Manuelles Löschen von Phishing-Nachrichten aus Mitarbeiterpostfächern

Rechtliche und technische Grenzen

Julian Hunter/Fabian Ballreich/Kai Julian Kemmler/Melanie Volkamer[*]

Die IT-Sicherheit von Organisationen ist in Anbetracht der steigenden Zahl von Cyberangriffen sowie der weiter zunehmenden Digitalisierung von Arbeitsabläufen wichtiger denn je. Eine gängige Angriffsmethode auf Organisationen ist die Verwendung von Phishing-Mails, mittels derer wichtige interne Informationen oder Zugangsdaten abgegriffen werden können. Zur effektiven Bekämpfung von Phishing in Organisationen ist es zweckmäßig, dass Phishing-Mails zentralisiert durch IT-Mitarbeitende gelöscht werden können. Eine entscheidende Rolle für die rechtliche Zulässigkeit einer zentralisierten Löschung spielt die Frage, ob ein Arbeitgeber an das Fernmeldegeheimnis gebunden ist, wenn er seinen Arbeitnehmern die Privatnutzung des betrieblichen E-Mail-Dienstes erlaubt. Dieser Beitrag beleuchtet die technischen und rechtlichen Herausforderungen bei der Bekämpfung von Phishing und arbeitet heraus, unter welchen Voraussetzungen eine manuelle und zentralisierte Löschung von Phishing-E-Mails aus Mitarbeiterpostfächern zulässig ist.

Inhaltsübersicht

---

[*] Prof. Dr. Melanie Volkamer ist Professorin am Karlsruher Institut für Technologie (KIT). Sie leitet dort die Forschungsgruppe Security, Usability, and Society (SECUSO) und ist PI der Kastel Security Research Labs. Julian Hunter ist Wissenschaftlicher Mitarbeiter am Karlsruher Institut für Technologie (KIT). Fabian Ballreich ist Wissenschaftlicher Mitarbeiter und Doktorand in der Forschungsgruppe Security, Usability, and Society (SECUSO) am Karlsruher Institut für Technologie (KIT). Kai Julian Kemmler ist Wissenschaftlicher Mitarbeiter am Karlsruher Institut für Technologie (KIT) und Rechtsreferendar.

Dieser Beitrag wurde vom Topic „Engineering Secure Systems“ der Helmholtz-Gemeinschaft mit Unterstützung der KASTEL Security Research Labs Karlsruhe gefördert.

I. Einleitung

Die Zahl von Cyberangriffen ist in den vergangenen Jahren rapide gestiegen. Eine der größten Gefahren für die Informationssicherheit von Organisationen stellen dabei Angriffe mithilfe von Phishing-Nachrichten dar.[1]

Im Gegensatz zu bloßen Spam-Nachrichten, die in der Regel lediglich unerwünschte Inhalte wie Werbung enthalten, sind Phishing-Nachrichten darauf ausgelegt, das Opfer durch Täuschung zur Preisgabe wertvoller Informationen zu bewegen.

Wenn die Gefahr besteht, dass Anmeldedaten oder vertrauliche Informationen abgegriffen werden, steht dabei nicht nur die Informationssicherheit und der Datenschutz auf dem Spiel, sondern auch die Integrität der Netzwerke und Systeme. Individuelle Schäden und Gefahren können also schnell in organisationelle und systemische Schäden und Gefahren umschlagen. Das Verhindern von Angriffen oder zumindest die Unterdrückung und Herabsetzung deren Effektivität hat daher für Organisationen jeglicher Größe und aller Sektoren eine übergeordnete Priorität.[2]

Gängige Maßnahmen sind beispielsweise interne Meldesysteme und – schon vorgelagert – die Schulung von Mitarbeitern. Sie haben jedoch die systematische Schwäche, dass sie zwar geschulte, aber dennoch unerfahrene Mitarbeiter in die Gewährleistung der IT-Sicherheit miteinbinden, die etwa unter Zeitdruck, Unkenntnis und anderen Umständen doch den Phishing-Angriff guten Glaubens ermöglichen. Darüber hinaus werden zumeist automatisierte Filter eingesetzt, die aber zum Teil lediglich verdächtige E-Mails kennzeichnen, also immer noch die Gefährdung erhalten, und im Übrigen nur einen Teil der eingehenden Phishing-Nachrichten erkennen. Daher stellt sich die Frage,

[1] Bitkom e. V. „Welche der folgenden Arten von digitalen IT-Angriffen haben innerhalb der letzten 12 Monate in Ihrem Unternehmen einen Schaden verursacht?“ (9.2023), Chart 1, abrufbar unter: https://de.statista.com/statistik/daten/studie/928943/umfrage/von-digitalen-angriffen-betroffene-unternehmen-nach-art-des-angriffs/.

[2] Bitkom e. V. Wirtschaftsschutz 2024, abrufbar auf der Website von Bitkom Research unter: https://bitkom-research.de/node/1040.

ob Phishing-Nachrichten auch zentralisiert, etwa durch Mitarbeiter der IT-Abteilung, aus Mitarbeiterpostfächern gelöscht werden dürfen. Dies wäre ein effektives Mittel, um die Abwehr von Phishing-Angriffen zu professionalisieren und gleichzeitig die Mitarbeiter von der Aufgabe und Verantwortung, derartige Angriffe zu erkennen und angemessen einzuordnen, zu entlasten.

Die folgenden Ausführungen beleuchten zunächst die typischen Angriffspunkte von Phishing. Der Beitrag erörtert dann die rechtlichen Grundlagen und Grenzen eines aktiven und manuellen Zugriffs durch Systemadministratoren auf E-Mail-Postfächer der Mitarbeiter. Zuletzt stellen wir Lösungsansätze vor, mit denen eine Löschung von schädlichen Nachrichten rechtskonform durchgeführt werden kann.

II. Problembeschreibung: Phishing

Eine allgemeingültige (kodifizierte) Definition von Phishing besteht bislang nicht. In diesem Rahmen definieren wir Phishing als eine „Methode, mit der ein Angreifer versucht, das Opfer durch Täuschung über elektronische Kommunikation zu Handlungen (zB Preisgabe von Informationen) zu verleiten, mit dem Ziel, dem Einzelnen oder der Organisation durch das Abgreifen von Informationen zu schaden oder weitere Schäden zu ermöglichen oder zu begünstigen".

In diesem Rahmen grenzen wir ab von schädlichen E-Mails, welche nicht lediglich auf das Abgreifen von Informationen gerichtet sind, sondern unmittelbar die Anlagen oder Dienste des Opfers beeinträchtigen (zB virenbehaftete E-Mails).

Klassischerweise nutzen Angreifer verschiedene Elemente zur Gestaltung von Phishing-Nachrichten, wie etwa manipulierte Absenderangaben und Links, täuschend echte Logos oder eine personalisierte Anrede. Etwa ist es ohne weitere Sicherheitsmaßnahmen standardmäßig, durch Ausnutzung konzeptbedingter Eigenschaften der Internetkommunikation, bei E-Mail-Nachrichten möglich, die beim Empfänger angezeigten Absenderangaben (Name und Adresse) zu manipulieren und hierdurch vermeintlich legitime Absender zu imitieren. Der Anzeigename lässt sich technisch durch den Angreifer im E-Mail-Header[3] definieren und muss nichts mit der tatsächlichen Absenderadresse zu tun haben.[4]

1. Angriffspunkt für Phishing im Allgemeinen

Angreifer setzen bei der Gestaltung des Inhaltes von Phishing-Nachrichten häufig auf Internetlinks, welche die Eingabe von Zugangsdaten auf gefälschten Anmeldeseiten, die Preisgabe sensibler Informationen oder den Download von Schadprogrammen zum Ziel haben. Letztere können auch direkt mit der Nachricht übersendet werden. Letztlich ist das Ziel immer, den Empfänger zur Durchführung einer bestimmten Aktion oder Preisgabe sensibler Informationen zu verleiten.

Des Weiteren setzen Angreifer bei der Gestaltung von Phishing-Nachrichten sehr häufig auf sog. „Social Engineering", wobei menschliche Faktoren und psychologische

---

[3] Der E-Mail-Header ist der Abschnitt einer E-Mail, der technische Informationen über die Übertragung und den Ursprung der Nachricht enthält, wie Absender- und Empfängeradressen, Datum und Zeit des Versands, sowie Routing-Informationen wie die IP-Adressen der beteiligten Mailserver.

[4] Vgl. IETF RFC 5322 Internet Message Format, abrufbar unter: https://datatracker.ietf.org/doc/html/rfc5322.

Mechanismen ausgenutzt werden, um die Empfänger der Nachrichten zu bestimmten Verhaltensweisen zu verleiten. Angreifer versuchen so bei Empfängern beispielsweise besonders negative (zB Zeitdruck durch Mahnung) oder besonders positive Emotionen (zB Gewinnversprechen) auszulösen und damit erlernte Mechanismen zur Erkennung von Phishing-Angriffen zu umgehen. [5]

2. Phishing in Organisationen

Organisationen sind im Allgemeinen stärker gefährdet als Privatnutzer, da bei ihnen größere Schäden entstehen können und sie beispielsweise oft gezielt aus politischen oder wettbewerblichen Gründen angegriffen werden. Ihre umfangreichen IT-Systeme bieten eine größere Angriffsfläche, und ihre oft dezentrale oder internationale Struktur erschwert ein einheitliches IT-Sicherheitsmanagement.

Angriffe auf Organisationen mittels Phishings zielen in der Regel darauf ab, die IT-Infrastruktur der Organisation anzugreifen, zu kompromittieren und dadurch zu schädigen. Hierdurch können Angreifer etwa Daten abgreifen, den Betrieb der Systeme stören oder Erpressungen (oftmals über sog. „Ransomware“[6]) durchführen. Weiterhin kann eine kompromittierte IT-Infrastruktur als Ausgangspunkt für Angriffe auf andere Organisationen dienen.

Angriffswege können hierbei in verschiedene Kategorien eingeteilt werden. Ein häufig verwendeter Weg ist die Verbreitung von Schadprogrammen als Anhang oder per Link. Angreifer setzen hierbei darauf, dass die Empfänger einer Phishing-Nachricht diese fälschlicherweise als legitim einstufen und ein Programm ausführen.

Ein weiterer Angriffsweg, der ebenfalls auf die Kompromittierung der Infrastruktur zielt, liegt darin, Zugangsdaten für Accounts von Organisationsangehörigen abzugreifen und hierüber Zugriff auf die IT-Infrastruktur zu erhalten. Primäre Ziele für derartige Angriffe sind Personen, die innerhalb der Organisation erweiterte Berechtigungen haben. Exemplarisch kann die Kompromittierung des Accounts eines Systemadministrators weitreichende Auswirkungen auf den Betrieb der IT-Infrastruktur haben und daher ein besonders lohnendes Ziel sein.

Doch auch Mitarbeiter ohne erweiterte Rechte dienen häufig als Ziel für Angriffe, da diese wiederum gute Ausgangspositionen bieten, um weitere interne und zielgerichtete Angriffe auf andere Mitarbeiter zu starten. Umso mehr Informationen Angreifer über die internen Strukturen einer Organisation haben, desto besser können Angriffe hierauf ausgerichtet werden.

3. Maßnahmen von Organisationen

Um entsprechende Schäden und Gefahren zu vermeiden, ist das Ziel von Abwehrmaßnahmen stets, die Zustellung von betrügerischen Nachrichten an Mitarbeiter zu minimieren, bestenfalls ganz zu verhindern oder diese zumindest für das Problem zu sensibilisieren.

Die technische Erkennung von Phishing-Nachrichten durch entsprechende Filter ist nur zu einem gewissen Anteil erfolgsversprechend, da derartige Nachrichten im Hinblick auf Inhalt und Aufbau legitimen Nachrichten häufig sehr ähnlich sind oder zum

---

[5] Hierzu Bundesamt für Sicherheit in der Informationstechnik („BSI“), https://www.bsi.bund.de/dok/11287460.

[6] Siehe BSI, https://www.bsi.bund.de/dok/ransomware-links.

Teil sogar Kopien tatsächlicher Nachrichten darstellen. Die Erkennung von Nachrichten mit potenziell schädlichen Anhängen (zB ausführbaren Dateien) wird häufig eingesetzt, kann jedoch nur beschränkt Wirkung entfalten.[7] So kann beispielsweise durch die Verwendung komprimierter Archivdateien (zB „.zip-Dateien“) eine Erkennung erschwert werden, da hierfür die Dateien zuerst entpackt werden müssen, was zusätzliche Rechenressourcen und Zeit erfordert. In einem alternativen Angriffsszenario werden derartige Dateien mit einem Passwort versehen, wodurch eine Überprüfung des Inhaltes für Mailfilter unmöglich gemacht wird.

Präventive organisatorische Maßnahmen (zB das „NoPhish“-Konzept[8]) verfolgen das Ziel, Nutzer für das Thema Phishing bzw. Nachrichten mit betrügerischem Inhalt zu sensibilisieren und einfache Handlungsweisen zur Erkennung zu vermitteln. Für den Aufbau derartiger Security Awareness können in einer Organisation beispielsweise Videos mit Bezug zu unterschiedlichen Angriffsstrategien oder Online-Kurse Anwendung finden, bei denen das vermittelte Wissen direkt anhand realistischer Nachrichten getestet werden kann.

Nutzer können zudem durch geeignete technische Hilfsmittel (zB TORPEDO[9]) bei der Erkennung von Phishing-Nachrichten unterstützt werden, indem beispielsweise in E-Mails enthaltene Links für wenige Sekunden blockiert werden. Hierdurch wird zur Prüfung der Links angeregt und das Risiko durch voreilige oder unbeabsichtigte Klicks reduziert. Derartige technische Hilfsmittel können beispielsweise auch bei der Identifizierung des Wer-Bereichs unterstützen und hiermit verschiedene Verschleierungstaktiken adressieren. Der Wer-Bereich einer Webadresse besteht aus den beiden Begriffen, die durch einen Punkt getrennt sind und sich vor dem ersten alleinstehenden Schrägstrich „/“ befinden. Im Allgemeinen wird dieser Bereich auch mit dem Begriff „Domain“ bezeichnet.

Ferner können organisationsinterne Meldeverfahren für Phishing-Nachrichten etabliert und gegenüber den Mitarbeitern kommuniziert werden. Beispielsweise ist es möglich, eine zentrale E-Mail-Adresse zur Weiterleitung von erkannten Nachrichten einzurichten, auf die alle beteiligten Stellen in der Organisation (zB Informationssicherheitsbeauftragter, CERT, IT-Abteilung, etc.) zugreifen und direkt reagieren können. Alternativ gibt es auch den Ansatz, den Nutzern in den verwendeten E-Mails Clients eigene Buttons anzuzeigen, über die eine verdächtige E-Mail mit einem Klick gemeldet werden kann.

4. Aktives Löschen von Phishing-Mails

Alle zuvor genannten Ansätze haben gemein, dass sie Routinen schaffen, die durch erhöhte Aufmerksamkeit das Abgreifen von Daten oder die Schädigung der IT-Systeme unter Mitwirkung eines getäuschten Mitarbeiters vorbeugen sollen. Dennoch lässt sich durch diese Maßnahmen ein gewisses Restrisiko nicht ausräumen. Wenn Phishing-Nachrichten in einer Organisation in Wellen an eine große Anzahl von Empfängern gesendet werden und viele Mitarbeiter gleichzeitig solche Nachrichten in ihren Postfächern vorfinden, steigt mit der Anzahl der Empfänger die Wahrscheinlichkeit,

---

[7] Singh et al. (2023) Modelling an Efficient Approach to Analyse Clone Phishing and Predict Cyber-Crimes. In: Shakya, S., Papakostas, G., Kamel, K.A. Mobile Computing and Sustainable Informatics. Lecture Notes on Data Engineering and Communications Technologies, vol 166.

[8] https://secuso.org/nophish.

[9] https://secuso.org/torpedo.

dass sich auch jemand von einer dieser Phishing-Nachrichten täuschen lässt. Es lässt sich übergreifend für alle dargestellten Konstellationen feststellen: Wenn die Nachricht erst einmal gesehen und auf sie beispielsweise durch Preisgabe von Informationen oder bereits durch Klicken auf einen schadhaften Link oder Anhang reagiert wurde, dann kommt eine entsprechende Maßnahme durch Systemadministratoren in der Regel zu spät. Es muss in diesem Fall von Sicherheitslücken abhängig von den herausgegebenen Daten ausgegangen und umfangreiche Gegenmaßnahmen (zB Sperrung von Accounts, Beschränkung des Zugriffs von außen, etc.) eingeleitet werden.

Die beteiligten Stellen in der Organisation erkennen bei einer Welle von Phishing-Nachrichten durch etablierte interne Meldeprozesse häufig schnell, dass ein Angriff stattfindet, sind aber nur begrenzt in der Lage, effektive Gegenmaßnahmen zu ergreifen. Eine gängige Maßnahme ist beispielsweise, die Benachrichtigung aller potenziell betroffenen Mitarbeiter, verbunden mit der Aufforderung, entsprechende Phishing-Nachrichten ohne weitere Interaktion direkt zu löschen.

Es wäre jedoch wesentlich effektiver und verlässlicher, wenn die betroffene E-Mail direkt von den zuständigen Stellen gelöscht werden könnte, sodass die Empfänger hierzu gar nicht mehr aktiv werden müssten. Dies gilt für Nachrichten, die an eine Vielzahl von Empfängern in einer Organisation oder gezielt an einzelne Mitarbeiter versendet werden, gleichermaßen. Hierbei müssten allerdings IT-Mitarbeiter auf Postfächer adressierter Mitarbeiter zugreifen. Dabei stellt sich die Frage der rechtlichen Zulässigkeit eines solchen Eingriffs.

III. Rechtliche Zulässigkeit der Maßnahmen

Die rechtliche Beurteilung dessen, ob ein Arbeitgeber auf E-Mails seiner Arbeitnehmer zugreifen darf, dreht sich im Kern um die Frage, ob der Arbeitgeber an das strenge Fernmeldegeheimnis und Telekomunikationsdatenschutzrecht nach dem TTDSG gebunden ist, oder aber das (ebenfalls strenge, aber flexiblere) allgemeine Datenschutzrecht anwendbar ist. Dies ist seit jeher in Literatur und Rechtsprechung umstritten[10] und auch nach der Telekommunikationsrechtsreform 2021 nicht abschließend geklärt. Der Streit betrifft auch die Bekämpfung von Spam-, Phishing- oder Malware-Angriffen.[11] In der hier betrachteten Konstellation soll dezidiert eine manuelle Löschung von Phishing-Mails durchgeführt werden, um Ungenauigkeiten automatisierter Nachrichtenfilter auszugleichen und das Risiko eines erfolgreichen Phishing-Angriffs zu minimieren, indem der Personenkreis derjenigen, die mit der Löschung von Phishing-Nachrichten betraut sind, verkleinert wird.

Grundsätzlich bewegt sich die Fragestellung im Spannungsverhältnis zwischen IT-Sicherheit einerseits und dem Fernmeldegeheimnis sowie Arbeitnehmerdatenschutz andererseits.

1. Fernmeldegeheimnis

Das Fernmeldegeheimnis ergibt sich auf grundrechtlicher Ebene in Deutschland aus Art. 10 GG sowie auf europäischer Ebene aus Art. 8 EMRK und Art. 7 EU-GRCh. Die

---

[10] Siehe Darstellung des Streitstands bei Dieckhoff/Assion ZD 2023, 371, 371 f.

[11] Sassenberg/Lammer DuD 2008, 461; Heidrich CR 2009, 168; Heidrich/Tschoepe MMR 2004, 75; BeckOK StGB/Weidemann, 63. Edition 2024, StGB § 206 Rn. 18.1 f.; Schönke/Schröder/Eisele, 30. Aufl. 2019, StGB § 206 Rn. 26; MüKoStGB/Altenhain, 4. Aufl. 2021, StGB § 206 Rn. 58.

EU trifft konkretere Vorgaben in der ePrivacy-Richtlinie.[12] Der deutsche Gesetzgeber hat diese Vorgaben in §§ 3 ff. des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes („TDDDG“) umgesetzt.

a) Verhältnis zwischen Fernmeldegeheimnis und Datenschutz

Die Vorschriften des Fernmeldegeheimnisses und des Telekommunikationsdatenschutzes sind gegenüber dem allgemeinen Datenschutzrecht vorrangig anwendbar. Das ergibt sich bereits allgemein aus dem Spezialitätsgrundsatz,[13] letztlich aber auch ausdrücklich aus Art. 95 DSGVO. Art. 95 DSGVO besagt, dass die DSGVO keine zusätzlichen Pflichten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste[14] auferlegt, soweit besondere Pflichten aus der ePrivacy-RL dasselbe Ziel verfolgen. Das erfasst insbesondere die Rechtmäßigkeit der Verarbeitung nach Art. 6 DSGVO. Art. 6 DSGVO wird durch die spezielleren Normen aus Art. 5 ff. ePrivacy-RL verdrängt, die in §§ 3 und 9 ff. TDDDG umgesetzt sind.[15] Daher ist für die Beurteilung möglicher Verarbeitungsvorgänge (insb. Maßnahmen zur Identifikation von Phishing-Mails sowie deren Löschung) zunächst entscheidend, ob E-Mails dem Anwendungsbereich des Fernmeldegeheimnisses unterfallen und ob der Arbeitgeber an das Fernmeldegeheimnis gebunden ist, wenn er seinen Arbeitnehmern einen E-Mail-Dienst zur Verfügung stellt.

b) Sachlicher Anwendungsbereich des Fernmeldegeheimnisses nach § 3 Abs. 1 TDDDG

Gegenstand des Fernmeldegeheimnisses nach § 3 Abs. 1 TDDDG ist der Inhalt der Telekommunikation und ihre näheren Umstände. Telekommunikation ist nach § 3 Nr. 59 TKG „der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen“. Hierunter fällt auch das Aussenden, Übermitteln und Empfangen von Signalen zur Übermittlung von E-Mails über das Internet.[17] Zum Inhalt der Kommunikation gehören alle Informationen, die Teil der eigentlichen Kommunikation zwischen den Kommunikationsparteien sind.[18] Unter näheren Umständen sind solche Informationen zu verstehen, die nicht zum Kommunikationsinhalt gehören, aber mit einem konkreten Kommunikationsvorgang zusammenhängen, insbesondere Verkehrsdaten nach § 3 Nr. 70 TKG. [19] Hierunter fallen insbesondere die IP-Adressen von Absender und Empfänger.[20]

Zur Überprüfung einer E-Mail auf einen Phishing-Verdacht kann sowohl die Auswertung des Headers als auch des Bodys[21] einer Nachricht aufschlussreich sein. Aus dem Header etwa lässt sich ein möglicher Betrugsversuch herleiten, wenn zB die IP-

---

[12] Richtlinie 2002/58/EG in der Fassung der Richtlinie 2009/136/EG.

[13] Gola/Heckmann/Piltz, 3. Aufl. 2022, DSGVO Art. 95 Rn. 15 f.; Taeger/Gabel/Golland, 4. Aufl. 2022, DSGVO Art. 95 Rn. 5 f.; vgl. Spiecker gen. Döhmann/Papakonstantinou/Hornung/De Hert/Papakonstantinou/De Hert, 1. Aufl. 2023, DSGVO Art. 95 Rn. 1.

[14] Bzw. Telekommunikationsdienste nach dem TKG und TDDDG.

[15] Taeger/Gabel DSGVO Art. 95 Rn. 11.

[17] EuGH MMR 2019, 514 mAnm Spies Rn. 34.

[18] Vgl. Assion/Assion, 1. Aufl. 2022, TTDSG § 3 Rn. 45.

[19] Gierschmann/Baumgartner/Baumgartner TDDDG § 3 Rn. 18; Assion/Assion TDDDG § 3 Rn. 27; Auernhammer/Heun, TDDDG § 3 Rn. 12.

[20] BGH NJW 2011, 1509; vgl. BVerfG ZUM-RD 2011, 396 Rn. 21.

[21] Der E-Mail-Body ist der Abschnitt einer E-Mail, der den eigentlichen Nachrichteninhalt enthält.

Adresse des Absenders nicht mit der IP-Adresse des vermeintlich versendenden E-Mail-Servers übereinstimmt.[22] Im Übrigen können sich Hinweise aber auch nur aus dem Body ergeben, etwa wenn eine Phishing-Mail von einem gehackten, echten E-Mail-Account verschickt wird, da hier die IP-Adressen im Header übereinstimmen. Das Fernmeldegeheimnis ist daher in Bezug auf diese Maßnahmen sachlich anwendbar.

c) Persönlicher Anwendungsbereich des Fernmeldegeheimnisses nach § 3 Abs. 2 TDDDG

An das Fernmeldegeheimnis gebunden sind Anbieter öffentlich zugänglicher Telekommunikationsdienste sowie ganz oder teilweise geschäftsmäßig angebotener Telekommunikationsdienste sowie an der Erbringung solcher Dienste Mitwirkende. Darüber hinaus verpflichtet sind Betreiber von öffentlichen Telekommunikationsnetzen und Betreiber von Telekommunikationsanlagen mit denen geschäftsmäßig Telekommunikationsdienste erbracht werden (§ 3 Abs. 2 TDDDG).

E-Mail-Dienste sind „interpersonelle Kommunikationsdienste" iSd § 3 Nr. 24 TKG und damit Telekommunikationsdienste (§ 3 Nr. 61 lit. b TKG).[23] Ein Arbeitgeber, der seinen Arbeitnehmern Kommunikationsmittel (zB E-Mail-Dienste) zur Verfügung stellt, ist in der Regel kein Anbieter öffentlich zugänglicher Telekommunikationsdienste iSd § 3 Nr. 44 TKG, da er den Telekommunikationsdienst nur seinen Arbeitnehmern und damit einem geschlossenen Personenkreis anbietet.[24] Allerdings wird teilweise vertreten, er könnte als Anbieter von ganz oder teilweise geschäftsmäßig angebotenen Telekommunikationsdiensten in Betracht kommen. Dies richtet sich danach, ob die Bereitstellung von Kommunikationsdiensten des Arbeitgebers an seine Arbeitnehmer als eine Leistung an Dritte zu sehen ist.[25]

Gestattet der Arbeitgeber den Arbeitnehmern ausdrücklich ausschließlich die geschäftliche Nutzung des E-Mail-Postfachs, so stellt er diesen Dienst nur „sich selbst", d.h. den Arbeitnehmern zur Nutzung für den Arbeitgeber, zur Verfügung. Es liegt somit keine geschäftsmäßig angebotene Leistung vor. Somit ist der Arbeitnehmer kein Anbieter von Telekommunikationsdiensten und kein Verpflichteter des Fernmeldegeheimnisses.[27]

Erlaubt der Arbeitgeber hingegen die private Nutzung des E-Mail-Postfachs, so erbringt er nach Auffassung der jüngsten Rechtsprechung den Arbeitnehmern in Bezug auf den privaten E-Mail-Verkehr eine Leistung an Dritte.[28]

---

[22] siehe hierzu: Verbraucherzentrale NRW, So lesen Sie den E-Mail-Header, https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/so-lesen-sie-den-emailheader-6077.

[23] ErwGr. 10, 17 RL (EU) 2018/1972; Säcker/Körber/Körber, 4. Aufl. 2023, TKG § 3 Rn. 31.

[24] Assion/Assion, TTDSG § 3 Rn. 92; Taeger/Gabel/Munz, TTDSG § 3 Rn. 17 f.; Wünschelbaum NJW 2022, 1561, 1564.

[25] § 3 Nr. 10 TKG 2004 definierte das geschäftsmäßige Erbringen von Telekommunikationsdiensten noch als „das nachhaltige Angebot von Telekommunikation für Dritte […]", eine Änderung war mit der Streichung im neuen TKG wohl nicht beabsichtigt; dazu Dieckhoff/Assion ZD 2023, 371, 375; Fokken NZA 2020, 629, 633; Kiparski/Nacimiento RDi 2021, 196, 204; Assion/Assion, TTDSG § 3 Rn. 70; Gierschmann/Baumgartner/Baumgartner TTDSG § 3 Rn. 34.

[27] Brink/Schwab ArbRAktuell 2018, 111, 112.

[28] OLG Thüringen BeckRS 2021, 28260 Rn. 35 ff.; vgl. LAG Hessen NZA-RR 2019, 130 Rn. 55 ff.; aA aber die Landesdatenschutzbehörde NRW und wohl auch weitere Datenschutzbehörden, LDI NRW 29. Jahresbericht 2024, S. 76 f.; ebenso Assion/Assion, TTDSG § 3 Rn. 72; Gierschmann/Baumgartner/Baumgartner TTDSG Rn. 50; LG Erfurt GRUR-RS 2021, 16480 Rn. 18;

Dieser Rechtsauffassung ist jedoch nicht zuzustimmen. Denn auch ein Arbeitgeber, der seinen Arbeitnehmern die private (Mit-)Nutzung des geschäftlichen E-Mail-Postfachs erlaubt, tritt dem Arbeitnehmer gegenüber nicht als geschäftsmäßiger Anbieter auf, der die Verantwortung für die Übermittlung privater Nachrichten trägt.[29] Denn die Erlaubnis der Privatnutzung soll gerade nicht dem Zweck dienen, dem Arbeitnehmer ein weiters privates Kommunikationsmittel bereitzustellen, sondern lediglich, dem Arbeitnehmer einer flexiblere Nutzung des betrieblichen Kommunikationsmittels zu gewähren. Daher erfolgt die Privatnutzung auch nicht außerhalb der „Sphäre" des Arbeitgebers, folglich findet kein Angebot an Dritte statt.[30]

Zweck der §§ 3 ff. TDDDG ist es außerdem, die private Kommunikation der Nutzer vor dem Zugriff desjenigen zu schützen, dem die Nutzer die Kommunikation für die Übermittlung aufgrund der technischen Begebenheiten anvertrauen müssen,[31] nämlich dem außenstehenden Telekommunikationsanbieter. Aus diesem Grund sind die Eingriffsbefugnisse des Telekommunikationsanbieters auf das Nötigste beschränkt, was zum Schutz vor unberechtigter oder missbräuchlicher Inanspruchnahme seiner Dienste durch den Nutzer erforderlich ist. Das Verhalten der Nutzer untereinander ist durch den außenstehenden Telekommunikationsanbieter daher grundsätzlich unangetastet zu lassen. Schutzvorkehrungen gegenüber dem anderen Nutzer zu treffen, etwa vor betrügerischer oder belästigender Kommunikation, obliegt dem Nutzer selbst.[32]

Stellt ein Arbeitgeber seinen Arbeitnehmern E-Mail-Dienste zur betrieblichen Nutzung zur Verfügung, ist er Nutzer und nicht Anbieter von Telekommunikationsdiensten iSd § 3 TDDDG. Somit ist er auch für die Abwendung von Gefahren verantwortlich, die nicht den Telekommunikationsdienst als solchen beeinträchtigen.[33] Gibt der Arbeitgeber seinen Arbeitnehmern die Möglichkeit, den betrieblichen E-Mail-Dienst auch für private Zwecke zu nutzen, so nimmt der Arbeitnehmer keinen separaten, privaten Dienst in Anspruch. Daher steht der Arbeitgeber auch nicht als außenstehender Dritter neben der Kommunikation, sondern aufseiten des Nutzers. Der Arbeitgeber hat daher auch ein berechtigtes Interesse daran, sich vor betrügerischer oder belästigender Kommunikation Dritter zu schützen, unabhängig davon, ob der Arbeitnehmer das betriebliche E-Mail-Postfach auch für private Zwecke nutzt.

NZA 2020, 629, 633; die BfDI hält eine Einstufung des Arbeitgebers als Anbieter von Telekommunikationsdiensten jedenfalls für möglich, BfDI Datenschutz und Telekommunikation (Info 5), Stand 1/2024 S. 41.

[29] Auf einen fehlenden Rechtsbindungswillen des Arbeitgebers abstellend die Landesdatenschutzbehörde NRW, LDI NRW 29. Jahresbericht 2024, S. 76 f.; ohne nähere Begründung LG Erfurt GRUR-RS 2021, 16480 Rn. 18.

[30] Vgl. LAG Berlin-Brandenburg BB 2016, 891 Rn. 81 mAnm Zimmermann; LAG Berlin-Brandenburg folgend den Ausführungen des ArbG Berlin BeckRS 2011, 70280.

[31] Vgl. Assion/Assion § 3 TDDDG Rn. 24.

[32] Nach aA soll der Telekommunikationsanbieter auch gegen Schädigungen seiner Kunden vorgehen können, so etwa Taeger/Gabel/Munz TTDSG § 3 Rn. 19; Geppert/Schütz/Hadidi TTDSG § 3 Rn. 24; wie hier aber Sassenberg/Lammer DuD 2008, 461, 463; wohl auch wie hier abstellend auf Filter als von den Kunden gewünschte Zusatzfeatures Assion/Assion § 3 TTDSG Rn. 117; ebenso Auernhammer/Heun § 3 TTDSG Rn. 56.

[33] Zum Schutz personenbezogener Daten, die durch Phishing-Angriffe gefährdet sind, auch verpflichtet nach Art. 25, 32 DSGVO.

d) Zeitpunkt des Zugriffs

Folgt man allerdings der Auffassung, der Arbeitgeber sei bei erlaubter Privatnutzung Anbieter von Telekommunikationsdiensten, kommt es für die Anwendbarkeit des Fernmeldegeheimnisses des Weiteren auf den Zeitpunkt des Zugriffs auf die Informationen an.

Das Fernmeldegeheimnis knüpft an das Kommunikationsmedium und den sich hieraus ergebenden Gefahren für die Vertraulichkeit an.[34] Das Fernmeldegeheimnis soll daher die Vertraulichkeit der Kommunikation unter Abwesenden schützen. Anders als bei einem privaten Gespräch unter Anwesenden müssen die Kommunikationsteilnehmer ihre Nachrichten in die Hände eines Kommunikationsmittlers (hier: Telekommunikationsanbieters) geben und darauf vertrauen, dass dieser niemandem unberechtigt Kenntnis über die Kommunikation verschafft und sicherstellt, dass die Kommunikation nicht auf dem Übertragungsweg abgehört wird.[35] Das Fernmeldegeheimnis stellt somit sicher, dass die Kommunikation auf dem Übertragungsweg durch den Anbieter des Telekommunikationsdienstes besonders geschützt wird.

E-Mails unterfallen daher während des Übertragungsvorgangs dem Fernmeldegeheimnis. Der Übertragungsvorgang umfasst aber nicht nur Daten „in transit", sondern auch noch, wenn sie auf dem E-Mail-Server „ruhen" und sich dabei noch nicht im Herrschaftsbereich des Nutzers befinden.[36] Der Grund für diese Ausweitung des schützenswerten „Übertragungsvorgangs" liegt darin, dass sich eine E-Mail, die sich noch lediglich auf dem Server des E-Mail-Anbieters befindet und auf die der Nutzer nur über einen Internetzugang zugreifen kann, noch nicht in einem für den Nutzer beherrschbaren Bereich befindet. Etwa ist es dem Nutzer nicht möglich, die E-Mail ohne Internetzugang durch rechtzeitige Löschung vor der unbefugten Kenntnisnahme eines Dritten zu schützen. Somit liegt die E-Mail weiterhin im Herrschaftsbereich des E-Mail-Anbieters und der Nutzer ist weiterhin schutzbedürftig.[37]

Der Schutz des Fernmeldegeheimnisses endet aber in dem Zeitpunkt, in dem die E-Mail nicht mehr lediglich auf einem zugangsgeschützten E-Mail-Server liegt[38] und der Arbeitgeber ohne Internetzugang auf die E-Mail zugreifen könnte.[39] Folglich wäre ein Zugriff auf solche Nachrichten, unabhängig davon, ob man den Arbeitgeber als Anbieter von Telekommunikationsdiensten betrachtet, nicht am Fernmeldegeheimnis zu messen, sondern am Datenschutzrecht, also insbesondere an den Vorschriften der DSGVO und des BDSG.

e) Zulässigkeit der Kenntnisverschaffung und Verarbeitung

Folgt man der Auffassung, der Arbeitgeber sei bei erlaubter Privatnutzung Anbieter von Telekommunikationsdiensten und ist der Übertragungsvorgang wie zuvor

---

[34] BVerfG NJW 2009, 2431 Rn. 46.

[35] Vgl. BVerfG NJW 2009, 2431 Rn. 47; BVerfG NJW 2007, 351 Rn. 53; BVerfG NJW 2002, 3619, 3620; BVerfG NJW 1992, 1875.

[36] BVerfG NJW 2009, 2431 Rn. 46; vgl. BVerfGE 100, 313 (363).

[37] Vgl. BVerfG NJW 2009, 2431 Rn. 46; vgl. VGH Hessen Beschl. v. 19.5.2009 – 6 A 2672/08.Z Rn. 14 ff.; vgl. Brink/Schwab, ArbRAktuell 2017, 111 (112); a.A. nach soll das Fernmeldegeheimnis nach § 3 TDDDG bereits enden, sobald der Adressat die Nachricht vom Server seines Anbieters von Telekommunikationsdiensten abruft, so mit Verweis auf EG 27 RL 2002/58/EG Auernhammer/Heun, TTDSG § 3 Rn. 16.

[38] OLG Thüringen BeckRS 2021, 28260 Rn. 44; BVerfG NJW 2009, 2431 Rn. 46.

[39] LAG Hessen NZA-RR 2019, 130 Rn. 58; vgl. BVerfG NJW 2009, 2431 Rn. 46.

beschrieben noch nicht abgeschlossen, ist die Kenntnisverschaffung über geschützte Informationen nur dann zulässig, wenn dies für die "Erbringung der Telekommunikationsdienste oder für den Betrieb ihrer Telekommunikationsnetze oder ihrer Telekommunikationsanlagen einschließlich des Schutzes ihrer technischen Systeme" erforderlich ist (§ 3 Abs. 3 Satz 1 TDDDG) oder sonst durch Gesetz zugelassen ist (§ 3 Abs. 3 Satz 3 und 4 TDDDG).

§ 3 Abs. 3 Satz 3 TDDDG ist keine Generalklausel, sondern erfordert einen ausdrücklichen Bezug zu Telekommunikationsvorgängen (sog. „kleines Zitiergebot").[40] Allgemeine datenschutzrechtliche Erlaubnistatbestände (insb. Art. 6 Abs. 1 lit. f DSGVO) sind nicht hierunter zu fassen.

Die Bekämpfung von Sicherheitsrisiken kann nach § 3 Abs. 3 Satz 1 TDDDG als Teil des Betriebsablaufs für die Rechtfertigung eines Eingriffs in das Fernmeldegeheimnis herangezogen werden.[41] Die Kenntnisnahme ist aber streng auf das für den Schutz der Systeme des Anbieters erforderliche Zwecke zu beschränken. Den datenschutzrechtlichen Vorschriften aus §§ 9–13 TDDDG kommen dabei Indizwirkung zu.[42] § 3 Abs. 3 Satz 1 TDDDG hat in Bezug auf die Bekämpfung von IT-Sicherheitsrisiken eine besondere Nähe zu § 12 TDDDG. Die Erforderlichkeit einer Maßnahme nach § 3 Abs. 3 Satz 1 TDDDG zu diesem Zweck muss daher restriktiv im Sinne des § 12 TDDDG ausgelegt werden.[43]

Nach § 12 Abs. 1 TDDDG dürfen Verpflichtete Verkehrsdaten verarbeiten, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen. Unter Störung ist nicht nur eine Veränderung der physikalischen Beschaffenheit der verwendeten Geräte zu fassen, sondern bereits eine Einschränkung ihrer Funktionen.[44]

Die Erhebung und Verwendung von Verkehrsdaten (zB IP-Adressen der Server eingehender Anfragen) kann zulässig sein, um Angriffe auf die IT-Infrastruktur des Telekommunikationsanbieters, wie zB DoS- oder DDoS-Angriffe, zu bekämpfen.[45] Hierbei müssen die Maßnahmen jedenfalls erforderlich sein, um eine abstrakte Gefahr für die Funktionsfähigkeit des Telekommunikationsbetriebs abzuwehren.[46] Der BGH hat angenommen, dass die Verarbeitung von Verkehrsdaten zur Bekämpfung ausgehender Spam- oder Phishing-Mails zulässig sein kann, da auch die Sperrung von IP-Adressbereichen durch anderen Anbieter zur Verhinderung von Spam- oder Phishing-Angriffen als „Störung" iSd § 12 Abs. 1 TDDDG zu sehen ist.[47] Die Überwachung ausgehender Kommunikation ist für die Funktionsfähigkeit der Dienste des Arbeitgebers allerdings regelmäßig nicht von großer Relevanz.

---

[40] Plath/Jenny, 4. Aufl. 2023, TTDSG § 3 Rn. 26; Assion/Assion TTDSG § 3 Rn. 130; Taeger/Gabel/Bernzen TTDSG § 4 Rn. 6.

[41] Gierschmann/Baumgartner/Baumgartner, 1. Aufl. 2023, TTDSG § 3 Rn. 57; Spindler/Schuster, 4. Aufl. 2019, TKG § 88 Rn. 50; Geppert/Schütz/Bock, 4. Aufl. 2013, TKG § 88 Rn. 26; Säcker/Körber/Waßmer, TTDSG § 3 Rn. 33; vgl. Geppert/Schütz/Hadidi, 5. Aufl. 2023, TTDSG § 3 Rn. 25.

[42] Assion/Assion TTDSG § 3 Rn. 57; Scheurle/Mayen/Mayen, 3. Aufl. 2018, TKG § 88 Rn. 74.

[43] Assion/Assion TTDSG § 3 Rn. 122; vgl. BeckOK IT-Recht/Heilmann/Herrmann, 16. Edition 2024, TTDSG § 3 Rn. 27.

[44] BGH ZD 2014, 461 Rn. 15 mAnm Eckhardt.

[45] Auernhammer/Heun TTDSG § 3, Rn. 55.

[46] BGH NJW 2011, 1509 Rn. 25 ff.

[47] BGH ZD 2014, 461 Rn. 15 mAnm Eckhardt.

Differenzierter sind jedoch eingehende E-Mails zu betrachten. E-Mails, die Viren oder andere Schadsoftware enthalten, sind grundsätzlich in der Lage, die IT-Infrastruktur des Arbeitgebers zu beeinträchtigen und damit eine Störung iSd § 12 Abs. 1 TDDDG herbeizuführen. Phishing-Mails sind in der Regel nicht in der Lage, die Funktionsfähigkeit der IT-Infrastruktur oder die Erbringung des Dienstes zu beeinträchtigen, da sie lediglich auf das Abgreifen von Informationen ausgerichtet sind. Somit kann die Bekämpfung solcher E-Mails auch nicht zum Zweck der Erkennung oder Beseitigung von Störungen iSd § 12 Abs. 1 TDDDG erfolgen.[48] Gleiches gilt für die Erforderlichkeit der Kenntnisnahme zum Schutz der technischen Systeme nach § 3 Abs. 3 Satz 1 TDDDG.

Das führt zu Wertungswidersprüchen, sofern man den Arbeitgeber als Anbieter von Telekommunikationsdiensten ansieht. Denn der Arbeitgeber würde insoweit eine Doppelrolle als Anbieter von Telekommunikationsdiensten und als Nutzer einnehmen, da er in Bezug auf die Privatnutzung als Telekommunikationsanbieter zu sehen wäre, ihn aber Angriffe auch auf Nutzerseite betreffen (dazu bereits oben Abschnitt III 1 c)). Der Arbeitgeber dürfte von Anbieterseite nach § 12 Abs. 1 TDDDG grundsätzlich Maßnahmen treffen, um Störungen seiner Anlagen und Dienste zu bekämpfen, die er einem Dritten, nämlich dem Arbeitnehmer erbringt bzw. zur Verfügung stellt.[49] Dies gilt aber eben nur, soweit der Angriff auf das Endgerät eine Störung darstellt. Bei Phishing-Mails ist dies aber in der Regel nicht der Fall. Sich gegenüber diesen zu schützen, liegt primär in der Verantwortung des Nutzers. In Bezug auf rein geschäftlich genutzte Postfächer ist dies für den Arbeitgeber, unter den Voraussetzungen der DSGVO und des BDSG, auch zulässig. Den Arbeitgeber durch die Erlaubnis der Privatnutzung als außenstehenden Dritten anzusehen und ihm insoweit die Schutzmöglichkeiten gegenüber Phishing-Angriffen zu entziehen oder jedenfalls zu erschweren, erscheint nicht sachgerecht. Auch haben Phishing-Mails in aller Regel keinen „beruflichen“ oder „privaten“ Charakter, sodass eine Abgrenzung hier nicht möglich wäre.

Eine solche Erweiterung des Schutzbereichs des Fernmeldegeheimnisses ist auch im Hinblick auf befürchtete Schutzlücken nicht angezeigt, denn die besondere Vertraulichkeit von Privatnachrichten in betrieblichen E-Mail-Postfächern findet auch im den allgemeinen Datenschutzvorschriften Berücksichtigung (dazu noch unten Abschnitt III 2 d) cc)).

f) Zwischenergebnis

Es ergeben sich Wertungswidersprüche aus der Regulierung des Arbeitgebers als geschäftsmäßiger Anbieter von Telekommunikationsdiensten iSd § 3 Abs. 2 Nr. 2 TDDDG, da der Arbeitgeber als solcher daran gehindert wäre, sich effektiv gegen Angriffe, die nicht unter den Störungsbegriff des § 12 TDDDG fallen zu schützen, was ihm aber als Nutzer möglich sein müsste. Der Arbeitgeber dürfte nur Maßnahmen gegen schädliche E-Mails treffen, nicht jedoch gegen Spam- und Phishing-Mails. In Bezug auf letztere müsste der Arbeitgeber die Mail zunächst zustellen und eine Einwilligung des Arbeitnehmers einholen oder abwarten, bis der Arbeitnehmer die Nachricht auf seinem Endgerät speichert,[50] um dann Maßnahmen unter der Geltung der DSGVO

---

[48] Vgl. Deusch/Eggendorfer K&R 2017, 93, 94 ff.

[49] Schutzobjekt des § 12 Abs. 1 TDDDG sind die eigenen Anlagen und Dienste des Telekommunikationsanbieters, vgl. Auernhammer/Heun, TTDSG § 12 Rn. 6. vgl. Plath/Jenny TTDSG § 12 Rn. 12.

[50] Zur zeitlichen Reichweite des Fernmeldegeheimnisses siehe Abschnitt III 1 d).

und des BDSG zu treffen. Dies erscheint nicht sachgerecht. Der Arbeitgeber nicht als Anbieter von Telekommunikationsdiensten einzustufen.

2. Allgemeiner Datenschutz

Folgt man richtigerweise der Ansicht, dass das Fernmeldegeheimnis auch bei erlaubter Privatnutzung nicht auf Arbeitgeber anwendbar ist, oder erfolgt ein Zugriff nach Ende des zeitlichen Anwendungsbereichs des Fernmeldegeheimnisses,[51] bemisst sich die Zulässigkeit des Zugriffs nach den allgemeinen Gesetzen, insbesondere dem allgemeinen Datenschutzrecht.[52] Die Anwendbarkeit der DSGVO und des BDSG setzt eine Verarbeitung personenbezogener Daten nach Art. 2 DSGVO bzw. § 1 BDSG voraus.

Das Abfragen und Auslesen von Daten aus einem E-Mail-Postfach stellt eine Verarbeitung dar, ebenso das Löschen potenziell schädlicher E-Mails (Art. 4 Nr. 2 DSGVO). Ob eine E-Mail ein personenbezogenes Datum darstellt, ist eine Frage des Einzelfalls, wird jedoch im Arbeitskontext regelmäßig zu bejahen sein, da der Arbeitgeber seinen Arbeitnehmern in der Regel einzelne E-Mail-Adressen zuweist und die jeweiligen Konten einem spezifischen Arbeitnehmer zuordnen kann.[53] Selbst bei gemeinschaftlich genutzten E-Mail-Postfächern lassen sich durch den Arbeitgeber mithilfe von Schichtplänen und ähnlichen Arbeitszeitangaben oftmals Rückschlüsse auf den Urheber einer Nachricht ziehen. Darüber hinaus können Header und Inhalt einer E-Mail Informationen über den anderen Kommunikationspartner beinhalten.[54] Die DSGVO und das BDSG ist daher in aller Regel anwendbar.

a) Verarbeitung im Beschäftigtenkontext nach § 26 Abs. 1 BDSG

Im Bereich des Arbeitnehmerdatenschutzes dürfen Mitgliedsstaaten unter den Voraussetzungen des Art. 88 DSGVO spezielle Regelungen treffen. Das hat der deutsche Gesetzgeber mit § 26 BDSG als Rechtsgrundlage für eine Verarbeitung personenbezogener Daten im Beschäftigungskontext getan.[55] § 26 BDSG geht, soweit sie speziellere Regelungen trifft, den allgemeinen Erlaubnissätzen aus Art. 6 DSGVO vor.[56]

§ 26 Abs. 1 BDSG besagt, dass personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses nur verarbeitet werden dürfen, wenn dies für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist. Zu dem nahezu wortgleichen § 23 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes („HDSIG“) hat der EuGH entschieden, dass dieser nicht die Voraussetzungen an eine „spezielle Regelung“ iSd Art. 88 DSGVO erfülle, wenn er lediglich die allgemeinen Regeln wiederhole.[57] Der Generalanwalt des EuGH hat in

---

[51] Siehe dazu Abschnitt III 1 d).

[52] LAG Hessen NZA-RR 2019, 130 Rn. 60.

[53] Fokken, NZA 2020, 629, 630; Vgl. Hoeren/Sieber/Holznagel/Schmitz Teil 16.2 Rn. 74 f.

[54] Dazu Brink/Schwab, ArbRAktuell 2018, 111.

[55] Das Bundesministerium für Arbeit und Soziales („BMAS“) und das Bundesministerium des Innern („BMI“) haben Anfang Oktober 2024 einen Referentenentwurf für eine Novelle des Arbeitnehmerdatenschutzrechts in Umlauf gebracht, in dem der § 26 BDSG durch ein Beschäftigtendatenschutzgesetz (BeschDG) ersetzt und erweitert werden soll. Im Angesicht der frühzeitigen Neuwahlen im Februar 2025 ist allerdings zum jetzigen Zeitpunkt nicht mit einer Verabschiedung zu rechnen.

[56] Vgl. BeckOK Datenschutzrecht/Riesenhuber, 49. Edition 2024, BDSG § 26 Rn. 113; Sydow/Marsch/Tiedemann, BDSG § 26 Rn. 19.

[57] EuGH NZA 2023, 487 mAnm Meinicke Rn. 71, 74.

seinen Schlussanträgen zu diesem Verfahren aber ausdrücklich vertreten, dass der § 23 HDSIG keine spezifischere Vorschrift iSd Art. 88 DSGVO sei und deswegen unangewendet bleiben müsse.[58] Gleiches gilt dann auch für den nahezu wortgleichen § 26 Abs. 1 BDSG.[59]

Da § 26 Abs. 1 BDSG in Bezug auf Art. 6 Abs. 1 lit. b und c DSGVO keine abweichenden Regelungen trifft, muss er unangewendet bleiben. Bis eine Folgeregelung erlassen wird, greifen stattdessen die allgemeinen Vorschriften aus Art. 6 Abs. 1 DSGVO.

b) Verarbeitung zur Erfüllung eines Vertrags nach Art. 6 Abs. 1 lit. b DSGVO

Nach Art. 6 Abs. 1 lit. b DSGVO ist eine Verarbeitung rechtmäßig, wenn sie zum Zwecke der Vertragserfüllung erforderlich ist. Die Vorschrift ist eng an den vertraglich vereinbarten Pflichten auszulegen.[60] Folglich ist eine Verarbeitung nicht für einen Vertrag erforderlich, wenn die vertragliche Leistung auch ohne die spezifische Verarbeitung erbracht werden kann.[61]

Eine störungsfreie Verfügbarkeit der betrieblichen IT-Systeme ist heutzutage für viele Unternehmen essenziell, da viele arbeitstechnische Prozesse digital stattfinden. Daher können Datenverarbeitungen zum Schutz der IT-Sicherheit grundsätzlich auch für die Erfüllung des Arbeits- oder Dienstvertrags erforderlich sein, wenn anderenfalls Gefahr droht, dass bestimmte Arbeitsleistungen nicht mehr erbracht werden können. Dies gilt aber allenfalls für Gefahren, die den Betriebsablauf unmittelbar einschränken können, insb. DoS/DDoS-Angriffe. Gleiches ließe sich annehmen bei E-Mails, die mit Viren oder anderen Schadsoftwares infiziert sind. Insoweit lassen sich die Ausführungen zu § 12 TDDDG (Abschnitt III 1 e)) entsprechend übertragen. Spam-Mails und Phishing-Mails, die lediglich auf das Erschleichen von Informationen beim Arbeitnehmer gerichtet sind, beeinträchtigen in der Regel nicht die Funktionsfähigkeit der für die Ausführung vertraglicher Pflichten notwendigen E-Mail-Dienste.[62] Sie sind an sich daher noch nicht geeignet, den Betriebsablauf in einer Weise zu beeinträchtigen, sodass die Ausführung vertraglicher Pflichten davon merklich beeinflusst wäre. Folglich ist die Verarbeitung von personenbezogenen Daten zur Abwehr von Spam- und Phishing-Angriffen für die Zwecke der Vertragserfüllung regelmäßig nicht erforderlich.

c) Verarbeitung zur Erfüllung einer gesetzlichen Pflicht nach Art. 6 Abs. 1 lit. c DSGVO

Nach Art. 6 Abs. 1 lit. c DSGVO ist eine Verarbeitung rechtmäßig, wenn sie zur Erfüllung einer Pflicht, dem der Verantwortliche unterliegt, erforderlich ist. IT- und

---

[58] EuGH GA Schlussanträge v. 22.9.2022, C-34/21 Rn. 75 ff.

[59] Vgl. BAG NZA 2023, 1404 Rn. 64.

[60] Heinzke/Engel ZD 2020, 189, 191; vgl. Simitis/Hornung/Spiecker gen. Döhmann/Schantz, 2. Aufl. 2025, DSGVO Art. 6 Abs. 1 Rn. 34; „auf das absolut Notwendige [beschränkt]“ EuGH ZD 2017, 324 Rn. 30; EuGH GRUR-RS 2010, 91284 Rn. 77.

[61] EDSA,Leitlinien 2/2019 Version 2.0 Rn. 17; in diesem Sinne auch Sydow/Marsch/Reimer, DSGVO Art. 6 Rn. 27 ff.; ebenso Simitis/Hornung/Spiecker gen. Döhmann/Schantz DSGVO Art. 6 Abs. 1 Rn. 35.

[62] Vergleichbar sind Verarbeitungen zum Zwecke der Betrugsbekämpfung, welche ebenfalls in der Regel nicht zur Vertragserfüllung erforderlich sind, so EDSA,Leitlinien 2/2019 Rn. 50; Heinzke/Engel, ZD 2020, 189, 193.

Datensicherheitspflichten ergeben sich insbesondere aus Art. 25 und 32 DSGVO sowie künftig aus dem Umsetzungsgesetz zur NIS2-Richtlinie[63] und aus Spezialgesetzen (zB Art. 15 AI Act). Diese Pflichten sehen aber lediglich allgemein vor, geeignete Maßnahmen zu treffen. Eine Verpflichtung iSd Art. 6 Abs. 1 lit. c DSGVO muss sich aber konkret auf die Verarbeitung personenbezogener Daten beziehen. Sofern dem Verantwortlichen hinsichtlich der Verarbeitung zur Erfüllung einer gesetzlichen Pflicht ein umfangreicher Ermessensspielraum zur Verfügung steht, ist die Vorschrift keine „spezifische Bestimmung" iSd Art. 6 Abs. 2 und 3 DSGVO.[64] Die Verarbeitung kann aber gegebenenfalls unter Art. 6 Abs. 1 lit. f DSGVO fallen.

d) Verarbeitung zur Wahrung berechtigter Interessen nach Art. 6 Abs. 1 lit. f DSGVO

Nach Art. 6 Abs. 1 lit. f DSGVO ist eine Verarbeitung personenbezogener Daten dann rechtmäßig, wenn sie zur Wahrung berechtigter Interessen erforderlich ist und die Interessen des Betroffenen die berechtigten Interessen des Verantwortlichen an der Verarbeitung nicht überwiegen. Die Vorschrift hat daher drei kumulative Voraussetzungen: Erstens muss von dem für die Verarbeitung Verantwortlichen oder von einem Dritten ein berechtigtes Interesse wahrgenommen werden, zweitens muss die Verarbeitung der personenbezogenen Daten zur Verwirklichung des berechtigten Interesses erforderlich sein und drittens dürfen die Interessen oder Grundrechte und Grundfreiheiten der Person, deren Daten geschützt werden sollen, gegenüber dem berechtigten Interesse des Verantwortlichen oder eines Dritten nicht überwiegen.[65]

aa) Berechtigtes Interesse

Der Verantwortliche muss ein berechtigtes Interesse an der Datenverarbeitung haben. Diese Interessen können rechtlicher, wirtschaftlicher sowie ideeller Natur sein.[66] Es werden in Art. 6 Abs. 1 lit. f DSGVO neben den berechtigten Interessen des Verantwortlichen auch ausdrücklich berechtigte Interessen Dritter berücksichtigt. Im Arbeitskontext kommen als Dritte insbesondere Geschäftspartner des Arbeitgebers in Betracht.

Das Interesse an Sicherheit und Integrität der IT-Infrastruktur stellt ein berechtigtes Interesse iSd Art. 6 Abs. 1 lit. f DSGVO dar.[67] Zum einen hat die Organisation ein sich aus der Berufsfreiheit (Art. 12 GG, Art. 15 EUGRCh) und der unternehmerischen Freiheit (Art. 16 EUGRCh) ergebendes Interesse an der Funktionsfähigkeit ihrer IT-Infrastruktur, da heutzutage ein immer größerer Teil der betrieblichen Abläufe digital erfolgt. Zum anderen ergibt sich auch ein schützenswertes Interesse aus der Eigentumsfreiheit (Art. 14 GG, Art. 17 EUGRCh), einerseits in Bezug auf die betriebliche Hardware, andererseits in Bezug auf geschütztes geistiges Eigentum, das sich auf den Servern der Organisation befindet.

---

[63] Richtlinie (EU) 2022/2555.

[64] Dazu bereits Art. 29-Datenschutzgruppe, WP 217, III.2.3; EDSA,Personenbezogene Daten rechtmäßig verarbeiten, https://www.edpb.europa.eu/sme-data-protection-guide/process-personal-data-lawfully_de#toc-4, vgl. auch ErwGr. 45 DSGVO.

[65] EuGH Urt. v. 4.7.2023 – C-252/21 Rn. 105 ff.; EuGH Urt. v. 17.6.2021 – C-597/19 Rn. 106.

[66] Simitis/Hornung/Spiecker gen. Döhmann/Schantz DSGVO Art. 6 Abs. 1 Rn. 100; Kühling/Buchner/Petri DSGVO Art. 6 Rn. 146a; OVG Lüneburg MMR 2017, 593 Rn. 15.

[67] EDSA, Leitlinien 1/2024, Konsultationsentwurf v. 8.10.2024 Rn. 126 ff.; ErwGr. 49 DSGVO; EuGH Urt. v. 4.7.2023 – C-252/21 Rn. 119.

Im Übrigen verpflichtet die DSGVO den Verantwortlichen nach Art. 25 und 32 DSGVO, technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten zu treffen. Nach Art. 32 Abs. 1 lit. b DSGVO schließt dies ausdrücklich Maßnahmen ein, die „die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer [sicherstellen]".

bb) Erforderlichkeit

Die Verarbeitung muss zur Wahrung des berechtigten Interesses auch erforderlich sein. Erforderlich ist eine Maßnahme dann, wenn die Verarbeitung auf das für die Zwecke absolut Notwendige beschränkt ist.[68] Dabei ist darauf abzustellen, ob das berechtigte Interesse nicht in zumutbarer Weise ebenso wirksam mit anderen, weniger eingriffsintensiven Mitteln, erreicht werden kann.[69]

Phishing- und Malware-E-Mails zielen gerade darauf ab, die Schwachstelle Mensch in der IT-Sicherheit einer Organisation auszunutzen. Den damit verbundenen Gefahren wird unter anderem durch Maßnahmen wie Mitarbeiterschulungen und automatisierte E-Mail-Filter oder Meldesystemen begegnet. Jedoch sind diese Maßnahmen, wie oben dargestellt (Abschnitt II 4), mit einem nicht unerheblichen Restrisiko verbunden. Automatisierte E-Mail-Filter können verdächtige E-Mails nur auf Grundlage vordefinierter Eigenschaften erkennen, sodass hier sowohl auf der falsch-positiven als auch auf der falsch-negativen Seite Fehlerpotenzial besteht. Schulungen und Meldesysteme setzen voraus bzw. sehen vor, dass der durchschnittliche Mitarbeiter in den Umgang mit verdächtigen Mails involviert ist. Hierbei kann es ebenfalls zu Falscheinschätzungen oder Versehen kommen, was zulasten der IT-Sicherheit geht. Schulungen können dieses Risiko nur bis zu einem gewissen Grad mindern. Bei der (zentralisierten) manuellen Löschung ließe sich sicherstellen, dass speziell geschultes Personal die primäre Handhabung verdächtigter E-Mails übernimmt, wodurch zum einen die Trefferquote steigt, zum anderen das Risiko versehentlicher Schäden sinkt. Die zuvorderst genannten Maßnahmen stellen zwar mildere Mittel im Vergleich zur manuellen Löschung dar, allerdings sind sie nicht in gleicher Weise geeignet, ein hohes Maß an IT-Sicherheit zu gewährleisten. Somit ist das Erreichen eines entsprechend hohen IT-Sicherheitsniveaus nicht in zumutbarer Weise ebenso wirksam mit anderen, weniger eingriffsintensiven Mitteln zu erreichen und damit das manuelle Löschen erforderlich. Bevor eine Phishing-Mail zentralisiert gelöscht werden kann, müssen aber zunächst Maßnahmen getroffen werden, um diese E-Mails zu identifizieren.

Eine Einsichtnahme des Inhalts ist dabei grundsätzlich nicht erforderlich, da sich Phishing-Mails in der Regel auch auf anderen Wegen identifizieren lassen. Hinweise können sich etwa durch den Vergleich von IP-Adressen der bei der Übertragung beteiligten Mailserver ergeben. Hierzu können beispielsweise Informationen einer bereits gegebenen Phishing-Nachricht automatisiert mit den Nachrichten in den sonstigen Postfächern abgeglichen werden. Dafür sind technisch betrachtet verschiedene Optionen gegeben.

Zum einen können die im E-Mail-Header enthaltenen Übertragungspfade untersucht werden, die Aufschluss über den Versandweg einer Nachricht vom Server des Absenders über verschiedene andere Mailserver zum Server des Empfängers geben. Durch

---

[68] EuGH GRUR 2023, 1131 Rn. 109 mwN, Rn. 126.

[69] EuGH GRUR 2023, 1131 Rn. 108; EuGH Urt. v. EuGH Urt. v. 22.6.2021 – C-439/19 Rn. 110; EuGH Urt. v. 17.6.2021 – C-597/19 Rn. 110; EuGH Urt. v. 4.5.2017 – C-13/16 Rn. 30 mwN.

einen Vergleich dieser Pfade können identische bzw. ähnliche Nachrichten identifiziert werden, ohne Einsicht in Inhaltsdaten zu nehmen.

Eine weitere Möglichkeit zum Abgleich ist die Berechnung eines Prüfwertes ähnlich dem Prinzip einer Hashfunktion für alle Nachrichten, wobei sich für gleiche bzw. ähnliche Nachrichten auch gleiche bzw. ähnliche Prüfwerte ergeben.[70] Von einem vorliegenden Prüfwert ist kein Rückschluss auf den tatsächlichen Inhalt der ursprünglichen Nachricht möglich. Durch Vergleich des Prüfwertes einer gegebenen Phishing-Nachricht mit den Werten der Nachrichten in den Postfächern ist es nun möglich, Rückschluss auf die Existenz gleichartiger Phishing-Nachrichten zu ziehen, ohne den Inhalt der Nachrichten unmittelbar in die Prüfung miteinzubeziehen.

Die vorgenannten Maßnahmen sind geeignet, Phishing-Nachrichten zu identifizieren, wenn sie in Wellen auftreten und sofern bereits eine Phishing-Nachricht gemeldet wurde. Somit ist ein direkter Zugriff auf den Klartext des Nachrichteninhalts in der Regel nicht erforderlich. Nur sofern diese oder ähnliche Maßnahmen nicht zweifelsfrei darlegen können, dass es sich bei der untersuchten E-Mail um eine Phishing-Mail handelt, kann eine Einsichtnahme („Kontrollblick“) des Nachrichteninhalts eines zuständigen Mitarbeiters erforderlich sein.

Werden zur Durchführung dieser Maßnahmen personenbezogene Daten (zB Metadaten wie IP-Adressen) gespeichert, sind diese nicht länger aufzubewahren als für die Identifikation einer möglichen Phishing-Mail unbedingt erforderlich[71] (vgl. Art. 5 Abs. 1 lit. e DSGVO).

cc) Interessenabwägung

Zuletzt dürfen die Interessen des Betroffenen die berechtigten Interessen des Verantwortlichen an der Verarbeitung nicht übersteigen.

Aufseiten des Betroffenen steht insbesondere ein Geheimhaltungsinteresse, was sich allgemein aus dem Recht auf Privatsphäre (Art. 7 Var. 1 EUGRCh) und Datenschutz (Art. 8 EUGRCh) ergibt, aber auch mittelbar aus anderen Grundrechten wie der Meinungsfreiheit (Art. 11 EUGRCh) oder der Vereinigungsfreiheit insb. mit Blick auf Gewerkschaftszugehörigkeit (Art. 12 EUGRCh).

Die Abwägung der Interessen hängt von einer Vielzahl an Faktoren ab. Zunächst ist freilich die Gewichtung der Interessen, Grundrechte und Grundfreiheiten des Betroffenen selbst in die Bewertung mit einzubeziehen.[72]

Des Weiteren müssen die Auswirkungen der Verarbeitung auf den Betroffenen Berücksichtigung finden hinsichtlich der Art der Daten, des Verarbeitungskontextes und

---

[70] Derartige Verfahren werden allgemein unter dem Begriff *fuzzy hashing* zusammengefasst und finden in verschiedenen Bereichen der IT-Sicherheit Anwendung. Im Kontext von Phishing-Nachrichten werden diese bereits bei der Erkennung und Filterung eingesetzt, wobei eingehende E-Mails mit bereits bekannten hinsichtlich der Ähnlichkeit verglichen werden. Beispiele für verschiedene Implementierungen sind etwa ssdeep (https://github.com/ssdeep-project/ssdeep), TLSH (https://github.com/trendmicro/tlsh) oder spamsum (https://www.samba.org/ftp/unpacked/junkcode/spamsum/README).

[71] Der BGH hat für die Speicherung von IP-Adressen zur Erkennung und Beseitigung von Störungen eine Dauer von bis zu sieben Tagen für zulässig erachtet, BGH MMR 2011, 341 Rn. 22, 28, 33; BGH ZD 2014, 461 Rn. 6 ff. mAnm Eckhardt; Ebenso BfDI, aber „höchstens sieben Tage“, BfDI Datenschutz und Telekommunikation (Info 5), Stand 1/2024 S. 44; BfDI und BNetzA Leitfaden für eine datenschutzgerechte Speicherung von Verkehrsdaten Stand 30.9.2022 S. 7; krit. aber Geppert/Schütz/Braun TTDSG § 12 Rn. 14; Breyer MMR 2011, 573, 575.

[72] EDSA, Leitlinien 1/2024, Konsultationsentwurf v. 8.10.2024 Rn. 36.

der etwaigen weiteren Folgen der Verarbeitung.[73] Hierbei ist vor allem zu berücksichtigen, welche Sensibilität die verarbeiteten Daten haben[74] (insb. Art. 9 oder 10 DSGVO aber auch, ob es sich um private oder geschäftliche Kommunikation handelt), welche Menge an Daten insgesamt und pro Betroffenem verarbeitet werden[75] und wie lange sie gespeichert werden[76] und welche Risiken für den Betroffenen aus der Verarbeitung der jeweiligen Daten entstehen können (zB Entscheidungen auf Grundlage der Verarbeitung, rechtliche Konsequenzen, Gefahr von Diskriminierung oder Diffamierung, Gefahr finanzieller Schäden).[77] Im Beschäftigtendatenschutz ist besonders das Abhängigkeitsverhältnis, aber auch das besondere Näheverhältnis zwischen Arbeitgeber und Arbeitnehmer in die Bewertung mit einzubeziehen.[78] Auch ist insbesondere einzubeziehen, ob durch die Maßnahme ein Überwachungsklima und gegebenenfalls ein Anpassungsdruck entsteht.[79]

Diese Risiken und Schutzbedürfnisse können dadurch mitigiert werden, dass der Arbeitgeber besondere Schutzmaßnahmen trifft. Dies ist bei der Interessenabwägung zu berücksichtigen. Die bloße Existenz notwendiger Sicherheitsmaßnahmen trägt allerdings kein großes Gewicht zugunsten des Verantwortlichen, da diese einzurichten bereits seine Pflicht nach Art. 25 DSGVO ist.[80]

Ebenfalls eine wichtige Rolle bei der Interessenabwägung spielen die berechtigten Erwartungen des Betroffenen.[81] Diese können sich zunächst aus den Informationen ergeben, die der Verantwortliche den Betroffenen nach Art. 12–14 DSGVO und darüber hinaus bereitstellt.[82] Insbesondere fällt ins Gewicht, ob der Betroffene die Verarbeitung überhaupt kennt.[83] Darüber hinaus können sich auch Erwartungen aus dem Verhältnis zwischen Verantwortlichem und Betroffenem ergeben, sowie aus der Umgebung der Verarbeitung.[84] Hierbei ist auch zu berücksichtigen, dass der Arbeitnehmer bei einer verbotswidrigen Privatnutzung des geschäftlichen E-Mail-Postfachs nicht von einem besonderen Schutz der Vertraulichkeit seines Postfachs ausgehen kann.

---

[73] EDSA, Leitlinien 1/2024, Konsultationsentwurf v. 8.10.2024 Rn. 32; vgl. Taeger/Gabel/Taeger, DSGVO Art. 6 Rn. 149; vgl. auch EGMR EuZW 2018, 169 Rn. 121.

[74] Simitis/Hornung/Spiecker gen Döhmann/Schantz DSGVO Art. 6 Abs. 1 Rn. 107; Herfurth, ZD 2018, 514, 516.

[75] EDSA, Leitlinien 1/2024, Konsultationsentwurf v. 8.10.2024 Rn. 43; Robrahn/Bremert, ZD 2018, 291, 294; Herfurth, ZD 2018, 514, 516; Simitis/Hornung/Spiecker gen. Döhmann/Schantz DSGVO Art. 6 Abs. 1 Rn. 108.

[76] Herfurth, ZD 2018, 514, 519.

[77] EDSA, Leitlinien 1/2024, Konsultationsentwurf v. 8.10.2024 Rn. 45; Simitis/Hornung/Spiecker gen. Döhmann/Schantz DSGVO Art. 6 Abs. 1 Rn. 109.

[78] EDSA, Leitlinien 1/2024, Konsultationsentwurf v. 8.10.2024 Rn. 43; Herfurth, ZD 2018, 514, 518; vgl. auch ErwGr. 47 Satz 2 DSGVO.

[79] Vgl. BAG NZA 2017, 1205 Rn. 30.

[80] EDSA; Leitlinien 1/2024, Konsultationsentwurf v. 8.10.2024 Rn. 48; Robrahn/Bremert, ZD 2018, 291, 295.

[81] ErwGr. 47 DSGVO; Simitis/Hornung/Spiecker gen. Döhmann/Schantz DSGVO Art. 6 Abs. 1 Rn. 110; EDSA, Leitlinien 1/2024, Konsultationsentwurf v. 8.10.2024 Rn. 32; vgl. auch EGMR EuZW 2018, 169 Rn. 121.

[82] EDSA, Leitlinien 1/2024, Konsultationsentwurf v. 8.10.2024 Rn. 53.

[83] ErwGr. 47 Satz 4 DSGVO; vgl. dazu die Rechtsprechung des BAG zur Mitarbeiterüberwachung allgemein BAG NJW 2005, 313; zur verdeckten Überwachung BAG NJW 2017, 843; BAG NZA 2011, 571; BAG NJOZ 2005, 2708; BAG NJW 2017, 3258; zur offenen Überwachung BAG NZA 2023, 1105; BAG NZA 2018, 1329.

[84] EDSA, Leitlinien 1/2024, Konsultationsentwurf v. 8.10.2024 Rn. 54.

In Bezug auf die berechtigten Erwartungen des Arbeitnehmers ist zunächst zu sagen, dass sich Angriffserkennungssysteme sowohl bei betrieblicher IT-Infrastruktur als auch bei der Nutzung von E-Mail-Diensten speziell als gängige Praxis etabliert haben. Dass zu diesem Zweck Verkehrsdaten verarbeitet werden müssen, wird für den Arbeitnehmer in der Regel nicht überraschend sein. Erlaubt der Arbeitgeber den Arbeitnehmern auch die private Nutzung der geschäftlichen E-Mail-Adresse, so kann der Arbeitnehmer berechtigterweise erwarten, dass der Arbeitgeber besondere Maßnahmen zum Schutz der Vertraulichkeit dieser Nachrichten trifft. Darüber hinaus richten sich die berechtigten Interessen auch nach den durch den Arbeitgeber zur Verfügung gestellten Informationen.[85] Es ist dem Arbeitgeber zu empfehlen, den Arbeitnehmer im Vorhinein ausdrücklich und transparent über durchgeführte Methoden zu informieren.

Da jedes E-Mail-Postfach gleichsam Ziel eines Phishing-Angriffs sein kann, erstrecken sich die Abwehrmaßnahmen auch auf alle Mitarbeiterpostfächer. Somit sind alle Mitarbeiter zunächst unterschiedslos von der Datenverarbeitung betroffen. Da die Anzahl betroffener Personen hoch und die Verarbeitung nicht auf einen zeitlichen Rahmen begrenzt ist, müssen an anderer Stelle mildernde Maßnahmen getroffen werden, damit nicht die Gefahr eines unzulässigen, permanenten Überwachungsdrucks besteht.[86] So ist etwa die Menge und Sensibilität der verarbeiteten personenbezogenen Daten dadurch zu reduzieren, dass zunächst nur Abgleiche von Metadaten oder Prüfwerten[87] (siehe oben Abschnitt III 2 d) bb)) vorgenommen werden, um Hinweise auf mögliche Phishing-Nachrichten zu erlangen.

Werden im Rahmen einer nicht einzelfallbezogenen Datenverarbeitung im Vorfeld personenbezogene Daten gespeichert, ist durch technische und organisatorische Maßnahmen sicherzustellen, dass ein späterer Zugriff auf diese Daten lediglich durch Mitarbeiter (idR der IT-Abteilung), die mit der Löschung von Phishing-Nachrichten betraut sind, beschränkt ist und darüber hinaus die Daten nicht zu Zwecken weiterverarbeitet werden, die nicht mit dem Zweck der Erhebung kompatibel sind (vgl. Art. 6 Abs. 4 DSGVO).

Ein umfassender, nicht einzelfallbezogener Zugriff auf den Inhalt von E-Mails der Arbeitnehmer ist, erst recht bezüglich privater E-Mails, aber auch bezüglich geschäftlicher E-Mails, nicht zulässig, weil dadurch ein permanenter Überwachungs- und Anpassungsdruck entstehen kann.[88]

Ein „Kontrollblick“ auf den Inhalt einer E-Mail kann höchstens dann zulässig sein, wenn ein erhärteter Verdacht auf eine oder mehrere Phishing-Mails besteht. Zum einen ist das Gefährdungspotential in diesem Fall noch einmal verstärkt, zum anderen besteht nur eine sehr geringe Gefahr, dass sich die verdächtigte E-Mail tatsächlich als E-Mail mit privatem Inhalt herausstellt.

Der Löschung einer bereits sicher identifizierten Phishing-Mail stehen keine schwerwiegenden Interessen des Betroffenen entgegen.[89] Der Arbeitnehmer hat in der Regel kein Interesse an dem Erhalt einer Phishing-Mail, sodass dessen Interessen nicht überwiegen.

---

[85] Beispielsweise in Arbeitsverträgen, Betriebsvereinbarungen, Datenschutzerklärungen aber auch Aushängen und anderen Informationsquellen.

[86] Vgl. BAG NZA 2017, 1205 Rn. 30.

[87] D.h. anonymisierten oder pseudonymisierten Daten.

[88] Vgl. BAG NZA 2017, 1205 Rn. 30.

[89] Simitis/Hornung/Spiecker gen. Döhmann/Schantz DSGVO Art. 6 Abs. 1 Rn. 117.

IV. Ergebnis

Die Bedrohungslage durch Phishing-Angriffe gestaltet sich vielseitig. Um ihr effektiv zu begegnen, ist die zentralisierte, manuelle Löschung von Phishing-Nachrichten eine praktikable und besonders effiziente und leichte Maßnahme. Dies darf jedoch nicht zu einer durchgehenden, umfassenden Mitarbeiterüberwachung führen. Erst recht darf dies nicht dazu führen, dass Arbeitgeber exzessive Einblicke in private Kommunikation der Arbeitnehmer erlangen.

Unabhängig davon, ob ein Arbeitgeber seinen Arbeitnehmern die private Nutzung der betrieblichen E-Mail erlaubt oder nicht erlaubt, ist ein anlassloser Zugriff auf Nachrichteninhalte zum Zweck der Bekämpfung von Phishing unzulässig, da dies zu einer umfassenden Mitarbeiterüberwachung und damit zu einem permanenten Überwachungs- und Anpassungsdruck führen würde. Die Interessen des Arbeitnehmers überwiegen dann die berechtigten Interessen des Arbeitgebers nach Art. 6 Abs. 1 lit. f DSGVO.

Einer Organisation, die eine manuelle Löschung einführen möchte, ist zu empfehlen, den Arbeitnehmern die private Nutzung des geschäftlichen E-Mail-Kontos, zB im Arbeitsvertrag oder einer Betriebsvereinbarung, zu untersagen. Die Maßnahmen zur Erkennung und Identifikation von Phishing-Nachrichten sollten darüber hinaus so ausgestaltet sein, dass sie zunächst keine Einsichtnahme des Nachrichteninhalts erfordern. Eine Einsichtnahme des Nachrichteninhalts („Kontrollblick“) kann aber dann zulässig sein, wenn bereits ein erhärteter Verdacht besteht, dass es sich bei der untersuchten E-Mail um Phishing handelt, aber dennoch keine absolute Sicherheit besteht. Die Organisation sollte außerdem sicherstellen, dass die Mitarbeiter über das Verfahren der manuellen Löschung sowie die damit verbundenen Zugriffs- und Datenverarbeitungsvorgänge ausreichend informiert sind. Durch technische und organisatorische Maßnahmen sollte außerdem sichergestellt sein, dass ein Zugriff auf diese Daten lediglich auf zuständige Mitarbeiter beschränkt ist und darüber hinaus die Daten nicht zu anderen Zwecken weiterverarbeitet werden. Ebenso sind bei Identifikation von und bei Zugriff auf identifizierte Phishing-Mails die sonstigen datenschutzrechtlichen Grundsätze einzuhalten. Insbesondere ist dabei das Verfahren im Sinne der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) so zu konzipieren, dass möglichst wenig personenbezogene Daten verarbeitet werden und dass diese im Sinne der Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO) gelöscht werden, sobald sie nicht mehr für die Identifizierung von Phishing-Angriffen erforderlich sind. Zusätzliche Maßnahmen wie Mitarbeiterschulungen oder die Etablierung geeigneter Meldeprozesse sind weiterhin erforderlich und sinnvoll. Meldungen verdächtiger Nachrichten unterstützen beispielsweise das für die manuelle Löschung zuständige IT-Personal bei der Identifizierung betrügerischer E-Mails. Des Weiteren sind Mitarbeiterschulungen erforderlich, um ein Grundwissen bei der Erkennung von Phishing-Nachrichten aufzubauen und Fälle abzusichern, in denen eine betrügerische E-Mail nicht rechtzeitig durch die manuelle Löschung aus betroffenen Postfächern entfernt wird, beziehungsweise es sich nicht um eine Welle von Phishing-Nachrichten handelte.

The IT security of organizations is more important than ever in view of the rising number of cyber attacks and the increasing digitalization of work processes. A common attack method on organizations is the use of phishing emails, which can be used to steal important internal information or access data. To effectively combat phishing in

organizations, it is appropriate that phishing emails can be deleted centrally by IT employees. A decisive role for the legal admissibility of centralized deletion is played by the question of whether an employer is bound by telecommunications secrecy if he allows his employees to use the work email service for personal purposes. This article sheds light on the technical and legal challenges in the fight against phishing and works out the conditions under which manual and centralized deletion of phishing emails from employee mailboxes is permissible.