

# Betriebs Berater



21 | 2016

Recht | Wirtschaft | Steuern

23.5.2016 | 71. Jg.  
Seiten 1217–1280

## **DIE ERSTE SEITE**

**Prof. Dr. iur. Swen Bäuml**, StB/Wirtschaftsjurist  
Die Steuergesetzgebung der Großen Koalition

## **WIRTSCHAFTSRECHT**

**Dr. Mark C. Hilgard**, RA  
Der Freistellungsanspruch beim Unternehmenskauf | 1218

## **STEUERRECHT**

**Christian Schoppe**, StB, und **Carolin Reichel**, StBin  
Vertreterbetriebsstätten ab 2017 | 1245

**Dr. Stefan Rogge**, RA/StB  
Die Anforderungen an eine Mitunternehmerstellung im Rahmen einer  
Freiberuflerpraxis | 1252

## **BILANZRECHT UND BETRIEBSWIRTSCHAFT**

**Michael Deubert**, WP/StB, und **Dr. Stefan Lewe**, WP/StB  
Beurteilung der Gleichwertigkeit von Drittstaaten-Konzernabschlüssen nach  
§ 292 HGB am Beispiel der Swiss GAAP FER | 1260

## **ARBEITSRECHT**

**Dr. Mark Zimmer**, RA/FAArbR, und **Alicia Helle**  
Tests mit Tücke – Arbeitsrechtliche Anforderungen an Social Engineering Tests | 1269

Dr. Mark Zimmer, RA/FAArbR, und Alicia Helle, cand. iur.

# Tests mit Tücke – Arbeitsrechtliche Anforderungen an Social Engineering Tests

Die Gewährleistung von IT-Sicherheit stellt Unternehmen vor immer größere Herausforderungen. Während Systeme von Privatanwendern besonders von der Nutzung veralteter Software, Spam und kompromittierten Webseiten gefährdet werden, haben Unternehmen mit der Sicherheitslücke „Mensch“ zu kämpfen (s. Abb. auf S. 1270). Nicht sensibilisierte Mitarbeiter und ihre „digitale Sorglosigkeit“, besonders in sozialen Netzwerken, ermöglichen versierten „Social Hackern“, Sicherheitstechnologien von Unternehmen zu überwinden und damit an die Kronjuwelen der Unternehmen zu kommen oder den Betriebsablauf zu schädigen. Neben Aufklärung und Training der eigenen Mitarbeiter versprechen sog. Social Engineering Tests Abhilfe, bei denen das korrekte Verhalten der Mitarbeiter diesbezüglich geprüft wird. Freilich sind sie nur in rechtlichen Grenzen zulässig. Bei der Beurteilung ihrer Rechtmäßigkeit ist vor allem das allgemeine Persönlichkeitsrecht gegen die Unternehmenssicherheit abzuwägen.

## I. Interesse und Pflicht zum Ergreifen geeigneter Schutzmaßnahmen

Social Engineering nutzt gezielt die „Schwachstelle Mensch“ und menschliche Eigenschaften wie Faulheit, Sorglosigkeit, Redseligkeit, Autoritätshörigkeit und Naivität aus. Mitarbeiter werden geschickt beeinflusst, um so an Informationen und Datenbanken zu gelangen.<sup>1</sup> Aus wirtschaftlicher Sicht besteht ein starkes unternehmerisches Interesse, Social Engineering zu verhindern. Die Weitergabe sensibler Daten, mit Datenpannen zusammenhängende Reputationsschäden, Wirtschafts- und Industriespionage, Abgreifen von Know-how und der Verlust interner Informationen und Betriebs- und Geschäftsgeheimnisse, können gravierende Schäden verursachen.<sup>2</sup> Zudem hat die Geschäftsleitung auch eine rechtliche Verpflichtung, angemessene Schutzmaßnahmen zu ergreifen. Compliance-Anforderungen umfassen als wesentlichen Aspekt die IT-Sicherheit.<sup>3</sup> So fallen etwa unter die Pflichten eines AG-Vorstands nach § 91 Abs. 2 AktG auch interne Sicherheitsmaßnahmen für die IT und deren Kontrolle.<sup>4</sup> Entsprechendes gilt auch für andere Unternehmensformen.<sup>5</sup> Nachlässigkeit diesbezüglich birgt ein persönliches Haftungsrisiko für die Mitglieder der Leitungsebenen gegenüber der Gesellschaft, kann den Ordnungswidrigkeitstatbestand nach § 130 Abs. 1 OWiG erfüllen und zu Schadensersatzansprüchen Dritter wie Kunden und Aktionären führen.<sup>6</sup>

## II. Social Engineering Tests als mögliche Schutzmaßnahme

Der Arbeitgeber muss der konkreten Gefahr begegnen, die durch einen kombinierten Angriff von außen (Social Engineers) „über innen“ (Mitarbeiter) droht. Um ein adäquates Schutzniveau zu erreichen, ist

zunächst erforderlich, klare und stets aktualisierte Leitlinien in Form von Sicherheitsregeln (Policies, Social Media Guidelines, Codes of Conduct) aufzustellen, die im Rahmen des Direktionsrechts, einer Betriebsvereinbarung oder auf individualvertraglicher Basis Bestandteil des Arbeitsvertrags werden können.<sup>7</sup> Der Arbeitgeber sollte zudem organisatorische Maßnahmen ergreifen um die Einhaltung der Sicherheitsregeln zu gewährleisten (etwa Mitarbeiterschulungen in Form von Workshops und Seminaren unter Verwendung von Anschauungsmaterialien wie Lehrvideos).

Eine effektive Methode zur Sensibilisierung im Betrieb und zur Entdeckung von Sicherheitslücken sind Social Engineering Tests. Hierbei handelt es sich um (meist unangekündigte) Tests durch spezialisierte Dienstleister. Sie stellen das Verhalten der Mitarbeiter in entsprechenden Szenarien unter Anwendung von Social-Engineering-Techniken<sup>8</sup> auf die Probe. Damit wird dem einzelnen Arbeitnehmer das Bedrohungsszenario vor Augen geführt, der „Ernstfall“ geprobt und eine realitätsnahe Kontrolle erzielt. In der betrieblichen Praxis werden nämlich Cyberangriffe oft in ihrer Gefahr unterschätzt – sei es durch Nachlässigkeit, mangelnde Sensibilisierung oder ein trügerisches Sicherheitsempfinden.

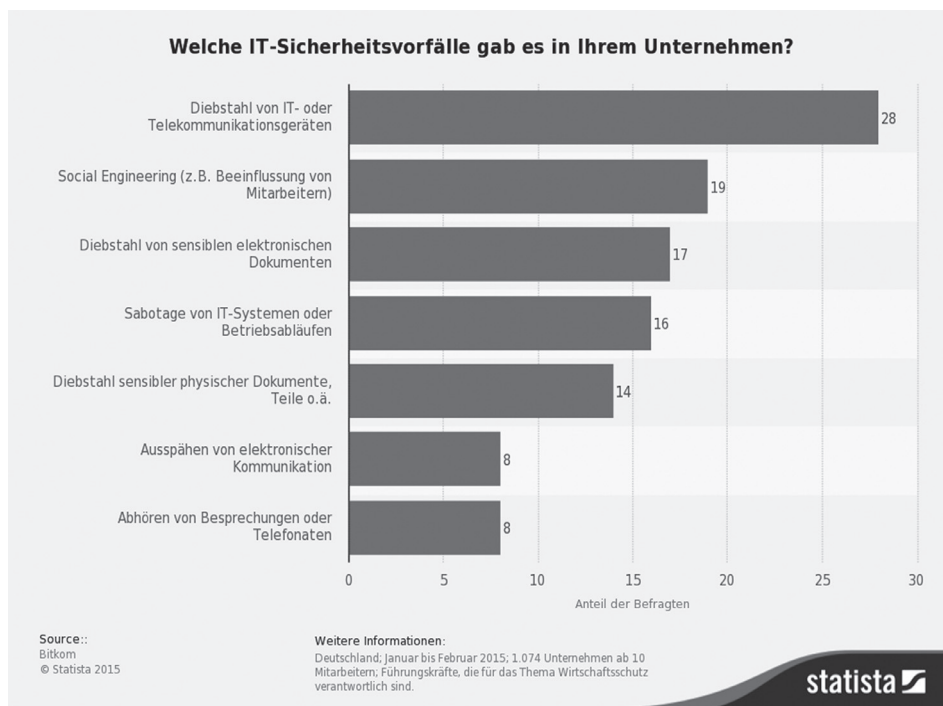
## III. Zulässigkeit von Social Engineering Tests

Grundsätzlich hat der Arbeitgeber das Recht zu prüfen, ob Arbeitspflichten ordnungsgemäß erfüllt werden.<sup>9</sup> Allerdings läuft jede Mitarbeiterkontrolle Gefahr, mit dem allgemeinen Persönlichkeitsrecht<sup>10</sup> der Arbeitnehmer zu kollidieren oder gegen die arbeitsvertraglichen Fürsorgepflichten des Arbeitgebers zu verstoßen.<sup>11</sup>

### 1. Rechtliche Grundlage für Social Engineering Tests

Fraglich ist, ob und in welchen rechtlichen Grenzen Social Engineering Tests (im Folgenden auch „Tests“) zulässig sind.

- 
- 1 Grützner/Jakob, Compliance von A–Z, 2015; Lipski, Social Engineering, 2009, S. 7.
  - 2 Oberwetter, NJW 2011, 417, 420.
  - 3 Vgl. auch Entwurf der EU-Richtlinie zur Netzwerk und Informationssicherheit v. 18.12.2015 (NIS-Richtlinie) und das deutsche IT-Sicherheitsgesetz v. 17.7.2015.
  - 4 Rath/von Barby, in: Umnuß (Hrsg), Corporate Compliance Checklisten, 2012, Kap. 7, Rn. 4–6.
  - 5 Z. B. § 43 I GmbHG oder § 33 I Nr. 1 WpHG.
  - 6 Schmidt, BB 2009, 1295, 1295 f.; Heckmann, MMR 2006, 280 ff.
  - 7 Vgl. Schmidt, BB 2009, 1295, 1298.
  - 8 Etwa mittels sogenannter Trojaner, „Spear-Phishing“, „Brute-Force Attacks“, „Dumpster-Diving“ oder „Fake President Attacks“, aber auch per Telefon oder von Angesicht zu Angesicht.
  - 9 Maschmann, AuA 2000, 519.
  - 10 In seinen Ausprägungen des Rechts am eigenen Bild, der Vertraulichkeit des Wortes, dem Ehrschutz, dem Recht auf informationelle Selbstbestimmung, dem Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, schützt das Allgemeine Persönlichkeitsrecht den Arbeitnehmer vor einer zu weitgehenden Überwachung seiner Person, BAG, 4.4.1990 – 5 AZR 299/89, NJW 1990, 2272.
  - 11 § 241 Abs. 2 BGB im Arbeitsverhältnis besondere persönliche Bindung der Vertragspartner, Pflicht zu gegenseitigen Rücksichtnahme, wobei die grundrechtlichen Wertungen zu berücksichtigen sind, BAG, 15.7.1987 – 5 AZR 215/86, BB 1987, 2300, NZA 1988, 53.



### a) Duldungspflicht aufgrund arbeitsvertraglicher Nebenpflichten

Möglicherweise hat der Arbeitnehmer die Durchführung von Tests bereits aufgrund einer impliziten arbeitsvertraglichen Rücksichtnahme-, Loyalitäts- und Schadensabwendungspflicht (§ 242 BGB) zu dulden. Grundsätzlich sollten Arbeitnehmer-Kontrollen allerdings offen durchgeführt werden (sporadisches „über die Schulter schauen“) und nur in Ausnahmefällen (aufgrund konkreter Verdachtsmomente, schwerer Arbeitspflichtverletzungen und Ausschöpfen milderer Mittel) heimlich durchgeführt werden.<sup>12</sup> Mit diesem Grundsatz scheinen klassische Social Engineering Tests zu kollidieren, weil sie verdeckt durchgeführt werden und sich präventiv – ohne konkreten Verdacht – gegen bestimmte Personen oder Personengruppen wenden. Allerdings bezwecken die Tests nicht, ein kündigungserhebliches Verhalten zu dokumentieren, sondern die Unternehmenssicherheit zu gewährleisten. Der Arbeitgeber kann seine Mitarbeiter im Zusammenhang mit dem Einsatz neuer Medien sinnvollerweise nicht jederzeit unverdeckt und für sie frei erkennbar beaufsichtigen.<sup>13</sup> Gerade wegen der Selbstständigkeit im Internet muss es Arbeitgebern möglich sein das Verhalten und die Fähigkeiten der dort eingesetzten Arbeitnehmer zu überprüfen.<sup>14</sup> Aufgrund des hohen Risikos der Angriffe und der Schwierigkeiten effektiver Sensibilisierung kann deshalb von einer Duldungspflicht ausgegangen werden, wenn und soweit der Test in angemessener Art und Weise durchgeführt wird.

### b) Mehr Spielraum durch Einwilligung?

Zweifelhaft erscheint, ob eine Einwilligung des Arbeitnehmers dem Arbeitgeber mehr Spielraum bei der Ein- und Durchführung der Tests geben kann. Angesichts des typischerweise zwischen Arbeitnehmer und Arbeitgeber bestehenden strukturellen Ungleichgewichts unterliegen arbeitsvertragliche Abmachungen einer gerichtlichen Inhaltskontrolle am Maßstab der §§ 242, 315 BGB (bzw. bei Formulararbeitsverträgen §§ 307, 310 Abs. 4 BGB)<sup>15</sup> und müssen (bei Verarbeitung personenbezogener Daten) die datenschutzrechtliche Anforderung an „Freiwilligkeit“ im Sinne von § 4a BDSG erfüllen. Eine Blankoermächtigung zur Durchführung jeder Art von Kontrolltests ist mit rechtlichen Unsicherheiten befrachtet und daher allenfalls dann sinnvoll, wenn sie hinreichend deutlich gefasst ist.

### c) Mehr Rechte durch Betriebsvereinbarung?

Fraglich ist, ob eine Betriebsvereinbarung dem Arbeitgeber mehr Rechte zur Durchführung von Tests geben kann. Die Verpflichtung die freie Entfaltung der Persönlichkeit zu schützen (§ 75 Abs. 2 BetrVG) verbietet zwar nicht jede einschränkende Vereinbarung, jedoch sind auch hierbei zwingend geltende Grenzen zu wahren und stehen nicht zur Disposition der Betriebsparteien.<sup>16</sup> Deshalb können sich auch hierdurch keine intensiveren Kontrollbefugnisse ergeben.

### d) Verhältnismäßigkeitsprinzip

Unabhängig von einer Regelung durch Betriebsvereinbarung oder Einwilligung sind die Tests jedenfalls nur dann gerechtfertigt, wenn sie verhältnismäßig sind.<sup>17</sup> Dem Persönlichkeitsrecht des Arbeitnehmers müssen mindestens gleichwertige schutzwürdige Belange des Arbeitgebers gegenüberstehen. Das erfordert eine Abwägung zwischen den widerstreitenden Interessen des Arbeitgebers an einer Sicherung seines Unternehmens (Art. 12 Abs. 1, 14 Abs. 1 GG) und der Arbeitnehmer an der Wahrung ihres allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG).<sup>18</sup> Das Übermaßverbot gilt für das „ob“ und das „wie“ eines Tests.<sup>19</sup>

### 2. Grundsätzliche Zulässigkeit eines Tests („ob“)

Bezüglich der Frage, „ob“ solche Tests im Betrieb durchgeführt werden, ist der unternehmerische Ermessensspielraum durch das Verhältnismäßigkeitsprinzip beschränkt. Nur wenn konkrete Gefährdungen für sein Unternehmen ersichtlich sind, es sich um eine kritische Infrastruktur handelt und/oder mit sensiblen Daten Dritter umgegangen wird, besteht das schutzwürdige Interesse des Arbeitgebers.<sup>20</sup> Tests ohne jeden Anhaltspunkt einer Gefährdung durch Social Engineering (etwa nur zur Abschreckung oder Täuschung der Mitarbeiter) sind unzulässig.<sup>21</sup>

### 3. Rahmen für die Durchführung der Tests („wie“)

Bei Vorbereitung und Durchführung der Tests sind bestimmte Vorgaben einzuhalten.

<sup>12</sup> Vgl. Maschmann, AuA 2000, 519.

<sup>13</sup> Maschmann, NZA 2002, 13, 15.

<sup>14</sup> BAG, 18.11.1999 – 2 AZR 743/98, BB 2000, 672, RdA 2001, 49, 53 m. Anm. Ricken.

<sup>15</sup> Franzen, in: Erf. Komm., 16. Aufl. 2016, § 4a BDSG, Rn. 2.

<sup>16</sup> BAG, 26.8.2008 – 1 ABR 16/07, BB 2008, 2743, NZA 2008, 1187, 1188.

<sup>17</sup> Maschmann, NZA 2002, 13, 15.

<sup>18</sup> BAG, 12.1.1988 – 1 AZR 352/86, NZA 1988, 621, 622; BGH, 25.5.1954 – I ZR 211/53, BGHZ 13, 334, 338.

<sup>19</sup> Maschmann, NZA 2002, 13, 14.

<sup>20</sup> Kuhn/Willemsen, DB 2016, 111, 113.

<sup>21</sup> Maschmann, NZA 2002, 13, 16.

### a) Keine willkürliche Auswahl der Testpersonen

Ziel des Tests ist gewöhnlich ein einzelner Mitarbeiter als Angriffsobjekt. Hierfür wählt der Arbeitgeber einen oder mehrere Arbeitnehmer aus, wobei er keine willkürlichen Entscheidungen treffen darf, sondern seine Entscheidung anhand klarer Kriterien (z. B. ein von Cyberangriffen gefährdeter Arbeitsplatz) festmachen oder mittels Zufalls-generator auswählen sollte. Ein diskriminierendes Verhalten – etwa nur Auswahl bestimmter Gruppen ohne sachlichen Grund wäre nach § 242 BGB unzulässig.<sup>22</sup> Anderes gilt womöglich, wenn der Arbeitgeber darlegen kann, dass es z. B. insbesondere älteren oder jüngeren Belegschaftsmitgliedern an entsprechender Sensibilisierung fehlt und daher verstärkter Trainingsbedarf in Form von Social Engineering Tests besteht.

### b) Auswahl der externen Dienstleister und schriftliche Vereinbarung

Bezüglich der Auswahl des externen Dienstleisters treffen den Arbeitgeber Sorgfalts- und Nachforschungspflichten. Aus seiner Fürsorgepflicht hat er dafür zu sorgen, dass Eingriffe in das allgemeine Persönlichkeitsrecht seiner Arbeitnehmer von vertrauenswürdigen (zertifizierten) Anbietern wahrgenommen werden.

Mit dem Dienstleister müssen klare Vereinbarungen in Bezug auf die Durchführung der Tests, die Festlegung bestimmter Tabu-Zonen (etwa bestimmte Datenbanken mit sensiblen Informationen oder bestimmte Projekte<sup>23</sup>), den Zeitraum der Durchführung und die nachträgliche Behandlung des gewonnenen Materials (Weiterleitung, Löschung etc.) getroffen werden. Der Arbeitgeber sollte sich die Einhaltung der Rahmenbedingungen vertraglich zusichern lassen.<sup>24</sup> Zudem sollte eine Geheimhaltungsvereinbarung mit dem Dienstleister abgeschlossen werden.

### c) Mitarbeiterschulungen zur Vorbereitung

Bevor der Social Engineering Test durchgeführt wird, müssen die Sicherheitsvorschriften festgelegt und den Mitarbeitern vermittelt werden. Mehrdeutige, widersprüchliche oder unpraktikable Verhaltensanweisungen machen die Tests angreifbar. Als milderer Mittel käme in Betracht, einen Zeitraum zu nennen, innerhalb dessen mit „Routine-Kontrollen“ dieser Art zu rechnen ist.<sup>25</sup> Da dies allerdings den Untersuchungszweck gefährden würde, dürfte es ausreichend sein, dass Social Engineering im Allgemeinen Gegenstand von Schulungen war.<sup>26</sup>

## 4. Datenschutzrechtliche Anforderungen an die Tests

Um das Recht auf informationelle Selbstbestimmung zu wahren,<sup>27</sup> sollte sich die konkrete Durchführung der Sicherheitstests an den Geboten der Datensparsamkeit bzw. Datenvermeidbarkeit<sup>28</sup> und dem Erforderlichkeitsprinzip ausrichten, insbesondere sollten die gewonnenen Erkenntnisse des Tests zeitnah anonymisiert oder zumindest pseudonymisiert werden.<sup>29</sup>

### a) Übermittlung der Arbeitnehmerdaten

Über den ausgewählten Arbeitnehmer werden dem externen Dienstleister gewisse „Start“-Informationen (beispielsweise Alter, Ausbildung, Hobbys) – somit personenbezogene Daten im Sinne des § 3 Abs. 1 BDSG – bereitgestellt. Der Arbeitgeber sollte nur solche Informationen auswählen, die ein „echter“ Social Engineer mit gewissem Zeitaufwand auch ermitteln würde, nicht etwa (intern bekannte) sen-

sible Informationen über die Arbeitnehmer weiterleiten.<sup>30</sup> Die Übermittlung an den externen Dienstleister ist eine datenschutzrechtlich relevante Verarbeitung im Sinne von § 3 Abs. 4 S. 2 Nr. 4a BDSG.<sup>31</sup> Hierfür bedarf es einer Einwilligung oder einer gesetzlichen Grundlage (§ 4 Abs. 1 BDSG). Da eine ordnungsgemäße Einwilligung einerseits den Zweck der Tests gefährden würde und andererseits fraglich ist, ob im Arbeitsverhältnis die Anforderungen des § 4a BDSG erfüllt sind, kommt als Spezialvorschrift im Verhältnis zu § 28 Abs. 1 S. 1 Nr. 2 BDSG für Beschäftigungsverhältnisse § 32 Abs. 1 Nr. 1 BDSG in Betracht. Zwar erfolgt die Datenerhebung, -verarbeitung und -nutzung im Rahmen der Tests vornehmlich zu beschäftigungsunabhängigen<sup>32</sup> Zwecken (v. a. Unternehmenssicherheit). Gleichwohl besteht jedenfalls auch ein Zusammenhang betrieblicher Compliance-Schulungsmaßnahmen mit der Person des Arbeitnehmers und seinem Beschäftigungsverhältnis.<sup>33</sup>

Übermittlung und Verwendung der Daten sind gestattet, wenn ein berechtigtes Arbeitgeberinteresse vorliegt und schutzwürdige Interessen des betroffenen Arbeitnehmers nicht entgegenstehen. Je gefährdeter das Unternehmen und die Position des konkret gewählten Arbeitnehmers, desto eher muss das Recht auf informationelle Selbstbestimmung gegenüber dem Interesse des Arbeitgebers, seinem Recht am eingerichteten und ausgeübten Gewerbebetrieb und sein Eigentumsrecht zurücktreten.<sup>34</sup> Ein „nicht gefährdetes“ Unternehmen ist bei der derzeitigen Gefährdungssituation nur noch in restriktiven Fällen anzunehmen, etwa bei ‚harmlosen‘ Betriebsstätten mit lediglich sporadischem Einsatz von Datenverarbeitungsprogrammen und keinerlei abstrakter Gefahr eines Cyberangriffs. Sinnvoll kann allerdings eine Zuordnung der Mitarbeiter in Risikogruppen sein,<sup>35</sup> wobei beispielhaft ein Ingenieur in der Automobilbranche mit Zugang zu Betriebs- und Geschäftsgeheimnissen eher eine Übermittlung dulden muss, als der Verkäufer eines Zoofachgeschäfts. Der Name des Mitarbeiters sollte nur dann übermittelt werden, wenn dies für den Test oder die Reaktion des Arbeitgebers (s. u. IV.) erforderlich ist.

Der Arbeitgeber muss zudem gewährleisten, dass das erforderliche Datensicherheitsniveau eingehalten wird. Die Vertraulichkeit und Integrität muss während des gesamten Tests gegeben sein (d. h. keine unverschlüsselte Übermittlung der Daten, zertifizierte Anbieter, keine Cloud in Ländern mit niedrigerem Datenschutzniveau als der EU).

22 Maschmann, AuA 2000, 519, 520.

23 Vgl. Kuhn/Willemsen, DB 2016, 111, 112.

24 Etwa vom BSI zertifizierte IT-Sicherheitsdienstleister.

25 Maschmann, NZA 2002, 13, 16.

26 A. A. ArbG Gelsenkirchen, 9.4.2009 – 5 Ca 2327/08, BeckRS 2010, 74340, in einem Fall unangekündigter „Testkäufe“. Seiner Ansicht nach müssen ökonomische Interessen des Arbeitgebers insoweit hinter dem allgemeinen Persönlichkeitsrecht der Arbeitnehmer zurücktreten.

27 Das Recht, grundsätzlich selbst darüber zu bestimmen, welche persönlichen Daten man preisgeben möchte, wurde zunächst als Abwehrrecht gegen den Staat entwickelt. Heute ist es auch in seiner Ausstrahlung auf das Verhältnis Privater untereinander (Drittwirkung des Grundrechts) allgemein anerkannt; vgl. Stögmüller, CR 2008, 435, 437.

28 § 3a S. 1 BDSG.

29 § 3a S. 2 BDSG; zu den Legaldefinitionen vgl. § 3 Abs. 6 und 6a BDSG.

30 Kuhn/Willemsen, DB 2016, 111, 114.

31 Die externen Dienstleister sind „Dritte“ im Sinne von § 3 Abs. 8 BDSG; es liegt gerade keine Auftragsdatenverarbeitung (§ 11 BDSG) vor, denn der Arbeitgeber bleibt nicht „Herr der Daten“.

32 Noch weitergehend Kuhn/Willemsen, DB 2016, 111, 113, die die Weitergabe an die Dienstleister als „beschäftigungsfremd“ ansehen.

33 Kort, DB 2011, 651; a. A. und enger Anwendungsbereich von § 32 BDSG auf die Erfüllung beiderseitiger Hauptleistungspflichten, Jousen, NZA 2011, Beil. 1, 35, 40 f.

34 Stögmüller, CR 2008, 435, 437.

35 Schmidt, BB 2009, 1295, 1299.

## b) Betriebliche Bekanntmachung

Eine betriebliche Bekanntmachung der Testergebnisse sollte aufgrund möglicher Stigmatisierungswirkung nur anonym erfolgen. Auch die Veröffentlichung guter Testabsolventen in „Bestenlisten“ sollte namentlich nur unter Einwilligung des Betroffenen erfolgen.

## 5. Dokumentation der Tests

Der Arbeitgeber hat ein Interesse daran die simulierten Angriffe zu dokumentieren: dadurch können das Material analysiert, Schwachstellen lokalisiert, Gegenstrategien entwickelt und der Test zur Sensibilisierung im Rahmen späterer Schulungen genutzt werden. Will sich der Arbeitgeber nicht nur auf die Gedankenprotokolle der Test-Dienstleister verlassen, benötigt er Video-, Foto-, und Tonaufnahmen. Diese bedeuten einen Eingriff in das allgemeine Persönlichkeitsrecht und bedürfen gesonderter Prüfung (s. sogleich).

### a) Videoaufnahmen

Zu untersuchen ist, ob eine Dokumentation des Tests mittels Videoaufzeichnung datenschutzrechtlich zulässig wäre. § 6b BDSG ist mangels öffentlich-zugänglichem Raumes – der relevante Arbeitsplatz wird meist ein Büroraum ohne Kundenverkehrswidmung sein – nicht (auch nicht analog) anwendbar.<sup>36</sup> § 32 Abs. 1 S. 2 BDSG passt gleichfalls nicht, denn es geht nicht um die repressive Aufklärung von Straftaten.<sup>37</sup> Der externe Dienstleister wird im Regelfall aus Präventionsgründen zur Vermeidung abstrakter zukünftiger Angriffe und zur Gewährleistung effektiver Compliance engagiert. Alle Mitarbeiter unter Generalverdacht zu stellen, ist trotz hoher Gefährdung betrieblicher IT-Anlagen nicht möglich.<sup>38</sup>

Die Zulässigkeit der Videoüberwachung im Rahmen der Tests richtet sich daher nach § 32 Abs. 1 S. 1 BDSG.<sup>39</sup> Unabhängig vom Streit um das Verhältnis von § 28 BDSG zu § 32 BDSG<sup>40</sup> führt die Interessenabwägung in hier zu behandelnden Fällen wohl regelmäßig zum gleichen Ergebnis. Auch hiernach muss allerdings der systematische Zusammenhang zu § 32 Abs. 1 S. 1 BDSG gesehen und eine entsprechende Verhältnismäßigkeitsprüfung vorgenommen werden.

Insgesamt ist der Einsatz von Videokameras mit rechtlichen Risiken verbunden. Daher ist es ratsam, Videotechnik restriktiv einzusetzen und weniger einschneidende Mittel zu wählen (z. B. professionelle Social Engineering Schulungsvideos, Nachspielen einzelner Situationen sowie Protokolle und Checklisten der Dienstleister); insbesondere unter Berücksichtigung des geringen Erkenntnisgewinns von Videos ohne Tonmitschnitt (vgl. § 201 StGB, dazu sogleich).

### b) Audioaufnahmen

Audioaufnahmen aus dem Test könnten eine gewichtige Erkenntnisquelle darstellen. Die Weitergabe sensibler Informationen lässt sich häufig nur akkurat durch Abhören oder Mithören von Telefon/Mitarbeitergesprächen nachweisen. Bei Audioaufnahmen ist das Recht am eigenen Wort betroffen. Grundsätzlich darf ein Arbeitnehmer selbst darüber entscheiden, ob sein gesprochenes Wort auf Tonträger aufgenommen wird und welche Personen Kenntnis vom Gesprächsinhalt erhalten sollen.<sup>41</sup> Geschützt wird die Vertraulichkeit des Wortes, weil mündliche Äußerungen in dem Bewusstsein der Flüchtigkeit und jederzeitigen Korrigierbarkeit erfolgen.<sup>42</sup> Um ein Strafbarkeitsrisiko der externen Dienstleister nach § 201 Abs. 1 Nr. 1 StGB und des Arbeitgebers zur Anstiftung dazu auszuschließen, kann mit dem Dienstleister vereinbart werden, Telefonate nur durch Gedäch-

nisprotokolle zu dokumentieren. In Ausnahmefällen – etwa bei einem gegenwärtigen, rechtswidrigen Angriff auf das Know-how des Unternehmens im kollusiven Zusammenwirken mit einem Mitarbeiter – kann eine Rechtfertigung durch Notwehr und Nothilfe nach § 32 StGB in Betracht kommen.<sup>43</sup> Hat der Arbeitnehmer den „Verrat“ bereits ausgesprochen, ist eine (weitere) Gesprächsaufzeichnung „auf Verdacht“ nicht mehr von § 32 StGB umfasst. Allerdings besteht eine fortdauernde Beeinträchtigung (Dauergefahr) der Interessen des Arbeitgebers und die Tonaufnahmen können unter Umständen durch Notstand nach § 34 StGB gerechtfertigt sein.<sup>44</sup> Die Interessenabwägung fällt zugunsten des Arbeitgebers aus, wenn der Arbeitnehmer die Vergänglichkeit der Worte benutzt, um Betriebs- und Geschäftsgeheimnisse zu verraten.<sup>45</sup> Auch die spätere Verwertung in einem Straf- oder Arbeitsprozess zur Überführung des illoyalen Mitarbeiters kann gleichfalls über § 34 StGB gerechtfertigt werden, weil nur so die fortbestehende Gefahr einer neuerlichen Rechtsgutsverletzung beendet werden kann.<sup>46</sup> Im Umkehrschluss folgt daraus, dass ein permanentes Abhören – nur zur „Vorbeugung“ von Straftaten – in der Regel unzulässig ist.

## 6. Beteiligung des Betriebsrats

In der Praxis brisant sind Beteiligungsrechte des Betriebsrates bei Social Engineering Tests.

### a) Unterrichtsrechte

Damit der Betriebsrat die Interessen der Arbeitnehmer wirksam vertreten kann, muss er wissen, was im Betrieb vor sich geht. Nach § 80 Abs. 2 BetrVG hat der Betriebsrat daher ein aufgaben- und anlassbezogenes Informationsrecht gegenüber dem Arbeitgeber.<sup>47</sup> Die Pflicht auf umfassende und rechtzeitige (Einflussnahme auf die Planungen des Arbeitgebers muss noch möglich sein) Unterrichtung wird ausgelöst, wenn der Betriebsrat eine bestimmte Information für eine der ihm gesetzlich zugewiesenen Aufgaben benötigt (§ 80 Abs. 1 S. 1 BetrVG). Im Fall der Tests muss der Betriebsrat insbesondere darüber wachen, dass die Datenschutzvorschriften zugunsten des Arbeitnehmers eingehalten werden und es muss ihm möglich sein zu prüfen, ob ein mitbestimmungspflichtig relevanter Sachverhalt vorliegt.<sup>48</sup>

Als Gegenstück dieser Informationspflicht hat der Arbeitgeber einen Anspruch auf Vertraulichkeit über die geplante Maßnahme seitens des Betriebsrates. Eine Mitteilung an die Belegschaft könnte den Test-erfolg gefährden, daher kann – dem Rechtsgedanken des § 79 Abs. 1

36 BAG, 29.6.2004 – 1 ABR 21/03, BB 2005, 102, NZA 2004, 1278 m. Hinw. auf BT-Drs. 14/4329, 38.

37 BAG, 12.2.2015 – 6 AZR 845/13, NZA 2015, 741, 747, Rn. 70, 73, 75; § 32 Abs. 1 S. 2 BDSG orientiert sich inhaltlich an den strengen Anforderungen des BAG in seinem Ur. v. 27.3.2003 – 2 AZR 51/02 (BB, 2003, 2578, NZA 2003, 1193) zur verdeckten Überwachung von Beschäftigten, BT-Drs. 16/13657, 21.

38 Pötters/Traut, RDV 2013, 132, 136; Kort, DB 2011, 651, 652; LAG Baden-Württemberg, 6.5.1998 – 12 Sa 115/97, BB 1999, 1439.

39 BT-Drs. 16/13657, 36.

40 Franzen, RdA 2010, 257, 260; ders., in: Erf. Komm., 16. Aufl. 2016, Rn. 3; Bierehoven, CR 2010, 203, 206. – Die Gesetzesbegründung ist in dieser Hinsicht widersprüchlich: BT-Drs. 16/13657, 20f., 29, 34f.

41 BVerfG, 31.1.1973 – 2 BvR 454/71, NJW 1973, 891, 892.

42 Di Fabio, in: Maunz/Dürig, Grundgesetz-Kommentar, 75. EL 2015, Art. 2 GG, Rn. 196.

43 Röckl/Fahl, NZA 1998, 1035, 1040 bezüglich Videoaufnahmen.

44 Kühl, in: Lackner/Kühl, StGB, 28. Aufl. 2014, Rn. 13.

45 Graf, in: MüKo Strafrecht, 2. Aufl. 2012, Rn. 51.

46 BVerfG, BGH, 24.11.1981 – VI ZR 164/79, NJW 1982, 277, 278.

47 BAG, 23.3.2010 – 1 ABR 81/08, NZA 2011, 811, 812.

48 BAG, 26.1.1988 – 1 ABR 34/86, NZA 1988, 620, 621; hierzu kann es erforderlich sein, dass der Arbeitgeber Unterlagen (etwa Muster-Vereinbarung mit dem Audit-Dienstleister und Checklisten) zur Verfügung stellt.

BetrVG entsprechend<sup>49</sup> – von einer Pflicht des Betriebsrates zur Verschwiegenheit ausgegangen werden, beziehungsweise dem Arbeitgeber ein Anspruch auf Unterzeichnung einer entsprechenden Vereinbarung zugestanden werden.

#### b) Auskunft nach § 96 BetrVG

Möglicherweise hat der Betriebsrat einen Anspruch auf Mitteilung der Ergebnisse und Auswertung des Tests gemäß § 96 Abs. 2 BetrVG. Das wäre der Fall, wenn es sich bei dem betreffenden Test um eine Maßnahme der Berufsbildung handelt. Dies sind Maßnahmen, die „dem Arbeitnehmer gezielt Kenntnisse und Erfahrungen vermitteln, die ihn zur Ausübung einer bestimmten Tätigkeit erst befähigen oder es ermöglichen die beruflichen Kenntnisse und Fähigkeiten zu erhalten“ (§1 Abs. 3 BBiG).<sup>50</sup> Das BAG hat allerdings einen Anspruch des Betriebsrates auf Mitteilung von Ergebnissen aus der Durchführung einer Kundenbefragung über die Kompetenz und Freundlichkeit des Personals verneint, weil es darin keine berufsbezogene systematische Vermittlung sah.<sup>51</sup> Dieses Kriterium wird bei einem Social Engineering Test im konkreten Fall zu prüfen sein. Unerheblich ist hierbei, dass die Maßnahme von externen Dritten durchgeführt wird, denn aufgrund seines beherrschenden Einflusses auf die Maßnahme ist der Arbeitgeber als Verantwortlicher zu sehen.<sup>52</sup>

#### c) Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 1 BetrVG

Fraglich ist, ob der Betriebsrat ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 1 BetrVG hat. Dieses wird nur bei gestaltenden Maßnahmen ausgelöst, die auf das Ordnungsverhalten der Arbeitnehmer einwirken.<sup>53</sup> Zudem fällt nur das Ordnungs-, nicht das Arbeitsverhalten unter die Norm.<sup>54</sup> Erfasst werden Kontrollregelungen mit deren Hilfe die Ordnung im Betrieb durchgesetzt werden soll, etwa Torkontrollen und stichprobenartige Taschenkontrollen.<sup>55</sup> Die verdeckte Überprüfung der Einhaltung von Sicherheitsvorschriften mittels Social Engineering Tests enthält keine „Regelung“, welche sich unmittelbar auf die Ordnung des Betriebes auswirkt. Die Tests sollen ein realitätsnahes Szenario schaffen, in welchem sich der Arbeitnehmer genauso verhält wie sonst auch<sup>56</sup> und nicht sein Verhalten beeinflussen und damit das Ergebnis verfälschen.<sup>57</sup>

#### d) Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG

Die Tests könnten eine Verhaltens- und Leistungskontrolle durch technische Einrichtung darstellen. § 87 Abs. 1 Nr. 6 BetrVG soll den Arbeitnehmer vor Eingriffen in sein allgemeines Persönlichkeitsrecht schützen und zu einer angemessenen Ausgestaltung der geplanten Maßnahme führen. Unter einer technischen Einrichtung ist jedes optische, mechanische, akustische oder elektronische Gerät zu fassen.<sup>58</sup> Das Mitbestimmungsrecht wird dann ausgelöst, wenn das Verhalten oder die Leistung des Arbeitnehmers überwacht werden soll. Es genügt, dass eine technische Einrichtung dazu *geeignet* ist, das Verhalten oder die Leistung der Arbeitnehmer zu kontrollieren.<sup>59</sup> Die Überwachung von Verhalten oder Kontrolle setzt logischerweise die Individualisierbarkeit der Daten zu den einzelnen Arbeitnehmern voraus, denn bei anonymisierten Daten ist keinerlei Personen-Rückbezug und individuelle Leistungskontrolle mehr möglich. Die technische Einrichtung muss die Individualisierung allerdings nicht selbst vornehmen; es reicht aus, wenn die Daten unter Heranziehung anderer Informationen (beispielsweise einem

Schichtplan) einem bestimmten Arbeitnehmer zugerechnet werden können.<sup>60</sup>

Somit hat der Betriebsrat ein Mitbestimmungsrecht, wenn der Test mithilfe technischer Einrichtungen zur Aufzeichnung des Arbeitnehmerverhaltens erfolgt. Das Mitbestimmungsrecht kann vermieden werden, wenn der Arbeitgeber ausschließlich auf Gedankenprotokolle oder rein anonymisiertes Material zurückgreift.

#### e) Zustimmungspflicht nach § 99 BetrVG

Eine Zustimmungspflicht nach § 99 Abs. 2 Nr. 3 BetrVG aufgrund der Beauftragung eines Dritten besteht bei den Tests nicht. Zwar liegt eine „Einstellung“ bereits dann vor, wenn Personen auch wenn sie nicht als Arbeitnehmer beschäftigt werden sollen, in den Betrieb eingegliedert werden um zusammen mit den dort schon tätigen Arbeitnehmern den arbeitstechnischen Zweck durch weisungsgebundene Tätigkeit zu verwirklichen.<sup>61</sup> Allerdings ließe sich eine solche Eingliederung nur bejahen, wenn der externe Dienstleister als quasi verdeckter Detektiv in das Unternehmen eingeschleust wird. Ein solches Vorgehen ist bei Social Engineers jedoch weder üblich noch nötig.

## IV. Rechtsfolgen von Social Engineering Tests

Nach Durchführung des Tests stellt sich die Frage wie die gewonnenen Erkenntnisse verwendet werden können. Bei Beurteilung der rechtlichen Folgen ist zwischen zulässigen und unzulässigen Tests zu unterscheiden.

### 1. Auswirkungen zulässiger Tests

Besteht ein Arbeitnehmer den Test nicht, stellt sich die Frage nach der Zulässigkeit arbeitsrechtlicher Sanktionen für das Fehlverhalten des Arbeitnehmers. Je nach Schwere der Pflichtverletzung kommen Ermahnungen, förmliche Abmahnungen, ordentliche und außerordentliche Kündigungen in Betracht. Zwar hat der Arbeitgeber das Verhalten in gewisser Weise „proviziert“, dennoch steht einer arbeitsrechtlichen Maßnahme nicht generell das Verbot unzulässiger Rechtsausübung nach § 242 BGB entgegen.<sup>62</sup> Im Rahmen einer Interessenabwägung wird allerdings zu berücksichtigen sein, dass der Arbeitgeber durch die Tests die Pflichtverletzung erst veranlasst hat.<sup>63</sup>

49 Bei der Kenntnis über die Social Engineering Audits handelt es sich nicht ein Betriebs- und Geschäftsgeheimnis.

50 *Kania*, in: Erf. Komm., 16. Aufl. 2016, § 96 BetrVG, Rn. 5f.; vgl. *Deckers/Deckers*, NZA 2004, 139, 142.

51 BAG, 28.1.1992 – 1 ABR 41/91, BB 1992, 1488, NZA 1992, 707, 708; dabei handelte es sich um eine Einweisung gemäß § 81 BetrVG.

52 BAG, 4.12.1990 – 1 ABR 10/90, NZA 1991, 388, 390.

53 Vgl. nur *Fitting et al.*, BetrVG, 2016, § 87, Rn. 64f.; *Zimmer/Heymann*, BB 2010, 1853, 1854; *Kuhn/Willemsen*, DB 2016, 111, 116.

54 *Kania*, in: Erf. Komm., 16. Aufl. 2016, § 87 BetrVG, Rn. 18.

55 *Kania*, in: Erf. Komm., 16. Aufl. 2016, § 87 BetrVG, Rn. 19.

56 *Deckers/Deckers*, NZA 2004, 139, 140.

57 BAG, 18.4.2000 – 1 ABR 22/99, BB 2000, 2521, NZA 2000, 1176, 1177.

58 Beispiele: Telefone, Datenverarbeitungssysteme (Arbeitsplatzrechner, Office Software), Standard Internetprogramme (z.B. Internet Explorer, MS Outlook Express) enthalten Überwachungskomponenten (History bzw. Verlaufsfunktion, Cache), Programme zur Überwachung des Datenverkehrs mit dem Internet, Security Incident and Event Management Systeme (SIEM).

59 BAG, 6.12.1983 – 1 ABR 43/81, BB 1984, 850, NJW 1984, 1476, 1484.

60 *Däubler*, Gläserne Belegschaften?, 2015, Rn. 753.

61 Vgl. etwa BAG, 12.11.2002 – 1 ABR 60/01, NZA 2004, 1289, 1291; BAG, 9.12.2008 – 1 ABR 74/07, DB 2009, 743, Rn. 16; *Thüsing*, in: Richardi, Betriebsverfassungsgesetz, 15. Aufl. 2016, Rn. 31.

62 *Ernst*, NZA 2002, 585, 590; BAG, 18.11.1999 – 2 AZR 743/98, BB 2000, 672, NJW 2000, 1211, 1213 (Ehrlichkeitskontrollen), BAG, 27.6.2001 – 7 AZR 496/99, BB 2001, 2328 (Testkäufe).

63 Vgl. BAG, 18.11.1999 – 2 AZR 743/98, BB 2000, 672.

Aufgrund dieses Beitrags ist es dem Arbeitgeber in der Regel zumutbar, zunächst eine Ermahnung auszusprechen und den Mitarbeiter zur Sensibilisierung für die bedrohten Sicherheitsaspekte (ggf. erneut) zu schulen. Anderes kann gelten, wenn der Arbeitgeber die grundsätzliche Möglichkeit solcher Tests bereits angekündigt hat und einen gewissen zeitlichen Rahmen dafür gesetzt hat. Dann kann dem Arbeitnehmer eher ein vorwerfbares Versagen im zu erwartenden und vorbereitbaren Test vorgeworfen werden.<sup>64</sup> Liegt hingegen ein „Stoß ins kalte Wasser“ vor und hat der Arbeitgeber zuvor keine klaren Verhaltensanweisungen gegeben, ist ihm eine Kündigung im Regelfall verwehrt.<sup>65</sup>

Strafrechtliche Sanktionen kommen im Normalfall nicht in Betracht. Gibt der Arbeitnehmer im Rahmen des Tests Betriebs- und Geschäftsgeheimnisse an den Dienstleister weiter (etwa Kundenlisten, Preiskalkulationen und Investitionsplanungen oder technische Skizzen und Konstruktionspläne) wird der Tatbestand des § 17 UWG (Geheimnisverrat) in der Regel nicht erfüllt. Meist fehlt es bereits an einem bewussten und gewollten Verhalten und nötigem Vorsatz des Arbeitnehmers; zumindest erklärt sich der Arbeitgeber durch die Beauftragung des Dritten mit einer möglichen Weitergabe von Betriebs- und Geschäftsgeheimnissen einverstanden. Damit entfällt entweder – tatbestandsausschließend – der Wille zur Geheimhaltung als wesentliches Merkmal des Geheimnisbegriffes bzw. wirkt die Einwilligung zumindest als Rechtfertigung.<sup>66</sup> Entsprechend machen sich weder der Arbeitgeber noch der externe Dienstleister als „Lockspitzel“ wegen Anstiftung strafbar. Ihnen fehlt der Tatvollendungswille in Bezug auf eine tatsächliche Rechtsgutsverletzung und damit der notwendige doppelte Anstiftervorsatz.<sup>67</sup>

War der Eingriff in das Persönlichkeitsrecht aufgrund erheblicher Sicherheitsinteressen gerechtfertigt (s.o. III.), kann das so gewonnene Material auch in einem späteren Arbeitsgerichtsprozess verwertet werden – die Rechtfertigungsgründe wirken dann zugunsten des Arbeitgebers fort.<sup>68</sup>

## 2. Auswirkungen unzulässiger Tests

Bei unzulässig durchgeführten Sicherheitstests kann der betroffene Arbeitnehmer Unterlassung weiterer Tests in dieser Form verlangen.<sup>69</sup> Bei unwiederbringlicher Zerstörung der Vertrauensbasis kommt eine außerordentliche Kündigung des Arbeitnehmers in Betracht.

Allerdings folgt nicht aus jedem Beweiserhebungsverbot zwangsläufig ein Beweisverwertungsverbot.<sup>70</sup> Deshalb ist zu klären welche Auswirkungen Erkenntnisse aus unzulässigen Tests im Prozess haben. Im Ergebnis ist erneut eine Abwägung erforderlich, denn in der gerichtlichen Verwertung liegt ein erneuter Eingriff, der einer sachlichen Rechtfertigung unter Beachtung des Verhältnismäßigkeitsprinzips bedarf.<sup>71</sup> In der Regel folgt jedoch aus einem unzulässigen Test in konsequentem Schutz des Persönlichkeitsrechts ein Beweisverwertungsverbot<sup>72</sup> und nur in Ausnahmefällen – wenn der Täter nicht anders zu überführen ist – kann eine Interessenabwägung zugunsten des Arbeitgebers ausfallen.

Bei der Frage, ob aus der Verletzung von Mitbestimmungsrechten ein Beweisverwertungsverbot folgt muss unterschieden werden, ob das verletzte Mitbestimmungsrecht nur der Sicherung der Ordnung des Betriebes oder dem individuellen Schutz einzelner Arbeitnehmer dient.<sup>73</sup> § 87 Abs. 1 Nr. 6 BetrVG setzt zwar einen kollektiven Bezug voraus, dennoch geht es um den Schutz des Einzelnen vor Eingriffen in sein Persönlichkeitsrecht.<sup>74</sup> Ein eigenständiges Beweisverwertungs-

verbot besteht jedoch nicht, wenn der Betriebsrat der Verwendung des Beweismittels und der darauf gestützten Kündigung zustimmt und die Beweisverwertung nach den allgemeinen Grundsätzen gerechtfertigt ist.<sup>75</sup>

## V. Zusammenfassung

Die Geschäftsleitung hat nicht nur wirtschaftliche Interessen, sondern auch rechtliche Pflichten zum Schutz des Gesellschaftsvermögens. Dazu gehören insbesondere Betriebs- und Geschäftsgeheimnisse sowie sonstige Daten. Um diese vor unbefugtem Zugriff durch Angriffe mittels Social Engineering von außen zu schützen, können solche Angriffe mittels Tests simuliert werden. Wahrt der Arbeitgeber das Verhältnismäßigkeitsprinzip, die Vertraulichkeit der Daten und wählt die Test-Dienstleister mit Bedacht aus, können Social Engineering Tests zu mehr betrieblicher IT-Sicherheit eingesetzt werden. Wird bei dem Test das Arbeitnehmergehalten durch technische Einrichtungen überwacht, kommt ein Mitbestimmungsrecht des Betriebsrats in Betracht.

**Dr. Mark Zimmer** ist LLP Partner im Münchener Büro von Gibson, Dunn & Crutcher. Der Fachanwalt für Arbeitsrecht berät seit 20 Jahren Unternehmen in allen arbeitsrechtlichen Angelegenheiten. Einen weiteren Schwerpunkt bilden nationale und internationale Untersuchungen wegen Betrugs, Untreue und Korruption („Fraud“). Über zahlreiche Publikationen und Vorträge hinaus ist Herr Zimmer durch zwei Lehraufträge hervorgetreten.



**Alicia Helle** ist studentische Hilfskraft am Lehrstuhl für Staats- und Verwaltungsrecht, Völkerrecht, Europäisches und Internationales Wirtschaftsrecht an der Universität Passau und Coach für den International Jessup Moot Court, an dem sie 2015 teilnahm. Ihren Schwerpunkt im Medien- und Informationsrecht hat sie im März 2016 erfolgreich abgeschlossen, wobei insbesondere das Datenschutzrecht im Mittelpunkt ihrer wissenschaftlichen Arbeit stand.



64 Kuhn/Willemsen, DB 2016, 111, 116.

65 Ein grundsätzliches Beweiserhebungs- und Verwertungsverbot im Fall von unangemeldeten Testkäufen annehmend das ArbG Gelsenkirchen, 9.4.2009 – 5 Ca 2327/08, BeckRS 2010, 74340 (m. Hinweis auf höchstrichterliche Rechtsprechung in Frankreich).

66 Diemer, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 205. EL 2015, Rn. 25 m. w. N.

67 Heine/Weißer, in: Schönke/Schröder, Strafgesetzbuch, 29. Aufl. 2014, Rn. 21 f.

68 Maschmann, NZA 2002, 13, 21.

69 Entsprechend §§ 1004, 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1, 1 Abs. 1 GG bzw. § 823 Abs. 2 BGB i.V.m. § 4 BDSG.

70 BGH, 21.2.1964 – 4 StR 519/63, BGHSt 19, 325, 331; BGH, 22.2.1978 – 2 StR 334/77, BGHSt 27, 355, 357; BGH, 17.3.1983 – 4 StR 640/82, BGHSt 31, 304, 308; BGH, 9.4.1986 – 3 StR 551/85, BGHSt 34, 39, 52.

71 BVerfG, 19.12.1991 – 1 BvR 382/85, BB 1992, 708; BVerfG, 13.2.2007 – 1 BvR 421/05, NJW 2007, 753; OLG Karlsruhe, 25.2.2000 – 10 U 221/99, NJW 2000, 1577.

72 BGH, 24.11.1981 – VI ZR 164/79, NJW 1982, 277, 278; BAG, 2.6.1982 – 2 AZR 1237/79, NJW 1983, 1691.

73 Rhotert, BB 1999, 1378, 1379.

74 Maschmann, NZA 2002, 13, 21; a. A. BAG, [27.3.2003 – 2 AZR 51/02], BB 2003, 2578; Dzida/Grau, NZA 2010, 1201.

75 BAG, 27.3.2003 – 2 AZR 51/02, BB 2003, 2578, NJW 2003, 3436, 3438 f. bzw. 3. Leitsatz).