WIE ICH AN DEINE DATEN KAM ODER DARK PATTERNS UND PHISHING IM BESCHÄFTIGTENKONTEXT

Hartmut Schmitt / Christian K. Bosse / Aljoscha Dietrich / Svenja Polst

Projektleiter, HK Business Solutions GmbH, Mellinweg 20, 66280 Sulzbach, DE, hartmut.schmitt@hk-bs.de, http://www.hk-bs.de

Wissenschaftlicher Mitarbeiter, Institut für Technologie und Arbeit, Trippstadter Str. 113, 67663 Kaiserslautern, DE, christian.bosse@ita-kl.de, https://ita-kl.de

Wissenschaftlicher Mitarbeiter, Lehrstuhl für Rechtsinformatik, Universität des Saarlandes, 66123 Saarbrücken, DE, aljoscha.dietrich@uni-saarland.de, https://www.legalinf.de

Wissenschaftliche Mitarbeiterin, Fraunhofer IESE, User Experience & Requirements Engineering, Fraunhofer-Platz 1, 67663 Kaiserslautern, DE, svenja.polst@iese.fraunhofer.de, https://www.iese.fraunhofer.de/de/competencies/security.html

Schlagworte: ***Beschäftigtendatenschutz, Social Engineering, Dark Strategies, soziotechnisches System***

Abstract: *Ein maßgeblicher Aspekt der Digitalisierung betrifft die Verarbeitung personenbezogener Daten und führt daher zu einer höheren Bedeutung des Datenschutzes. Bei der Praxis datenschutzrechtlicher Einwilligungen zeigt sich jedoch ein Trend zu immer subtileren Techniken, die Betroffenen so zu manipulieren, dass sie entgegen ihren eigentlichen Interessen handeln – etwa durch Dark Patterns und Nudging. In diesem Beitrag stellen wir dar, inwiefern diese Praktiken im Beschäftigtenkontext Anwendung finden, welche psychologischen Wirkzusammenhänge sie nutzen, wie sie aus datenschutzrechtlicher und arbeitswissenschaftlicher Sicht einzuordnen sind, und schlagen mögliche Lösungsansätze vor.*

1. Motivation

Im Bereich Beschäftigtendatenschutz gibt es umfangreiche Rechtsprechungen und Literatur, die regeln, wie mit Daten von Beschäftigten zu verfahren ist. So geben Rechtsprechungen und Literatur zum Beispiel einen Rahmen für Videoüberwachung im Arbeitskontext vor. Jedoch gibt es auch Teilgebiete des Beschäftigtendatenschutzes, die aus Mangel an Vorgaben in einem rechtlichen Graubereich liegen. In diesem Graubereich befinden sich Datenverarbeitungen, bei denen psychologische Faktoren ins Spiel kommen oder das Verhalten der Beschäftigten manipuliert wird. Verschärft wird die Situation in diesem Graubereich durch die zunehmende Digitalisierung der Wirtschaft. Denn neue Möglichkeiten der Datenerhebung und -nutzung, die sich in Bezug auf personenbezogene Daten der Beschäftigten ergeben, wecken neue Begehrlichkeiten, nicht zuletzt seitens der Arbeitgeber[1]. Eine Auflösung dieses Graubereichs sollte eigentlich auch im Sinne der Unternehmen sein, um den abschreckenden Sanktionen der DSGVO zu entgehen. Jüngstes Beispiel ist die verhängte Rekordstrafe von 35 Millionen Euro gegen H&M.[2] Hinzu kommen geänderte Arbeitsformen und -modelle, beispielsweise der durch die Corona-Pandemie ausgelöste Homeoffice-Boom, der den Wunsch vieler Arbeitgeber befeuerte, ihre Mitarbeiter, die nicht mehr in der räumlichen Einflusssphäre des Unternehmens waren, stärker zu überwachen.[3]

---

1 Christian K. Bosse, Aljoscha Dietrich, Patricia Kelbert, Hagen Küchler, Hartmut Schmitt, Jan Tolsdorf, Andreas Wessner: Beschäftigtendatenschutz: Rechtliche Anforderungen und Technische Lösungskonzepte. In: Jusletter IT 28. Februar 2020.

2 Vgl. Schemm, M.: https://datenschutz-hamburg.de/pressemitteilungen/2020/10/2020-10-01-h-m-verfahren.

3 Vgl. Moorstedt, M.: https://www.sueddeutsche.de/digital/home-office-ueberwachung-tracking-chef-zoom-1.4868739, SZ, 2020.

Über den Beschäftigtenkontext hinaus gewinnt der Themenkomplex *Dark Patterns*, *Nudging* und *Social Engineering* sowohl in der Forschung als auch in der öffentlichen Wahrnehmung zunehmend an Bedeutung. Im Kern geht es um eine Manipulation von Personen mithilfe von Praktiken, deren Ursprung häufig in der Psychologie liegt bzw. die sich mit psychologischen Modellen erklären lassen. Auf Basis dieser Modelle wurde in der IT-Security-Literatur[4] beschrieben, wie sich durch geschickte Manipulation von Personen ein unberechtigter Zugang zu Systemen erreichen lässt. Diese Praktiken, bei denen oft nicht scharf zwischen Online- und Offline-Welt unterschieden werden kann, sind nicht immer als negativ zu bewerten. Ein gutes Beispiel hierfür ist das Nudging, bei dem es darum geht, (subtil) einen Anstoß zu einem bestimmten sozial erwünschten Verhalten zu geben, also „bessere" Entscheidungen herbeizuführen.[5] Mit der gleichen Technik können Personen jedoch auch dazu gebracht werden, entgegen ihren eigentlichen Absichten zu handeln, etwa zu freizügigen Privacy-Einstellungen zuzustimmen.

In diesem Beitrag zeigen wir auf, wie entsprechende Praktiken in die Welt des Beschäftigtendatenschutzes übertragen werden (können) beziehungsweise dort eingesetzt werden, um das Datenschutzniveau zu senken. Zunächst beschreiben wir, wer überhaupt ein möglicher Angreifer sein kann, also wer ein entsprechendes Interesse haben kann, und über welche Mittel er verfügt. Im Folgenden stellen wir Praktiken vor, die dazu geeignet sind, Arbeitnehmer unbewusst zu manipulieren, so dass diese entgegen ihren eigentlichen Interessen handeln und mehr über sich preisgeben, als sie beabsichtigen. Diese Thematik beleuchten wir aus juristischer sowie arbeitswissenschaftlicher Perspektive und skizzieren Lösungsansätze. Hierbei fokussieren wir ausschließlich datenschutzrechtliche Aspekte, nehmen jedoch keine arbeits- oder strafrechtliche Einordnung vor.

2. Verwandte Themenbereiche

Insbesondere in der IT-Sicherheit, wo der Mensch traditionell als das schwächste Glied in der Sicherheitskette gilt[6], gibt es eine Reihe von Angriffsarten, die mit Verhaltensmanipulationen im Bereich Beschäftigtendatenschutz vergleichbar sind. Diese Angriffsarten haben jedoch meist andere Angriffsziele, nämlich Unternehmensdaten von hohem Wert. Der folgende Überblick soll dabei helfen, vergleichbare Praktiken und bestimmte Phänomene der Verhaltensmanipulation besser zu verstehen – ihre Gemeinsamkeiten mit den in Abschnitt 3 beschriebenen Praktiken aus dem Beschäftigtendatenschutz, aber auch bestehende Unterschiede.

Als *Social Engineering* werden Methoden der Verhaltensmanipulation bezeichnet, bei denen menschliche Eigenschaften wie z. B. Hilfsbereitschaft, Vertrauen oder Respekt vor Autorität ausgenutzt werden, um unberechtigten Zugang zu Informationen oder IT-Systemen zu erlangen.[7] Die meistverbreitete Form[8] ist das sogenannte *Phishing* (abgeleitet von password und fishing), bei dem Cyberkriminelle versuchen, mittels gefälschter E-Mails und Webseiten Zugangsdaten zum Onlinebanking, zu Onlineshops oder ähnliches zu erlangen. Dient das Social Engineering dem Eindringen in ein fremdes Computersystem oder Netzwerk, so bezeichnet man dies auch als *Social Hacking*.[9] Arbeitgeber oder Vorgesetzte werden beim Social Engineering gemeinhin nicht als Angreifer thematisiert.[10]

---

4 Siehe z. B. Anderson, Ross J. (2008): Security Engineering: A Guide to Building Dependable Distributed Systems, S. 17 ff. Wiley, Indianapolis.

5 Thaler, R. H.; Sunstein, C. R. (2008): Nudge: Improving Decisions about Health, Wealth, and Happiness. Yale University Press.

6 Angela Sasse, Sacha Brostoff, Dirk Weirich (2001): Transforming the 'Weakest Link' – a Human/Computer Interaction Approach to Usable and Effective Security. In: BT Technology Journal 19(3), S. 122 ff.

7 Vgl. Anderson, S. 40 ff.

8 Bundesamt für Sicherheit in der Informationstechnik (2020): Phishing: Wie der Datenklau funktioniert. https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/Phishing_Datenklau.html.

9 Walter Fumy, Joerg Sauerbrey (Hrsg.): Enterprise Security. 2006. Publicis, Erlangen.

10 Siehe z. B. Social-Engineer, Inc. (2020): Categories of Social Engineers https://www.social-engineer.org/framework/general-discussion/categories-social-engineers/.

Als *Dark Patterns* werden wiederkehrende Muster bezeichnet, die bei der Gestaltung von Benutzeroberflächen eingesetzt werden, um den Nutzer irrezuführen oder zu nicht gewollten Handlungen zu verleiten.[11] Eigentlich sind dies Anti-Patterns – also Beispiele, wie man es nicht machen sollte –, die jedoch bewusst in unethischer oder betrügerischer Weise eingesetzt werden. Den systematischen Einsatz solcher Dark Patterns bezeichnen Bösch et al. als *Dark Strategies*.[12] Für den Schutz der Privatsphäre von Verbrauchern sind Dark Patterns mittlerweile zu einem flächendeckenden Problem geworden. Sie verleiten Nutzer dazu, möglichst viele persönliche Daten mit Unternehmen zu teilen, so dass Datenschutzgesetze in der Praxis an Wirkung verlieren.[13] Ein prominentes Beispiel ist die Umsetzung der ePrivacy-Richtlinie (Richtlinie 2002/58/EG).[14]

Der Begriff *Nudging* beschreibt Methoden, die das Verhalten von Menschen beeinflussen, ohne dabei auf Verbote oder ökonomische Anreize zurückzugreifen. Thaler & Sunstein bezeichnen diese Form der Verhaltenssteuerung in eine sozial erwünschte Richtung bei gleichzeitiger Wahrung der individuellen Freiheit als libertären Paternalismus.[15] Zu den wirksamsten Nudges gehört das Setzen von Default-Regeln und Voreinstellungen. Im Bereich Datenschutz zählen zu den Default-Nudges beispielsweise die in Art. 25 (2) DSGVO vorgesehenen datenschutzfreundlichen Voreinstellungen („Privacy by Default"). Bei *digitalen Nudges* wird das Nudging-Konzept auf Designelemente in der Benutzeroberfläche übertragen; eine Teilmenge davon sind sogenannte *Privacy Nudges*, die auf „bessere" Entscheidungen des Betroffenen in Bezug auf seine Privatheit abzielen.[16] Beispiele digitaler Privacy Nudges, die im Arbeitsumfeld genutzt werden können, sind *Defaults* (datenschutzfreundliche Voreinstellungen), *Farbelemente* zum Hervorheben datenschutzfreundlicher Optionen, *Informationen,* um fundiertere Entscheidungen zu treffen, *Feedback* zum bisherigen Nutzungsverhalten des Betroffenen, *Zeitverzögerungen*, damit beispielsweise eine Datenfreigabe rückgängig gemacht werden kann, und das *Prinzip der sozialen Norm* (Orientierung am Verhalten anderer).[17]

Ebenso wie die Angriffsarten im Bereich Beschäftigtendatenschutz mit denen der IT-Sicherheit vergleichbar sind, sind dies auch die „Angreifer", denen wir uns im folgenden Abschnitt widmen.

3. Angreifer

Personenbezogene Beschäftigtendaten wecken Begehrlichkeiten bei ganz unterschiedlichen *Angreifern*. Den Begriff Angreifer verwenden wir hier im Sinne der IT-Sicherheit für Personen, die an Daten gelangen möchte, zu deren Verarbeitung sie keine Berechtigung haben. In diesem Beitrag fokussieren wir ausschließlich auf Angreifer, die *innerhalb des Unternehmens* sitzen, also Arbeitgeber, Vorgesetzte oder Kollegen. Unternehmensexterne wie beispielsweise Industriespione, Erpresser, Konkurrenten, Störer oder staatliche Akteure – etwa im Zusammenhang mit Finanzstraftaten – sind nicht Gegenstand unserer Betrachtung. Wir gehen von Angreifern aus, die über üblicherweise zu erwartende Mittel verfügen, d. h., sie haben keine Spezialkenntnisse im Hacking und setzen auch keine Ressourcen ein, um externe Experten zu engagieren. Die größte Entscheidungs-

11 Siehe z. B. Übersicht unter https://darkpatterns.org/types-of-dark-pattern.html.

12 Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, Stefan Pfattheicher: „Tales from the Dark Side: Pri-vacy Dark Strategies and Privacy Dark Patterns" in: Proceedings on Privacy Enhancing Technologies PoPETs 2016 (4), S. 237 ff. Sciendo.

13 Sebastian Rieger & Caroline Sinders (2020): Dark Patterns: Design mit gesellschaftlichen Nebenwirkungen. Stiftung Neue Verantwortung e. V., Berlin.

14 Natasha Lomas (2020): Cookie consent tools are being used to undermine EU privacy rules, study suggests. https://techcrunch.com/2020/01/10/cookie-consent-tools-are-being-used-to-undermine-eu-privacy-rules-study-suggests/; Gerhard Seuchter, Veronika Beimrohr, Dawn Branley-Bell: The Crux of Cookies Consent: A Legal and Technical Analysis of Shortcomings of Cookie Policies in the Age of the GDPR. In: Jusletter IT 28. Februar 2020.

15 Thaler, R. H.; Sunstein, C. R. (2003): Libertarian Paternalism. In: The American Economic Review 93(2), S. 175 ff. American Economic Association. Thaler & Sunstein betrachten insbesondere vom Staat eingesetztes Nudging; dieses kann, wenn es im Internet stattfindet, bis in den Bereich Cybergovernance hineinreichen.

16 Sabrina Schomberg, Torben Jan Barev, Andreas Janson, Felix Hupfeld: Ansatz zur Umsetzung von Datenschutz nach der DSGVO im Arbeitsumfeld: Datenschutz durch Nudging INFORMATIK 2019, S. 327 Bonn 2019.

17 Ebd., S. 332 ff.

befugnis und Einflussmöglichkeit hat hierbei der *Arbeitgeber*. Dieser kann beispielsweise Entscheidungen treffen, welche Hard- und Software verwendet wird und wie diese gestaltet ist. *Vorgesetzte* können aufgrund ihrer Position Druck auf andere Beschäftigte ausüben und sie so zur Preisgabe von Informationen (auch über andere Beschäftigte) bringen. Besonders wirkungsvoll ist dies, wenn sie diesen Druck auf Beschäftigte mit weitreichenden Rechten anwenden, etwa IT-Administratoren. Die Möglichkeiten der einfachen *Angestellten* sind meist am geringsten, so dass diese nur auf psychologische Manipulation oder die Vortäuschung einer anderen Identität zurückgreifen können, um ihre Ziele zu verfolgen. Im Folgenden skizzieren wir zur Illustration von Angriffsszenarien zwei fiktive Beispiele für interne Angreifer, in Abschnitt 4 beschreiben wir deren Vorgehen:

Christina Eva Offner steht als Hauptgeschäftsführerin eines Start-ups ca. 70 Beschäftigten vor. Gewinnmaximierung ist ihr oberstes Ziel. Deshalb möchte sie die Unternehmensprozesse mittels Datenanalyse effizienter gestalten. Ihr mittlerweile entlassener Datenschutzbeauftragter meinte, dass sie bestimmte Daten, die im Unternehmen anfallen, aufgrund des Personenbezugs zu den Beschäftigten nur mit deren Einwilligung verwenden darf. Christina sieht darin kein Problem. Sie ist sicher, dass sie all ihre Beschäftigten überzeugen kann, die Einwilligung zur Verarbeitung sämtlicher Daten zu geben.

Marvin Boss ist Teamleiter in einem mittelständischen Unternehmen. Er strebt die Position als Bereichsleiter an, wofür er hart arbeitet, aber anders als man vermuten mag. Er investiert viel Zeit und Energie in das Finden von Argumenten für sich und gegen seine Kontrahenten. Mittlerweile ist er auch Profi darin, die Argumente seinen Vorgesetzen scheinbar beiläufig vorzutragen: „Wusstet ihr schon, dass Karin umgezogen ist? Angeblich eine größere Wohnung, bestimmt mit Kinderzimmer. Da wird es nicht mehr lange dauern, bis sie ein oder zwei Jahre ausfällt." „Bob arbeitet in letzter Zeit häufig abends, seine E-Mails sind unfreundlich und Kaffee trinkt er auch ohne Ende. Er ist eindeutig überlastet. Zum Glück ist er kein Bereichsleiter, sein Zustand würde ja alle belasten." Seine Kontrahenten sind Marvin gegenüber sehr reserviert. Über ihr Privatleben und ihre Arbeitsbelastung reden sie mit ihm nicht. Aber Marvin hat seine Mittel, um an die Infos zu kommen.

4. Kompromittierung des Beschäftigtendatenschutzes

Gegenstand unserer Untersuchung sind Praktiken, wie sie beispielsweise von den beschriebenen Angreifern ausgeführt werden können, um den Beschäftigtendatenschutz aufzuweichen – Praktiken, die nicht grundsätzlich verboten sind, aber dennoch ethisch bedenklich, da sie gegen Grundprinzipien der Selbstbestimmtheit und des Persönlichkeitsschutzes verstoßen. Mögliche *Angriffspunkte* für solche Praktiken sind bestimmte *psychologische Grundprinzipien*, die im Kontext des Beschäftigtendatenschutzes von potentiellen Angreifern ausgenutzt werden können. Der Sozialpsychologe Cialdini bezeichnete diese Prinzipien auch als „Waffen der Einflussnahme".[18]

- Reziprozität: Wenn uns jemand einen Gefallen tut oder etwas schenkt, fühlen wir uns zur Gegenleistung verpflichtet und geben hierbei sogar oft mehr zurück, als wir erhalten haben.
- Commitment und Konsistenz: Haben wir eine Entscheidung getroffen oder in einer Sache Stellung bezogen, so tendieren wir dazu, daran festzuhalten.
- Soziale Bewährtheit: Wenn wir uns unsicher sind, wie wir uns verhalten sollen, orientieren wir uns oft am Verhalten anderer. Je mehr Personen dies tun, desto eher halten wir deren Verhalten für richtig. Wir richten uns also nach der (vermeintlichen) sozialen Norm.
- Sympathie: Von Personen, die wir sympathisch oder attraktiv finden, lassen wir uns eher beeinflussen. Dieser Effekt wird verstärkt durch Ähnlichkeit, Lob und Anerkennung.

[18] Robert B. Cialdini: „Influence: The Psychology of Persuasion". Revised Edition 2009. Harper Collins. New York, NY.

- Autorität: Wir stimmen eher Personen zu, die wir als Autoritäten betrachten, beispielsweise weil sie über mehr Wissen, Erfahrung oder Expertise verfügen als wir selbst.
- Knappheit: Dinge, die es nur in begrenzter Anzahl oder nur für eine bestimmte Zeit gibt, betrachten wir als besonders wertvoll. Verstärkt wird dieser Effekt, wenn wir mit anderen Menschen in Konkurrenz stehen.
- Zusammengehörigkeit: Von Mitgliedern einer Gruppe, der wir angehören, lassen wir uns leichter beeinflussen als von Außenstehenden.

Daneben gibt es eine Reihe *weiterer Faktoren*[19], deren sich mögliche Angreifer bedienen können, wie:

- Appell an Werte wie Hilfsbereitschaft und Loyalität,
- Ausnutzen von persönlichem oder beruflichem Vertrauen,
- Kurze Bedenkzeit bei Anfragen, so dass der Betroffene nicht über mögliche Konsequenzen seiner Handlung nachdenken kann,
- Danaergeschenke (Beispiel: Erlaubnis zur privaten Nutzung von Diensthandys, mit denen die Beschäftigten dann ausgespäht werden) oder
- datenschutzunfreundliches Design (Auswahlmöglichkeiten und Handlungsoptionen in einer Benutzeroberfläche sind so gestaltet, dass der Betroffene mit höherer Wahrscheinlichkeit personenbezogene Daten freigibt).

Die folgenden *zwei Beispiele* beschreiben, wie Angreifer im Arbeitskontext vorgehen können, um den Beschäftigtendatenschutz zu kompromittieren, und verdeutlichen die zugrundeliegenden psychologischen Prinzipien. Diese Beispiele bilden die Grundlage für die Diskussion aus juristischer und arbeitswissenschaftlicher Perspektive, die in den Abschnitten 5 und 6 folgt.

Beispiel „Einwilligungsabfrage"

Christina schreibt eine Mail an ihre Beschäftigten, um deren Einwilligung zur Prozessdatenerhebung einzuholen. In der Mail steht unter anderem: *„Die meisten Start-ups werten Prozessdaten aus. Eine stichprobenartige Umfrage in unserem Unternehmen hat ergeben, dass 89% der Befragten es gut finden, wenn wir ebenfalls Prozessdaten auswerten. Erteilt mir bitte bis heute 15 Uhr eure Einwilligung zur Erhebung und Auswertung der Daten. Morgen Vormittag werde ich auf alle zukommen, von denen ich bis dahin keine Einwilligung erhalten habe, um mehr über die Hintergründe dafür zu erfahren. Durch die Einwilligung helft ihr Kosten zu sparen, wodurch ihr zum Erfolg des Unternehmens beitragt. Der Erfolg unseres Unternehmens liegt uns doch allen sehr am Herzen. Als eure CEO zähle ich auf euch! Eure Christina Eva Offner"*

In diesem Beispiel sind mehrere Formen der Einflussnahme enthalten.

- Ausnutzen der Autorität: Christina betont ihre Position als CEO, um die Einwilligung der Beschäftigten zu erhalten, und baut eine Drohgebärde auf („werde ich auf alle zukommen").
- Soziale Bewährtheit: Mit Formulierungen wie „die meisten Startups" und „89% der Befragten" weist Christina auf die soziale Norm hin.
- Kurze Bedenkzeit: Die Anweisung, noch am selben Tag zu reagieren, baut zeitlichen Druck auf.
- Zusammengehörigkeit betonen: Christina weist auf die gemeinsame Vision („Erfolg unseres Unternehmens") hin.

Beispiel „Erlangen sensibler Daten"

Marvin möchte weitere handfeste Belege dafür sammeln, dass Bob ungeeignet ist für die Position als Bereichsleiter. Dafür sucht Marvin das Gespräch mit Alice, einer Vertrauten von Bob: *„Ich mache mir Sorgen um Bob und suche konkrete Lösungen, um ihm zu helfen. Du bist doch eine so hilfsbereite Kollegin, die immer*

[19] Siehe z. B. Ana Caraban, Evangelos Karapanos, Daniel Gonçalves, Pedro Campos: 23 Ways to Nudge: A Review of Technology-Mediated Nudging in Human-Computer Interaction. In: CHI ,19: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, Paper 503, S. 1–15.

ein offenes Ohr für ihre Kollegen hat. Hat er dir gegenüber erwähnt, weshalb er überlastet ist? […] In einer Mail hat er sich also darüber geäußert. Kannst du mir diese Mail zukommen lassen? Ich werde natürlich sorgsam damit umgehen. Du kannst mir vertrauen. Als Teamleiter bin ich es gewohnt mit sensiblen Daten umzugehen. […] Warum zögerst du? Ich habe dir neulich doch auch auf dem kurzen Dienstweg eine Mail zukommen lassen. Da kannst du mir doch auch den Gefallen tun. Die Mail würde mir wirklich helfen."

In diesem Beispiel sind folgende Formen der Einflussnahme enthalten:

– Verwendung von Lob: In dem Beispiel lobt Marvin Alice für ihre Fürsorglichkeit gegenüber Kollegen. Mit diesem Lob versucht er sympathisch zu erscheinen.
– Ausnutzen von Vertrauen: Marvin betont seine Vertrauenswürdigkeit und führt einen vermeintlichen Beweis dafür an.
– Reziprozität: Marvin weist Alice auf einen Gefallen hin, den er ihr getan hat. Er impliziert, dass sie in seiner Schuld steht und diese Schuld nun begleichen kann.

5. Juristische Perspektive

Die zuvor beschriebenen Praktiken liegen rechtlich gesehen in einem Graubereich. Die Praktiken bilden zwar ein breites Spektrum ab, teilen sich jedoch als gemeinsame Grundlage das Ausnutzen von Verhaltensanomalien. Hiermit ist gemeint, dass es sich bei dem Menschen um keinen *Homo oeconomicus* handelt, sondern dass sein Handeln von Heuristiken und Biases bestimmt wird. Dies lässt sich vorhersagen und bewusst ausnutzen.[20]

Eine weitere Analyse der beschriebenen Praktiken macht erkennbar, dass es grundsätzlich darum geht, die betroffene Person (bzw. hier den Beschäftigten) durch Manipulation dazu zu bringen, eine bestimmte Handlung durchzuführen, die sie sonst möglicherweise nicht vornehmen würde.[21] Im hier betrachteten Kontext des betrieblichen Datenschutzrechts, betrifft dies konkret die Willenserklärung bzw. die Einwilligung. Weinzierl führt aus, dass die allgemeine datenschutzrechtliche Einwilligung nach Art. 4 Nr. 11, Art. 7 DSGVO keinen Schutz vor Ausnutzung durch Verhaltensanomalien bietet. Ursächlich sei das der Verordnung zugrundliegende – wohl überholte – Menschenbild des rationalen und informierten Menschen. Es stellt sich jedoch die Frage, ob sich diese Bewertung auch im arbeitsrechtlichen Kontext so treffen lässt. Der deutsche Gesetzgeber hat hier von der Öffnungsklausel des Art. 88 DSGVO Gebrauch gemacht und für den Beschäftigtendatenschutz § 26 BDSG geschaffen[22], welcher in Absatz 2 besondere Anforderungen an die Einwilligung stellt.

Das Abhängigkeitsverhältnis und das strukturelle Ungleichgewicht zwischen Beschäftigtem und Arbeitgeber – wie etwa beim Beispiel *Christina Eva Offner* aus Abschnitt 3 – erfordert eine *echte* Einwilligung, die sich insbesondere dadurch auszeichnet, dass sie freiwillig erfolgt. Zur Beurteilung der Freiwilligkeit verlangt § 26 Abs. 2 S. 1 eine Berücksichtigung der „bestehende[n] Abhängigkeit der beschäftigten Person sowie [der] Umstände, unter denen die Einwilligung erteilt worden ist". Aufhorchen lässt hier der Begriff „Umstände", welcher hoffen lässt, dass sich hierunter auch eine Manipulation, etwa durch Dark Patterns, subsumieren lässt. Jedoch lassen sich weder in der Gesetzesbegründung[23] noch in der Literatur[24] hierzu Ansätze entdecken. Bezüglich der Umstände werden *lediglich* rein rationale Beispiele genannt, etwa der Art der Daten und der Eingriffstiefe oder auch der

[20] Vgl. Weinzierl: Dark Patterns als Herausforderung für das Recht – Rechtlicher Schutz vor der Ausnutzung von Verhaltensanomalien, NVwZ 2020, 1087ff. Hier beschrieben konkret am Beispiel Dark Patterns.

[21] Vgl. Ebenda; Brignull, Dark Patterns: dirty tricks designers use to make people do stuff, 8.7.2010, https://www.90percentofeverything.com/2010/07/08/dark-patterns-dirty-tricks- designers-use-to-make-people-do-stuff/.

[22] An Zulässigkeit der bereichsspezifischen Regelung der Einwilligung gibt es Zweifel, da teilweise davon ausgegangen wird, dass nur Konkretisierungen zulässig sind, aber keine Abweichungen nach oben oder unten, vgl. Taeger/Gabel/Zöll, 3. Aufl. 2019, BDSG § 26 Rn. 73.

[23] Vgl. BT-Drs. 18/1135 v. 24.2.2017, 98.

[24] Vgl. BeckOK DatenschutzR/Riesenhuber, 33. Ed. 1.8.2020, BDSG § 26 Rn. 46 ff.; Gola/Heckmann/Gola, 13. Aufl. 2019, BDSG § 26 Rn. 131 ff.; Taeger/Gabel/Zöll, 3. Aufl. 2019, BDSG § 26 Rn. 75 ff.

Zeitpunkt der Einwilligung. Liegt dieser Zeitpunkt vor Abschluss des Arbeitsvertrags, kann von einer besonderen Drucksituation ausgegangen werden. § 26 Abs. 2 S. 3 bekräftigt wieder das zugrundeliegende Menschenbild des *Homo oeconomicus*, da die Freiwilligkeit etwa dann vorliegt, wenn ein tatsächlicher rechtlicher oder ökonomischer Vorteil besteht. Ein Beschäftigter scheint jedoch schutzlos gegen die in Abschnitt 4 beschrieben manipulativen Techniken zu sein. Dies verweist auf eine mögliche Regelungslücke, wie sie von Weinzierl bereits bzgl. der allgemeinen datenschutzrechtlichen Einwilligung der DSGVO beschrieben wurde.[25]

Wenn der Angreifer aktiv auf die Technologieauswahl und Gestaltung einwirken kann und dies dazu nutzt, beispielsweise Dark Patterns in der betrieblich genutzten Software zu implementieren, stellt sich die Frage, wie dies aus datenschutzrechtlicher Sicht zu bewerten ist. Ausgangspunkt hierfür kann der Art. 25 Abs. 2 DSGVO sein – Datenschutz durch datenschutzfreundliche Voreinstellungen. Demnach muss „der Verantwortliche [...] geeignete technische und organisatorische Maßnahmen [treffen], die sicherstellen, dass durch Voreinstellungen nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden." Diese Regelung besagt implizit, dass *nicht erforderliche Daten* nicht „durch Voreinstellung" verarbeitet werden dürfen. Hiermit wird konkret die (technische) Umsetzung der Datenminimierung gem. Art. 5 Abs. 1 lit. c DSGVO verlangt. Es stellt sich jedoch auch die Frage, was unter einer Voreinstellung genau zu verstehen ist. Martini & Weinzierl[26] sagen hierzu, dass der Fokus der Regelung auf der „Art und Weise, wie technische Funktionalitäten eines Dienstes eingebunden und ausgewählt werden" liegt. Als typische Beispiele werden die Trackingeinstellungen eines Webbrowsers oder datensammelnde Betriebssysteme genannt.[27] Verboten ist hierbei wohl nur ein sogenanntes Opt-out, also eine für den Betroffenen ungünstige Voreinstellung, die dieser aktiv abwählen muss. Es soll der „wahre" Wille zum Vorschein kommen (sogenanntes Debiasing), der Betroffene soll also vor dem Verantwortlichen bewahrt werden.[28] Dies spricht dafür, dass zumindest einige der im Abschnitt 4 genannten Praktiken einen Verstoß gegen Art. 25 Abs. 2 DSGVO – Datenschutz durch datenschutzfreundliche Voreinstellung – und somit auch gegen die Verordnung i. S. d. Art. 77 ff. DSGVO darstellen dürften. Hieraus ergeben sich aber wohl keine direkten Folgen für die Rechtmäßigkeit der Verarbeitung, welche in diesem Kontext lediglich auf dem Erlaubnistatbestand der Einwilligung fußen kann. Dass die Einwilligung des Beschäftigten wohl keinen Schutz vor den beschrieben manipulativen Praktiken aufweist, wurde im vorherigen Absatz dargelegt, auch ein Verstoß gegen das Gebot *Datenschutz durch datenschutzfreundliche Voreinstellungen* ändert dies nicht.[29] Jedoch kann auch ein Verstoß gegen Art. 25 Abs. 2 DSGVO durchaus sanktionsbewehrt sein, nach Art. 83 Abs. 4 lit. a sind Geldbußen von bis zu 10 Millionen Euro bzw. bis zu 2 % des weltweiten Jahresumsatzes möglich.[30]

6. Betrachtung der Gefahrenpotenziale im soziotechnischen System

In einer digitalisierten Arbeitswelt, die durch eine hohe Dynamik gekennzeichnet ist, wird der Schutz von unternehmensinternen und insbesondere sensiblen Daten immer wichtiger. Einhergehend mit der Digitalisierung werden die Daten- und Informationssicherheit sowie der Datenschutz in den Fokus gerückt. Um den Schutz sensibler Daten zu gewährleisten, werden immer wieder neue technologische Möglichkeiten entwickelt und zum Einsatz gebracht. Daten werden verschlüsselt gespeichert, Sicherheitsnetzwerke- und Protokolle installiert und der Zugriff mit Hilfe von Passwörtern, Smartcards oder biometrischen Merkmalen digital gesichert. Ähnlich wie bei der Einführung neuer Technologien wird auch im Bereich der IT-Sicherheit oftmals außer Acht gelassen, dass ein Unternehmen ein komplexes soziotechnisches System ist, das neben der technischen

[25] Weinzierl, a.a.O., 1088.
[26] Vgl. Martini, Weinzierl, Mandated Choice, RW 2019, S. 296.
[27] Vgl. Kühling/Buchner/Hartung, 3. Aufl. 2020, DS-GVO Art. 25 Rn. 25.
[28] Vgl. Martini, Weinzierl, Mandated Choice, RW 2019, S. 300.
[29] Ebenda, 307.
[30] Vgl. Hansen, Artikel 25. In Simits /Hornung/Spiecker (Hrsg.), Datenschutzrecht, Nomos, 2019, Rn. 25.

ebenso eine organisationale und soziale Sphäre besitzt.[31] Wird zum Beispiel bei der Umsetzung von Maßnahmen zum Datenschutz nur die technische Sphäre betrachtet, so können durch die enge Verknüpfung und die Wechselwirkungen mit den anderen Sphären Lücken und Hintertüren entstehen. Das Zusammenwirken der Sphären bietet Angreifern vielfältige Möglichkeiten, auch ohne direkten technischen Zugriff an sensible Daten – beispielsweise Beschäftigtendaten oder persönliche Informationen wie in den beschriebenen Beispielen – zu gelangen. So wird in den letzten Jahren vermehrt der Mensch im sozialen Gefüge des Unternehmens als Schwachstelle der Informationssicherheit identifiziert und mit Hilfe kreativer Taktiken ausgenutzt. Als Ursache wird in der einschlägigen Literatur im Bereich Social Engineering das mangelnde Bewusstsein für die Informationssicherheit bei den Beschäftigten angeführt, aus dem eine unmittelbare Bedrohung durch Sicherheits- und Vertraulichkeitsverletzungen für Unternehmen resultieren kann.[32]

Eine Möglichkeit, dieser Bedrohung entgegen zu wirken, sind regelmäßige Sensibilisierungskampagnen zur Informationssicherheit, sogenannte Awareness-Programme, mit deren Hilfe das Bewusstsein sowie die Bedeutung der Aufrechterhaltung ständiger Wachsamkeit erhöht werden.[33] Solche Schulungen und Programme, basierend auf gängigen Trainingsmethoden und Simulationsszenarien, sensibilisieren jedoch meist nur gegenüber Angriffen von Externen, die vermehrt über Social-Media-Dienste wie zum Beispiel Twitter, Snapchat oder Facebook gestartet werden.[34]

Wie die Beispiele in diesem Beitrag zeigen, existieren jedoch ebenfalls Bedrohungen der Sicherheit personenbezogener Daten und sensibler Informationen im internen Bereich von Unternehmen und Organisationen. Insbesondere in der sozialen Sphäre können soziale Bindungen und informelle Kommunikation zu einer bewussten wie unbewussten Verletzung des Datenschutzes führen. Die vertrauensvolle Natur des Menschen stellt hier eine große Herausforderung für alle Sicherheitsmechanismen und -trainings dar. Ein besonderes Gefahrenpotenzial resultiert aus einem entsprechenden Umfeld der Beschäftigten auf organisationaler Ebene. So fördert beispielsweise eine Unternehmenskultur, die auf einem ausgeprägten Gemeinschaftsgefühl, einem absoluten Vertrauensverhältnis und einer Integration von sozialen Interaktionen in den Arbeitsalltag beruht, die informelle Kommunikation und soziale Bindung enorm.

Betrachtet man beispielsweise die Phasen eines Social-Engineering-Angriffs genauer, so wird deutlich, dass durch ein solch vertrauensvolles Umfeld und soziale Bindungen bereits die erste Hälfte der vier Angriffsphasen absolviert ist:[35]

(1) das Sammeln von (persönlichen) Informationen,
(2) der Aufbau einer sozialen Beziehung,
(3) das Ausnutzen der verfügbaren Informationen und der sozialen Beziehung zum Erhalt der gewünschten sensiblen Informationen und
(4) der Ausstieg, möglichst ohne Spuren zu hinterlassen.

---

31 Vgl. Ulich, E. (2011) Arbeitspsychologie, 7. Auflage, Schäffel-Poeschel Verlag; Bosse, C. K.; Dietrich, A.; Kelbert, P.; Küchler, H.; Schmitt, H.; Tolsdorf, J.; Wessner, A. (2020): Beschäftigtendatenschutz: Rechtliche Anforderungen und technische Lösungskonzepte. In: E. Schweighofer, W. Hötzendorf, F. Kummer und Editions Weblaw (Hg.): Verantwortungsbewusste Digitalisierung. Tagungsband des 23. Internationalen Rechtsinformatik Symposions IRIS 2020. 1.Erstauflage (Colloquium).

32 Vgl. u. a. Aldawood, H.; Skinner, G. (2019) An academic review of current industrial and commercial cyber security social engineering solutions. ICCSP ,19: Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, S.110–115; Mouton, F.; Leenen, L.; Venter, H.S. (2016) Social engineering attack exampley, templates and scenarios. Computer & Security, Jg. 59, S. 186–209.

33 Vgl. Sallai, G. (2016) Social Engineering Audit and Security Awareness Programme. KPMG: Amstelveen.

34 Vgl. Wilcox, H.; Bhattacharya, M.; Islam, R. (2014) Social engineering through social media: An investigation on enterprise security. In Proceedings of the International Conference on Applications and Techniques in Information Security, Lisbon, Portugal, 16–20 November 2014; S. 243–255; Wilcox, H.; Bhattacharya, M. (2015) Countering social engineering through social media: An enterprise security perspective. In: Lecture Notes in Computer Science, Springer: Cham, S. 54–64.

35 Vgl. Mouton, F.; Leenen, L.; Venter, H.S. (2016) Social engineering attack exampley, templates and scenarios. Computer & Security, Jg. 59, S. 186–209.

In einem engen oder gar persönlichen Verhältnis mit reger informeller Kommunikation fällt es Kollegen oder Vorgesetzten nicht schwer, kompromittierende Informationen zu sammeln oder moralische Pflichtschulden aufzubauen und diese gegebenenfalls zum Zweck eines Angriffs einzusetzen. Die gute Kenntnis der Kollegen oder Mitarbeiter ermöglicht es, eine Angriffstaktik selektiv auf die Persönlichkeitsmerkmale und weiteren inhärenten Eigenschaften der anvisierten Person auszurichten.[36]

Folglich ist es die Aufgabe der Unternehmensführung, mit Hilfe entsprechender Maßnahmen, Regeln und Prinzipien über alle drei Sphären einer Organisation hinweg solchen Bedrohungen frühzeitig entgegenzuwirken. Ausgewählte Ansätze werden im folgenden Abschnitt aufgezeigt.

7. Lösungen

Lösungsansätze mit dem Ziel manipulative Praktiken zu vermeiden, sollten durchaus auch im Sinne des Arbeitgebers sein. Neben dem Vertrauen der Beschäftigten und einer gesunden Unternehmenskultur dürfte auch die Angst vor den möglichen Sanktionen, etwa bei Verstößen gegen die DSGVO, motivierend wirken. Zwar scheint eine so erlangte Einwilligung unter eine Regelungslücke zu fallen, jedoch kann auch der Verstoß gegen den Grundsatz „Datenschutz durch datenschutzfreundliche Voreinstellungen“ durchaus mögliche Bußgelder und Strafen nach sich ziehen (vgl. auch Abschnitt 5).

Auch wenn es mehrere Strategien gibt, um unlauteren Praktiken zur Umgehung oder Aufweichung des betrieblichen Datenschutzes entgegenzuwirken, gibt es kein „perfektes“ Sicherheitssystem gegen Bedrohungen wie das Social Engineering. Eine Reihe der beschriebenen Angriffsformen findet über betrieblich genutzte EDV-Systeme statt und macht sich eine bewusst datenschutzunfreundliche Gestaltung der Benutzeroberfläche dieser Systeme zu Nutze. Um solchen Praktiken zu begegnen, können Heuristiken oder Checklisten angewendet werden, mit denen die Benutzeroberfläche beispielsweise gezielt auf das Qualitätskriterium Usable Privacy[37] (benutzer- und datenschutzfreundliche Gestaltung) oder auf das Nichtvorhandensein von Dark Patterns überprüft werden kann. Datenschutzunfreundlichem Design von EDV-Systemen kann entgegengewirkt werden, indem eine Prüfung durch Externe stattfindet, denn Externe sind weniger anfällig für die vorgestellten Praktiken.

Da technische Hilfsmittel allein nicht ausreichen, werden diese sowohl bei kleinen als auch bei großen Unternehmen zunehmend durch Ausbildungs- und Sensibilisierungsprogramme ergänzt.[38] Mit ihnen wird die Strategie der Aufklärung verfolgt. Die meisten Menschen sind sich der in Abschnitt 4 beschriebenen psychologischen Grundprinzipien nicht bewusst und können deren Ausnutzung daher nur schwer aktiv entgegenwirken. Daher sollten Beschäftigte regelmäßig über die Grundprinzipien, Methoden und Anzeichen für deren Ausnutzung aufgeklärt werden und es sollten ihnen konkrete Strategien an die Hand gegeben werden, der Ausnutzung entgegenzuwirken. Durch diese Sensibilisierungs- und Aufklärungsmaßnahmen wird es den Beschäftigten eher möglich sein, in einem Gespräch das Interesse des Gegenübers an personenbezogenen Daten zu identifizieren, was zunächst z. B. durch eine Sympathiebekundung oder ein Lob verdeckt wird.

Eine andere Strategie ist das Verdeutlichen der sozialen Norm. Beispielsweise kann die (gewünschte) soziale Norm sein, dass keine Daten im Unternehmen geteilt werden, die auf eine Überforderung eines Beschäftigten hinweisen. Diese soziale Norm kann etabliert werden, indem eine Organisationsanweisung dazu erlassen wird, die Norm in Datenschutzschulungen verdeutlicht wird und Strafen für Verstöße kommuniziert werden.

---

[36] Vgl. hierzu u. a. Conteh, N.Y.; Schmick, P.J. (2016) Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, Vol 23., Iss. 6, S. 31-38; Mann, I. (2017) Hacking the Human: Social Engineering Techniques and Security Countermeasures; Routledge: London.

[37] Vgl. Johansen, J.; Fischer-Hübner, S. (2019): Making GDPR Usable: A Model to Support Usability Evaluations of Privacy. Privacy and Identity Management 2019, S. 275–291.

[38] Vgl. Aldawood, H.; Skinner, G. (2019) Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. Future Internet, Vol. 11 Iss. 3, S. 73.

Regelungen haben auch den Effekt, dass Beschäftigte eine Argumentationsgrundlage haben, wieso sie einem Gefallen nicht nachgehen. Argumente wie „ich würde ja gerne helfen, aber ich möchte mir auch keinen Ärger einfangen – das ist doch auch in deinem Sinne“ erleichtern es, Autoritäten zu widersprechen.

Die Einführung der beschriebenen Maßnahmen impliziert, dass es Mitglieder eines Unternehmens mit böswilligen Absichten gibt. Die Maßnahmen können daher als Katalysator für Misstrauen wirken. Daher ist es wichtig, die Maßnahmen behutsam einzuführen und eine Kultur des Vertrauens zu pflegen.

8. Fazit

Die Ausnutzung von Verhaltensanomalien, also subtile Techniken, die Betroffene so manipulieren, dass sie entgegen ihren eigentlichen Interessen handeln, erregt in vielen Disziplinen zunehmendes Interesse. Die in diesem Beitrag vorgestellten manipulativen Praktiken verdeutlichen, dass IT-Sicherheit in einem sozialen Kontext nicht nur mit rein technisch Lösungen umgesetzt werden kann, sondern auch soziale Lösungs- und Schutzkonzepte erfordert. Ein Großteil der Literatur konzentriert sich bisher auf externe Angreifer, jedoch können insbesondere im Arbeitsumfeld auch interne Akteure eine oft übersehene bzw. nur wenig beachtete Gefahr darstellen.

Im Kern rütteln die beschriebenen Praktiken vor allem an dem Grundverständnis, dass der Mensch rational und informiert entscheidet. Da dieses Menschenbild des *Homo oeconomicus* jedoch laut Weinzierl wohl das Leitbild des Datenschutzrechts darstellt, bietet die DSGVO bzw. das BDSG dementsprechend auch wenig Schutz vor Dark Patterns und ähnlichen manipulativen Praktiken.[39]

9. Danksagung

Diese Arbeit wurde durch das Forschungsprojekt „TrUSD – Transparente und selbstbestimmte Ausgestaltung der Datennutzung im Unternehmen“ unterstützt, finanziert durch das Bundesministerium für Bildung und Forschung (BMBF).

[39] Vgl. Weinzierl, a.a.O., 1088.