D. Demmler, D. Krupka, H. Federrath. (Hrsg.): INFORMATIK 2022,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2022 601

Technische und Rechtliche Auseinandersetzung mit Weiterleitungs-URLs in E-Mails aus Security-Gründen

Dirk Müllmann[1], Maxime Veit[2], Melanie Volkamer [3]

Abstract: Häufig sind Links in E-Mails eingebunden, um Empfänger*innen einfach auf Webseiten oder Webseiteninhalte hinweisen zu können. Dazu wird hinter einem Link die entsprechende URL (auch Webadresse genannt) hinterlegt. 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 in Form von Weiterleitungs-URLs, die der Mailserver der Empfänger*innen aus Security-Gründen integriert, und anderseits in solcher, bei der die Weiterleitungs-URL von Absender*innen aus Marketinggründen verwenden werden. Ziel dieses Aufsatzes ist es, die Gruppe der Weiterleitungs-URLs aus Security-Gründen aus technischer und rechtlicher Sicht zu untersuchen und Empfehlungen für ihren Einsatz abzuleiten.

Keywords: URL-Security-Check, E-Mail, IT-Sicherheit, Datenschutz, Weiterleitungs-URL

1 Beschreibung

Die Möglichkeit, Links in E-Mails einzubetten, birgt den Vorteil der schnellen Auffindbarkeit konkreter Webseiten. Sie hat aber auch Nachteile: Angreifer*innen, häufig als Phisher*in bezeichnet, verschicken authentisch wirkende E-Mails, bei denen hinter den Links Phishing-URLs hinterlegt sind. Klicken Empfänger*innen auf einen solchen Link, führt die URL sie zu einer Phishing-Webseite. Diese versucht entweder Schadsoftware auf das Gerät der Empfänger*innen zu laden oder versucht möglichst authentisch auszusehen, damit Empfänger*innen dort sensible Daten, wie z.B. die Login-Daten der Originalseite eingeben.

Diese Form des Cyber-Angriffs stellt eine zunehmende Gefahr für Unternehmen und Privatpersonen dar.[4] Dies liegt unter anderem daran, dass die E-Mails immer authentischer von den Angreifer*innen gestaltet werden und Phishing-Mails häufig nur noch an den URLs hinter den Links als solchen entlarvt werden können. Die URL wird an Desktop-

[1] Dirk Müllmann ist Wissenschaftlicher Mitarbeiter am Institut für die Entwicklung sicherer Systeme am KIT sowie an der Goethe-Universität Frankfurt/Main am Lehrstuhl von Prof. Spiecker gen. Döhmann.
[2] Maxime Veit ist Wissenschaftlicher Mitarbeiter am KIT bei der Forschungsgruppe SECUSO.
[3] Prof. Dr. Melanie Volkamer ist ordentliche Professorin am Karlruher Institut für Technologie (KIT) und Leiterin der Forschungsgruppe SECUSO.
[4] Wirtschaftsschutz 2021. (2021). bitkom. https://www.bitkom.org/sites/default/files/2021-08/bitkom-slides-wirtschaftsschutz-cybercrime-05-08-2021.pdf.

doi:10.18420/inf2022_49

Geräten und Laptops in der sog. Statusleiste und je nach E-Mail-Client zusätzlich in einem Tooltip angezeigt (siehe Abbildung 1). Auf mobilen Geräten ist es in der Regel möglich, durch ein längeres Berühren des Links an die Information zur URL zu gelangen.

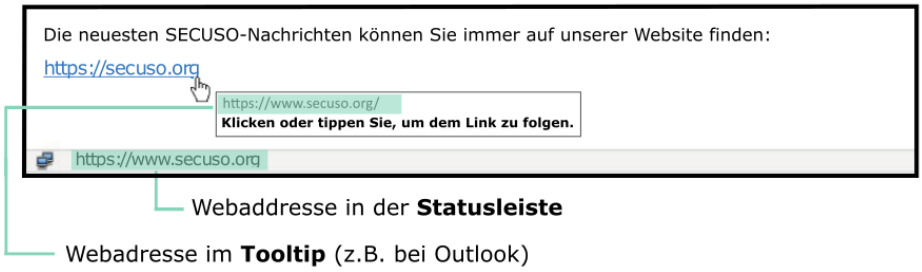

Abb. 1: Linkziel im Tooltip und Statusleiste

Eingehende E-Mails werden zwar üblicherweise beim Ankommen am Mailserver einem Security-Check unterzogen, der auch in der E-Mail enthaltene URLs prüft. Häufig sind die URLs zu diesem Zeitpunkt aber noch nicht als Phishing-URL bekannt. Somit kann die Mail nicht automatisch als Phishing-Mail erkannt und entsprechend behandelt werden. Als Konsequenz landen diese Phishing E-Mails in den Posteingängen der Empfänger*innen.

Um das Risiko, Opfer von Phisher*innen zu werden, zu minimieren, werden sowohl in der Praxis als auch in der Wissenschaft bisher zwei Ansätze verfolgt: (1) Die Einführung von Security-Awareness-Maßnahmen, mit denen die Teilnehmenden lernen, Phishing-Mails – insbesondere anhand der URL hinter den Links – zu erkennen[5] und (2) die Einführung von Security-Indikatoren, die Empfänger*innen helfen die URL vor dem Klicken des Links zu prüfen.[6] Zunehmend setzen Unternehmen und Organisationen auch einen dritten Ansatz ein: (3) Die Ziel-URLs werden durch entsprechende Security-Weiterleitungs-URLs ersetzt. Dies kann entweder vor oder nach Zustellung der E-Mail stattfinden. Entweder wird der Security-Check so erweitert, dass der Mailserver eine E-Mail nach ihrem Eingang zunächst wie bisher überprüft, im Fall der Zustellung der E-Mail aber alle Ziel-URLs durch entsprechende Weiterleitungs-URLs ersetzt, oder die E-Mail

[5] Vgl. Reinheimer, B. M., Aldag, L., Mayer, P., Mossano, M., Düzgün, R., Lofthouse, B., Von Landesberger, T., & Volkamer, M. (2020). An investigation of phishing awareness and education over time: When and how to best remind users [PDF]. https://doi.org/10.5445/IR/1000122566 ; Vgl. Tschakert, K. F., & Ngamsuriyaroj, S. (2019). Effectiveness of and user preferences for security awareness training methodologies. Heliyon, 5(6), e02010. https://doi.org/10.1016/j.heliyon.2019.e02010.

[6] Vgl. Volkamer, M., Renaud, K., Reinheimer, B., & Kunz, A. (2017). User experiences of TORPEDO: TOoltip-poweRed Phishing Email DetectiOn. Computers & Security, 71, 100–113. https://doi.org/10.1016/j.cose.2017.02.004 ; Vgl. Petelka, J., Zou, Y., & Schaub, F. (2019). ; Put Your Warning Where Your Link Is: Improving and Evaluating Email Phishing Warnings. Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 1–15. https://doi.org/10.1145/3290605.3300748.

wird zugestellt und die Ersetzung der Ziel-URLs erfolgt erst bei der Anzeige der E-Mail im E-Mail-Client oder im Webbrowser.

Gegenstand der vorliegenden Untersuchung ist der dritte Ansatz, das Ersetzen der Ziel-URLs hinter Links durch Security-Weiterleitungs-URLs. Hierbei wird nach dem Klick auf den Link und vor der Weiterleitung an die Ziel-URL diese zunächst durch einen URL-Security-Check geprüft und nur dann aufgerufen, wenn die Ziel-URL als niedriges Risiko eingestuft wird. Grundsätzlich kann der Security-Check von dem Anbieter, der auch den Mailserver betreibt, oder von einem externen Anbieter durchgeführt werden.

Abb. 2: Weiterleitungs-URL in Statusleiste und Ziel-URL im Tooltip

Um vor dem Aufruf der Ziel-URL den URL-Security-Check durchführen zu können, wird im vorderen Teil der Security-Weiterleitungs-URL (d.h. insbesondere der Bereich der Second-Level-Domain und der Top-Level-Domain) auf den Server, der diesen URL-Security-Check durchführt, verwiesen. Dieser Teil ist somit in jeder Security-Weiterleitungs-URL identisch. Der hintere Teil der URL, d.h. die Information im Pfad oder Query, ist jeweils unterschiedlich. Je nach eingesetztem URL-Security-Check kann die Ziel-URL im hinteren Teil der URL noch enthalten sein. Falls nicht, sieht der hintere Teil der URLs wie eine zufällige Zeichenfolge aus. Je nach Umsetzungsform des E-Mail-Clients wird im Tooltip entweder die ursprüngliche Ziel-URL angezeigt und die Security-Weiterleitungs-URL ist nur in der Statusleiste zu sehen (siehe Abbildung 2) oder die Empfänger*innen haben nur Zugriff auf die Security-Weiterleitungs-URL hinter dem Link, nicht jedoch auf die Ziel-URL (siehe Abbildung 3).

Abb. 3: Weiterleitungs-URL in Statusleiste und im Tooltip

Durch die Verwendung des URL-Security-Checks wird die Wahrscheinlichkeit erhöht, Phishing-URLs zu entdecken und deren Aufruf zu verhindern. Der Vorteil gegenüber dem

Security-Check vor der Zustellung der E-Mail durch den Mailserver ist, dass in der Zwischenzeit die Ziel-URL als Phishing-URL bekannt geworden sein kann. Allerdings bietet auch dies keinen 100%igen Schutz. Insbesondere, wenn E-Mails unmittelbar nach dem Erhalt der Nutzer*innen bearbeitet werden, ist es fraglich, ob eine URL in der kurzen Zeitspanne als Phishing-URL gemeldet wird und der URL-Security-Check zu einem anderen Ergebnis kommt als der ursprüngliche Security-Check.

2 Technische Bewertung

In diesem Unterkapitel wird der Ansatz aus technischer Sicht bewertet, wobei der Fokus auf Security und Usability Problemen liegt.

2.1 Zusammenspiel mit Security-Awareness-Maßnahmen

Im Rahmen von Security-Awareness-Maßnahmen wird erklärt, dass viele Phishing-Mails an der Plausibilität von Absender*innen und Inhalt erkannt werden können und dass alle Phishing-Mails mittels Überprüfung der URL hinter dem Link entlarvt werden können. Für diese Überprüfung wird erläutert, dass es bei der Kontrolle der URL insbesondere auf die Prüfung der Kombination aus Second-Level-Domain und Top-Level-Domain (dem sog. Wer-Bereich) ankommt (siehe Abbildung 4).[7] Dieses Erkennungsmerkmal ist jedoch hinfällig, wenn die Ziel-URLs nicht angezeigt werden, weil sie durch Weiterleitungs-URLs ersetzt wurden, die immer aus der gleichen Kombination von Second-Level-Domain und Top-Level-Domain bestehen, da sie immer zum gleichen URL-Security-Check führen. Dies gilt je nach Umgebung für alle URLs bzw. für diejenigen, die in weitergeleiteten E-Mails sind.

Abb. 4: Kombination aus Second-Level-Domain und Top-Level-Domain

Die Awareness-Maßnahmen müssen also um Hinweise zur Funktionsweise des neuen URL-Security-Checks erweitert werden. Für den Fall, dass Adressat*innen der Security Maßnahmen nur E-Mails an einem E-Mail-Client lesen, der im Tooltip die ursprüngliche Ziel-URL und die Weiterleitungs-URL in der Statusbar anzeigt (siehe Abbildung 2), kann die Erklärung der Security-Awareness-Maßnahme zur Prüfung von URLs beibehalten werden, solange es sich nicht um weitergeleitete E-Mails handelt. Für diese Fälle sowie

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

für den Fall, dass Adressat*innen E-Mails auch in mobilen Umgebungen abrufen, in denen ihnen die Ziel-URL nicht angezeigt wird, müssten die Inhalte der Security-Awareness-Maßnahme angepasst werden.

Falls die Weiterleitungs-URL so gestaltet ist, dass die Ziel-URL im hinteren Teil der URL zu finden ist, sollte in der Security-Awareness-Maßnahme erklärt werden, wie die URL und insbesondere der Wer-Bereich im entsprechenden hinteren Teil der Weiterleitungs-URL geprüft werden kann. Zudem könnte das Problem auftreten, dass der hintere Teil der Weiterleitungs-URL (und damit der für die Prüfung relevante Aspekt) möglicherweise nicht vollständig in der Statusleiste zu sehen ist, da der Platz in der Statusleiste für die komplette URL nicht ausreicht. Auch hierauf ist in der Security-Awareness-Maßnahme hinzuweisen.

Falls die Weiterleitungs-URL hingegen keine Informationen über die Ziel-URL enthält und diese auch nicht angezeigt wird, ist die Erklärung zur Prüfung der URL vor dem Öffnen eines Links nicht mehr relevant und sollte aus der Security-Awareness-Maßnahme entfernt werden. In diesem Fall würden die Adressat*innen nur noch das Absender-Feld und den Inhalt der E-Mail auf Plausibilität prüfen und müssten sich im Übrigen auf den URL-Security-Check verlassen. Dieser kann die Ziel-URL anders als Empfänger*innen der E-Mail nicht im erweiterten Kontext auf Plausibilität prüfen, also etwa, ob der Link zur restlichen E-Mail passt oder ob Empfänger*innen die Webseite hinter der Ziel-URL kennen. Dies schränkt die Empfänger*innen von E-Mails in der Umsetzung eines effektiven Schutzes vor Phishing-Angriffen ein. Darüber hinaus kann es, sofern Security-Awareness-Maßnahmen bereits durchgeführt wurden, für die Anwender*innen verwirrend sein und sich negativ auf die Effektivität der Maßnahme auswirken, wenn erklärt wird, dass die zuvor erlernte eigene Überprüfung mit dem neuen Security-Check nicht mehr angewendet werden kann. Im schlimmsten Fall hat dies zur Folge, dass Empfänger*innen sich blind auf den URL-Security-Check verlassen und jeden Link unreflektiert anklicken. Die menschliche Firewall zur Prüfung der Links vor dem Klick fiele dann weg. Für diesen Fall gilt außerdem, dass ein sog. Mismatch zwischen einer im Linktext angegebenen URL und einer Ziel-URL (siehe Abbildung 5), anders als in der Security-Awareness-Maßnahme hingewiesen, nicht mehr zwangsläufig auf eine Phishing-URL hindeutet, sondern in der ständigen Ersetzung der Ziel-URL durch den URL-Security-Check begründet ist. Daher ist dieser Inhalt der Security-Awareness-Maßnahme zu aktualisieren – ggf. mit den bereits genannten negativen Konsequenzen.

Abb. 5: Link Mismatch zwischen Link-URL und Ziel-URL. Phisher*innen versuchen die Opfer durch eine vertrauenswürdige URL im Text in die Irre zu führen.

Insgesamt ist vor der Einführung von Security-Weiterleitungs-URLs also zunächst zu prüfen, inwieweit Security-Awareness-Maßnahmen gegenläufig sind und angepasst werden müssen.

Eine weitere große Herausforderung im Kontext der Einführung eines URL-Security-Checks besteht darin, dass bei Adressat*innen nicht der Eindruck entstehen sollte, dass durch die Einführung des URL-Security-Checks alle Links sicher angeklickt werden können, weil der URL-Security-Check die Prüfung übernimmt. Wenn es nicht gelingt, dies klar zu kommunizieren, würde das Security-Niveau durch die Einführung des URL-Security-Checks sogar reduziert und nicht gesteigert werden.

Hinzu kommt, dass Studien fehlen, die untersuchen, ob Nutzer*innen nach Security-Awareness-Maßnahmen Phishing-URLs besser erkennen als ein solcher URL-Security-Check. Es ist anzunehmen, dass die Ergebnisse solcher Studien stark vom Kontext, wie etwa unterschiedlicher Nutzergruppen und ob zusätzlich die Ziel-URL verfügbar ist oder nicht, abhängen und die Frage nur im Einzelfall beantwortet werden kann.

2.2 Probleme durch weitergeleitete bzw. beantworte E-Mails

Dadurch, dass der URL-Security-Check die URL hinter dem Link vor der Zustellung der E-Mail verändert, wird im Falle einer Weiterleitung bzw. Beantwortung der E-Mail die Weiterleitungs-URL zur Ziel-URL. Wenn diese E-Mails an Empfänger*innen geschickt werden, die nicht den gleichen URL-Security-Check nutzen, dann sorgt die Ziel-URL (ursprüngliche Weiterleitungs-URL) hinter den Links für Irritationen, da je nach Form des Links ein Link-Mismatch festgestellt wird und die Ziel-URL nicht wie gewohnt überprüft werden kann.

Das reduziert das Security-Niveau der Empfänger*innen. Wenn diese auf den Link klicken, wird die URL zunächst auch vom URL-Security-Check der Absender*innen geprüft. Sie können aber in Ermangelung von Informationen über das Angebot nicht einschätzen, inwieweit sie sich auf diesen URL-Security-Check verlassen können. Dieses Problem kann jedoch gelöst werden, indem die Weiterleitungs-URL beim Verschicken senderseitig wieder in die ursprüngliche Ziel-URL umgewandelt wird.

2.3 Probleme mit dem Einsatz von S/MIME und PGP

Einige Unternehmen und Privatpersonen nutzen zum Signieren und Verschlüsseln ihrer E-Mails S/MIME oder PGP. Dies erlaubt es Sender*innen E-Mails digital zu signieren, selbst wenn Empfänger*innen kein entsprechendes Schlüsselpaar besitzen. Wenn nun eine digital signierte E-Mail beim Mailserver ankommt und der Security-Check entscheidet, dass die E-Mail zugestellt wird, würde, sofern die Ersetzung nicht erst im E-Mail-Client realisiert wird, dieser auch hier die URLs ersetzen. Dies hat allerdings zur Folge, dass E-Mail-Clients eine Security-Intervention anzeigen, weil die digitale Signatur durch die nachträgliche Veränderung der E-Mail ungültig wird. Nun könnte zwar im Rahmen der

Security-Awareness-Maßnahme erklärt werden, dass dies eine Nebenwirkung des neuen URL-Security-Checks ist, allerdings können solche Äußerungen – wie oben erwähnt – auf Empfänger*innen verwirrend wirken. Alternativ könnte die Funktionalität des Clients angepasst werden, sodass eine entsprechende Security-Intervention nicht mehr angezeigt wird bzw. die Überprüfung der Signatur so angepasst wird, dass zunächst die Ziel-URL wieder in die E-Mail integriert und dann die Signatur überprüft wird. Weiterhin könnte der Security-Check des Mailservers auch so konfiguriert werden, dass die Ziel-URL bei digital signierten E-Mails nicht durch eine Weiterleitungs-URL ersetzt wird. Dies könnte bei Empfänger*innen aber erneut zu Verwirrung führen, weil diese teilweise E-Mails mit und teilweise ohne Weiterleitungs-URL vorfinden. Dies müsste daher in der Security-Awareness-Maßnahme im Rahmen der Einführung des neuen URL-Security-Checks erläutert werden.

Darüber hinaus ist das Einführen von Weiterleitungs-URLs durch den Security-Check am Mailserver nur möglich, wenn E-Mails nicht verschlüsselt sind. Sollen S/MIME oder PGP eingesetzt werden, um E-Mails zu verschlüsseln, dann könnte das Einsetzen von Weiterleitungs-URLs aufseiten der E-Mail-Clients[8] anstelle auf der des Mailservers Abhilfe schaffen. Dies hätte jedoch den Nachteil, dass nur besagter E-Mail-Client verwendet werden kann, der über die entsprechend notwendige Funktionalität verfügt. Diese Funktionalität müsste entweder durch den E-Mail-Client nativ unterstützt oder durch eine entsprechende Erweiterung, wie dies etwa bei Thunderbird und Outlook möglich ist,[9] ergänzt werden. Diese Möglichkeit besteht jedoch insbesondere für mobile E-Mail-Clients wie Apple-Mail oder Gmail für Android nicht, sodass der Nutzer mit solchen E-Mail-Clients nicht durch den URL-Security-Check geschützt, aber die menschliche Prüfung auch nicht behindert wäre.

2.4 URL-Security-Check erhält Passwort-Reset-Links

Bei vielen Online-Diensten ist es möglich Passwörter zurückzusetzen. Hierzu wird häufig eine E-Mail mit einem entsprechenden Passwort-Reset-Link verschickt. Klicken Empfänger*innen auf diesen Link so erhält der URL-Security-Check ebenfalls die URL um das Passwort zurückzusetzen. Die Betreiber*innen und/oder Entwickler*innen des URL-Security-Checks könnten sich so Zugriff auf die entsprechenden Konten verschaffen. Dies ist besonders kritisch, wenn die URL-Security-Check-Betreiber*innen/-Entwickler*innen andere Personen sind als die Mailserver-Betreiber*innen. Hier ist ein großes Maß an Vertrauen in die URL-Security-Check-Betreiber*innen/Entwickler*innen notwendig, dass diese lediglich die URL gegen Phishing-Datenbanken prüfen und nicht weiterverwenden bzw. speichern.

[8] E-Mail-Clients umfassen so wohl solche die über den Browser aufgerufen werden (Webmail), als auch lokale Programme.

[9] E-Mail-Client Thunderbird erweiterbar durch Add-ons. https://addons.thunderbird.net/de/thunderbird/ ; E-Mail Client Outlook erweiterbar durch Add-Ins. https://docs.microsoft.com/de-de/office/dev/add-ins/outlook/outlook-add-ins-overview .

2.5 Zwischenfazit

Aus technischer Sicht entstehen diverse Probleme beim Einsatz des herkömmlichen Mailserver-seitigen URL-Security-Checks. Zunächst sind die herkömmlichen Security-Awareness-Maßnahmen nicht mehr ausreichend und müssten, soweit dies möglich ist, angepasst werden. Zudem können Probleme bei der Weiterleitung und Beantwortung von E-Mails entstehen und der sinnvolle Einsatz von digital signierten E-Mails verhindert werden. Zuletzt ist die Ausführung des URL-Security-Checks aufseiten des Mailservers bei eingesetzter E-Mail-Verschlüsselung nicht möglich.

Um den eben genannten technischen Problemen entgegenzutreten und einen Mehrwert mittels URL-Security-Checks für die IT-Sicherheit bieten zu können, sollte der Einsatz wie folgt erfolgen: (1) die Ersetzung der URL sollte lokal im Client erfolgen, sodass es keine Probleme mit S/MIME bzw. PGP gibt und bei einer Weiterleitung bzw. Beantwortung der E-Mail nur noch die ursprüngliche Ziel-URL enthalten ist; (2) im E-Mail-Client sollten beide URLs angezeigt werden, wie es beispielsweise in Abbildung 2 gezeigt wird; (3) im Rahmen der Awareness-Maßnahmen sollte sichergestellt werden, dass die Empfänger*innen von E-Mails verstehen, dass sie nach wie vor angehalten sind, die Ziel-URL vor dem Klicken des Links zu prüfen.

3 Rechtliche Bewertung

Das Ersetzen einer URL hinter einem Link in einer E-Mail aus Gründen der IT-Sicherheit berührt sowohl den Schutz personenbezogener Daten als auch das Telekommunikationsgeheimnis. Durch die Nutzung könnte sogar gegen strafrechtliche Normen, insbesondere die §§ 206 und 303a StGB[10], verstoßen werden.[11] Die Frage der Zulässigkeit und die rechtlich zu betrachtenden Probleme richten sich wesentlich danach, in welchem Umfeld ein solches System eingesetzt wird. Hierbei ist insbesondere zwischen dem Einsatz für E-Mails im privaten Kontext und am Arbeitsplatz zu unterscheiden. Um eine inhaltliche Konzentration, auf die im Kontext von Weiterleitungs-URLs relevanten Probleme erreichen zu können, soll im Rahmen der rechtlichen Analyse von der Prämisse ausgegangen werden, dass die Funktionalität des eingesetzten URL-Security-Checks strikt auf das Erkennen von Links in E-Mails, die Umwandlung in Weiterleitungs-URLs sowie auf die Weiterleitung über den sicheren Link beschränkt ist. Von der Vornahme anderer Analysen soll somit ebensowenig ausgegangen werden, wie von einer missbräuchlichen Nutzung von Links zur Passworterneuerung. Für die Betrachtung soll zudem

[10] Danach ist die Verletzung des Fernmeldegeheimnisses unter den Voraussetzungen des § 206 StGB strafbar. Ebenso kann die Löschung, Unterdrückung, das Unbrauchbarmachen und Verändern von Daten gemäß § 303a StGB strafbar sein.

[11] Vgl. OLG Karlsruhe, Beschl. v. 10.01.2005, 1 Ws 152/04, Rn. 18 ff.; Heidrich/ Tschoepe, MMR 2004, 75, 76 ff.; 79 f.; Eckhardt in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 4. Aufl., 2019, §88 TKG, Rn. 67; Schröder in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl., 2019, Kap. 3, Rn. 39; Sassenberg/Mantz, BB 2013, 889, 892 f.

angenommen werden, dass die zuvor ausgesprochenen Empfehlungen zum optimalen Einsatz von URL-Security-Checks berücksichtigt werden, sodass dessen Durchführung das Potenzial für eine Verbesserung der IT-Sicherheit bietet. Problematisch ist dabei letztlich nur die Analyse und Veränderung der Links, da wir im Folgenden davon ausgehen, dass eine weitere Speicherung und Nutzung z.B. zur Auswertung von Angaben, wie wohin die ursprünglichen Links führten, nicht erfolgt. Vor diesem Hintergrund steht rechtlich somit nur in Frage, ob eine E-Mail von dem System auf das Vorhandensein von Links ausgewertet und solche durch Security Links ersetzt werden dürfen.

3.1 Einsatz im privaten Umfeld

Der Einsatz im privaten Kontext und die damit verbundene Beeinträchtigung des Telekommunikationsgeheimnisses und des Schutzes personenbezogener Daten kann durch die Einwilligung der*s E-Mail-Empfängers*in gerechtfertigt werden, die diese*r regelmäßig durch seine*ihre Zustimmung zu den Nutzungsbedingungen eines E-Mail-Providers oder -Clients erteilt. Erforderlich ist insoweit selbstverständlich, dass die Anforderungen an die wirksame Erteilung einer datenschutzrechtlichen Einwilligung gewahrt werden.[12] Neben den Rechten des*r Empfängers*in werden durch das Ersetzen eines Links jedoch auch die Rechte des*r Absenders*in, als anderem Teil der Kommunikation, betroffen. Dabei ist in Fällen, in denen eine Veröffentlichung von E-Mails ohne die Zustimmung des*r Absenders*in oder gar gegen seinen*ihren Willen erfolgt, anerkannt, dass sowohl eine Persönlichkeitsrechtsverletzung[13] als, bei ausreichender Schöpfungshöhe, auch eine Urheberrechtsverletzung[14] im Raum stehen kann. Hierfür wird im Wesentlichen auf die Interessenlagen in den anerkannten Fallkonstellationen der allgemeinen Zugänglichmachung von Briefen rekurriert.[15] Anders als in den gerichtlich entschiedenen Konstellationen findet im vorliegenden Fall jedoch keine Veröffentlichung der Inhalte und somit keine Zugänglichmachung zu einem unbestimmten Personenkreis statt. Dies lässt urheberrechtliche Bedenken ausscheiden. Zugleich wird das Interesse an der Vertraulichkeit des Wortes, aus dem sich die Verletzung des Persönlichkeitsrechts maßgeblich herleitet,[16] durch die Ersetzung der URL hinter dem Link, wenn überhaupt, nur unwesentlich beeinträchtigt. Der Ersetzung wird unabhängig davon, ob später überhaupt auf den Link geklickt werden wird, durchgeführt.

[12] Vgl. die Definition der Einwilligung in Art. 4 Nr. 11 DSGVO, wobei insbesondere die Freiwilligkeit und die Informiertheit der Einwilligung in der Praxis problematisch sein können (hierzu: Uecker, ZD 2019, 248; Klement in: Simitis/Hornung Spiecker gen. Döhmann, DSGVO, 2019, Art. 7 Rn. 48 f.; 73 ff.).

[13] LG Saarbrücken, Urt. v. 16.12.2011, 4 O 287/11; OLG Stuttgart, Urt. v. 10.11.2010, 4 U 96/10; LG Köln, Urt. v. 28.05.2008, 28 O 157/08; OLG Hamburg, Beschl. v. 04.02.2013; 7 W 5/13.

[14] Wissenschaftlicher Dienst des Bundestages, Die unbefugte Veröffentlichung privater Chat-Nachrichten Dritter, 2021, S. 12 f.

[15] LG Saarbrücken, Urt. v. 16.12.2011, 4 O 287/11; OLG Stuttgart, Urt. v. 10.11.2010, 4 U 96/10; LG Köln, Urt. v. 28.05.2008, 28 O 157/08.

[16] LG Saarbrücken, Urt. v. 16.12.2011, 4 O 287/11; OLG Hamburg, Beschl. v. 04.02.2013; 7 W 5/13.

Dies steigert die Tiefe des Eingriffs. Der tatsächliche Inhalt der Nachricht kann dabei andererseits jedoch ebenso wenig erfasst werden wie deren Absender*in. Selbst wenn eine Einwilligung des*r Absenders*in in eine automatische Ersetzung seiner*ihrer Links nicht erfolgt ist und auch nicht einfach angenommen werden kann, kann sie aufgrund einer vorzunehmenden Interessenabwägung erfolgen, wenn das Interesse des*r Empfängers*in, der seine*ihre Einwilligung erteilt hat, die Interessen des*r Absenders*in überwiegen.[17] Dies wird in der vorliegenden Konstellation regelmäßig der Fall sein. So findet das Ersetzen der URLs hinter Links automatisiert statt, wobei keine Analyse des eigentlichen Mailinhalts erfolgt. Die Vertraulichkeit der Kommunikation wird somit rein formal, aber nicht materiell berührt. Dem steht ein wichtiges Interesse des*r Empfängers*in gegenüber, der*die sich durch den Einsatz des Systems vor der Infiltration durch Schadsoftware schützen möchte. Trotz der unklaren Studienlage in Bezug auf die tatsächlichen Auswirkungen der Verwendung eines URL-Security-Checks (vgl. 1.2.1), kann dieser bei korrekter Anwendung (vgl. Empfehlungen in 1.2.5) einen echten Beitrag zur Verbesserung des IT-Sicherheit leisten. In weiterer Konsequenz können so sogar weitere IT-Systeme geschützt werden, indem keine Weiterverbreitung von Schadsoftware, z.B. über Adressbücher, erfolgt. Dem Interesse der IT-Sicherheit ist somit, nicht nur, aber insbesondere aus Empfänger*innensicht, einiger Stellenwert zuzuschreiben.

Datenschutzrechtlich kann ebenfalls auf die erteilte Einwilligung des*r Empfängers*in abgestellt werden. Der*die Absender*in einer E-Mail wird regelmäßig auch keine datenschutzrechtliche Einwilligung gegenüber dem Anbieter oder Client des*r E-Mail-Empfängers*in abgegeben haben. Vor dem Hintergrund der zu den Persönlichkeitsrechten des*r Absenders*in gemachten Ausführungen ergäbe sich eine datenschutzrechtliche Verarbeitungsgrundlage jedoch aus dem Überwiegen der berechtigten Interessen des*r Empfängers*in im Zusammenhang mit der IT-Sicherheit seiner*ihrer informationstechnischen Systeme gemäß Art. 6 Abs. 1 lit. f) DSGVO.

3.2 Einsatz am Arbeitsplatz

Es erscheint jedoch fraglich, ob der Einsatz eines entsprechenden Systems am Arbeitsplatz rechtlich zulässig ist, da zu seiner Funktion der Zugriff auf die E-Mail-Inhalte der Mitarbeitenden erforderlich ist.

Auch wenn dies zunehmend kritisiert wird,[18] besteht in Rechtsprechung und Literatur Einigkeit darüber, dass der*die Arbeitgeber*in den Inhalt einer E-Mail nur unter strengen Voraussetzungen einsehen darf. Dabei wird unterschieden, ob nur die dienstliche Nutzung von E-Mails am Arbeitsplatz erlaubt ist oder, ob der*die Arbeitnehmer*in das Mailsystem

[17] LG Saarbrücken, Urt. v. 16.12.2011, 4 O 287/11.

[18] Seifert in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 88 DSGVO, Rn. 150.

auch privat nutzen darf. [19] Bei der rein dienstlichen Nutzung darf der*die Arbeitgeber*in auf das Konto zugreifen, die Verbindungsdaten prüfen und sogar den Inhalt der dienstlichen E-Mails zur Kenntnis nehmen.[20] Ist dagegen auch die private Nutzung des Accounts erlaubt, gilt der*die Arbeitgeber*in als Anbieter*in von Telekommunikationsdiensten im Sinne des § 3 Nr. 1 TKG und ist gegenüber den Mitarbeiter*innen gemäß § 3 Abs. 1, 2 Nr. 2 TTDSG zur Wahrung des Fernmeldegeheimnisses verpflichtet.[21] In diesen Fällen ist es ihm*ihr verwehrt, auf den Mailverkehr seiner Mitarbeitenden zuzugreifen.[22] Dies gilt umso mehr als § 3 Abs. 3 TTDSG nunmehr festlegt, dass ein über das für den Schutz technischer Systeme erforderliche Maß hinausgehendes Kenntnisverschaffen von Inhalt und Umständen der Telekommunikation für Erbringer*innen von Telekommunikationsdienstleistungen verboten und die Verwendung von auf diesem Weg erlangten Informationen nur in engen Grenzen möglich ist. In der Literatur wird vorgeschlagen, die Mitarbeitenden aufzufordern, dienstliche und private E-Mails getrennt zu führen und zu speichern.[23] Allerdings ist eine Unterscheidung zwischen privater und geschäftlicher Korrespondenz ohne deren Mitwirkung nach wie vor nicht möglich.[24]

Der vorliegende Fall weist jedoch Parallelen zum Problem der Filterung von E-Mails durch Spam-Filter auf. In einem Kontext, in dem nur dienstliche E-Mails erlaubt sind, ist

[19] Seifert in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 88 DSGVO, Rn.148; Byers in: Weth/Herberger/Wächter/Sorge (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Kap. X., Rn. 21; Schröder in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl., 2019, Kap. 3, Rn. 39; Reichold, in Kiel/Lunk/Oetker, Münchener Handbuch zum Arbeitsrecht, Band I: Individualarbeitsrecht, 4. Aufl.,2018, §55, Rn. 35.

[20] Seifert in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 88 DSGVO, Rn. 149; Reichold, in Kiel/Lunk/Oetker, Münchener Handbuch zum Arbeitsrecht, Band I: Individualarbeitsrecht, 4. Aufl., 2018, §55, Rn. 35; Byers in: Weth/Herberger/Wächter/Sorge (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Kap. X., Rn. 22.

[21] Seifert in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 88 DSGVO, Rn. 150; Reichold, in Kiel/Lunk/Oetker, Münchener Handbuch zum Arbeitsrecht, Band I: Individualarbeitsrecht, 4. Aufl., 2018, §55, Rn. 35.

[22] Seifert in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 88 DSGVO, Rn. 150; Reichold, in Kiel/Lunk/Oetker, Münchener Handbuch zum Arbeitsrecht, Band I: Individualarbeitsrecht, 4. Aufl., 2018, §55, Rn. 35; Schröder in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl., 2019, Kap. 3, Rn. 39; Byers in: Weth/Herberger/Wächter/Sorge (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Kap. X., Rn. 21 f.

[23] Schröder in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl., 2019, Kap. 3, Rn. 42; Byers in: Weth/Herberger/Wächter/Sorge (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Kap. X., Rn. 22.

[24] Byers in: Weth/Herberger/Wächter/Sorge (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Kap. X., Rn. 22.

eine Filterung angesichts der oben beschriebenen Rechtslage unproblematisch.[25] Soweit aber auch privater Mailverkehr erlaubt ist, muss wiederum das Fernmeldegeheimnis beachtet werden.[26] Die sofortige Löschung jeder Spam-Mail wird daher als problematisch angesehen.[27] Lediglich die Löschung von E-Mails, die eine Gefahr für das IT-System des Unternehmens darstellen, weil sie Schadsoftware enthalten, ist aus Sicherheitsgründen zulässig.[28] In diesen Fällen sollten daher so genannte Quarantänelösungen vorgesehen werden, bei denen Spam-Mails in einen separaten Ordner verschoben werden und dort abrufbar sind, oder es besteht die Möglichkeit, den Betreff einer Nachricht mit dem Zusatz „Spam“ zu kennzeichnen.[29] Auf diese Weise werden zwar der Auffindeort der E-Mail oder aber ihr Betreff geändert, jedoch werden sie und ihr Inhalt weder unterdrückt, noch werden die in ihr enthaltenen Informationen insofern verändert oder verfälscht, als die ursprüngliche Nachricht nicht mehr transportiert würde, so dass auch der strafrechtliche Schutz des Fernmeldegeheimnisses nicht betroffen ist.[30]

Wendet man die betrachteten Grundsätze auf die vorliegende Fallgestaltung an, so kann man zu dem Schluss kommen, dass ihr Einsatz in Fällen, in denen nur eine dienstliche Nutzung am Arbeitsplatz zulässig ist, unproblematisch erscheint. Sind jedoch auch private E-Mails betroffen, muss der*die Arbeitgeber*in wiederum das Fernmeldegeheimnis wahren. Grundsätzlich dürfte er*sie daher nicht auf den Mailverkehr seiner*ihrer Angestellten zugreifen. Allerdings ist er*sie als Diensteanbieter*in im Sinne des § 3 Nr. 1 TKG auch nach § 165 Abs. 1 S. 1 TKG verpflichtet, angemessene technischen Vorkehrungen und sonstigen Maßnahmen zum Schutz des Fernmeldegeheimnisses und gegen Verletzungen des Schutzes personenbezogener Daten zu treffen.[31] Dies sieht auch § 3 Abs. 3 S. 1 TTDSG explizit als Ausnahme vom Fernmeldegeheimnis vor. Ein optimal

[25] Sassenberg/Mantz, Die (private) Emailnutzung im Unternehmen, BB 2013, 889, 892; Fuhlrott, in: Kramer, IT-Arbeitsrecht, 2. Aufl., 2019, Kap. B, Rn. 520 f.

[26] Sassenberg/Mantz, Die (private) Emailnutzung im Unternehmen, BB 2013, 889, 892; Fuhlrott, in: Kramer, IT-Arbeitsrecht, 2. Aufl., 2019, Kap. B, Rn. 520 f.

[27] Sassenberg/Mantz, Die (private) Emailnutzung im Unternehmen, BB 2013, 889, 892 f.; Eckhardt, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 4. Aufl., 2019, §88 TKG, Rn. 62; Fuhlrott, in: Kramer, IT-Arbeitsrecht, 2. Aufl., 2019, Kap. B, Rn. 520; vgl. auch: OLG Karlsruhe, Beschl. v. 10.01.2005, 1 Ws 152/04, Rn. 21 ff.

[28] Sassenberg/Mantz, Die (private) Emailnutzung im Unternehmen, BB 2013, 889, 892; Sassenberg/Lammer, Zulässigkeit der Spam-Filterung im Unternehmen, DuD 2008, 461, 463; Heidrich/Schöpe, MMR 2004, 75, 78; Fuhlrott, in: Kramer, IT-Arbeitsrecht, 2. Aufl., 2019, Kap. B, Rn. 520 f.; OLG Karlsruhe, Beschl. v. 10.01.2005, 1 Ws 152/04, Rn. 25; VG Karlsruhe, Urt. v. 19.09.2007, 7 K 851/04, Rn. 23.

[29] Sassenberg/Mantz, Die (private) Emailnutzung im Unternehmen, BB 2013, 889, 892 f.

[30] Sassenberg/Mantz, Die (private) Emailnutzung im Unternehmen, BB 2013, 889, 892 f.; Heidrich/Tschoepe, Rechtsprobleme der E-Mail-Filterung, MMR 2004, 75, 78; OLG Karlsruhe, Beschl. v. 10.01.2005, 1 Ws 152/04, Rn. 22.

[31] Eckhardt, in: Geppert/Schütz (Hrsg.), BeckOK TKG, 4. Aufl., 2013, § 109, Rn. 15; Schommertz/Gerhardus, in: Scheuerle/Mayen, TKG, 3. Aufl., 2018, § 109, Rn. 3.

implementierter Security-Check hat das Potential vor schädlichen Links in E-Mails zu schützen, deren Folgen Datenverluste, die Infizierung ganzer IT-Systeme in Unternehmen und der Zugriff auf Informationen durch Unbefugte sind.

Problematisch erscheint im Rahmen dieser Schutzmaßnahme jedoch, dass der Inhalt einer E-Mail analysiert werden muss, um festzustellen, ob ein Link in der E-Mail enthalten ist. Es ist jedoch zu beachten, dass Spam-Filter auch den Inhalt (Body) der E-Mail heranziehen, um zu beurteilen, ob es sich um Spam handelt. Selbst dies erfolgt im vorliegenden Fall jedoch nicht, sodass weder Inhalt noch Absender*in analysiert, sondern nur Links identifiziert werden. Deren Inhalt, in Form der Weiterleitung zu einer bestimmten Zielseite, wird auch nicht so verändert, dass die durch sie transportierten Informationen verfälscht würden, da der ursprüngliche Link nicht gelöscht, sondern, wenn überhaupt nur durch ein Informationsfenster ergänzt wird. Damit bleibt auch der ursprüngliche Inhalt der E-Mail erhalten und wird nicht unterdrückt.

Ein weiterer kritischer Aspekt ist, dass nicht nur E-Mails mit schädlichen Links von der Analyse betroffen sind, sondern auch solche ohne Links oder mit Links, die nicht zu problematischen Seiten führen. Im Rahmen eines Spamfilters werden aber auch alle E-Mails, also auch die ungefährlichen, geprüft, um zwischen potentiell gefährlichen und nicht gefährlichen E-Mails zu unterscheiden. Wenn man vorher und ohne Prüfung einer E-Mail wüsste, ob sie potentiell gefährlich ist, bräuchte man keinen Filter. Eine Kategorisierung ist also nicht möglich, ohne jede E-Mail zu analysieren.

E-Mails enthalten in der Regel personenbezogene Daten, die bei der Auswertung auch vom Programm zumindest miterfasst werden. Es liegt daher auch eine Verarbeitung personenbezogener Daten im Sinne von Art. 2 Nr. 1, 2 DSGVO. Da das Programm am Arbeitsplatz eingesetzt werden soll, ist die Öffnungsklausel des Art. 88 Abs. 1 DSGVO auf den Beschäftigungskontext anwendbar. Vor diesem Hintergrund ist die maßgebliche Rechtsnorm daher § 26 BDSG. Solange keine Einwilligung des*r Arbeitnehmers*in vorliegt (vgl. § 26 Abs. 2 BDSG), muss die Verarbeitung der Daten daher erforderlich sein. Die Erforderlichkeit ist gegeben, wenn das Interesse an der Datenverarbeitung bei der Abwägung der widerstreitenden Interessen das Interesse an der Nichtverarbeitung der Daten überwiegt.[32] Im vorliegenden Zusammenhang steht also das Interesse des*r Arbeitsgebers*in an der Sicherheit und Integrität der informationstechnischen Systeme in seinem*ihrem Unternehmen dem Interesse der Arbeitnehmer*innen gegenüber, dass die sie betreffenden personenbezogen Daten nicht verarbeitet werden. Dies geschieht bei einem anwendungskonformen URL-Security-Check auch nicht, da sie weder als personenbezogene Daten erkannt, verstanden oder zugeordnet, noch gespeichert oder weiterverarbeitet werden. Vor diesem Hintergrund ist das Schutzbedürfnis des*r Arbeitnehmers*in deutlich geringer als das Interesse und die Pflicht des*r

[32] BT-Drs. 18/11325, S.97; Riesenhuber, in: Wolff/Brink (Hrsg.), BeckOK Dstenschutzrecht, 34. Ed. 01.11.2020, §26 BDSG, Rn. 113; Zöll, in: Taeger/Gabler (Hrsg.), DSGVO - BDSG, 3. Aufl., 2019, §26 BDSG, Rn. 23.

Arbeitgebers*in, die IT-Sicherheit seiner*ihrer Systeme mithilfe eines optimal implementierten URL-Security-Checks (siehe Empfehlungen in 1.2.5) zu gewährleisten.

Bei der Implementierung eines solchen Tools sollte der Betriebsrat beteiligt werden, da durch die Technik seine Rechte und Aufgaben berührt werden können, z.B. § 80 Abs. 1 Nr. 1, § 87 Abs. 1 Nr. 6 BetrVG. Da sich der Einsatz des Tools auf die Arbeitsabläufe am Arbeitsplatz der Arbeitnehmer*innen auswirkt, werden Informationspflichten des*r Arbeitgebers*in, § 81 Abs. 2 BetrVG,[33] sowie Vorschlagsrechte der Arbeitnehmer*innen, § 82 Abs. 1 BetrVG,[34] ausgelöst.

4 Fazit und Empfehlung

Die Nutzung von Weiterleitungs-URLs hat das Potenzial die IT-Sicherheit sowohl in Unternehmen als auch im privaten Bereich zu verbessern, sofern sie richtig umgesetzt und, im dienstlichen Kontext, in geeignete Security-Awareness-Maßnahmen eingebettet wird. Aus technischer Sicht sollte es den Empfänger*innen von E-Mails möglich sein, vor dem Klick auf den Link zu prüfen, ob die URL, die sie letztlich aufrufen wollen, plausibel und vertrauenswürdig ist. Hierzu bedarf es jedoch in den meisten Fällen einer entsprechenden Sensibilisierung durch Security-Awareness-Maßnahmen. Um die URL-Security-Checks durchführen zu können, ist es erforderlich eine Weiterleitungs-URL anstelle der Ziel-URL einzubinden. Dabei sollte weiterhin die Möglichkeit der Prüfung der Ziel-URL, sowie die vertrauenswürdige Verarbeitung anfallender Daten durch die URL-Weiterleitung gewährleistet werden. Auch ist für das Ersetzen der URL und die Weiterleitung die Verwendung eines internen Dienstes einem externen Dienstleister vorzuziehen. Wird ein externer Dienst verwendet, muss dieser insbesondere beim URL-Security-Check angesichts der potenziellen Einwirkungsmöglichkeiten besonders vertrauenswürdig und die Beschränkung der Funktionalität vertraglich geregelt sein.

Bei einer Weiterleitungs-URL kann zudem in geeigneter Weise die Ziel-URL im hinteren Teil lesbar enthalten sein. Dies ermöglicht in vielen Fällen weiterhin das Anwenden der Security-Awareness-Maßnahmen zur Prüfung der Ziel-URL, wobei Empfänger*innen den Aufbau der Weiterleitungs-URL für den verwendeten Dienst jedoch kennen und ihm vertrauen müssen. Zudem muss die URL vom E-Mail-Client in geeigneter Weise und ausreichender Länge angezeigt werden, sodass der Wer-Bereich der URL dargestellt wird. Dies ist jedoch nicht immer möglich. Daher ist für den URL-Security-Check eine Ersetzung seitens E-Mail-Client wie in Abschnitt 2.5 näher beschrieben zu empfehlen.

[33] Vgl. Kania, in: Müller-Glöge/Preis (Hrsg.), Erfurter Kommentar zum Arbeitsrecht, 21. Aufl, 2021, §81 BetrVG, Rn. 13; Werner, in: Rolfs/Giesen/Kreikebohm/Meßling/Udsching (Hrsg.), BeckOK Arbeitsrecht, 58. Ed., 01.12.2020, §81 BetrVG, Rn. 8.

[34] Vgl. Kania, in: Müller-Glöge/Preis (Hrsg.), Erfurter Kommentar zum Arbeitsrecht, 21. Aufl, 2021, §82 BetrVG, Rn. 3 f.; Werner, in: Rolfs/Giesen/Kreikebohm/Meßling/Udsching (Hrsg.), BeckOK Arbeitsrecht, 58. Ed., 01.12.2020, §81 BetrVG, Rn.1.

Eine andere Implementierung könnte zu einer Verringerung der Sicherheit führen, was eine neue rechtliche Bewertung erforderlich machen würde.

Rechtlich erscheint ein Einsatz von Weiterleitungs-URLs aus Gründen der IT-Sicherheit sowohl im privaten als auch im dienstlichen Umfeld möglich. Hierbei ist jedoch ebenso eine optimale Implementierung des Systems als auch seine Einbettung in geeignete Security-Awareness-Maßnahmen zu fordern. Zudem ist eine Beschränkung der Funktionalität des eingesetzten Tools auf die für Weiterleitungs-URLs erforderlichen Maßnahmen notwendig. Da in diesen Fällen von der potentiellen Verbesserung der IT-Sicherheit durch den Einsatz von Weiterleitungs-URLs auszugehen ist, überwiegt dann aber das Interesse am Einsatz der Technik die entgegenstehenden Rechte nicht einwilligender Betroffener.