ist eine Überprüfung der Ziel-URL grundsätzlich möglich (z.B. https://weiterleitungs-service.de/?redirect=newsletterbetreiber.de/produkt1). Dies setzt voraus, dass die Weiterleitungs-URL auch tatsächlich zur angegebenen Ziel-URL führt. Angreifer*innen könnten in diesem Szenario aber einen Dienst implementieren, der es ihnen ermöglicht, eine vertrauenswürdige Ziel-URL im hinteren Teil ihrer Weiterleitungs-URL erscheinen zu lassen, die jedoch ignoriert wird und zur Seite der Angreifer*innen führt. Empfänger*innen von solchen Newsletter und Marketing-E-Mails müssten dann wissen, welche Weiterleitungs-URL-Dienste überhaupt vertrauenswürdig sind, also auch dorthin weiterleiten wie im hinteren Teil der URL angegeben. Im Rahmen von Anti-Phishing-Awareness-Maßnahmen müssten daher die bekanntesten vertrauenswürdigen Dienste vorgestellt werden. Empfänger*innen wären dann angehalten, nicht auf Links von anderen als den vorgestellten Diensten zu klicken, um einem Phishing-Angriff zu begegnen. Darüber hinaus müsste im Rahmen der Anti-Phishing-Awareness-Maßnahmen der Aufbau der Weiterleitungs-URL dieser Dienste erläutert werden. Der Aufbau innerhalb eines Dienstes ist zwar für alle Absender*innen und Links identisch, er unterscheidet sich jedoch von Dienst zu Dienst, weshalb sich keine allgemeingültigen Regeln zur Erkennung von Ziel-URLs aus dem Pfad von Weiterleitungs-URLs ableiten lassen. Für den sicheren Umgang mit diesen Diensten wäre es also notwendig, die bestehenden Anti-Phishing-Awareness-Maßnahmen zu erweitern und sicherzustellen, dass Empfänger*innen die Regeln anwenden können. Anbetracht der Tatsache, dass die Identifikation der registrierten Domain bereits vielen Bürger*innen Probleme macht, kann bei diesem Ansatz zwar theoretisch das

[13] Angreifer*innen könnten auch einen Newsletter erstellen und diesen mit Weiterleitungs-URLs zu ihren Phishing Webseiten anreichern.

Security Risiko gering gehalten werden, fraglich ist, ob die Awareness-Maßnahmen dies leisten können oder ob auch bei diesem Ansatz das Security Risiko steigt.

Eine Technik, die die Problematik bei der Nutzung von externen Dienstleistern entschärfen könnte, ist die Verwendung von kryptografischen Signaturen mittels S/MIME oder PGP. Hierbei könnten die Absender*innen den Inhalt der E-Mail signieren, was wiederum den Empfänger*innen im E-Mail-Client angezeigt wird. Damit können die Empfänger*innen überprüfen, ob der Inhalt tatsächlich von den angegebenen Absender*innen stammt. Sofern sie den Absender*innen vertrauen, könnte damit auch das Anklicken von Links, die anhand ihrer Weiterleitungs-URL nicht überprüft werden können eingesetzt werden ohne das Security-Risiko zu erhöhen. Die Verwendung kryptografischer Signaturen findet allerdings in Newslettern (bzw. allgemein in E-Mails) aktuell noch sehr selten Anwendung.

III. Rechtliche Einordnung

Die rechtliche Bewertung der Verwendung von Weiterleitungs-URLs muss vor dem Hintergrund des Zusammenspiels der privatsphäreschützenden Normen der DSGVO[14] und des TTDSG[15] erfolgen, das der Umsetzung der E-Privacy Richtlinie[16] dient und die datenschutzrechtlichen Regelungen des TKG[17] und des TMG[18] ersetzt.

1. Einschlägige Normen und das Verhältnis ihrer Anwendungsbereiche

Während die DSGVO die Verarbeitung personenbezogener Daten regelt, adressiert das TTDSG den Schutz der Privatsphäre unabhängig davon, ob ein Personenbezug vorliegt oder nicht.[19] Es ist auf Anbieter von Telekommunikations- (vgl. § 3 Nr. 1 TKG) und Telemediendiensten (vgl. § 2 Abs. 2 Nr. 1 TTDSG) anwendbar, die eine Niederlassung im Geltungsbereich des Gesetzes haben, hier Dienstleistungen erbringen oder Waren bereitstellen (§ 1 Abs. 3 TTDSG).

---

[14] Verordnung (EU) 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. L 119, 4. Mai 2016, S. 1 – 88 – in der Folge DSGVO.

[15] Telekommunikation-Telemedien-Datenschutz-Gesetz.

[16] Richtlinie 2002/58/EG vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. L. 201, 31. Juli 2002, S. 37 – 47 – in der Folge E-Privacy RL.

[17] Telekommunikationsgesetz.

[18] Telemediengesetz.

[19] DSK, Orientierunghilfe Telemedien 2021, S. 8; Herrmann in: Assion (Hrsg.), TTDSG, 2022, § 1, Rn. 22; Gierschmann in: Gierschmann/Baumgartner, TTDSG, 2023, §1, Rn. 8; Klabunde/Selmayr in: Ehmann/Selmayr, DSGVO, 2. Aufl., 2018, Art. 95, Rn.4.

Für die Abgrenzung der Anwendungsbereiche ist darauf abzustellen, ob eine Verarbeitung personenbezogener Daten erfolgt oder nicht. Werden keine personenbezogenen Daten verarbeitet, sind ausschließlich die Regeln des TTDSG anwendbar.[20] Erfolgt dagegen eine Verarbeitung, muss für die Bestimmung der einschlägigen Normen zwischen dem Speichern und Auslesen in der Endeinrichtung und der anschließenden Verarbeitung der ausgelesenen Daten unterschieden werden. Da angesichts der Kollisionsregel des Art. 95 DSGVO die Regelung der E-Privacy Richtlinie und die ihrer Umsetzung in nationales Recht dienenden Normen denen der DSGVO vorgehen, ist auf das Speichern und Auslesen von Informationen personenbezogener Daten in Endeinrichtungen § 25 TTDSG anzuwenden.[21] Für die Rechtmäßigkeit der anschließenden Verarbeitung dieser personenbezogenen Daten gelten dann jedoch in Ermangelung von Sondernormen im TTDSG wieder die allgemeinen Regeln der DSGVO.[22]

2. Rechtliche Bewertung von Weiterleitungs-URLs in Newslettern

Bereits der Versand des Newsletters wird in aller Regel auf der Einwilligung der Empfänger*innen beruhen,[23] wenn auch teilweise andere Möglichkeiten zur datenschutzrechtlichen Rechtfertigung eines Newsletterversands angenommen werden.[24] Vorliegend ist jedoch vielmehr die Frage der Rechtmäßigkeit der Nutzung von Weiterleitungs-URLs in Newslettern durch deren Versender*innen und die Auswertung der mittels dieser Weiterleitungs-URLs erlangten Informationen von Interesse.

a) Speichern und Auslesen von Informationen in der Endeinrichtung

Gemäß § 25 Abs. 1 TTDSG ist für die Speicherung von Informationen in der Endeinrichtung der Endnutzer*innen oder den Zugriff auf Informationen, die bereits dort gespeichert sind, die

[20] Vgl. auch Nebel, CR 2021, 666, 667; Sydow in: Sydow/Marsch (Hrsg.), DS-GV O – BDSG, 3. Aufl., 2022, Art. 95 DSGVO, Rn.11.
[21] Golland in: Taeger/Gabel (Hrsg.), DSGVO-BDSG-TTDSG, 4. Aufl., 2022, Art. 95 DSGVO, Rn. 26; Sydow in: Sydow/Marsch (Hrsg.), DS-GV O – BDSG, 3. Aufl., 2022, Art. 95 DSGVO, Rn. 9f.; Holländer in:Wolff/Brink/v.Ungern-Sternberg (Hrsg.), BeckOK DatenschutzR, Art. 95 DSGVO, Rn. 6.
[22] DSK, Orientierungshilfe Telemedien, 2021, S. 5.
[23] Rehker/Lachenmann in: Korneg/Lachenmann (Hrsg.), Formularhandbuch Datenschutzrecht, 3. Aufl., 2021, III. Einwilligung in Werbeversand/Newsletter; Conrad/Hausen in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, 3. Aufl., 2019, §36, Rn. 190 ff.
[24] Landesbeauftragte für den Datenschutz und die Informationsfreiheit (Hrsg.), 26. Tätigkeitsbericht, 2021, 4.2, S. 40 ff.; zur Bestandskundenausnahme nach § 7 Abs. 3 Nr. 1 – 4 UWG und deren datenschutzrechtlichen Auswirkungen vgl. nur Schneider, ZD 2023, 261, 262.

Einwilligung der Endnutzer*innen erforderlich. Ausnahmen gelten nach § 25 Abs. 2 TTDSG lediglich für die Fälle, dass die Speicherung oder der Zugriff nur zum Zweck der Übertragung einer Nachricht über ein öffentliches Kommunikationsnetz erfolgt (§ 25 Abs. 2 Nr. 1 TTDSG) oder sie unbedingt erforderlich ist, damit ein Anbieter eines Telemediendienstes einen von den Nutzer*innen ausdrücklich gewünschten Dienst zur Verfügung stellen kann (§ 25 Abs. 2 Nr. 2 TTDSG). Diese Ausnahmen sind restriktiv auszulegen. Daher darf im Fall des *„ausdrücklich gewünschten Dienstes"* nicht pauschal unterstellt werden, dass mit dem Aufruf eines Angebots dessen gesamte Funktionalität gewünscht ist.[25] Ebenso ist die Erforderlichkeit streng und als technische Erforderlichkeit zu verstehen, bei der in Bezug auf zeitliche, inhaltliche und personelle Dimensionen unterschieden werden muss.[26]

Vor diesem Hintergrund kann, je nach Ausgestaltung der Prozesse in der Zwischeninstanz, bereits der Aufruf an sich eine Einwilligung erforderlich machen. Denn im Rahmen des Aufrufens eines Links über Laptops, Mobiltelefone und Tablets, die als Endgerät iSd. § 2 Abs. 2 Nr. 6 TTDSG gelten,[27] erfasst § 25 Abs. 1 TTDSG neben jeder Art der Informationsspeicherung auch Techniken, durch die ohne Wissen der Nutzer*innen in deren Endgeräte eingedrungen werden kann, um *Zugriff* auf Informationen oder Aktivitäten zu erhalten.[28] Ein *Zugriff* auf Informationen ist dabei definiert als jede gezielte, nicht von Nutzer*innen veranlasste Übermittlung von Browserinformationen, soweit es nicht um zwangsläufig oder aufgrund der Browsereinstellungen übermittelte Daten handelt (z.B. Browser-Fingerprinting).[29] Es genügt hierfür somit das Auslesen von Endgeräteigenschaften, zum Beispiel mittels JavaScript; unzureichend ist jedoch die lediglich vorgenommene Übermittlung der IP-Adresse, der URL, des User-Agent-String oder der eingestellten Sprache.[30] Vor dem Hintergrund der technischen Funktionsweise von Weiterleitungs-URLs ist daher regelmäßig von einem einwilligungspflichtigen *Zugriff* auf Informationen im Sinne der Norm auszugehen. Hieran ändert auch die vorliegend allein in Betracht kommende Ausnahme des

[25] DSK, Orientierungshilfe Telemedien, 2021, S. 19 ff.; Schmitz in: Geppert/Schütz, Beck`scher TKG-Kommentar, 5. Aufl., 2023, §25 TTDSG, Rn. 85; Ettig in: Taeger/Gabel (Hrsg.), DSGVO-BDSG-TTDSG, 4. Aufl., 2022, §25, Rn. 42.
[26] DSK, Orientierungshilfe Telemedien, 2021, S. 22 ff.; Schneider in: Assion (Hrsg.), TTDSG, 2022, §25, Rn. 36; a.A. Hanloser in: Gierschmann/Baumgartner (Hrsg.), TTDSG, 2023, §25, Rn. 107; Ettig in: Taeger/Gabel (Hrsg.), DSGVO-BDSG-TTDSG, 4. Aufl., 2022, §25, Rn. 44.
[27] DSK, Orientierungshilfe Telemedien, 2021, S. 6; Schneider in: Assion (Hrsg.), TTDSG, 2022, §25, Rn. 22.
[28] ErwGr, 24 f. E-Privacy RL; DSK, Orientierungshilfe Telemedien, 2021, S. 7; Schmitz in: Geppert/Schütz, Beck`scher TKG-Kommentar, 5. Aufl., 2023, §25 TTDSG, Rn. 36; Hanloser in: Gierschmann/Baumgartner (Hrsg.), TTDSG, 2023, §25, Rn. 60.
[29] DSK, Orientierungshilfe Telemedien, 2021, S. 8.
[30] DSK, Orientierungshilfe Telemedien, 2021, S. 8; Schneider in: Assion (Hrsg.), TTDSG, 2022, §25, Rn. 23.

§ 25 Abs. 2 Nr. 2 TTDSG nichts. Denn der Aufruf der Zwischeninstanz ist nicht unbedingt erforderlich, um einen vom Nutzer*innen ausdrücklich gewünschten Telemediendienst, hier in Form des Newsletters, zur Verfügung zu stellen. Dieser kann seine Informationsfunktion auch durch den direkten Aufruf der gewünschten Inhaltsseite und somit ohne den Zugriff auf die Informationen des Endgeräts durch die Weiterleitung erfüllen.[31] Eine technische Erforderlichkeit ist somit keinesfalls gegeben.[32] Zudem werden die Nutzer*innen den Zugriff auf die Informationen für eine spätere Auswertung zu Werbezwecken und zur Profilbildung im Kontext eines Informationsangebots durch Newsletter in der Regel weder wünschen noch erwarten,[33] sodass auch kein ausdrücklich vom Nutzer*innen gewünschter Telemediendienst vorliegt.

b) Anschließende Analyse der erhobenen Daten

Datenschutzrechtlich ebenso problematisch bei der Verwendung von Weiterleitungs-URLs in E-Mails aus Marketinggründen ist die mit ihrer Hilfe oftmals im Anschluss an den Informationszugriff vorgenommenen Datenanalyse. Im Rahmen von Newsletterwerbung können durch die Verwendung von individuellen Weiterleitungs-URLs personenbezogene oder -beziehbare Daten der Newsletterempfänger*innen gesammelt und ausgewertet werden, sodass mit ihrer Hilfe Profiling für Marketingzwecke betrieben werden kann. Das ist jedoch in aller Regel lediglich zulässig, sofern Betroffene hierzu ihre Einwilligung erteilt haben, in einigen Fällen aber auch auf der Grundlage einer Interessenabwägung nach Art. 6 Abs. 1 lit. f) DSGVO.[34] Diese Alternative erscheint jedoch insoweit problematisch, als Marketingzwecke den wesentlichen Verarbeitungszweck darstellen. Eine Interessenabwägung im Rahmen der genannten Norm kann daher regelmäßig nur dann zugunsten des*r Datenverarbeiters*in ausgehen, sofern die Eingriffstiefe in die Rechte und Interessen der Betroffenen sehr gering ist. Dies wäre z.B. der Fall, wenn nur die IP-Adresse gespeichert wird. Es kann somit je nach

[31] Vgl. auch Schneider, ZD 2023, 261, 265; Hanloser in: Gierschmann/Baumgartner (Hrsg.), TTDSG, 2023, §25, Rn. 60.
[32] Für die vergleichbare Situation von Cookies zu Marketingzwecken s. Moos, MMR 2019, 732, 737; Rauer/Ettig, ZD 2021, 18, 20; Schneider in: Assion (Hrsg.), TTDSG, 2022, §25, Rn. 36.
[33] So auch: Schneider, ZD 2023, 261, 265; vgl. auch Lorenz, ZD 2023, 531.
[34] Kremer in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, 3. Aufl., 2019, § 28, Rn. 65; DSK, Orientierungshilfe Direktwerbung, 2022, S. 5; Eckhardt, ZD 2022, 307; Möller, VuR 2022, 449; Specht in: Specht/Manz (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 9, Rn. 74; vgl. auch EuGH, Urt. v. 01.10.2019, C-673/17 (Planet 49), MMR 2019, 732; BGH, NJW 2020, 2540.

Umfang der verarbeiteten Daten erforderlich sein, die Eingriffstiefe durch andere Maßnahmen, wie z.B. eine nur teilweise Speicherung der IP zu verringern.

c) Probleme der Einwilligungserteilung

Sowohl das Speichern und Auslesen von Informationen aufgrund der Verwendung von Weiterleitungs-URLs nach § 25 Abs. 1 TTDSG als auch die sich regelmäßig daran anschließende Verarbeitung von auf diese Weise erhobenen Daten gemäß Art. 6 Abs. 1 lit. a) DSGVO sind daher regelmäßig von der Einwilligung der betroffenen Newsletterabonnenten abhängig. Diese Einwilligungen können dabei grundsätzlich auch bereits im Rahmen des initialen Abonnements des Newsletters abgefragt und von den Betroffenen „gebündelt" erteilt werden.[35] Bei nachträglicher Verwendung der Technik ist das Einholen der Einwilligung in diese Art der Datenverarbeitung auch von Bestandsempfänger*innen jedenfalls angesichts § 25 Abs. 1 TTDSG zwingend erforderlich.

Oftmals ist jedoch fraglich, ob bei der Einholung einer originären oder nachträglichen Einwilligung die gesetzlichen Anforderungen an die Einwilligungserteilung gewahrt werden. Sie ergeben sich, auch für die nach § 25 Abs. 1 TTDSG zu erteilende Einwilligung ins Speichern und Auslesen von Informationen auf oder aus dem Endgerät, aus Art. 4 Nr. 11, Art. 7 und Art. 8 DSGVO.[36] Bei der gebündelten Erteilung von Einwilligungen ist dabei insbesondere darauf zu achten, dass erkennbar ist, dass mehrere Einwilligungen erteilt werden und in Bezug auf die Einwilligung in die Auswertung der erhobenen Daten nach Art. 6 Abs. 1 lit. a) DSGVO eine konkrete Beschreibung der Verarbeitungszwecke erfolgt.[37] Ein generelles Problem in Bezug auf die Erfüllung der gesetzlichen Anforderungen an datenschutzrechtliche Einwilligungen stellt jedoch deren *Freiwilligkeit* dar (vgl. Artt. 4 Nr. 11, 7 Abs. 4 DSGVO). So auch im vorliegenden Fall.

Die Datenverarbeitung im Zusammenhang mit Weiterleitungs-URLs wird regelmäßig Bestandteil der umfassenden Datenschutzerklärung des Unternehmens sein. Im Rahmen der

---

[35] DSK, Orientierungshilfe Telemedien, 2021, S. 9; Zur grundsätzlichen Möglichkeit der Bündelung von Einwilligungen vgl. EDSA, Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen, 2.0, Fn. 17; Schneider, ZD 2023, 261, 265.

[36] DSK, Orientierungshilfe Telemedien, 2021, S. 9 ff; Schmitz in: Geppert/Schütz, Beck`scher TKG-Kommentar, 5. Aufl., 2023, §25 TTDSG, Rn. 40; Hanloser in: Gierschmann/Baumgartner (Hrsg.), TTDSG, 2023, §25, Rn. 65; Ettig in: Taeger/Gabel (Hrsg.), DSGVO-BDSG-TTDSG, 4. Aufl., 2022, §25, Rn. 24.

[37] DSK, Orientierungshilfe Telemedien, 2021, S. 10, 12f.; Schneider, ZD 2023, 261, 265.

Einwilligungserteilung in das Abonnement eines Newsletters wird für die Informationen in Bezug auf die damit verbundene Datenverarbeitung, wie deren Rechtsgrundlage und Zwecke, regelmäßig bloß pauschal auf diese verwiesen. Die Einwilligung setzt jedoch voraus, dass Einwilligende abschätzen können, welche Auswirkungen die Erteilung der Einwilligung für sie hat, wobei sie die Umstände der Datenverarbeitung und die Tragweite ihrer Einwilligung eindeutig erkennen können müssen[38]. Die Erklärung muss dabei für eine*n Durchschnittsnutzer*in mühelos lesbar sein, was auch bedeutet, dass der Umfang der Information im Verhältnis zum eingegangenen Geschäft angemessen sein muss.[39] Die Erfüllung dieser Anforderung erscheint fraglich, sofern die Informationen, die eine Verarbeitung der mittels Weiterleitungs-URL in Newslettern gewonnenen Daten betreffen, einen Teil der gesamten Datenschutzerklärung des Unternehmens darstellen. Betroffene sehen sich dann angesichts der Zusammenfassung aller Informationen in einem Dokument einer Masse von für ihr Anliegen überwiegend irrelevanten Informationen gegenüber und sind gezwungen etliche Seiten einer Datenschutzerklärung dahingehend zu filtern, ob sie mit der Verarbeitung in Verbindung stehen. Bei der Bewertung der Zumutbarkeit eines solchen Gestaltung einer Datenschutzerklärung und des daraus resultierenden Umfangs der wahrzunehmenden Informationen muss zugleich aber berücksichtigt werden, dass der Verantwortliche mit der Bereitstellung der dort aufgeführten Angaben seiner gesetzlichen Informationspflicht nach Art. 13 DSGVO nachkommt. Böswilligen und unlauter handelnden Verantwortlichen bietet sich so jedoch dennoch die Möglichkeit, Betroffene durch die gesetzlich vorgesehenen Informationen in einer nicht zu bewältigenden Flut von Auskünften zu begraben, was den Sinn des Art. 13 DSGVO in sein Gegenteil verkehrte.

Wenn ein Verantwortlicher bewusst auf diesen Effekt setzt, kann ein Dark Pattern vorliegen, also eine Gestaltung, die versucht, Nutzer*innen zu unbeabsichtigten, ungewollten und potentiell schädlichen Entscheidungen zu bewegen, die sich gegen ihre und zugunsten der Interessen der Verarbeiter ihrer personenbezogenen Daten richten.[40] Konkret könnte bei einem solchen Vorgehen ein sog. *„Overloading“* vorliegen, also die Konfrontation der Nutzer*innen mit einer großen Menge von Anfragen, Informationen, Optionen oder Möglichkeiten, um sie

[38] Buchner/Kühling in Kühling/Buchner, DSGVO, 3. Aufl., 2020, Art. 4 Nr. 11, Rn. 8.
[39] BGH, NJW 2020, 2540, 2544, Rn. 32 ff.; LG Frankfurt, DuD 2016, 613, 616; Buchner/Kühling in Kühling/Buchner, DSGVO, 3. Aufl., 2020, Art. 1, Rn. 60.
[40] EDPB, Guideline 03/2022 on Deceptive Design Patterns in Social Media Platform Interfaces, Version 2.0, 14.02.2023, S.3.

zu veranlassen, mehr Daten weiterzugeben oder unbeabsichtigt die Verarbeitung personenbezogener Daten entgegen den Erwartungen der betroffenen Person zuzulassen.[41] Es kann neben der Freiwilligkeit der Einwilligung ebenso die Transparenz der Information nach Art. 12 Abs. 1 DSGVO in Frage stellen und die Wahrung des Prinzips der Transparenz und Verarbeitung nach Treu und Glauben gemäß Art. 5 Abs. 1 lit. a) DSGVO zweifelhaft erscheinen lassen.[42]

Wann ein Fall des rechtswidrigen Overloading vorliegt, ist im konkreten Einzelfall zu entscheiden. Zur Orientierung bietet sich ein Vergleich zur Bewertung von Allgemeinen Geschäftsbedingungen an, bei denen die von der Rechtsprechung in Bezug auf ihren zulässigen Umfang entwickelten Grundsätze ebenfalls auf dem Gebot der Transparenz basieren.[43] Hiernach muss die Länge insbesondere in einem vertretbaren Verhältnis zur Bedeutung des Geschäfts stehen.[44] Im vorliegenden Fall der Einwilligung im Kontext eines Newsletterabonnements dürfte insofern jedenfalls von einem sehr alltäglichen und mit geringer Bedeutung versehenen Geschäft ausgegangen werden, weshalb der zu tolerierende Umfang herabgesetzt sein dürfte. Zugleich geht die Rechtsprechung bei Internetgeschäften aber davon aus, dass zeitlicher Druck bei der Bewertung der Angemessenheit des Umfangs nicht in die Abwägung einzubeziehen sei. In diesen Situationen bleibe es den Nutzer*innen selbst überlassen, wie lange sie sich mit dem Text auseinandersetzen wollten.[45] Vor diesem Hintergrund spielt es bei der Bewertung der Zumutbarkeit daher keine Rolle, ob die datenschutzrechtliche Einwilligung im Kontext einer extra hierfür vom Anbieter bereitgestellten Webseite erfolgt, die bewusst vom Nutzer*innen zum Zweck der Newsletteranmeldung aufgerufen wurde, oder aber im Kontext eines anderen Kontakts zum Verantwortlichen erteilt wird, z.B. während eines Bestellprozesses, den der Nutzer*innen eigentlich schnell beenden möchte. Die Verantwortung zur Wahrnehmung läge allein bei den Nutzer*innen, solange kein zeitlicher Druck von außen aufgebaut wird.

---

[41] EDPB, Guideline 03/2022 on Deceptive Design Patterns in Social Media Platform Interfaces, Version 2.0, 14.02.2023, S.3, 65ff.
[42] EDPB, Guideline 03/2022 on Deceptive Design Patterns in Social Media Platform Interfaces, Version 2.0, 14.02.2023, S. 65f.
[43] Vgl. nur OLG Köln, MMR 2020, 709, 710, Rn. 49 f. mwN.; Grüneberg in: Grüneberg (Hrsg.), Bürgerliches Gesetzbuch, 81. Aufl., 2022, §305, Rn. 39.
[44] Vgl. nur OLG Köln, MMR 2020, 709, 710, Rn. 50; Becker in: Hau/Poseck (Hrsg.), BeckOK BGB, 67. Ed., 2023, §305, Rn. 60; Grüneberg in: Grüneberg (Hrsg.), Bürgerliches Gesetzbuch, 81. Aufl., 2022, §305, Rn. 37.
[45] Vgl. nur OLG Köln, MMR 2020, 709, 710, Rn. 50.

Praktisch kann der Gefahr des Overloadings durch die Einhaltung einfacher Strukturierungs- und Gestaltungsmethoden in der Datenschutzerklärung begegnet werden. Weist sie z.B. eine Gliederung auf, die das Auffinden bestimmter Verarbeitungsarten durch ein verlinktes Inhaltsverzeichnis unmittelbar ermöglicht oder wird die Einwilligung mit dem konkret einschlägigen Abschnitt der Datenschutzerklärung verlinkt, werden die Anforderungen an den zumutbar wahrzunehmenden Umfang der Information regelmäßig gewahrt sein.

Neben dem Overloading kann die Freiwilligkeit der Einwilligung jedoch im Einzelfall auch durch eine Verletzung des Kopplungsverbots nach Art. 7 Abs. 4 DSGVO in Frage gestellt sein. Die von der Einwilligung erfassten Daten sind in der Regel nämlich nicht für die Bereitstellung der mit dem Newsletter verbundenen Informationen erforderlich. Eine Einwilligung ist nur dann freiwillig, wenn Nutzer*innen die Freiheit haben, die Einwilligung in bestimmte Datenverarbeitungsvorgänge, die für die Erfüllung des Vertrages nicht erforderlich sind, einzeln zu verweigern, ohne dazu gezwungen zu sein, auf die Nutzung des angebotenen Dienstes völlig zu verzichten.[46] Diese vom EuGH für soziale Netzwerke getroffene Feststellung lässt sich auf andere Arten der Datenverarbeitung wie den vorliegenden Fall der Analyse von Nutzer*innendaten durch den Einsatz von Weiterleitungs-URLs übertragen. Das der Verarbeitung zugrundeliegende Interesse des Verarbeiters besteht nämlich in beiden Fällen in der Datenanalyse zu kommerziellen Werbe- und Profilingzwecken, die für die eigentlich Bereitstellung des Newsletters auch nicht benötigt werden.[47] Im Gegenteil: Die Analyse des Nutzer*innenverhaltens verstärkt vielmehr den von einem Newsletter grundsätzlich ausgehenden Werbeeffekt für ein Unternehmen durch eine Betrachtung der konkreten Interessen und des Verhaltens der Adressat*innen. Als Lösung für dieses Problem schlägt der EuGH das Angebot einer gleichwertigen Alternative gegen ein angemessenes Entgelt vor.[48] Dies erscheint auch im vorliegenden Fall umsetzbar.

---

[46] EuGH, Urt. v. 04.07.2023, C-252/21, Rn. 150, ECLI:EU:C:2023:537; vgl. auch Klabunde in: Ehmann/Selmayr (Hrsg.), DSGVO, 2. Aufl., 2018, Art. 4, Rn. 51.
[47] Vgl. Nebel, CR 2021, 666, 671.
[48] EuGH, Urt. v. 04.07.2023, C-252/21, Rn. 150, ECLI:EU:C:2023:537.

IV. Fazit und Empfehlung

Die Nutzungsmöglichkeiten von Weiterleitungs-URLs sind vielfältig - sowohl im Kontext von Marketingzwecken, als auch bei ihrem Einsatz aus Security-Gründen[49]. Weiterleitungen aus Security-Gründen haben das Potential die Sicherheit in Unternehmen aber auch im privaten Bereich zu verbessern. Dies setzt nicht nur eine Umsetzung voraus, die IT-sicherheitstechnische Empfehlungen beachtet, sondern gerade im dienstlichen Kontext auch eine Einbettung in geeignete Anti-Phishing-Awareness-Maßnahmen.

Im Kontext von Weiterleitungs-URLS im Marketingumfeld sind der Zugriff auf die regelmäßig vom Endgerät der Nutzer*innen abgerufenen Informationen, aber auch die Sammlung und Auswertung personenbezogener Daten in den meisten Fällen von Einwilligungen der Newsletterempfänger*innen abhängig zu machen. Hierbei kann, je nach Einzelfall, insbesondere die Freiwilligkeit dieser Einwilligungen problematisch sein. Bedient sich der Verantwortliche für den Einsatz von Weiterleitungs-URLs externer Dienste, wie z.B. Link-Shortener oder externen Zwischeninstanzen, kann die Verarbeitung je nach Ausgestaltung und sofern sie auf der Grundlage eines Vertrages erfolgt eine Auftragsdatenverarbeitung, gemeinsame Verantwortlichkeit oder eigene Verarbeitung der dritten Partei zu werten sein.

Aus technischer Sicht muss es den Empfänger*innen von E-Mails möglich sein, vor dem Klick auf den Link zu prüfen, ob die URL plausibel und vertrauenswürdig ist. Hierzu bedarf es, jedenfalls im beruflichen Kontext, zunächst einer Sensibilisierung durch entsprechende Anti-Phishing-Awareness-Maßnahmen. Eine solche Prüfung ist jedoch je nach Umsetzungsform von Weiterleitungs-URLs nicht ohne Weiteres möglich, da sie z.B. durch den Einsatz externer Dienste erschwert oder verhindert wird. Es sollte demnach darauf geachtet werden, eine Umsetzungsform zu wählen, bei der die Möglichkeit der Prüfung der Ziel-URL gegeben ist. Darüber hinaus muss die vertrauenswürdige Verarbeitung anfallender Daten trotz Einsatz der URL-Weiterleitung gewährleistet werden.

Sowohl beim Einsatz von Weiterleitungs-URLs aus Security- als auch bei deren Verwendung aus Marketinggründen ist daher die Verwendung eines internen Dienstes der eines externen Dienstleisters als Zwischensatz der Weiterleitung sowie für das Ersetzen der Ziel-URL vorzuziehen. Für die Verwendung aus Marketinggründen, ist zudem die Bereitstellung des

[49] Müllmann, D., Veit, M., & Volkamer, M. (2022). Technische und Rechtliche Auseinandersetzung mit Weiterleitungs-URLs in E-Mails aus Security-Gründen. 52. GI-Jahrestagung, Hamburg, 26.-30.09. 2022.

Weiterleitungsdienstes auf dem eigenen Server zu präferieren, da hierdurch eine zu den Absender*innen passende Domain zum Einsatz kommt und kein Konflikt zu gängigen Anti-Phishing-Awareness-Maßnahmen entsteht.