Handlungsempfehlungen

Projekt ITS.APT – Dokument 2.4

Autoren:

Felix Bieker, Linda Mohammadi und

Harald Zwingelberg

für das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein

sowie

Tim Hey und Robert Ortner

für das Institut für Informations-, Telekommunikations-, und Medienrecht, Universität Münster

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Das Projekt ITS.APT erhält Förderung durch das

Bundesministerium für Bildung und Forschung.

Beiträge nach beteiligten Projektpartnern

Kapitel A-G und I sowie Annex II

Mitarbeiter des ULD (Felix Bieker, Linda Mohammadi und

Harald Zwingelberg)

Kapitel H und J sowie Annex I

Mitarteiter des ITM (Tim Hey und Robert Ortner)

Redaktionsschluss: Dezember 2018.

Inhalt

A. Einleitung

I. Zum Projekt

Infrastrukturen der Informationstechnik (IT) werden immer häufiger das Ziel von Cyberattacken mit teils großen wirtschaftlichen und ideellen Schäden. Es kommt etwa zu Beeinträchtigungen des Betriebs der betroffenen Institution und/oder Datenverluste, die die Reputation beeinträchtigen oder gar Haftungsfälle generieren. Zudem können sie zum Verlust von personenbezogenen Informationen und Betriebsgeheimnissen führen. Besonders gravierend sind die Folgen eines solchen Angriffs dann, wenn kritische Infrastrukturen (KRITIS), wie Krankenhäuser, Versorgungs- oder Verkehrseinrichtungen betroffen sind, da diese eine besonders wichtige Bedeutung für das staatliche Gemeinwesen haben.

Zur Bewertung der IT-Sicherheit in Unternehmen werden in der Regel sog. penetration tests durchgeführt. IT-Sicherheitsdienstleister versuchen dabei, in das IT-System einzudringen, um Sicherheitsschwachstellen oder Lücken zu ermitteln, die dann geschlossen werden können. Die Überprüfung der Verwundbarkeit von IT-Infrastrukturen ist dabei jedoch regelmäßig auf Aspekte der technischen Sicherheit limitiert. Außen vor bleiben Risiken, die auf Seiten der Nutzer des Systems entstehen, indem sie bspw. unangemessen auf Sicherheitshinweise reagieren.

Dieses Defizit war der Ausgangspunkt eines vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Verbundprojekts „IT-Security Awareness Penetration Testing“ (ITS.APT), das es sich zum Ziel gesetzt hat, das IT-Sicherheitsbewusstsein der Nutzer*innen eines IT-Systems zu messen und Wege zu finden, es zu verbessern. Dazu wurden die ITS.APT-Software das entwickelt, die aus dem ITS.APE-Framework und dem ITS.APT-Client besteht und die IT-Attacken auf das Computersystem, wie Phishing Mails oder sog. SQL-Injections, simuliert.

Die Nutzer*innen nehmen diese IT-Attacken in Form von angezeigten Artefakten, also fremd anmutenden Anzeigen auf dem Bildschirm, wahr. Die Reaktionen der Nutzer*innen auf die IT-Angriffe werden, ebenfalls mittels der ITS.APT-Software, protokolliert und können schließlich Erkenntnisse über deren IT-Sicherheitsbewusstsein liefern. Beispielsweise spricht das direkte Löschen einer Phishing E-Mail eher für ein erhöhtes Sicherheitsbewusstsein, während das Anklicken eines Links in der Phishing E-Mail eher für das Gegenteil spricht. Die ITS.APT-Software mit ihren beiden Komponenten und diese Handlungsempfehlungen sollen

den rechtssicheren Einsatz der ITS.APT-Software ermöglichen und werden im Folgenden als ITS.APT-Methode bezeichnet

In einem groß angelegten Feldtest an einem Klinikum der Maximalversorgung in Schleswig-Holstein als KRITIS-Betreiber wurden die Beschäftigten des Klinikums als Nutzer*innen der dortigen IT-Systeme getestet. Der Test fand unter normalen Arbeitsbedingungen statt, um möglichst authentische Ergebnisse zu gewährleisten. Die Maßnahme wurde zuvor entsprechend der geltenden gesetzlichen Bestimmungen mit dem Personalrat (PR) abgestimmt und in einer den Beschäftigten zugänglichen Dienstvereinbarung transparent beschrieben. Im Anschluss an diesen ersten Test wurden die Beschäftigten gezielt auf das Erkennen von IT-Angriffen geschult. Anschließend wurde die gleiche Testgruppe wiederum durch simulierte IT-Angriffe getestet, um zu evaluieren, welche Schulungsmaßnahme am effektivsten ist und das IT-Sicherheitsbewusstsein am besten steigert.

II. Zum Dokument

Ziel des Dokuments ist es, anderen KRITIS-Betreibern aufzuzeigen, wie die ITS.APT-Methode datenschutzfreundlich und rechtskonform angewendet werden kann. Dazu werden die im Projektverlauf gewonnen Erfahrungen durch den Einsatz der ITS.APT-Software im Klinikbetrieb des KRITIS-Betreibers gesammelt und anderen KRITIS-Betreibern in Form von Handlungsempfehlungen zum datenschutzfreundlichen und rechtssicheren Einsatz der ITS.APT-Methode zur Verfügung gestellt.

Im Projekt wurden insbesondere datenschutz-, arbeits- und haftungsrechtliche Aspekte untersucht. Dabei haben sich diverse Schwerpunkte herausgebildet, auf die dementsprechend auch der Fokus dieser Handlungsempfehlung gerichtet ist. Demnach werden zunächst die datenschutzrechtlichen Anforderungen dargestellt und Empfehlungen zur rechtskonformen Gestaltung der Testdurchführung gegeben (Kapitel B). In Kapitel C wird sodann aufbauend auf den rechtlichen Erwägungen die technische Umsetzung dargestellt und auf besondere Herausforderungen hingewiesen. Kapitel D beschäftigt sich mit den zu gewährleistenden Betroffenenrechten. In Kapitel E wird die neue Meldepflicht bei Datenschutzverletzung vorgestellt und in Kapitel F werden allgemeine Hinweise zur Übertragung von personenbezogenen Daten in Drittländer erteilt. In Kapitel G wird angesprochen, inwiefern die Voraussetzungen der Testdurchführung auf andere Szenarien übertragbar sind. Sodann wird in Kapitel H auf die arbeitsrechtlichen Aspekte eingegangen und erläutert, aus welchen Gründen eine Dienst-/Betriebsvereinbarung im Rahmen einer rechtssicheren Umsetzung

geschlossen werden sollte. In Annex I wird außerdem eine Mustervereinbarung zur Verfügung gestellt. In Kapitel I werden praktische Hinweise zur Erstellung eines notwendigen Verzeichnisses der Verarbeitungstätigkeiten und zur Durchführung einer erforderlichen Datenschutz-Folgenabschätzung gegeben. Zu dem Verzeichnis findet sich in Annex II ein entsprechendes Muster. Schließlich werden in Kapitel J die Haftungsrisiken beleuchtet und praktische Hinweise erteilt, wie diese minimiert werden können.

III. Zum Einsatz der ITS.APT-Methode

Der rechtskonforme Einsatz, des der ITS.APT-Software soll durch diese Empfehlungen sichergestellt werden. Zum besseren Verständnis sollen zunächst die Ziele und Stufen der ITS.APT-Methode zusammengefasst werden: Gegenstand ist die Durchführung eines Tests zur Erfassung, Messung und Auswertung des IT-Sicherheitsbewusstseins von Beschäftigten eines KRITIS-Betreibers. Zu diesem Zweck werden verschiedene Aktivitäten durchgeführt, die die hierfür erforderlichen Daten generieren. Die ITS.APT-Methode unterteilt sich hierbei in drei Stufen:

- In der ersten Stufe werden Beschäftigte des KRITIS-Betreibers gezielt in Situationen versetzt, die eine Reaktion auf Basis ihres jeweiligen IT-Sicherheitsbewusstseins erzeugen. Beispielsweise werden sie an ihrem Arbeitsplatz-Computer mit einer Warnmeldung eines Antivirusprogrammes konfrontiert, mit einer eingehenden Phishing-E-Mail, einer selbsttätig startenden, bildschirmfüllenden Videowiedergabe oder mit einem anderweitigen anormalen Verhalten. Die jeweiligen Reaktionen der Beschäftigten auf diese künstlich erzeugten IT-Sicherheitsvorfälle (Artefakte) werden protokolliert.
- In der zweiten Stufe erhalten die Beschäftigten eine gezielte Schulung in Hinblick auf IT-Sicherheit am Arbeitsplatz, die auch jene Anomalitäten thematisiert, denen die Beschäftigten in der ersten Stufe ausgesetzt wurden.
- In der dritten Stufe werden die nun geschulten Beschäftigten erneut mit künstlich erzeugten IT-Sicherheitsvorfällen (Artefakten) am Arbeitsplatz konfrontiert. Wie in der ersten Stufe werden dabei die Reaktionen der Beschäftigten protokolliert.

Aus den derart gewonnenen Daten sollen dann im Nachgang Erkenntnisse über Art und Qualität des Erfolges von Schulungsmaßnahmen zur Schärfung des IT-Sicherheitsbewusstseins bei den Probanden gewonnen werden.

Dabei wird grundsätzlich von zwei verschiedenen Einsatzszenarien ausgegangen. Im ersten Einsatzszenario setzt der KRITIS-Betreiber selbst die ITS.APT-Methode ein, im zweiten Szenario geschieht dies über einen IT-Dienstleister. Je nach angewandtem Szenario können sich die zu beachtenden rechtlichen Anforderungen ändern.

B. Datenschutzrechtliche Anforderungen und Empfehlungen zur rechtskonformen Gestaltung der Testdurchführung

Die zur Testdurchführung entwickelte Software muss in das IT-System des KRITIS-Betreibers eingebracht werden. Neben der Beachtung reiner Datensicherheitsaspekte, müssen dabei selbstverständlich auch und gerade die einschlägigen datenschutzrechtlichen Bestimmungen eingehalten werden. Im Hinblick auf die anvisierte Testdurchführung im laufenden Betrieb und Alltag des KRITIS-Betreibers, sind rechtliche und praktische Grenzen aufzuzeigen, um das Risiko von Datenpannen zu minimieren. In diesem Dokument werden wird auf vertieft die einschlägigen Normen des Datenschutzrechts in erster Linie aus der ab dem 28. Mai 2018 geltenden EU-Datenschutzgrundverordnung[1] (DSGVO) eingegangen. Mit den Vorschriften der DSGVO zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen soll das Datenschutzrecht in der EU vereinheitlicht werden. Die DSGVO wird die aus dem Jahr 1995 stammende Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutzrichtlinie) ersetzen. Im Gegensatz zur aktuell noch geltenden Datenschutzrichtlinie muss die DSGVO nicht in nationales Recht umgesetzt werden, sondern gilt in allen EU-Mitgliedstaaten unmittelbar. Je nach Anwendbarkeit sind ggf. einzelne Vorschriften aus den entsprechenden (angepassten) Landesdatenschutzgesetzen oder aus dem neuen Bundesdatenschutzgesetz weiterhin zu beachten, sofern die DSGVO nicht vorrangig gilt. Des Weiteren werden u. a. auch die Vorschriften aus dem Telekommunikationsgesetz (TKG) und dem Telemediengesetz (TMG) betrachtet. Schließlich werden die sich aus den entsprechenden Vorschriften der o. g. Gesetze und die sich daraus ergebenden Konsequenzen für die Testdurchführung zusammengefasst.

I. Anwendbares Recht

Die DSGVO ist ab dem 25. Mai 2018 grundsätzlich die maßgebliche Rechtsgrundlage für jede Verarbeitung personenbezogener Daten durch Unternehmen und Behörden. Sie ist in allen Mitgliedstaaten der Europäischen Union unmittelbar anzuwenden.

Für den Bereich des Beschäftigtendatenschutzes gem. Art. 88 DSGVO, der für die ITS.APT-Methode von hoher praktischer Relevanz ist, sind die Vorschriften des BDSG als Ergänzung zu betrachten.

Wenn eine öffentliche Stelle personenbezogene Daten für die Strafverfolgung und -vollstreckung, einschließlich der Gefahrenabwehr, erhebt, ist die DSGVO gem. Art. 2 Abs. 2 lit. d DSGVO nicht anwendbar. Die Verarbeitung personenbezogener Daten in diesem Bereich bestimmt sich gem. § 45 BDSG nach Teil 3 des BDSG, der die Richtlinie zum Datenschutz im Bereich der Strafverfolgung und Vollstreckung (JI-Richtlinie)[2] umsetzt. Es ist aber zu beachten, dass der Einsatz der ITS.APT-Methode zur Überprüfung und Verbesserung des IT-Sicherheitsbewusstseins der Beschäftigten keine Datenerhebung zum Zweck der Strafverfolgung oder -vollstreckung darstellt, sodass auch hier die DSGVO anwendbar ist.

Zudem gelten weiterhin bereichsspezifische Regelungen: Geht es etwa um die Verarbeitung personenbezogener Daten im Rahmen von sog. Telekommunikations- und Telemediendiensten, sind gegenwärtig das Telekommunikations-, bzw. das Telemediengesetz anwendbar. In diesem Kontext wird künftig die ePrivacy-Verordnung zu beachten sein, welche sich zum Redaktionsschluss dieses Berichts noch im Gesetzgebungsverfahren befindet.

Sofern das Bundesdatenschutzgesetz (BDSG) oder eines der Landesdatenschutzgesetze ergänzend zur DSGVO oder in Umsetzung der JI-Richtlinie auf einen Sachverhalt anwendbar ist, bestimmt sich die Anwendbarkeit nach der Organisationsform der (für die Datenverarbeitung) verantwortlichen Stelle sowie ggf. nach ihrem Sitz. Verantwortliche Stelle ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, (Art. 4 Nr. 7 DSGVO).

[2] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. EU L 119/89

Die deutschen Datenschutzgesetze von Bund wie Ländern unterscheiden öffentliche von nichtöffentlichen Stellen und regeln deren jeweilige Verantwortlichkeiten in Bezug auf die Verarbeitung personenbezogener Daten in verschiedenen Abschnitten.

Das BDSG gilt für öffentliche Stellen des Bundes und für öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie Bundesrecht ausführen oder als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt. Für öffentliche Stellen der Länder gilt das jeweilige Landesdatenschutzgesetz, sofern ein solches existiert.

Des Weiteren gilt das BDSG gem. § 1 für nichtöffentliche Stellen. Nichtöffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht den o. g. Definitionen unterfallen. Soweit eine nichtöffentliche Stelle aber hoheitliche Aufgaben der öffentlichen Verwaltung wahrnimmt, ist sie gem. § 2 Abs. 4 BDSG wiederum als öffentliche Stelle zu behandeln.

Für die Anwendung der ITS.APT-Methode ist das Datenschutzrecht zu beachten:

- Für nichtöffentliche Stellen (Unternehmen) sind die DSGVO und das BDSG anwendbar.
- Für öffentliche Stellen (Behörden) des Bundes sind die DSGVO und das BDSG anwendbar.
- Für öffentliche Stellen (Behörden) der Länder sind die DSGVO und das jeweilige LDSG anwendbar.

II. Personenbezogene Daten

Das Datenschutzrecht zielt darauf ab, „die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten“ zu schützen (Art. 1 Abs. 2 DSGVO). Es findet dementsprechend nur auf die Verarbeitung personenbezogener Daten Anwendung. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen (Art. 4 Nr. 1 DSGVO). Gem. Art. 4 Nr. 1 Hs. 2 DSGVO wird eine natürliche Person als identifizierbar angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen

Identität dieser natürlichen Person sind. Ist also eine Angabe einer bestimmten Person zuzuordnen, handelt es sich um ein personenbezogenes Datum.[3] Es macht datenschutzrechtlich keinen Unterschied, ob ein Datum einer bestimmten oder bestimmbaren Person zuzuordnen ist.[4] Wenn sich ein Datum also nicht direkt einer (bestimmten) Person zuordnen lässt, liegt dennoch per Definition ein Personenbezug vor, wenn die Person „bestimmbar" ist. In der juristischen Literatur wird diesbezüglich die Frage aufgeworfen, ob die Person anhand der vorliegenden Daten „objektiv" oder „relativ" bestimmbar sein muss, um von einem personenbezogenen Datum auszugehen.[5] Objektive Bestimmbarkeit der Person meint, dass die Person allgemein – für eine beliebige Stelle – identifizierbar ist. Es kommt nicht nur auf die Kenntnisse, Mittel und Möglichkeiten der datenverarbeitenden Stelle an. Ist es für jedermann absolut unmöglich, einen Zusammenhang zwischen einem Datum und einer natürlichen Person herzustellen, so fehlt es an der Bestimmbarkeit.[6] Ein Personenbezug besteht daher erst dann nicht, wenn Einzelangaben von niemandem oder aber nur mit einem unverhältnismäßig großen Zeit-, Kosten- und Arbeitsaufwand (geleistet durch eine beliebige Stelle) einer natürlichen Person zuzuordnen wären.[7] Relative Bestimmbarkeit der Person hingegen stellt auf die Kenntnisse, Mittel und Möglichkeiten der konkreten datenverarbeitenden Stelle ab. Hiernach besteht ein Personenbezug schon nicht, wenn die Einzelangaben von dieser Stelle nicht oder nur mit einem unverhältnismäßig großen Zeit-, Kosten- und Arbeitsaufwand einer natürlichen Person zugeordnet werden könnte.[8] Grundsätzlich ist in jedem Fall für die Feststellung der Bestimmbarkeit zu berücksichtigen, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden können. Dabei sollten nach der DSGVO auch die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen berücksichtigt werden, sofern bei der Feststellung der Bestimmbarkeit einer natürlichen Person objektive Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden.[9] Im Hinblick auf die zunehmenden technischen Möglichkeiten der automatisierten Datenverarbeitung ist es extrem schwer umsetzbar zu verhindern, einen Personenbezug (wieder-) herzustellen.[10] Inzwischen sind weitreichende technische

[3] Paal/Pauly/*Ernst*, DSGVO, Art. 4 Rn. 8.
[4] Paal/Pauly/*Ernst*, DSGVO, Art. 4 Rn. 9.
[5] Vgl. hierzu auch (im Zusammenhang mit Pseudonymen) ITS.APT Dokument 2.1 „Arbeitsrechtliche Betrachtung".
[6] Paal/Pauly/*Ernst*, DSGVO, Art. 4 Rn. 9.
[7] Paal/Pauly/*Ernst*, DSGVO, Art. 4 Rn. 10.
[8] An den „unverhältnismäßig hohen Aufwand" sind sehr hohe Anforderungen zu stellen, vgl. hierzu Paal/Pauly/*Ernst*, DSGVO, Art. 4 Rn. 50.
[9] Erwägungsgrund Nr. 26 der DSGVO.
[10] Vgl. hierzu sogleich unter V.

Möglichkeiten bzw. Mittel verfügbar, scheinbar anonyme Daten dennoch den Betroffenen zuzuordnen. Aus diesem Grund sind nunmehr höhere Anforderungen an die Anonymisierung zu stellen. Liegt etwa eine Erschwerung der Bestimmbarkeit einer natürlichen Person durch „zu hohen Aufwand" vor, spricht dies eher für eine Pseudonymisierung[11] als für eine Anonymisierung.[12] Wird jedoch tatsächlich eine Anonymisierung angenommen, da eine natürliche Person unter Heranziehung aller objektiven Faktoren auch unter Berücksichtigung der verfügbaren Technologien nicht einmal identifizierbar ist, so findet das Datenschutzrecht keine Anwendung.[13] Das Datenschutzrecht findet nur Anwendung bei personenbezogenen Daten, was bei anonymisierten Daten nicht (mehr) der Fall ist.

Grundrechtlich ist das Datenschutzrecht auf EU-Ebene hauptsächlich auf das Recht auf Schutz personenbezogener Daten gem. Art. 8 EU-Grundrechte-Charta (GrCh) und das Recht auf Schutz der Privatsphäre gem. Art. 7 GrCh gestützt. Nach beiden Rechten besteht bei der Verarbeitung personenbezogener Daten ein Eingriff, der gem. Art. 52 (1) GrCh gerechtfertigt werden muss. Auf deutscher Ebene tritt das Recht der Einzelnen, selbst über „Preisgabe und Verwendung der ihre Person betreffenden Daten zu entscheiden" hinzu. Dieses Recht auf informationelle Selbstbestimmung wurde erstmals 1983 durch das „Volkszählungsurteil" des Bundesverfassungsgerichts (BVerfG) als Teil des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i.V.m. Art. 1 GG hergeleitet.[14]

III. Kategorien personenbezogener Daten

Im Hinblick auf personenbezogene Daten können je nach Art und Verarbeitungszusammenhang verschiedene Rechtsnormen relevant werden. Im Folgenden sollen einige Kategorien von Daten kurz im Hinblick auf die sich für die Testdurchführung ergebenden Besonderheiten beleuchtet werden.

1. Medizin-/Gesundheits-/Patientendaten

Die Verarbeitung besonderer Kategorien personenbezogener Daten ist grundsätzlich untersagt, Art. 9 Abs. 1 DSGVO. Dabei handelt es sich dem Wortlaut nach um Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie

[11] Ausführlich zu den Voraussetzungen der Pseudonymisierung Paal/Pauly/*Ernst*, DSGVO, Art. 4 Rn. 40-47.
[12] Paal/Pauly/*Ernst*, DSGVO, Art. 4 Rn. 50.
[13] Erwägungsgrund Nr. 26 der DSGVO.
[14] BVerfG, Urteil vom 15. Dezember 1983, Az. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83

die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Für jede eine rechtskonforme Verarbeitung personenbezogener Daten muss grundsätzlich zunächst eine Rechtsgrundlage nach Art. 6 DSGVO vorliegen. Art. 9 Abs. 2 DSGVO regelt sodann die Ausnahmen, in denen die Verarbeitung besonderer Kategorien von personenbezogenen Daten zulässig ist. Gegebenenfalls sind konkretisierende oder spzialgesetzteliche Regelungen zur Verarbeitung solcher Kategorien von Daten im Bundesdatenschutzgesetz, im jeweiligen Landesdatenschutzgesetz der Länder oder einschlägigen Spezialgesetzen (SGB, Regelungen zu Heilberufen, Steuerrecht) zu berücksichtigen, da die Mitgliedstaaten gemäß Art. 9 Abs. 4 DSGVO zusätzliche Bedingungen, einschließlich Beschränkungen einführen oder aufrechterhalten können, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist.

Grund für den Schutz dieser besonderen Kategorien von Daten, die auch als sensibel bezeichnet werden, ist der Umstand, dass es sich um höchstpersönliche Daten handelt, die in einem spezifischen Zusammenhang mit Grundfreiheiten und Grundrechten stehen. Ein Zusammenhang besteht dabei nämlich nicht nur mit Art. 8 EU-Grundrechte-Charta (GRCh), sondern u. a. auch mit Art. 7 GRCh (Achtung des Privat- und Familienlebens) sowie Art. 1 GRCh (Würde des Menschen), Art. 10 (Gedanken-, Gewissens- und Religionsfreiheit) etc.[15] Diese sensiblen personenbezogenen Daten sind besonders schützenswert, da im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten auftreten können,[16] , z.B. typischerweise als Grundlage für Diskriminierungen sind.

Gemeinsam genannt mit u. a. Daten über politische Meinungen und religiöse Überzeugungen werden Gesundheitsdaten einem besonderen Schutz unterstellt. Die besondere Schutzbedürftigkeit von Gesundheitsdaten ist in den Datenschutzgesetzen festgeschrieben. Zusätzlich unterliegen Gesundheitsdaten als Patientengeheimnis der beruflichen Schweigepflicht.[17] In Art. 4 Nr. 15 DSGVO werden Gesundheitsdaten legaldefiniert als „personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren

[15] Paal/Pauly/*Frenzel*, DSGVO, Art. 9 Rn. 1.
[16] Kühling/Buchner/*Weichert*, DSGVO, Art. 9 Rn. 1; Erwägungsgrund Nr. 51 der DSGVO.
[17] § 203 StGB sowie standesrechtlich gemäß § 9 der (Muster-) Berufsordnung der Ärzte bzw. Berufsordnungen anderer Heilberufe.

Gesundheitszustand hervorgehen“. Der Begriff der Gesundheitsdaten ist weit auszulegen und erfasst bereits die Tatsache, dass eine Person überhaupt als Patient bei einem Arzt in Behandlung ist.[18] Alle Daten, die Schlüsse auf den früheren, gegenwärtigen und (voraussichtlich) künftigen Gesundheitszustand einer natürlichen Person zulassen, sind als Gesundheitsdaten zu qualifizieren.[19] Dazu zählen etwa klassische Angaben zu Untersuchungsergebnissen, zu chronischen oder akuten Krankheiten, Diagnosen, Therapien, Ultraschallergebnissen, Röntgenbildern, Medikamenten, Impfungen etc. Umfasst sind des Weiteren auch Angaben über Aufenthalte in gesundheitsrelevanten Einrichtungen wie z. B. Krankenhäusern, Kurkliniken, Pflegeheimen sowie Angaben über Kommunikationsinhalte bzw. über Bestands-, Verkehrs- und Inhaltsdaten des Telekommunikationsverkehrs zwischen Betroffenen und Gesundheitseinrichtungen.[20] Auch mittels sog. Wearables bzw. Gesundheits-Apps erhobene und verarbeitete Daten – etwa Pulsschlag, Blutdruck oder Körpertemperatur - sind Gesundheitsdaten, die dem strengen Schutz unterfallen.[21]

Die Verarbeitung besonderer Kategorien personenbezogener Daten ist gemäß Art. 9 Abs. 2 lit a) DSGVO grundsätzlich zulässig, wenn die betroffene Person in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke eingewilligt hat. Die informierte Einwilligung in die Verarbeitung besonderer Arten von Daten muss in jedem Fall ausdrücklich erfolgen, also die besonderen Daten explizit nennen. Wegen der Schutzbedürftigkeit der sensiblen Daten ist eine konkludente Einwilligung nicht ausreichend.[22]

Wenn Daten einer dieser o.g. Kategorien zuzuordnen sind, sind sie als sensibel zu betrachten. Eine Ansehung des einzelnen Datums findet nicht mehr statt. Irrelevant für die Einordnung in eine dieser Gruppen ist, ob das Datum explizit sensibel ist – wie etwa konkrete Werte aus einer Patientenakte – oder ob sich die Sensibilität aus dem Gesamtzusammenhang, also mittelbar, ergibt. Dies kann etwa dann relevant werden, wenn Mischdatensätze ausgewertet werden, die sowohl aus sensiblen als auch aus nicht-sensiblen Daten bestehen.[23] Im Übrigen ist zu beachten, dass für eine umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten eine Datenschutz-Folgenabschätzung gemäß Art. 35 Abs. 3 lit b) DSGVO erforderlich ist. Flankierend stehen Gesundheitsdaten auch unter dem besonderen Schutz anderer Rechtsnormen. Die Offenbarung von anvertrauten Informationen ist für

[18] Paal/Pauly/Frenzel, DSGVO, Art. 9 Rn. 15.
[19] Schaffland/Wiltfang/*Schaffland/Holthaus*, DSGVO, Art. 4 Rn. 207; Erwägungsgrund Nr. 35 der DSGVO.
[20] Kühling/Buchner/*Weichert*, DSGVO, Art. 9 Rn. 39.
[21] *Kopp/Sokoll*, NZA 2015, 1352 (1357).
[22] Paal/Pauly/*Frenzel*, DSGVO, Art. 9 Rn. 21.
[23] Gola/*Schulz*, DSGVO, Art. 9 Rn. 11.

Angehörige der Heilberufe, insbesondere Ärzte und deren Mitarbeiter, strafbewährt (§ 203 StGB). Die Berufsordnungen der Landesärztekammern normieren die Schweigepflicht und sanktionieren Verstöße. Schließlich bestehen auch aus dem zivilrechtlichen Behandlungsvertrag Unterlassungs- und Schadensersatzansprüche bei unberechtigter Weitergabe von Patientendaten.

Sofern für den Testversuch keine Gesundheitsdaten oder sonstige besondere Kategorien personenbezogener Daten direkt erhoben werden, kann die Regelung des Art. 9 DSGVO zur Verarbeitung sensibler Daten relevant sein, wenn Tests im Umfeld einer kritischen Infrastruktur wie z. B. eines Krankenhauses und unter Einbeziehung des IT-Systems stattfinden sollen. Von der Überlegung, beispielsweise Screenshots oder Screencasts von den Bildschirmen der Probanden anzufertigen, um Reaktionen besser dokumentieren zu können, sollte aus Gründen der hohen Schutzbedürftigkeit der besonderen Kategorien personenbezogener Daten Abstand genommen werden. Es besteht die Gefahr, dass neben den durch die Testdurchführung erzeugten Artefakten auch Dokumente geöffnet und auf dem Bildschirm sichtbar sind, die z. B. Gesundheitsdaten von Patienten enthalten. Eine Erhebung von sensiblen Daten im Sinne von Art. 9 DSGVO ist in solchen Fällen mangels Rechtsgrundlage – insbesondere der ausdrücklichen Einwilligung der Betroffenen – unzulässig.

Ein weiterer Grund für den Verzicht der Erhebung solcher besonderen Kategorien personenbezogener Daten, besteht darin, dass neben speziellen berufsrechtlichen Normen, auch die Verletzung der ärztlichen Schweigepflicht allgemein strafbewährt ist. § 203 StGB stellt die Verletzung von Privatgeheimnissen unter Strafe. Wer unbefugt ein fremdes Geheimnis offenbart, das ihm als Arzt, Apotheker oder Angehöriger eines anderen Heilberufs anvertraut worden oder sonst bekannt geworden ist, macht sich gem. § 203 Abs. 1 Nr. 1 StGB strafbar. Zu letzteren gehören u.a. Krankenschwestern und -pfleger, Kinderkrankenschwerstern und -pfleger, sowie Krankenpflegehelferinnen und -helfer. Gleiches gilt für deren berufsmäßig tätige Gehilfen und die Personen, die bei ihnen zur Vorbereitung auf den Beruf tätig sind (§ 203 Abs. 3 S. 2 StGB). Das technische Wartungs- und Bedienungspersonal ist von der Strafnorm grundsätzlich erfasst, vorausgesetzt es ist fest in die Organisation eingebunden. Allerdings wurde die Regelung bis 2017 nicht auf Auftragsverarbeiter angewendet, da es bei ihnen an einer hinreichenden arbeitsrechtlichen Weisungsgebundenheit fehlt. Soweit Auftragsverarbeiter mit dem § 203 StGB unterfallenden medizinischen Daten umgehen, basiert dies auf Grundlage von Einwilligungen zur Zeit der

Patienten. Diese Einwilligungen umfassen jedoch nicht den Einsatz der ITS.APT-Methode. Gegenwärtig ist geplant, die Strafnorm des § 203 StGB für eine Auftragsverarbeitung zu öffnen, indem die Weitergabe von Daten an „sonstige mitwirkende Personen“ nach § 203 Abs. 2 S. 3 StGB-E eine statthafte Offenbarung ist, soweit diese für die Inanspruchnahme der Tätigkeit der mitwirkenden Person erforderlich ist.[24] Allerdings sollte auch dann mit Blick auf die zu schützenden Informationen der Berufsgeheimnisträger eine Lösung zum Penetration Testing dennoch möglichst so gestaltet sein, dass Zugriffe auf solche Informationen nicht möglich bzw. erforderlich sind. Mit Blick auf die im Projekt ITS.APT vorgestellte konkrete Umsetzung von durchdacht ausgestalteten Artefakten wäre zudem im Einzelfall besonders zu begründen, warum ein Zugriff auf die geschützten Daten für die Durchführung des Tests erforderlich ist. Sollte eine Kenntnisnahme des Dienstleisters von Informationen, die dem § 203 StGB unterliegen, zwingend für die erfolgreiche Testdurchführung erforderlich sein, kann dies nach der Novelle des § 203 StGB statthaft sein. Zuvor ist jedoch zu prüfen, ob hier statt auf reale Mandanten- oder Patientendaten z.B. auf fiktive Daten zurückgegriffen werden könnte.

Die Norm dient dem Schutz des verfassungsmäßig gewährleisteten allgemeinen Persönlichkeitsrechts der Betroffenen, sowie dem des Rechts auf informationelle Selbstbestimmung, d.h. die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. „Offenbaren“ ist jede Mitteilung über die geheim zu haltende Tatsache an einen Dritten. Umfasst ist auch die Identität der Person, um deren Geheimnis es sich handelt. Das bedeutet, dass bereits die Tatsache, dass eine Person in einem Behandlungsverhältnis zu einem Arzt steht, geheim ist. Soweit es um strafrechtlich relevante Inhalte geht, die digital gespeichert sind, genügt die Einräumung der Verfügungsgewalt über die Daten, d.h., Weitergabe des Datenträgers oder der Datei. Zugriff Externer auf die IT-Systeme, mit denen Patientendaten verarbeitet werden, kann den Tatbestand mithin erfüllen. Bereits wenn die Möglichkeit der inhaltlichen Kenntnisnahme eingeräumt wird, z.B. durch Unterlassen gebotener Sicherungsmaßnahmen in Garantenstellung, ist der Tatbestand vollendet. Für den Einsatz der ITS.APT-Methode bedeutet dies, dass im Fall der Durchführung durch einen Auftragsverarbeiter, dieser nicht unmittelbaren Zugriff auf die IT-Infrastruktur des KRITIS-Betreibers erhalten darf. Andernfalls würden sich beteiligte Beschäftigte des KRITIS-Betreibers ggf. dem Risiko der Strafverfolgung aussetzen, was in jedem Falle vermieden werden soll.

[24] BT-Drucks. 18/11936 vom. 12.4.2017, S. 22 und S 28 f.

2. Empfehlungen zur Gestaltung der Artefakte

Aus den soeben dargestellten rechtlichen Anforderungen und Bedingungen lässt sich ableiten, dass bei Gestaltung der Artefakte sichergestellt werden sollte, dass keine internen Daten des KRITIS-Betreibers, und insbesondere keine besonderen Kategorien personenbezogener Daten, verarbeitet werden. Dies ist bei Artefakten, die auf dem Rechner bestimmte Dialogfenster öffnen, etwa eines falschen Virenscanners, oder die bestimmte Dateien auf dem Desktop ablegen und diese nach einer gewissen Zeit oder bei einer Interaktion der Beschäftigten wieder verschwinden lassen, sichergestellt. Bei simulierten Phishing-E-Mails ist dies jedoch anders. Soweit in diesen Links auf Seiten enthalten wird, bei denen etwa Text eingegeben wird, sollte zum einen keine Eingabe von sensiblen personenbezogenen Daten verlangt werden. Zum anderen sollten die konkret eingegebenen Daten nicht erhoben oder gar gespeichert werden. Vielmehr genügt es für den Zweck der Feststellung des IT-Sicherheitsbewusstseins der Beschäftigten festzustellen, ob diese mit der falschen Website interagiert haben; der Inhalt der Interaktion ist dabei nicht maßgeblich und daher nicht zu erfassen.

3. Beschäftigtendaten – Verkehrs- und Personaldaten

Wird die ITS.APT-Methode angewandt, werden personenbezogene Daten der Beschäftigten des KRITIS-Betreibers verarbeitet. Die Reaktion der Beschäftigten auf die Artefakte wird dabei untersucht. Es darf dabei keine Kontrolle der E-Mail-Postfächer der Beschäftigten stattfinden in dem Sinne, dass Einsicht in Absender und Adressaten der im Postfach gespeicherten E-Mails oder gar in E-Mail-Inhalte genommen wird. Aber eine Kontrolle des Verhaltens der Beschäftigten in Bezug auf Telekommunikationsvorgänge wird insofern ermöglicht, als ihre Reaktion auf die Artefakte gespeichert und für den Testleiter sichtbar gemacht wird. Es werden also Verkehrsdaten automatisiert erhoben und gespeichert.

Die Tests finden beim KRITIS-Betreiber statt. Alle untersuchten Beschäftigten müssen sich also in einem Beschäftigungsverhältnis mit dem KRITIS-Betreiber befinden. Datenschutz im Arbeitsverhältnis ist aus mehreren Gründen als besonders problematisch zu betrachten. In erster Linie liegt das an der Annahme einer „strukturellen Unterlegenheit“ des Beschäftigten gegenüber seinem Vertragspartner, die es dem Beschäftigten erschwert, ein angemessenes Datenschutzniveau gegenüber dem Arbeitgeber mit privatrechtlichen Mitteln sicherzustellen. Zudem hat der Arbeitgeber auch in einem gewissen Umfang ein berechtigtes Interesse, Daten seiner Beschäftigten zu erheben, um deren Arbeitsleistung zu kontrollieren.

Auch wenn er mit solchen Verhaltenskontrollen in das Recht auf informationelle Selbstbestimmung seiner Beschäftigten eingreift, kann dieser Eingriff gerechtfertigt sein.

Hinsichtlich der durch den Arbeitgeber erhobenen Daten ist zu unterscheiden: Zunächst muss der Arbeitgeber selbstverständlich einige Daten seiner Beschäftigten erheben und auch übermitteln; dies betrifft insbesondere den Bereich der Personaldaten, die zu Abrechnungs-, sowie Verwaltungszwecken (bspw. Anmeldung bei der Sozialversicherung) benötigt werden. Ebenso müssen im Laufe des Beschäftigungsverhältnisses z.B. genaue Angaben zu Höhe von Lohn oder Gehalt gemeldet werden, um dem Finanzamt die Ermittlung der genauen Höhe der fälligen Lohnsteuer zu ermöglichen.

Daneben fallen aber – je nach Art der Beschäftigung – auch weitere personenbezogene Daten der Beschäftigten beim Arbeitgeber an. Im Falle computergestützter Arbeitsplätze mit Internetzugang kann z.B. protokolliert werden, welche Websites durch die Beschäftigten besucht wurden.[25] Diese Fälle sind aufmerksam zu betrachten und zu bewerten, um sicher zu stellen, dass nur zu bestimmten vorab definierten Zwecken von einzelnen Daten Gebrauch gemacht wird und z.B. in größeren Unternehmen auch klare Zugriffsberechtigungen bestehen.

Bei computergestützten Arbeitsplätzen fallen v.a. „Verkehrsdaten“ an. „Verkehrsdaten“ sind gem. § 3 Nr. 30 TKG solche, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Erfasst sind mithin alle Daten einer Kommunikation, die keine Inhaltsdaten sind. Die Telekommunikations-, bzw. Verkehrsdaten der Beschäftigten sind personenbezogene Daten, die der Arbeitgeber durch Speicherung und Zugriff erhebt und verarbeitet. Personenbezogene Daten sind gemäß der Legaldefinition in Art. 4 Nr. 1 DSGVO „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen“. Der Anwendungsbereich des Datenschutzrechts ist also auch beim Vorliegen (lediglich) personenbeziehbarer Daten eröffnet. „Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.[26] Wenn bei Einsatz der ITS.APT-Methode demnach bspw. das Anklicken des Links in einer Spam-E-Mail einem bestimmten E-Mail-Konto zugerechnet

[25] Die Einführung einer solchen Maßnahmen wird jedoch regemäßig mitbestimmungspflichtig sein gem. § 87 Abs. 1 Nr. 1 und Nr. 8 BetrVG.
[26] Vergl. oben B. II.

werden kann und dieses E-Mail-Konto aufgrund der internen E-Mail-Adress-Zuteilung einem bestimmten Beschäftigten – und das entwickelte Programm die Rückführbarkeit auch nicht per se ausschließt – handelt es sich bei der Feststellung des Verhaltens um die Verarbeitung eines personenbeziehbaren Datums des Beschäftigten. Gleiches gilt, wenn über die IP-Adresse des abrufenden Rechners auf die abrufende Person geschlossen werden kann.

Verantwortliche Stelle, d.h. verantwortlich für die Einhaltung der Datenschutzvorschriften, ist gem. Art. 4 Nr. 7 DSGVO jede Person oder Stelle, die die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Der Arbeitgeber, hier der KRITIS-Betreiber ist bzgl. der Personal-, wie auch dienstlichen Kommunikationsdaten seiner Beschäftigten daher verantwortliche Stelle im Sinne des Gesetzes.

IV. Datensicherheit i.S.d. Art. 32 DSGVO

Die verantwortliche Stelle hat technische und organisatorische Maßnahmen zu treffen, Art. 32 DSGVO. Dazu zählen alle Maßnahmen, die die verantwortliche Stelle ergreifen kann, um die Datenschutzgrundsätze des Art. 5 DSGVO wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen.[27] Unter anderem ist es im Rahmen der getroffenen Maßnahmenden datenverarbeitenden Stellen häufig gestattet, bestimmte Daten zu „loggen“, d.h. zu speichern. Hierbei handelt es sich insbesondere um sog. „Protokolldaten“, die bspw. für Zugriffe berechtigter Personen, die Änderungen an automatisierten Verfahren bewirken können, zu speichern sind oder im Fall ausschließlich automatisierter Speicherung, Veränderung und Übermittlung personenbezogener Daten wann, durch wen und in welcher Weise die Verarbeitungen vorgenommen wurden.[28] Die Zugriffe müssen nachvollziehbar protokolliert werden und es sollten effektive Löschkonzepte der Speicherbegrenzung gemäß Art. 5 Abs.1 lit. e DSGVO entwickelt werden.[29]. Gründe für diese weitgehende Erlaubnis und Pflicht zur Protokollierung sind v.a. die Gewährleistung der Transparenz bzw. der Betroffenenrechte, einer Kontrollmöglichkeit der Handlungen von System-Administratoren sowie die Erfüllung der sog. Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO.[30] Die verantwortliche Stelle sollte interne Strategien, eine Art Datenschutzkonzept, festlegen und Maßnahmen, insbesondere im Sinne der Grundsätze aus Art. 25 DSGVO, ergreifen, um die

[27] Paal/Pauly/*Martini*, DSGVO, Art. 25 Rn. 27.
[28] Paal/Pauly/*Martini*, DSGVO, Art. 25 Rn. 28.
[29] Gola/*Nolte/Werkmeister*, DSGVO, Art. 25 Rn. 16.
[30] Gola/*Nolte/Werkmeister*, DSGVO, Art. 25 Rn. 18, 19.

Einhaltung der Bestimmungen der DSGVO nachweisen zu können.[31] . Für die nach Art. 25 DSGVO erhobenen und gespeicherten Daten besteht wegen des Zweckbindungsgrundsatzes gemäß Art.5 Abs. 1 lit. b DSGVO ein Verwendungsverbot für andere Zwecke, wie etwa der Verhaltens- oder Leistungskontrolle im Rahmen von Beschäftigungsverhältnissen.

- Bei der Einsatz der ITS.APT-Methode werden in jedem Fall personenbezogene Daten der Beschäftigten verarbeitet.
- Die über die Beschäftigten erhobenen Daten müssen minimiert werden.
- Die über die Beschäftigten erhobenen Daten dürfen nicht für eine Leistungskontrolle eingesetzt werden.
- Bei Gestaltung der Artefakte muss sichergestellt sein, dass keine Daten von Patient*innen, Kund*innen, Petent*innen, Verdächtigen, etc. verarbeitet werden.

V. Rechtsgrundlage der Verarbeitung

Personenbezogener Daten dürfen grundsätzlich nur verarbeitet werden, wenn dies auf einer Rechtsgrundlage im Sinne des Art. 6 Abs. 1 DSGVO beruht.

1. Einwilligung im Arbeitsverhältnis

Beim Einsatz der ITS.APT-Methode scheidet die Einholung einer Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO regelmäßig aus.

Einwilligung wird definiert als „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.“ (Art. 4 Nr. 11 DSGVO).

„Freiwillig“ setzt dementsprechend voraus, dass die Betroffenen die Möglichkeit haben, abzulehnen. Im Beschäftigungsverhältnis wird regelmäßig bezweifelt, ob Beschäftigte überhaupt „freiwillig“ einwilligen können. Grundsätzlich steht es der „Freiwilligkeit“ entgegen, wenn sich die Beteiligten nicht „auf Augenhöhe“ gegenüberstehen und damit

[31] Erwägungsgrund Nr. 78 der DSGVO; Gola/*Nolte/Werkmeister*, DSGVO, Art. 25 Rn. 19.

„faktisch ein Machtungleichgewicht besteht“. Ein solches wird regelmäßig bestehen, wenn die Einwilligung für die Ausübung der Arbeitstätigkeit erforderlich ist.

Zudem muss die Einwilligung informiert erfolgen, sodass die Beschäftigten über den Ablauf der Tests im Einzelnen und den Anforderungen der Art. 12 ff. DSGVO entsprechend informiert werden müssen, was jedoch für den Zweck der Untersuchung des IT-Sicherheitsbewusstseins der Beschäftigten nicht förderlich ist. Denkbar bliebe ein einwilligungsbasierter Test bei einer freiwilligen Teilnahme einer interessierten und über die Details aufgeklärten Testgruppe von Beschäftigten, die sich selbst zur Teilnahme anmelden (z.B. besonders IT-affine Beschäftigte). Eine solche Gruppe würde jedoch regelmäßig nicht die für Schärfung des IT-Sicherheits-Bewusstseins erforderliche Breite in der Belegschaft haben. Zudem stünde zu befürchten, dass der Personenkreis nicht angesprochen würde, bei dem ein besonderes hoher Schulungsbedarf zu erwarten ist.

Insgesamt ist damit eine informierte Einwilligung als Rechtsgrundlage für einen Pentest bei KRITIS-Betreibern regelmäßig nicht geeignet.

2. Andere Rechtsvorschrift: Dienst-/Betriebsvereinbarung

Der Datenschutz im Beschäftigungskontext ist im Wege einer Öffnungsklausel der weiteren Ausgestaltung den Mitgliedstaaten in den von Art. 88 DSGVO definierten Bereichen überlassen. Dabei dürfen gem. Art. 88 Abs. 1 i.V.m. EG 155 DSGVO auch Regelungen durch Kollektivvereinbarungen, worunter nach EG 155 auch Dienst-/Betriebsvereinbarungen fallen, zur Verarbeitung von personenbezogenen Beschäftigtendaten getroffen werden. Dies ist durch § 26 Abs. 4 u. 1 BDSG ausgestaltet, wonach Dienst-/Betriebsvereinbarungen als Rechtsgrundlage einer Verarbeitung gelten.

Eine Betriebsvereinbarung ist ein Vertrag zwischen Arbeitgeber und Betriebsrat in einem privatwirtschaftlichen Unternehmen. Im öffentlichen Dienst ist das Pendant eine Dienstvereinbarung. Diese Vereinbarungen bietet gegenüber einer Einwilligung der betroffenen Beschäftigten zahlreiche Vorteile: zunächst muss eine Dienst-/Betriebsvereinbarung nicht individuell mit allen der betroffenen Beschäftigten vereinbart werden, sondern wird über den Personal-/Betriebsrat abgeschlossen. Bei einer Einwilligung besteht die Gefahr, dass das exakte Verständnis der betroffenen Person des Erhebungszwecks potenziell die Reaktionen auf die Tests verfälschen. Bei einer Dienst-/Betriebsvereinbarung muss der Personal-/Betriebsrat vollumfänglich informiert werden. Es genügt jedoch, wenn eine Dienst-/Betriebsvereinbarung in allgemeiner Form bekanntgegeben wird. Die Zweckangabe sollte daher möglichst allgemein erfolgen. Allerdings muss die

Dienstvereinbarung zugleich den an eine Kollektivvereinbarung i.S.d. Art. 88 DSGVO und § 26 BDSG zu stellenden Anforderungen gerecht werden, um eine wirksame Rechtsgrundlage darzustellen.

Zudem ist eine Dienst-/Betriebsvereinbarung nicht nur eine datenschutzrechtliche Rechtsgrundlage, sondern es werden auch die Mitbestimmungsrechte des Personal- bzw. Betriebsrats gewahrt. Weitere Details zur Ausgestaltung einer solchen Vereinbarung finden sich unten, Teil H.

Eine Dienst-/Betriebsvereinbarung muss den Vorgaben des Art. 88 Abs. 2 DSGVO genügen.[32] Es gelten zudem alle allgemeinen gesetzlichen Anforderungen vom Grundsatz der Datensparsamkeit, über den Grundsatz der Transparenz und technische und organisatorische Maßnahmen bis zu den Betroffenenrechten.

VI. Weitere zu beachtende rechtliche Anforderungen

Neben den allgemeinen datenschutzrechtlichen Normen betreffen die beabsichtigten Maßnahmen auch weitere Normen aus angrenzenden Regelungsbereichen.

1. IT-Sicherheitsgesetz nebst zugehöriger Verordnungen

Das „IT-Sicherheitsgesetz“ (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme; IT-SiG) wurde im Juli 2015 verkündet[33] und trat noch im selben Monat in Kraft.

Das IT-SiG soll ausweislich seiner Zielsetzung[34] IT-Systeme „im Hinblick auf die Schutzgüter der IT-Sicherheit (Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität)“ verbessern. Insbesondere den Betreibern von sog. „Kritischen Infrastrukturen“ wird eine besondere „Verantwortung für das Gemeinwohl“ zugeschrieben,[35] weshalb diese durch das IT-SiG zur Einhaltung eines Mindestmaßes von IT-Sicherheit sowie zur Meldung relevanter Vorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI) als „nationale zentrale Stelle für IT-Sicherheit“ verpflichtet werden. Hierzu wurde dem BSI-Gesetz (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik; BSG) durch das IT-SiG mit § 2 Abs. 10 auch eine Definition des Begriffes „Kritische Infrastrukturen“ (KRITIS)

[32] Vgl. hierzu ITS.APT Dokument 2.1, S. 23 f.
[33] BGBl. I 2015, 1324; online verfügbar: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%255B@attr_id=%27bgbl115s1324.pdf%27%255D#__bgbl__%2F%2F*[%40attr_id%3D%27bgbl115s1324.pdf%27]__1453708895167
[34] BT-Drucks. 18/4096, S. 1.
[35] BT-Drucks. 18/4096, S. 2; BT-Drucks. 18/5121, S. 2.

hinzugefügt. Kritische Infrastrukturen sind demnach „Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und“ zudem „von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.“ Während ohnehin die allgemeine Abhängigkeit der Gesellschaft, Wirtschaft, Verwaltung und Gesundheitsversorgung von IT-Systemen zunimmt, ist diese Abhängigkeit im Falle von „Kritischen Infrastrukturen“ sogar existenziell.[36]

Wann genau in den einzelnen Sektoren Betreiber von Anlagen oder Teilen davon „kritische Dienstleistungen“ ausübt, wird im Verordnungswege (Rechtsverordnungen entsprechend der Ermächtigung § 10 Abs. 1 IT-SiG) festgelegt. Diese Festlegung ist in zwei Schritten im April und Juni 2017 in der „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz“ (BSI-Kritisverordnung) erfolgt. Danach ist die Beurteilung, ob es sich bei Anlagen oder Teilen davon um „Kritische Infrastrukturen“ handelt, von branchenspezifischen Schwellenwerten abhängig. Bei Krankenhäusern liegt der Schwellenwert so z.B. bei 30.000 vollstatoinären Fallzahlen pro Jahr. Im Umkehrschluss scheiden damit bereits kleinere Einheiten als „Kritische Infrastruktur“ im Sinne der Normen aus.

Soweit KRITIS-Betreiber seinen Beschäftigten gegenüber als Telekommunikationsdiensteanbieter einzuordnen ist (vgl. Dokument 2.1 – Arbeitsrechtliche Betrachtung), scheidet es mithin im Hinblick auf Telekommunikation bereits aus dem Grund als Betreiber einer kritischen Infrastruktur aus; 500.000 Beschäftigte werden nicht erreicht.

Ein Universitätsklinikum gehört dem Sektor Gesundheit an und hat als Einrichtung der Maximalversorgung regelmäßig einen sehr weiteren Einzugskreis. Einzelne Abteilungen oder Einrichtungen werden dann als „Kritische Infrastrukturen“ einzuordnen sein. Fehler in der IT, die zur Folge hätten, dass eine Versorgung der Patienten an den betroffenen Behandlungsplätzen nicht optimal gewährleistet ist, würden bedeuten, dass die Behandlungsplätze nicht zur Verfügung stehen. Dies würde wiederum zu Versorgungsengpässen führen.

[36] *Roßnagel*, DVBl. 2015, 1206 (1206).

Aus dem IT-SIG ergeben sich für die Erhebung und Verarbeitung von personenbezogenen Daten im Rahmen von IT-Security-Awareness-Tests der Beschäftigten im KRITIS-Betreibers im Ergebnis keine (weiteren) Rechtsgrundlagen oder Besonderheiten.

2. Telekommunikationsgesetz (TKG)

Bei Einsatz der ITS.APT-Methode ist es empfehlenswert, auch etwaige Reaktionen der Beschäftigten bezüglich des Kontakts des IT-Supports/Administrators zu erfassen. Dabei ist es aber wesentlich, dass nicht zu einer unerlaubten Überwachung der Beschäftigten kommt. Dafür sind etwa die Rechtsgrundlagen und Anforderungen des Telekommunikationsgesetzes (TKG) zu beachten. [37] Telekommunikationsdienste sind gemäß § 3 Nr. 24 TKG in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen. Diensteanbieter ist nach § 3 Nr. 6 TKG jeder, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt. Demzufolge betrifft das TKG hauptsächlich die Telekommunikationsinfrastruktur sowie die hierüber erbrachten Telekommunikationsdienstleistungen. Dies kann auch der Arbeitgeber sein, wie bereits im Rahmen der arbeitsrechtlichen Risikobewertung ausgeführt wurde.

Sofern es um die Erhebung der Verkehrsdaten der Telefonanlage geht, kann eine differenzierten Betrachtung erforderlich sein. Diese Frage stellt sich vor allem bei der Testdurchführung im Rahmen von ITS.APT, wenn die Reaktionen der Beschäftigten auf die simulierten IT-Angriffe insoweit gemessen werden, ob und wann die zuständige IT-Abteilung angerufen und um Hilfestellung gebeten wird bzw. wie viele Verbindungsversuche unternommen wurden.

Für den Fall, dass der Arbeitgeber seinen Arbeitnehmern die private Nutzung des Diensttelefons ausdrücklich gestattet, ist der Arbeitgeber als Telekommunikationsdiensteanbieter i. S. d. § 3 Nr. 6 TKG anzusehen.[38] Dies hätte sodann die Folge, dass der Arbeitgeber gemäß § 88 TKG das Fernmeldegeheimnis zu wahren hat. Für ihn gelten dann die Vorschriften aus dem TKG. Insbesondere darf er die Verkehrsdaten der Telefonanlage nur unter den in § 96 TKG genannten Voraussetzungen erheben.

[37] Siehe ITS.APT Dokument 2.1 S. 13ff.
[38] Dazu ITS.APT Dokument D2.1, S. 13f.

Oftmals stellt der Arbeitgeber jedoch neben der dienstlich genutzten Leitung eine weitere Leitung für private Telefongespräche zur Verfügung, in die sich die Beschäftigten mit einer bestimmten Vorwahl einwählen können. In dieser Konstellation ist die private Nutzung der dienstlichen Leitung grundsätzlich untersagt. Die Trennung der dienstlich genutzten Leitung von der privat genutzten Leitung dient in der Regel einer separaten Abrechnung. Die Trennung der Leitungen hat jedoch auch eine jeweils unterschiedliche rechtliche Beurteilung zur Folge. Soweit es um die Nutzung der dienstlichen Leitung geht, die ausschließlich für dienstliche Zwecke genutzt werden darf, ist der Arbeitgeber gemäß den obigen Ausführungen nicht als Telekommunikationsdiensteanbieter i. S. d. § 3 Nr. 6 TKG anzusehen, da die private Nutzung der dienstlichen Leitung ja gerade nicht ausdrücklich erlaubt und damit also verboten ist. Soweit die Beschäftigten jedoch die für private Gespräche zur Verfügung gestellte Leitung nutzen, ist der Arbeitgeber insoweit als Telekommunikationsdiensteanbieter zu qualifizieren. Demzufolge gelten für den Arbeitgeber die Vorschriften aus dem TKG und er hat das Fernmeldegeheimnis zu wahren, soweit es um die Nutzung der privaten Leitung geht.

Anders als bei der privaten E-Mail- und Internetnutzung ist bei der Nutzung einer Telefonanlage mit einer dienstlichen und einer privaten Leitung durchaus eine Trennung möglich. Für die differenzierte Betrachtung lässt sich insbesondere die Begründung des Entwurfs eines Telekommunikationsgesetzes[39] heranziehen. Dort heißt es: „Dem Fernmeldegeheimnis unterliegen damit z. B. Corporate Networks, Nebenstellenanlagen in Hotels und Krankenhäusern, Clubtelefone und Nebenstellenanlagen in Betrieben und Behörden, soweit sie den Beschäftigten zur privaten Nutzung zur Verfügung gestellt sind.“[40] Der Begriff „soweit“ deutet darauf hin, dass in jedem Fall eine Differenzierung zu erfolgen hat. Hätte der Gesetzgeber eine pauschale rechtliche Betrachtung zulassen wollen, so hätte der Satz in der Gesetzesbegründung auch „wenn sie den Beschäftigten zur privaten Nutzung zur Verfügung gestellt sind“ lauten können. Insbesondere heißt es in der Begründung des Gesetzentwurfs der Bunderegierung zur Regelung des Beschäftigtendatenschutzes: „Nach geltender Rechtslage wird ein Arbeitgeber, der seinen Beschäftigten die private Nutzung von dienstlich zur Verfügung gestellten Telekommunikationsdiensten erlaubt, als Diensteanbieter im Sinne von § 3 Nr. 6 TKG angesehen.“[41] Unter dem Ausdruck „von dienstlich zur Verfügung gestellten Telekommunikationsdiensten“ wird die privat genutzte Leitung nicht

[39] BT- Drucksache 13/3609, S. 53.
[40] BT- Drucksache 13/3609, S. 53.
[41] BT-Drucksache 17/4230, S. 43.

erfasst sein. Hier wurde bewusst der Begriff „Telekommunikationsdienste“ gewählt und gerade nicht pauschal auf „Telekommunikationsanlagen“ i. S. v. § 3 Nr. 23 TKG abgestellt. Wäre etwa die Formulierung „von dienstlich zur Verfügung gestellten Telekommunikationsanlagen“ gewählt worden, so wäre eine Differenzierung zwischen privat genutzter und dienstlich genutzter Leitung nicht möglich gewesen, da pauschal auf die Telefonanlage als technische Einrichtung und damit auf alle mit dieser Telekommunikationsanlage einhergehenden Telekommunikationsdienste umfasst wären. Bei einer am Wortlaut orientierten Betrachtung ist damit von der beabsichtigten Verarbeitung der Daten der Telefonanlage im Rahmen des Projekts ITS.APT lediglich die dienstliche Leitung betroffen. Da die private Nutzung dieser dienstlich zur Verfügung Leitung in der Regel untersagt ist, ist der Arbeitgeber insoweit also nicht als Telekommunikationsdiensteanbieter anzusehen. Die Vorschriften des TKG kommen insoweit nicht zur Anwendung.

Für eine Testdurchführung dürfen ausschließlich die Daten der Telefonate verarbeitet werden, die auf der dienstlichen Leitung erfolgen. Dies setzt voraus, dass für die Datenverarbeitung zwischen der dienstlichen und der privaten Leitung technisch differenziert werden kann und die Daten von privaten Telefonaten nicht erfasst werden.

Sofern etwa keine separaten Leitungen der Telefonanlage für jeweils dienstliche und private Gespräche zur Verfügung gestellt werden und die private Nutzung des Diensttelefons ausdrücklich erlaubt ist, so wird der Arbeitgeber seinen Beschäftigten gegenüber als Telekommunikationsdiensteanbieter betrachtet. In diesem Fall der erlaubten Privatnutzung sind auch die einschlägigen Normen des TKG als mögliche Rechtsgrundlagen für den Einsatz eines zukünftigen ITS.APT-Tools in Betracht zu ziehen allerdings auch die Beschränkungen des Telekommunikationsgeheimnisses zu beachten.

Für die Testdurchführung im Rahmen des Projektes hingegen dürfte sich keine Grundlage im TKG finden. § 100 Abs. 1 TKG gestattet, „soweit erforderlich“, die Erhebung und Verwendung von Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen. Diese Norm fokussiert auf den Erhalt der Funktionsfähigkeit der Telekommunikationsanlage selbst. Ein „Fehler“ liegt vor, wenn die Anlage in dem Sinne nicht mehr ordnungsgemäß funktioniert, dass es zu Fehlern bei der Übertragung von Nachrichten kommt.[42] Eine „Störung“ liegt nach der weiten Auslegung des BGH[43] z.B.

[42] BeckTKG/*Braun*, § 100 Rn. 8.
[43] Vgl. BGH Urteil vom 13.01.2011, Az. III ZR 146/11.

bereits vor, wenn „Internetdienstleister bestimmte IP-Adressbereiche eines anderen Internetanbieters sperren, weil von ihnen Schadprogramme oder massenweise sog. Spam-Mails versandt werden oder „Denial-of-Service-Attacken“ ausgehen“.[44] Dieses Sperren sei eine Veränderung der Telekommunikationsanlagen, die sodann nicht mehr nutzbar seien. Es wird mittelbar ein berechtigtes Interesse des Anlagenbetreibers, Spam-Mails von seiner Anlage fernzuhalten, anerkannt.

Aber in jedem Falle muss das Speichern personenbezogener Daten in diesem Zusammenhang dem „Erkennen, Eingrenzen oder Beseitigen“ der Störung oder des Fehlers dienen. Auch wenn nur die Varianten „Eingrenzen“ und „Beseitigen“ klar bereits eine bestehende Störung bzw. einen Fehler voraussetzen,[45] ist doch auch die Variante „Erkennen“ im Zusammenhang mit realen Störungen oder Fehlern zu lesen. Für den hier vorliegenden Fall kann die Norm mithin keine Datenerhebungsgrundlage sein: Die Messung von Nutzerreaktionen auf falsche Spam-Mails – wenn auch mit dem Ziel, sie anschließend zu schulen – ist nicht unmittelbar „erforderlich“ für das Erkennen von Störungen und Fehlern.

Zwar soll es genügen, dass die Datenerhebung und -verwendung geeignet, erforderlich und im engeren Sinn verhältnismäßig ist, um „abstrakten Gefahren für die Funktionstüchtigkeit des Telekommunikationsbetriebs entgegenzuwirken“,[46] d.h. ein konkreter Vorfall bzw. Verdacht wird nicht vorausgesetzt. Aber dennoch wird auf ein Sammeln von „Anhaltspunkten“ zum „Erkennen“ von Fehlern und Störungen abgestellt.[47] Wie ein Beschäftigter auf eine manipulierte Spam-Mail reagiert, steht hiermit nicht in ausreichend engem Zusammenhang. In diesem ersten Schritt – der Datenerfassung – geht es lediglich um die Feststellung der Nutzerreaktion. Dies ist ein dem eigentlichen Normzweck weit vorgelagerter Schritt. Dass eine Nutzerreaktion zu einer Störung bzw. einem Fehler der Telekommunikationsanlage führen könnte, wenn es sich um eine echte Spam-Mail handeln würde (etwa durch fahrlässiges Herunterladen eines Schadprogrammes), kann nicht das gezielte, bis zu sieben Tagen dauernde,[48] „Tracken“ von Beschäftigten gestatten.

3. Telemediengesetz (TMG)

Um zu einer Anwendbarkeit des Telemediengesetzes (TMG) für den Bereich Beschäftigten-E-Mail zu gelangen, müsste es sich bei dem KRITIS-Betreiber zunächst um

[44] BGH Urteil vom 13.01.2011, Az. III ZR 146/11, Rn. 35.
[45] BeckTKG/*Braun*, § 100 Rn. 9.
[46] BGH, Urteil vom 13.01.2011, Az. III ZR 146/11, Rn. 36.
[47] BGH, Urteil vom 13.01.2011, Az. III ZR 146/11, Rn. 39.
[48] Vgl. BGH zur nach § 100 TKG gestatteten Dauer.

eine Stelle handeln, die „Telemedien“ „zur Nutzung bereithält“ bzw. „den Zugang zur Nutzung vermittelt“ (Telemedien-)Diensteanbieter im Sinne des Gesetzes würde (§ 2 Nr. 1 TMG).

Der Anwendungsbereich des TMG ist in § 1 Abs. 1 TMG negativ definiert. Telemedien sind demnach „alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 des Telekommunikationsgesetzes [sind], die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, [sowie] telekommunikationsgestützte Dienste nach § 3 Nr. 25 des Telekommunikationsgesetzes oder Rundfunk nach § 2 des Rundfunkstaatsvertrages“ (§ 1 Abs. 1 S. 1 TMG). Für die Bestimmung eines Dienstes als „Telemedium“ ist mithin nicht die Form der Übertragung – wie wird Zugang gewährt, wie werden die für die Diensterbringung relevanten Daten übermittelt – entscheidend, sondern die für den Dienst erforderlichen Inhalte. Diese müssen elektronisch zur Verfügung gestellt werden.[49] Unerheblich ist, ob der Anbieter diese als eigene Telemedien (Content-Provider) oder bloß Serverkapazitäten für fremde Telemedien zur Verfügung stellt und so diese zur Nutzung bereithält (Host-Provider bzw. Service-Provider).[50] Typische Beispiele für Telemedien sind etwa Suchmaschinen, Informationsdienste, Webmail-Dienste etc.[51] Hinsichtlich des „Diensteanbieters“ unterscheidet § 1 Abs. 1 S. 2 TMG nicht zwischen privaten und öffentlichen Angeboten, bzw. auch nicht zwischen entgeltlichen und unentgeltlichen. Die sich aus dem TMG ergebenden Pflichten sind mithin von privaten, wie öffentlichen Anbietern zu beachten.[52] Der KRITIS-Betreiber könnte daher als Anbieter solcher Dienste betrachtet werden, wenn er z.B. für die Beschäftigten Webmail-Konten führt.

Allerdings ist die Anwendbarkeit des TMG – wie auch die des TKG[53] – im Arbeitgeber-Beschäftigten-Verhältnis umstritten, soweit die (auch) private Nutzung von Internet und dienstlicher E-Mail-Adresse den Beschäftigten gestattet wird. Im Kern geht es um die Frage, ob der Arbeitgeber an das Fernmeldegeheimnis gebunden ist, bzw. dessen einfachgesetzliche Umsetzung, hier § 88 Abs. 2 S. 1 TKG i.V.m. § 7 Abs. 2 S. 3 TMG.[54]

Gegen die Anwendung wird ausgeführt, dass die Beschäftigten dann auch als „Nutzer“ im Sinne des TMG anzusehen sein müssten. Nutzer ist „jede natürliche oder juristische Person,

[49] Spindler/Schuster/*Ricke*, TMG, § 1 Rn. 4.
[50] BeckOK InfoMedienR/*Martini,* TMG, § 2 Rn. 7.
[51] *Brink*, ZD 2015, 295 (296).
[52] Spindler/Schuster/*Ricke,* TMG, § 1 Rn. 14.
[53] Zur Anwendbarkeit des TKG im Arbeitgeber-Arbeitnehmer-Verhältnis vgl. IST.APT Dokument 2.1, S. 12 ff.
[54] *Brink*, ZD 2015, 295 (296).

die Telemedien nutzt, insbesondere um Informationen zu erlangen oder zugänglich zu machen“ (§ 2 Nr. 3 TMG), d.h. wer sich Inhalte ansieht, abruft oder herunterlädt, d.h. die Angebote in irgendeiner Weise nachfragt.[55] Der Beschäftigte, der im Rahmen eines Dienst- oder Arbeitsverhältnisses auf Telemedien zugreift, ist nach einer in der Literatur vorherrschenden Auffassung kein „Nutzer“ im Sinne des Gesetzes, da es bei nur dienstlich gestatteter Nutzung an der Eigenverantwortlichkeit der Nutzung mangelt.[56] Im Falle der Nichtanwendbarkeit des TMG sind die allgemeinen Datenschutzgesetze anzuwenden.

Ist beim KRITIS-Betreiber die private Nutzung untersagt, muss die Frage für das Ergebnis nicht beantwortet werden. Speziell zu den datenschutzrechtlichen Bestimmungen des TMG sei Folgendes ergänzend erwähnt: Der hier zu beurteilenden Sachverhalt weist die Besonderheit auf, dass es um die Anwendbarkeit des TMG – bzw. seiner datenschutzrechtlichen Bestimmungen – im Verhältnis Arbeitgeber-Beschäftigte geht, d.h. der KRITIS-Betreiber in seiner Eigenschaft als Arbeitgeber gegenüber den Beschäftigten. Anders als das TKG enthält das TMG mit § 11 Abs. 1 Nr. 1 eine Norm, die explizit die Bereitstellung von Telemediendiensten im Dienst- und Arbeitsverhältnis regelt. Hiernach gelten die Vorschriften des Abschnittes 4 (Datenschutz) nicht, soweit die Bereitstellung „im Dienst- und Arbeitsverhältnis zu ausschließlich beruflichen oder dienstlichen Zwecken“ erfolgt. Die §§ 14, 15 TMG, Die Voraussetzung der „Ausschließlichkeit“ wird als erfüllt angesehen, wenn der Arbeitgeber dem Arbeitnehmer die private Nutzung des Internets bzw. der dienstlichen E-Mail-Adresse untersagt.[57]

- Für den Einsatz der ITS.APT-Methode kommt eine Einwilligung als Rechtsgrundlage nicht in Betracht.
- Der Einsatz der ITS.APT-Methode ist über eine Betriebs-/Dienstvereinbarung rechtskonform möglich. Diese stellt nicht nur eine Rechtsgrundlage für die Verarbeitung der Daten der Beschäftigten dar, sondern dient auch der Einhaltung der arbeitsrechtlichen Regelungen.
- Weder aus dem TKG noch dem TMG lassen sich Rechtsgrundlagen für die Durchführung des Penetration Testing im Rahmen der ITS.APT-Methode herleiten.

[55] Spindler/Schuster/*Ricke*, TMG, § 2 Rn. 8.
[56] Spindler/Schuster/*Ricke*, TMG, § 2 Rn. 8.
[57] BeckOK InfoMedienR/*Martini*, TMG § 2 Rn. 10.

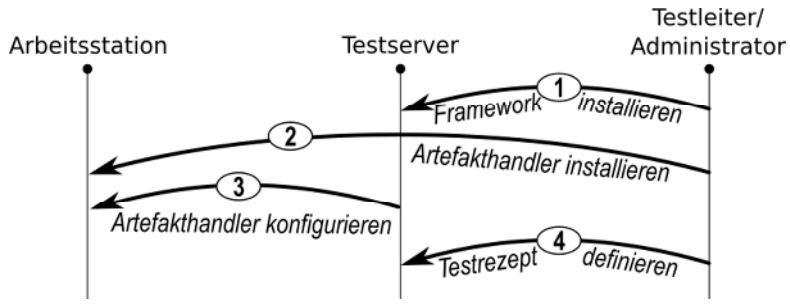
C. Technische Umsetzung

Das zuvor Gesagte muss auch technisch umgesetzt werden. Um dies datenschutzfreundlich zu gestalten, sollten die im Folgenden beschriebenen Schritte eingehalten werden. In diesem Abschnitt wird die Experimentdurchführung im Einzelnen beschrieben.

Der technische Ablauf der ersten und dritten Stufe soll in weitgehend identischer Art und Weise erfolgen, und untergliedert sich jeweils in vier verschiedene Phasen. Hinsichtlich der datenschutzrechtlichen Analyse der hierbei auftretenden Sachverhalte sind dabei die Einzelheiten eben dieser vier Phasen relevant, die im Folgenden genauer aufgeführt werden.

I. Installationsphase

Um die Durchführung der Tests an den Arbeitsplätzen der Probanden in geeigneter Weise vornehmen zu können, müssen deren Computer vor Beginn der ersten Testphase geeignet vorbereitet werden. Konkret erforderlich sind folgende Arbeitsschritte:



1. Das ITS.APE-Framework muss auf dem für die Testdurchführung vorgesehenen Testserver installiert werden. Dies erledigt üblicherweise ein Administrator auf Anweisung des Testleiters. Der Testserver dient dabei sowohl als serverseitige Komponente bei der Einspielung sicherheitsrelevanter Anzeigen bei den Probanden (Einbringung sog. Artefakte), etwa beim Versand von SPAM-Mails, als auch als Sammel- und Protokollierungsstelle für die aufgezeichneten Probandenreaktionen.
2. Auf den Arbeitsplatz-Computern der Probanden wird in diesem Arbeitsschritt der ITS.APT-Client installiert, der zur Steuerung der Anzeige von Artefakten sowie zur Protokollierung und Übertragung der jeweiligen Probandenreaktionen an den Testserver erforderlich ist. Auch dieser Schritt wird von einem Administrator auf Weisung des Testleiters durchgeführt.
3. In diesem optionalen Arbeitsschritt werden die verschiedenen Arbeitsplatz-Computer der Probanden beim Testserver registriert bzw. von diesem vorkonfiguriert, um im späteren Verlauf die notwendige Kommunikation zwischen Testserver und

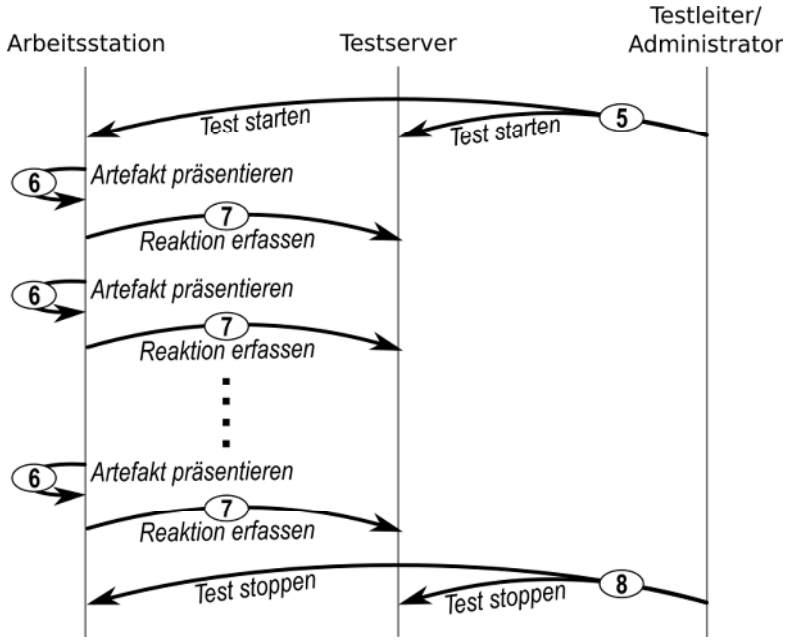
Arbeitsplatz-Computern optimal steuern zu können. Wie in den ersten beiden Arbeitsschritten erfolgt dies durch einen Administrator auf Weisung des Testleiters, sowie teilweise vollautomatisch durch die interne Kommunikation der verschiedenen Komponenten des ITS.APE-Frameworks.

4. Im letzten Arbeitsschritt der Installationsphase definiert der Testleiter auf dem Testserver die durchzuführenden Testläufe (sog. *Testrezept*) hinsichtlich
    a. Vorgesehener Dauer des Testlaufes
    b. Vorgesehener Liste von Probanden für den Testlauf
    c. Vorgesehener Liste von Arbeitsplatz-Computern für den Testlauf
    d. Vorgesehener Typen von Artefakten

Die Arbeitsschritte 1. und 2. sind dabei nur vor der ersten Testdurchführung zu vollziehen. Für den zweiten Testdurchlauf, in Stufe 3, sind nur Arbeitsschritt 4. und ggfs. Arbeitsschritt 3. erneut durchzuführen.

II. Durchführungsphase

In der Durchführungsphase werden die vorab installierten und konfigurierten Artefakte aktiv ausgeführt. Hierbei werden die Probanden unter definierten Umständen mit einem (visuellen, akustischen, o.Ä.) Artefakt konfrontiert, und ihre jeweilige Reaktion darauf wird protokolliert. Im Einzelnen ergeben sich folgende Arbeitsschritte:



5. Das Signal zum Start eines Testlaufes geht auf den Testleiter zurück. Die genaue Abfolge kann hier im Einzelnen abweichen, etwa, wenn das Startsignal an die Arbeitsstationen nicht direkt vom Testleiter sondern vom Testserver weitergeleitet

wird. Auch kann hier eine vorab konfigurierte zeitliche Steuerung den tatsächlichen Startzeitpunkt eines Durchlaufes definieren, dieser ist dann aber vorab vom Testleiter als zuständige (und ggfs. verantwortliche) Position konfiguriert worden. Ab diesem Zeitpunkt läuft der Test.

6. Während des Tests werden – ausgelöst durch zeitliche, arbeitsbedingte oder zufallsbasierte Trigger – die einzelnen im Testrezept definierten und konfigurierten Artefakte ausgeführt. Hierdurch wird jedes Mal (mindestens) ein Proband mit einer dem jeweiligen Artefakt zuzuordnenden Anormalität konfrontiert.
7. Nach Präsentation der jeweiligen Artefakte wird die Reaktion des/der Probanden auf diese Artefakte bestmöglich erhoben und auf dem Testserver protokolliert. Hierzu ist eine Datenübertragung zwischen Arbeitsstation und Testserver erforderlich, die artefaktrelevante Daten enthält, unter anderem:
    a. Datum und Uhrzeit,
    b. Identität der Arbeitsstation,
    c. Informationen über den Probanden (z.B. Benutzername/Pseudonym),
    d. Typ des Artefakts,
    e. auf der Arbeitsstation lokal erfasste Reaktion des Probanden (z.B. Fenster schließen),
    f. Reaktionszeit zwischen Artefaktpräsentation und Reaktion

Je nach Konfiguration der technischen Infrastruktur ist in diesem Schritt unter Umständen auch der Einbezug weiterer relevanter technischer Systeme erforderlich. Beispielsweise kann es erforderlich werden, folgende Zusatzdaten aus Drittsystemen zu erheben und dem Testserver zur Protokollierung zuzuleiten:

a. Identität des Probanden (z.B. aus einem zentralen Benutzerverzeichnis)
b. externe bzw. nicht direkt erfassbare Reaktion des Probanden (z.B. Anruf bei einer Support-Hotline)
c. Identität der Arbeitsstation (z.B. in stark virtualisierten Umgebungen)

Die Arbeitsschritte 6. und 7. werden für jedes Artefakt bzw. für jede Präsentation eines Artefaktes während der Testdauer wiederholt.

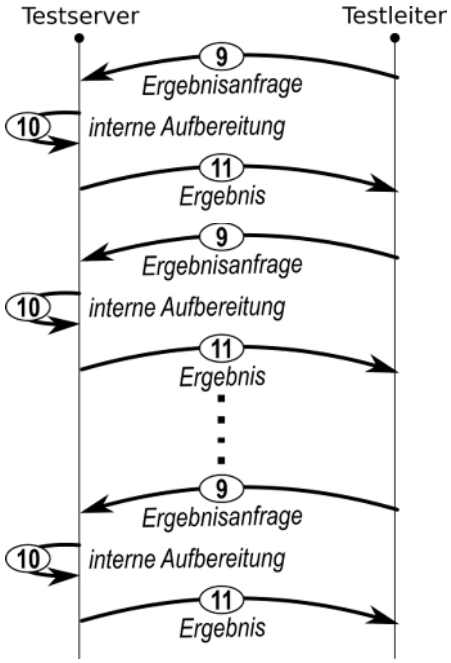
8. Der Testdurchlauf wird in diesem Arbeitsschritt gestoppt. Ein derartiger Stopp kann auf zwei verschiedenen Wegen erfolgen. Entweder erreicht der Testdurchlauf den vorab vom Testleiter definierten Abschlusszeitpunkt, oder der Testleiter unterbricht die Testdurchführung aktiv durch Auswahl der entsprechenden Aktion aus der

Bedienungsoberfläche des Testservers. In beiden Fällen werden die aktuell laufenden Instanzen der Arbeitsschritte 6. und 7. noch vollendet, es werden aber keine weiteren Artefaktpräsentationen mehr gestartet. Das Signal zur Beendigung des Tests kann dabei entweder durch den Testserver an die Arbeitsstationen verteilt werden oder es kann durch den Testleiter bzw. durch Administratoren manuell lokal auf den Arbeitsstationen erfolgen.

Mit Abschluss des 8. Arbeitsschrittes endet die Durchführungsphase.

III. Evaluation durch den KRITIS-Betreiber

Die interne Evaluation bzw. Aufbereitung der gesammelten Reaktionsdaten der Probanden geschieht teilweise während, spätestens aber nach Abschluss der Durchführungsphase. Ziel dieser Phase ist es, gezielt Informationen aus der Aggregation der gesammelten Daten zu gewinnen, etwa in Form statistischer Werte. Hierfür werden wiederholt die folgenden Arbeitsschritte durchgeführt:



9. Ausgelöst durch eine Aktion des Testleiters wird eine Datenanfrage nach bestimmten Datensätzen (oder Operationen auf diesen Datensätzen) an den Testserver übermittelt, auf welchem die gesammelten Reaktionsdaten der Probanden vorliegen. Gegebenenfalls werden hierbei entsprechende Eingabeparameter zur Ermittlung des jeweiligen Ergebnisses übertragen, beispielsweise:
    a. zu betrachtender Zeitraum
    b. zu betrachtende Liste von Probanden

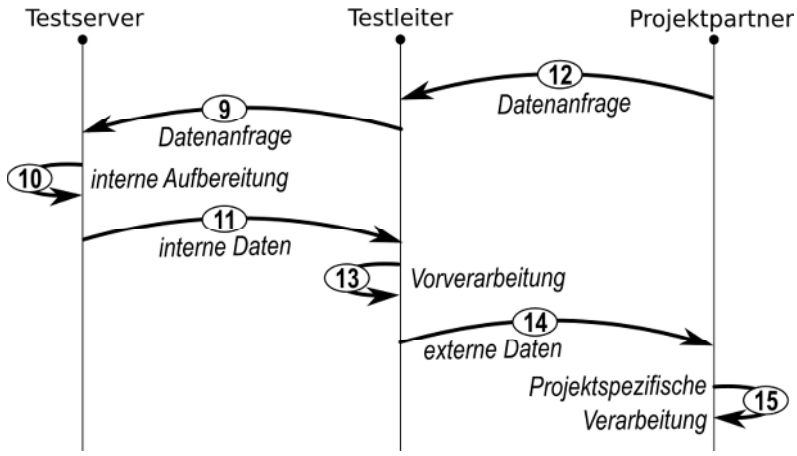
c. zu betrachtende Liste von Arbeitsstationen
d. zu betrachtende Liste von Artefakttypen
e. zu betrachtende Liste von Reaktionstypen

10. Im Rahmen einer programminternen Auswertung werden die angeforderten Daten nach Maßgabe der Parameter aus dem vorigen Arbeitsschritt abgerufen, aufbereitet und für die Rückübertragung vorbereitet, bzw. gemäß der Art der angeforderten Operation vorverarbeitet. Dieser Arbeitsschritt greift dabei auf die vollständige Datenbank mit Probandenreaktionen zu, die im Klartext als Rohdaten vorliegen.
11. Nach Ausführung entsprechender Aggregations- und Aufbereitungsoperationen wird das Ergebnis der Anfrage an den anfragenden Testleiter zurückgegeben bzw. in geeigneter Form (z.B. im Browser) dargestellt.

Die Arbeitsschritte 9. bis 11. werden je nach Bedarf wiederholt durchgeführt. Die so gewonnenen Erkenntnisse können auf Seiten des Testleiters für weitere Verarbeitungsschritte (z.B. für visuelle Aufbereitung) verwendet werden.

IV. Evaluation durch Auftragsverarbeiter

Ausgehend von der Zielstellung der Verwendung der ITS.APT-Methode werden in dieser Phase die Datenbestände aus der Durchführungsphase für die weitere Verwendung im Projektkontext bereitgestellt. Hierbei ist relevant, dass durch den KRITIS-Betreiber stets eine Vorabkontrolle der zu übermittelnden Daten erfolgt, da hier ggfs. eine organisatorische Domäne (Einflussbereich des KRITIS-Betreiber) verlassen wird. Im Einzelnen erfolgen hierbei folgende Arbeitsschritte:



12. Ausgehend von den für die Erzielung des Projektergebnisses erforderlichen Informationen werden durch die Projektpartner Anfragen zu bestimmten Daten über die Probandenreaktionen definiert und an den Testleiters beim KRITIS-Betreiber . Der

Testleiter nutzt dann die in Arbeitsschritt 9. bis 11. bestehenden Möglichkeiten zur Betreiber-internen Evaluation, um die zur Beantwortung der Anfragen erforderlichen Datenbestände und Informationen zusammenzutragen. Hierfür ist ggfs. eine mehrfache Durchführung der besagten Arbeitsschritte erforderlich.

13. Hat der Testleiter sämtliche erforderlichen Daten zur Beantwortung der spezifischen Projektanfrage zusammengetragen, ist gegebenenfalls eine Betreiber-interne Vorverarbeitung dieser Daten erforderlich. Dies kann etwa notwendig werden, um
    a. Personenbezug aus den Daten zu entfernen,
    b. Daten anderweitig zu anonymisieren oder zu pseudonymisieren,
    c. Daten mittels weiterer Informationsquellen zu verifizieren,
    d. Statistische Operationen auf gesammelten Eingabedaten durchzuführen,
    e. relevante Begleitinformationen zu den Daten und ihrem Erhebungskontext zu identifizieren und dem Anfrageergebnis entsprechend beizufügen

14. Nach entsprechender Vorverarbeitung werden die Ergebnisse zur Anfrage an die entsprechenden Projektpartner übermittelt. Hierbei verlassen sie die Einflussdomäne des KRITIS-Betreibers.
15. Nach Überstellung der Anfrageergebnisse an den anfragenden Projektpartner erfolgt dort die weitere Auswertung nach Maßgabe des Projektplans.

D. Gewährleistung der Betroffenenrechte

Die datenschutzrechtlichen Betroffenenrechte sind bei jeder automatisierten Verarbeitung personenbezogener Daten zu gewährleisten. Im Einzelnen handelt es sich um Information, Auskunft, Berichtigung, Löschung, sowie Einschränkung und Widerspruch. Auch das Recht auf Schadenersatz ist grundsätzlich. ein Betroffenenrecht. Letzteres wird ausführlich in unten, in Teil J behandelt.

I. Anspruchsgegner

Die Betroffenenrechte bestehen gegenüber der verantwortlichen Stelle (Verantwortlicher, Art. 4 Nr. 7 DSGVO). Dies ist hier der KRITIS-Betreiber. Bei der Umsetzung der ITS.APT-Methode ändert sich dies auch nicht, wenn ein IT-Dienstleisters mit der Durchführung der Tests beauftragt wird. Wie bereits oben erläutert, ist dieser als Auftragsverarbeiter tätig und daher nicht die verantwortliche Stelle. Zudem ist zu beachten, dass bei korrekter Umsetzung

der ITS.APT-Methode dem Auftragsverarbeiter lediglich pseudonymisierte Daten der Beschäftigten vorliegen.

II. Information, Art. 13 u. 14 DSGVO

Bei Erhebung personenbezogener Daten bei den betroffenen Personen sind diese nach Art. 13 DSGVO insbesondere über folgende Umstände der Datenverarbeitung aufzuklären: die datenverarbeitende Stelle, die Zwecke der Datenverarbeitung sowie die Rechtsgrundlage, die Dauer der Verarbeitung, die Rechte der betroffenen Person sowie den Empfängerkreis bei beabsichtigten Übermittlungen.

Sofern die Datenerhebung nicht bei der der betroffenen Person erfolgt, so erteilt der Verantwortliche ihr die gleichen Informationen wie nach Art. 13 DSGVO. Allerdings gilt dies gem. Art. 14 Abs. 5 DSGVO nicht, soweit die betroffene Person bereits über die Informationen verfügt, die Erteilung unmöglich ist oder einen unverhältnismäßigen Aufwand erfordert, die Erlangung oder Offenlegung durch andere Rechtsvorschriften ausdrücklich geregelt ist oder die personenbezogenen Daten dem Berufsgeheimnis unterliegen.

Dabei besteht die Gefahr, dass das exakte Verständnis der betroffenen Person des Erhebungszwecks aber potenziell die Reaktionen auf die Tests verfälschen.[58] Die Zweckangabe sollte daher möglichst allgemein erfolgen. Dies ist bei einer Dienstvereinbarung teilweise möglich. Eine solche muss zugleich die an eine Kollektivvereinbarung i.S.d. Art. 88 DSGVO und § 26 BDSG zu stellenden Anforderungen gerecht werden, um eine wirksame Rechtsgrundlage darzustellen. Im Ergebnis bedeutet dies, dass alle Angaben, die im Rahmen der Aufklärungspflicht zu machen sind (und weitere), in der Dienstvereinbarung enthalten sein werden, s. dazu auch unten, Teil H.

Vorliegend werden die Betroffenen im Rahmen der arbeitsrechtlichen Publizitätspflicht Kenntnis vom Inhalt der Dienstvereinbarung, welche die Datenerhebung regeln wird, nehmen können und somit die Möglichkeit haben, sich über alle gesetzlich maßgeblichen Aspekte zu informieren. Zum Beispiel kann der KRITIS-Betreiber Dienst-oder Betriebsvereinbarungen im Intranet bereitstellen und die Beschäftigten mithin mit einem an sie adressierten, verschlossenen Brief oder mittels einer E-Mail an ihre dienstlichen E-Mail-Adressen, die jeweils die Dienstvereinbarung oder die relevanten Auszüge enthalten, informieren.

[58] Vgl. ITS.APT Dokument 2.1.

III. Auskunft, Art. 15 DSGVO

Es besteht ein Recht der betroffenen Personen auf Auskunft gegenüber der datenverarbeitenden Stelle. Nach Art. 15 DSGVO umfasst der Auskunftsanspruch folgende Informationen: die Zwecke der Verarbeitung, die Kategorien der verarbeiteteten Daten, die Empfänger von Übermittlungen, die Dauer der Speicherung, das Bestehen eines Rechts auf Berichtigung oder Löschung/Einschränkung, das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde sowie die Herkunft der Daten, wenn diese nicht bei der betroffenen Person erhoben wurden.

Die Auskunft ist auf Antrag zu erteilen, d.h. im Unterschied zu Art. 13 und 14 DSGVO sind es hier die betroffenen Personen, die aktiv auf die datenverarbeitende Stelle zukommen müssen, bzw. dürfen, um die Informationen zu erhalten. Es gibt gesetzlich keine formalen Anforderungen für die Antragstellung oder die Auskunftserteilung, d.h. beides wäre grundsätzlich mündlich oder per E-Mail möglich, soweit letztere vor Einsicht Dritter geschützt ist.

Ziel dieser Regelung – wie auch der Informationspflicht – ist es, Transparenz herzustellen. Die betroffenen Personen sollen in die Lage versetzt werden, zu wissen, was ihre Kommunikationspartner über sie wissen und zu welchen Zwecken die Daten verwendet werden sollen. Gleichzeitig soll auch die Rechtsdurchsetzung ermöglicht werden; d.h. es geht um die Möglichkeit effektiv von seinen Rechten Gebrauch machen zu können.

IV. Widerspruch, Art. 21 DSGVO

Nach Art. 21 DSGVO haben die betroffenen Personen das Recht aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit Widerspruch gegen die Verarbeitung ihrer Daten allgemein oder gegen bestimmte Formen der Verarbeitung zu erheben. Dieses Recht bezieht sich vom Wortlaut her nur auf Verarbeitungen nach Art. 6 Abs. 1 lit. e und lit. f DSGVO, also Verarbeitungen zur Wahrnehmung einer öffentlichen Aufgabe oder zur Wahrung berechtigter Interessen. Dennoch sollte eine Im Falle eines Widerspruchs, ist gem. Art. 21 Abs. 1 DSGVO eine Abwägung vorzunehmen: Der Verantwortliche beendet die Verarbeitung, soweit er keine zwingenden schutzwürdigen Gründe für die Verarbeitung nachweisen kann, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, Art. 21 Abs. 1 S 2 DSGVO. Üblicherweise sollten – unter Berücksichtigung der grundsätzlichen Wertung, dass keine Person gegen oder ohne ihren Willen zum Testobjekt gemacht werden soll – die Daten der betroffenen Person gelöscht werden.

V. Berichtigung, Löschung und Einschränkung, Art. 16-18 DSGVO

Die Betroffenen haben schließlich das Recht die Berichtigung, Löschung oder Einschränkung der Verarbeitung ihrer personenbezogenen Daten zu verlangen. Soweit Daten unrichtig sind, besteht ein Recht auf Berichtigung (Art. 16 DSGVO).

Der Anspruch auf Löschung besteht gem. Art. 17 Abs. 1 DSGVO, wenn die Daten für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind, die betroffene Person Widerspruch eingelegt hat und dieser gegenüber dem Interesse der verantwortlichen Stelle überwiegt, die Daten unrechtmäßig verarbeitet wurden oder eine anderweitige Rechtsvorschrift dazu verpflichtet. „Löschen“ bedeutet, dass es unmöglich ist, die in den Daten gespeicherten Informationen wahrzunehmen.

Bei Einsatz der ITS.APT-Methode werden die Rohdaten bzw. die an den IT-Dienstleister herausgegebenen pseudonymisierten Daten mit Abschluss der Tests nicht mehr erforderlich in diesem Sinne sein und sind daher ohnehin zu löschen. Zu diesem Zeitpunkt können die Messergebnisse nur noch in anonymisierte Statistiken überführt werden. Für eine Dokumentation der Tests ist dies ausreichend, sodass es der personenbezogenen Daten der teilnehmenden Beschäftigten nicht mehr bedarf. Dementsprechend muss in der Dienst-/Betriebsvereinbarung die Löschung aller personenbezogenen Daten spätestens zum Ende der Tests festgeschrieben sein.

An die Stelle des Rechts auf Löschung kann das Recht auf Einschränkung der Verarbeitung treten. Dies bedeutet das gem. Art. 4 Nr. 3 DSGVO, dass die Daten mit dem Ziel markiert werden, dass ihre künftige Verarbeitung eingeschränkt wird.

Art. 18 Abs. 1 DSGVO zählt die Fälle auf, in denen die Verarbeitung personenbezogener Daten (nur) einzuschränken ist. Von Relevanz im hiesigen Zusammenhang könnte der Fall sein, dass die Richtigkeit der Daten von der betroffenen Person bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit nachweisen lässt (lit. a) , dass die betroffene Person bei unrechtmäßiger Verarbeitung anstelle der Löschung die Sperrung verlangt (lit. b). Ebenso kommt die Einschränkung statt Löschung in Betracht, wenn die betroffenen Personen durch die Löschung in der Verfolgung ihrer Rechte oder in sonstigen schutzwürdigen Belangen beeinträchtigen würde (lit. c). Zudem ist die Verarbeitung der Daten eingeschränkt, wenn eine betroffene Person Widerspruch i.S.v. Art. 21 DSGVO eingelegt hat und die Abwägung (siehe oben) noch nicht erfolgt ist.

Eine Einschränkung bedeutet ein „relatives Nutzungsverbot“; abgesehen von Ausnahmen gem. Art. 18 Abs. 2 DSGVO bezüglich der Speicherung der Daten oder der Verarbeitung mit Einwilligung, zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen, zum Schutz anderer natürlicher oder juristischer Personen oder aufgrund eines wichtigen öffentlichen Interesses der EU oder eines Mitgliedstaates, ist keine Verarbeitung der Daten gestattet.

Sollte es zu einer Berichtigung, Einschränkung oder Löschung wegen Unzulässigkeit der Verarbeitung (beim Einsatz der ITS.APT-Methode: Einwand eines Probanden) von Daten beim KRITIS-Betreiber kommen, muss dieser im Falle der Durchführung durch einen IT-Dienstleister, der die Daten pseudonymisiert erhalten hat, unverzüglich hiervon – unter Wahrung der Pseudonymität – unterrichten.

E. Datenschutzverletzungen

Sollte es zu einer Verletzung des Schutzes personenbezogener Daten kommen, so ist diese gem. Art. 33 Abs. 1 und 5 DSGVO von der verantwortlichen Stelle zu dokumentieren und unverzüglich an die Aufsichtsbehörde zu melden, wenn ein Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Ist diese Risiko als hoch einzustufen, müssen gem. Art. 34 DSGVO auch die betroffenen Personen benachrichtigt werden. Unterbleibt eine solche Meldung oder die Benachrichtigung, obwohl sie erforderlich gewesen wäre oder erfolgt sie zu spät, so kann dies gem. Art. 83 Abs. 4 lit. a DSGVO mit einem Bußgeld von bis zu 10.000.000 € oder 2% des gesamten weltweilten Jahresumsatzes geahndet werden.

Eine Datenschutzverletzung liegt gem. Art. 4 Nr. 12 DSGVO vor, wenn die Sicherheit der Daten, beabsichtigt oder unbeabsichtigt, verletzt wird und dies zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die verarbeitet werden. Umfasst sind somit Vertraulichkeits-, Verfügbarkeits- und Integritätsverletzungen. Die verdeutlicht die Nähe der Vorschrift zu denen über IT-Sicherheitsvorfälle: alle Datenschutzverletzungen sind auch IT-Sicherheitsverletzungen. Anderseherum sind alle IT-Sicherheitsverletzungen, die personenbezogene Daten betreffen, Datenschutzverletzungen. Es werden sämtliche Formen der Verarbeitung von personenbezogenen Daten im Sinne von Art. 4 Nr. 2 DSGVO erfasst. Es ist zudem unerheblich welche Arten oder Kategorien von personenbezogenen Daten verarbeitet werden, es genügt, wenn im Sinne von Art. 4 Nr. 1 DSGVO eine natürliche Person aufgrund der betroffenen Daten identifiziert oder identifizierbar wird.

Für Auftragsverarbeiter gilt gem. Art. 33 Abs. 2, dass sie eine Datenschutzverletzung dem Verantwortlichen stets unverzüglich melden müssen. Dabei gelten keine Ausnahmen. Auch der Auftragsverarbeiter unterliegt dabei einem Haftungs- und Regressanspruch nach Art. 82 DSGVO und kann gem. Art. 84 Abs. 4 DSGVO mit einem Bußgeld belegt werden.

Die verantwortliche Stelle muss neben der Dokumentation der Datenschutzverletzung, die gem. Art. 33 Abs.5 DSGVO stets vorzunehmen ist, auch eine Risikobeurteilung vornehmen. Dabei sind die Risiken für die Rechte und Freiheiten natürlicher Personen, insbesondere der durch die Datenschutzverletzung betroffenen Personen, zu betrachten. Eine solche Darstellung und Beurteilung ist als Teil einer Datenschutz-Folgenabschätzung, die vor dem Einsatz der hier dargestellten Methode durchgeführt werden muss, bereits vorzunehmen. Es kann folglich auf deren Ergebnisse zurückgegriffen werden. Im Übrigen ist aufgrund des besonderen Kontextes der Verarbeitung im Rahmen eines Beschäftigungsverhältnisses davon auszugehen, dass jedenfalls eine Meldung an die Aufsichtsbehörde bei jeglicher Art von Datenschutzverletzung erforderlich ist.

F. Übermittlung von Daten an Drittländer

Bei der Durchführung der Tests durch einen externen IT-Sicherheitsdienstleister ist zu beachten, dass für eine Übertragung personenbezogener Daten in Drittländer die besonderen Anforderungen des Kapitels V DSGVO gelten. Danach sind gem. Art. 44 DSGVO neben den generellen Vorschriften besondere Anforderungen einzuhalten, um sicherzustellen, dass das Schutzniveau bezüglich personenbezogener Daten aus der EU auch erhalten bleibt, wenn diese Daten außerhalb der EU übertragen und verarbeitet werden. Zunächst ist neben einer Rechtsgrundlage für die Verarbeitung an sich, eine Rechtsgrundlage für die Übermittlung notwendig. Dabei kann es sich um einen Angemessenheitsbeschluss der Kommission gem. Art. 45 DSGVO oder geeigneter Garantien i.S.v. Art. 46 DSGVO handeln. Unter letztere Kategorie fallen insbesondere Standdarddatenschutzklauseln und verbindliche interne Datenschutzvorschriften nach Art. 47 DSGVO. Es ist jedoch zu beachten, dass der EuGH im Urteil zur Rechtssache *Schrems*[59], den Angemessenheitsbeschluss der Kommission zur Übermittlung von personenbezogenen Daten in die Vereinigten Staaten von Amerika für nichtig erklärt hat und sich die Kritikpunkte aufgrund der Verbindung mit Art. 8 GrCh auch für andere Instrumente der Übermittlung in Drittländer, wie die Standarddatenschutzklauseln und verbindliche interne Datenschutzvorschriften, übertragen lassen. Auch die Artikel-29-

[59] EuGH, Urteil Schrems, C-362/14, ECLI: EU:C:2015:650.

Datenschutzgruppe hat in ihrem Bericht zum aktuellen Angemessenheitsbeschluss der Kommission zur Übermittlung in die Vereinigten Staaten von Amerika, dem sog. EU US Privacy Shield, schwerwiegende Bedenken geltend gemacht und sich vorbehalten, ein Verfahren vor dem EuGH anzustoßen.[60] Weiterhin sind gegenwärtig verschiedene Verfahren vor dem EuGH zur Frage der Übermittlung personenbezogener Daten in Drittländer anhängig.[61] Es ist daher stets in jedem Einzelfall gesondert zu prüfen, ob den in der Rechtsprechung des EuGH formulierten ausreichend Rechnung getragen wurde.[62]

G. Übertragbarkeit auf andere Szenarien

Im Folgenden soll abschließend kurz auf die Übertragbarkeit der rechtlichen Erwägungen zur Testdurchführung auf andere Szenarien eingegangen werden. Wenn diese Handlungsempfehlungen beachtet werden und sichergestellt wird, dass über die Artefakte keine internen personenbezogenen Daten abgefragt werden, lässt sich die ITS.APT-Methode auf sämtliche öffentliche und nichtöffentliche Stellen übertragen. In jedem dieser Fälle sind unbedingt die Rechte und Interessen der Beschäftigten zu wahren und zu gewährleisten, dass eine Rechtsgrundlage für die Datenverarbeitung gegeben ist, was durch die in diesem Dokument beschriebenen Maßnahmen sichergestellt werden kann.

H. Gestaltung einer Betriebs-/Dienstvereinbarung

Literaturhinweise: Beckschulze, Internet-, Intranet- und E-Mail-Einsatz am Arbeitsplatz – Rechte der Beteiligten und Rechtsfolgen bei Pflichtverletzungen, DB 2003, 2777; Benkert, Neuer Anlauf des Gesetzgebers beim Beschäftigtendatenschutz, NJW-Spezial 2017, 242; Decker/Deckers, Die Beteiligungsrechte des Betriebsrats beim Testkauf, NZA 2004, 139; Düwell/Brink, Beschäftigtendatenschutz nach der Umsetzung der Datenschutz-Grundverordnung: Viele Änderungen und wenig Neues, NZA 2017, 1081; Ernst, Der Arbeitgeber, die E-Mail und das Internet, NZA 2002, 585; Gebhardt/Umnuß, Anonymisierung als Weg aus der Mitbestimmung bei elektronischer Datenverarbeitung gemäß § 87 I Nr. 6 BetrVG?, NZA 2995, 103; Kort, Die Zukunft des deutschen Beschäftigtendatenschutzes – Erfüllung der Vorgaben der DS-GVO, ZD 2016, 555;

[60] Vgl. Artikel-29-Datenschutzgruppe Mitteilung für die Presse, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/Art29%20PM%20Privacy%20Shield%20EN.pdf;jsessionid=E1B85541C52DA2A2F56D6964621CD135.1_cid329?__blob=publicationFile&v=2.
[61] EuGH, Rs. Digital Rights Ireland/Kommission, T-670/16; Rs. La Quadrature du Net/Kommission, T-738/16.
[62] EuGH, Urteil Schrems, C-362/14, ECLI: EU:C:2015:650, insb. Rn. 68-103.

Lindemann/Simon, Betriebsvereinbarungen zur E-Mail-, Internet- und Intranet-Nutzung, BB 2001, 1950; Linsemaier, Normsetzung der Betriebsparteien und Individualrechte der Arbeitnehmer, RdA 2008, 1; Maschmann, Compliance versus Datenschutz, NZA-Beilage 2012, 50; Müllner, Verhalten und Leistung gemäß § 87 Abs. 1 Nr. 6 BetrVG, DB 1984, 1677; Raab, Betriebliche und außerbetriebliche Bildungsmaßnahmen, NZA 2008, 270; Thüsing, Verbesserungsbedarf beim Beschäftigtendatenschutz, NZA 2011, 16; Wybitul, Betriebsvereinbarungen und § 32 BDSG: Wie geht es nach der DS-GVO weiter?, ZD 2015, 559; Wybitul, E-Mail-Auswertung in der betrieblichen Praxis – Handlungsempfehlungen für Unternehmen, NJW 2014, 3605.

Wie vorstehend erläutert, eignet sich eine Dienst- oder Betriebsvereinbarung als datenschutzrechtliche Erlaubnisnorm bei der Umsetzung der ITS.APT-Methode. Eine solche Vereinbarung empfiehlt sich aber nicht nur aus diesem Grund, denn mit ihrer Hilfe lassen sich auch effektiv die Informations- und Mitbestimmungsrechte der Betriebs- bzw. Personalräte wahren. Die Rechte der Betriebsräte ergeben sich dabei aus dem Betriebsverfassungsgesetz, die der Personalräte richten sich abhängig von der Art der Stelle nach dem Bundespersonalvertretungsgesetz oder den jeweiligen Personalvertretungsgesetzen der Länder. So bestehen für den Betriebsrat Mitbestimmungsrechte hinsichtlich der Einführung und Ausgestaltung der Tests (§§ 87 Abs. 1 Nr. 6, 94 Abs. 2 Hs. 2 BetrVG), sowie hinsichtlich der Gestaltung der Personalfragebögen und der Schulungen (§§ 94 Abs. 1 S. 1, 98 Abs. 1 BetrVG). Um diese Mitbestimmungsrechte auch ordnungsgemäß wahrnehmen zu können, ist der Betriebsrat über die beabsichtigten Maßnahmen umfassend und fortlaufend zu unterrichten (§ 80 Abs. 2 BetrVG). Darüber hinaus hat der Betriebsrat ein Beratungsrecht bezüglich der Schulungen (§ 97 Abs. 1 BetrVG) und ein Recht bestimmte Arbeitnehmer für diese vorzuschlagen (§ 98 Abs. 3 BetrVG). Diese Rechte finden sich für die Personalvertretungen öffentlicher Stellen im Wesentlichen inhaltsgleich in den jeweiligen Landesgesetzen wieder. Um die Mitbestimmungsrechte zu wahren, würde zwar bereits eine formlose Absprache ausreichen. Allerdings ist eine schriftliche Fixierung der Absprachen in Form einer Betriebs-/Dienstvereinbarung rechtssicherer.

Zur Übersicht der Rechte der Betriebsvertretungen:

MITBESTIMMUNG	**Tests** (vor der Schulung)	**§ 87 I Nr. 6 BetrVG**: Mitbestimmung hinsichtlich der Einführung und Anwendung technischer Einrichtungen zur Überwachung des Verhaltens **§ 94 II 2. Hs. BetrVG**: Mitbestimmung hinsichtlich der inhaltlichen Ausgestaltung allgemeiner Beurteilungsgrundsätze, die in die Konstruktion der Tests einfließen
	Personal-fragebögen	**§ 94 I 1 BetrVG**: Mitbestimmung hinsichtlich der inhaltlichen Ausgestaltung von Fragebögen
	Schulungen	**§ 98 I BetrVG:** Mitbestimmung hinsichtlich der inhaltlichen Ausgestaltung von Maßnahmen der betrieblichen Berufsbildung
	Tests (nach der Schulung)	**§ 87 I Nr. 6 BetrVG:** (s.o.)
INFORMATION	**Tests** (vor der Schulung)	**§ 80 Abs. 2 BetrVG**: Rechtzeitige und umfassende Unterrichtung, damit ihm die Durchführung seiner Aufgaben möglich ist
	Personal-fragebögen	
	Schulungen	
	Tests (nach der Schulung)	

BERATUNG/VORSCHLAG	**Schulungen**	**§ 97 Abs. 1 BetrVG:** Beratungsrecht hinsichtlich der Durchführung von betrieblichen Berufsbildungsmaßnahmen **§ 98 Abs. 3 BetrVG**: Vorschlagsrecht hinsichtlich der Teilnahme bestimmter Arbeitnehmer an den Schulungen

Im Folgenden soll exemplarisch dargestellt werden, welche inhaltlichen Anforderungen an eine Betriebs- oder Personalvereinbarung zu stellen sind.

Die Betriebs-/Dienstvereinbarung sollte inhaltlich klar formuliert sein und alle wesentlichen Phasen der Testdurchführung erfassen. Neben dem Test an sich muss daher auch eine eventuelle Schulung sowie die Datenerhebung und deren Auswertung geregelt werden. Folgende Punkte sind dabei schwerpunktmäßig zu beachten:

Zunächst sind die Bewertungskriterien ausdrücklich zu benennen, anhand derer bestimmt werden soll, ob das Verhalten der Testperson für einen potentiellen Angreifer förderlich oder hinderlich wäre.

Des Weiteren empfiehlt es sich, allgemeine Grundsätze der Datenverarbeitung sowie des Persönlichkeitsschutzes aufzustellen. In dem Zusammenhang ist darauf einzugehen, welche Daten erhoben bzw. nicht erhoben werden. Insbesondere sollte darauf hingewiesen werden, dass die Gestaltung des Testszenarios keine Rückschlüsse auf private Belange oder Interessen

der Testpersonen zulässt und die Ergebnisse der Tests nicht zur Leistungs- oder Verhaltenskontrolle genutzt werden. Die DSGVO und das BDSG sehen zudem vor, dass personenbezogene Daten nicht anlasslos erhoben und verarbeitet werden dürfen. Dementsprechend ist der Zweck der Datenverarbeitung anzugeben, der vorliegend in der Durchführung der Tests liegt.

Im Weiteren sollte möglichst detailliert geregelt werden, welche Daten auf welche Art und Weise erfasst werden. Beispielsweise ist anzugeben, welche konkreten Informationen, wie Name oder Alter des Getesteten, erhoben werden und ob diese Daten kumuliert werden. Zudem muss geregelt werden, ob und unter welchen Umständen die Daten pseudonymisiert oder anonymisiert werden. Außerdem ist in der Vereinbarung festzulegen, durch wen die Daten verarbeitet werden, welche technischen Sicherheitsvorkehrungen getroffen werden und wie lange die Daten gespeichert werden. Schließlich ist auf die Rechte der Betroffenen, der Mitarbeitervertretung sowie eines eventuell vorhandenen Datenschutzbeauftragten einzugehen.

Im Annex I wird ein Muster einer solchen Betriebs-/Dienstvereinbarung zur Implementierung der ITS.APT-Lösung in die Praxis zur Verfügung gestellt. Diese Mustervereinbarung umfasst alle zu regelnden Aspekte, um eine Mitarbeiter-Testung durchzuführen und enthält u.a. Formulierungsvorschläge zu den oben genannten Anforderungen.

- Die Betriebs-/Dienstvereinbarung kann nicht nur als datenschutzrechtliche Erlaubnisnorm fungieren, sondern auch als Instrument zur Wahrung der Rechte der Personalvertretung eingesetzt werden.
- Sie muss die Testmethode, den Testablauf und die Art und Weise der Datenerhebung und Verarbeitung detailliert beschreiben.
- Durch die Gestaltung der Betriebs-/Dienstvereinbarung ist sicherzustellen, dass eine Leistungs- oder Verhaltenskontrolle der Beschäftigten ausgeschlossen wird.

I. Erstellen eines Verfahrensverzeichnisses und Durchführung einer Datenschutz-Folgenabschätzung

Die verantwortliche Stelle führt gemäß Art. 30 DSGVO ein Verfahrensverzeichnis. Dieses dient der Information der Betroffenen und der zuständigen Aufsichtsbehörde. Es ist von der verantwortlichen Stelle selbst zu erstellen und dient der Herstellung von Transparenz gegenüber den Betroffenen sowie zur besseren Überwachbarkeit der Datenverarbeitung, auch durch die zuständige Datenschutzaufsichtsbehörde. Da das Verzeichnis auch der Information der Betroffenen dient, sollte es möglichst zugänglich und verständlich formuliert sein.

Weiterhin ist das Verzeichnis eine wichtige Grundlage für eine Datenschutz-Folgenabschätzung gemäß Art. 35 Datenschutz-Grundverordnung, die für Verarbeitungstätigkeiten, die ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben, verpflichtend durchzuführen ist. Auch für die Durchführung eines Tests des IT-Sicherheitsbewusstseins unterstützt sie die verantwortliche Stelle bei deren Durchführung, da durch ein solches Verzeichnis und eine Datenschutz-Folgenabschätzung sichergestellt wir, dass die Datenflüsse und Verantwortlichkeiten innerhalb der Organisation festgelegt, Ansprechpartner verfügbar und die datenschutzrechtlichen Anforderungen umgesetzt sind.

Aufgrund der beratenden Funktion des Datenschutzbeauftragten sollte dieser frühzeitig in die Erstellung einbezogen werden.

Das Verfahrensverzeichnis enthält folgende Angaben:

- Den Namen und Kontaktdaten der verantwortlichen Stelle sowie des Datenschutzbeauftragten, soweit ein solcher bestellt ist.
- Eine Beschreibung der Zwecke und Rechtsgrundlagen der Datenverarbeitung. Dabei sollten der Sinn der Durchführung des Tests und der Ablauf beschrieben werden. Als Rechtsgrundlage sollte auf eine Betriebs-/Dienstvereinbarung zurückgegriffen werden, auf die an dieser Stelle verwiesen werden kann.
- Den Kreis der Betroffenen oder Betroffenengruppen. Dabei handelt es sich um die vorausgewählten Teilnehmer*innen des Tests, wie sie bereits in der Dienstvereinbarung festgelegt sind. Es sollten die ungefähre Anzahl der Betroffenen sowie die einzelnen Bereich/Dezernate/Abteilungen benannt werden.

- Die Kategorien personenbezogener Daten. Dabei ist zwischen den einzelnen Phasen des Tests, wie etwa dem Versand der Phishing-Mails, den Schulungen und der späteren Evaluation zu unterscheiden. Es sollte zudem vermerkt werden, wenn besondere Kategorien von Daten im Sinne von Art. 9 Datenschutz-Grundverordnung verarbeitet werden.
- Die Löschungs- und Aufbewahrungsfristen. Diese ergeben sich aus der Dienstvereinbarung. Die Daten sollten spätestens nach Abschluss der Tests und Evaluation gelöscht werden.
- Die Empfänger von Daten, sowohl innerhalb der verantwortlichen Stelle, als auch außerhalb. Dabei sollten die Datenflüsse genau dargestellt werden und die Verantwortlichkeiten klar definiert sein.
- Die Empfänger von Daten in einem Drittland oder eine Internationale Organisation, soweit eine solche Übertragung vorgesehen ist. Dieses wird in den meisten Fällen nicht notwendig sein und sollte daher, mit Rücksicht auf die Risiken eines solchen Transfers, nicht umgesetzt werden.
- Eine Beschreibung der technischen und organisatorischen Maßnahmen, um die Sicherheit der Verarbeitung gemäß Art. 32 Datenschutz-Grundverordnung sicherzustellen. Dabei empfiehlt sich eine Aufgliederung der einzelnen Maßnahmen nach den Schutzzielen des Standard-Datenschutz-Modells der Aufsichtsbehörden von Bund und Ländern.[63] Danach sind die Maßnahmen nach Verfügbarkeit (Wie wird gewährleistet, dass Verfahren und Daten zeitgerecht zur Verfügung stehen?), Vertraulichkeit (Wie wird gewährleistet, dass nur befugte Personen auf Daten und Verfahren zugreifen?), Integrität (Wie wird gewährleistet, dass Daten unversehrt, vollständig, zurechenbar und aktuell bleiben?), Transparenz (Wie wird gewährleistet, dass die automatisierte Verarbeitung von Daten mit zumutbaren Aufwand nachvollzogen, überprüft und bewertet werden kann), Intervenierbarkeit (Wie kann die Daten verarbeitende Stelle nachweisen, dass sie den Betrieb ihrer informationstechnischen Systeme steuernd beherrscht und dass Betroffene die ihnen zustehenden Rechte ausüben können?) und Nicht-Verkettbarkeit (Wie wird sichergestellt, dass Daten nur zu dem ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden) zu unterteilen. Dabei ist auch zu beurteilen, ob das Schutzniveau

[63] DSK, Das Standard-Datenschutzmodell - Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele. Aktuelle Versionen sind jeweils abrufbar unter: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/.

> angemessen ist und insbesondere die Risiken berücksichtigt, die mit der Verarbeitung verbunden sind, wie etwa durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

Ein Musterverfahrensverzeichnis, das die gesetzlichen Anforderungen in für die Betroffenen transparente Weise umsetzt findet sich in Annex II.

Aufgrund der Verarbeitung von Beschäftigtendaten und der Sensibilität der Überwachung der Beschäftigten durch die Simulation der IT-Sicherheitsvorfälle ist davon auszugehen, dass ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen, hier insbesondere der Beschäftigten, die an dem Test teilnehmen, i.S.v. Art. 35 Abs. 1 DSGVO besteht.

Die durch diesen Verarbeitungsvorgang entstehenden Risiken müssen angemessen durch Abhilfemaßnahmen bewältigt werden. Dies liegt in der Verantwortung der verantwortlichen Stelle nach Art. 24 DSGVO, der dies nicht unter den Vorbehalt der Höhe der Implementierungskosten stellt. Auch die Nichtdurchführung einer Datenschutz-Folgenabschätzung, wenn ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht ist an sich bereits gem. Art. 83 Abs. 4 DSGVO mit einer Bußgeldandrohung von bis zu 2% des weltweiten Jahresumsatzes versehen.

Das Forum Privatheit[64] hat ein Framework für die Durchführung einer Datenschutz-Folgenabschätzung entwickelt, das die rechtlichen Anforderungen, sowie die Forderungen der Artikel-29-Datenschutzgruppe[65] und der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK)[66] umsetzt. Die ausführliche Beschreibung enthält praktische Hilfestellung für die verantwortliche Stelle und baut auf dem Standard-Datenschutzmodell[67] der DSK auf, das der Umsetzung der datenschutzrechtlichen Anforderungen in der Praxis dient.

[64] Friedewald u.a., White Paper Datenschutz-Folgenabschätzung – Ein Werkzeug für einen besseren Datenschutz, 3. Auflage 2017, abrufbar unter: https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum-Privatheit-WP-DSFA-3-Auflage-2017-11-29.pdf.

[65] Artikel-29-Datenschutzgruppe, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 vom 4. April 2017, abrufbar unter: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=44137.

[66] DSK, Kurzpapier Nr. 5, Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO, abrufbar unter: https://www.lda.bayern.de/media/dsk_kpnr_5_dsfa.pdf.

[67] DSK, Das Standard-Datenschutzmodell - Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele. Aktuelle Versionen sind jeweils abrufbar unter: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/.

- Jede verantwortliche Stelle muss gem. Art. 30 DSGVO/ § 70 BDSG ein Verzeichnis der Verarbeitungstätigkeiten führen. Die ITS.APT-Methode ist im Sinne dieser Vorschriften eine Verarbeitungstätigkeit.
- Das Verfahren sollte so gestaltet werden, dass die Daten weitestgehend innerhalb der verantwortlichen Stelle verbleiben und auch bei der Durchführung durch einen IT-Dienstleister in Daten nur pseudonmyisierter Form von diesem verarbeitet werden.
- Auch wird i.d.R. eine Datenschutz-Folgenabschätzung durchzuführen sein. Diese kann auf dem Framework des Forums Privatheit aufbauen, das konkrete Hilfestellung bietet.

J. Handlungsempfehlungen zur Reduzierung von Haftungsrisiken

Literaturhinweise: Arkenau/Wübbelmann, Eigentum und Rechte an Daten – Wem gehören die Daten?, DSRITB 2015, 95; Dorner, Big Data und „Dateneigentum“, CR 2014, 617; Glasmacher/Pache, Geldentschädigungsanspruch bei Persönlichkeitsverletzungen, JuS 2015, 303; Hoeren, Dateneigentum – Versuch einer Anwendung von § 303a StGB im Zivilrecht, MMR, 2013, 486; Hoppe, Arbeitnehmerhaftung und ihre Auswirkungen auf die Nutzung betrieblicher Kommunikationsmittel, ArbRAktuell 2010, 388; Joussen, Der persönliche Anwendungsbereich der Arbeitnehmerhaftung, RdA 2006, 129; Krause, Geklärte und ungelöste Probleme der Arbeitnehmerhaftung, NZA 2003, 577; Larenz, Anmerkung zu BGH, Urteil vom 14. Februar 1958 („Herrenreiter“-Entscheidung), NJW 1958, 830; Libertus, Zivilrechtliche Haftung und strafrechtliche Verantwortlichkeit bei unbeabsichtigter Verbreitung von Computerviren, MMR 2005, 507; Pallasch, Einschränkung der Arbeitnehmerhaftung für betriebliche Tätigkeiten, RdA 2013, 338; Schwab, Haftung im Arbeitsverhältnis – 1. Teil: Die Haftung des Arbeitnehmers, NZA-RR 2016, 173; Schwab, Haftung im Arbeitsverhältnis – 2. Teil: Die Haftung des Arbeitgebers, NZA-RR 2016, 230; Waltermann, Besonderheiten der Haftung im Arbeitsverhältnis, JuS 2009, 193; Wilhelmi, Beschränkung der Organhaftung und innerbetrieblicher Schadensausgleich, NZG 2017, 681.

Diese Handlungsempfehlung stellt an dieser Stelle auch Informationen dazu bereit, welchen Haftungsrisiken derjenige ausgesetzt sein kann, der die ITS.APT-Methode in einer Kritischen Infrastruktur anwendet. Außerdem werden Ratschläge gegeben, auf welche Weise das Haftungsrisiko möglichst stark reduziert wird.

Dabei ist sowohl die Situation denkbar, dass der KRITIS-Betreiber die ITS.APT-Software selbst einsetzt als auch, dass er sich eines externen Dienstleisters bedient, der das IT-Sicherheitsbewusstsein der Mitarbeiter für ihn testet. Für beide Akteure soll dieses Dokument zeigen, wie die ITS.APT-Methode möglichst sicher angewendet werden kann. Im Folgenden

werden dazu die Haftungsrisiken anhand hypothetischer Haftungsszenarien aufgezeigt (I.). Sodann werden Empfehlungen zur Reduzierung dieser Risiken gegeben (II.).

I. Haftungsrisiken

Die möglichen Haftungsrisiken werden anhand von Szenarien aufgezeigt, die im Laufe des Projekts aufgetreten sind oder diskutiert wurden. Zunächst werden Schäden wegen der Nichtverfügbarkeit von Anwendungen behandelt (1.). In einem zweiten Fall wird auf eine mögliche Verletzung des Allgemeinen Persönlichkeitsrechts der Beschäftigten eingegangen (2.). Zuletzt wird die Haftung aufgrund von Datenverlusten diskutiert (3.).

1. Nichtverfügbarkeit von Anwendungen

Das erste Haftungsszenario befasst sich mit Zugriffsverzögerungen oder Ausfällen der IT-Systeme des Betreibers. Diese können aufgrund des Betriebs der ITS.APT-Software ausgelöst werden, wenn diese die vorhandene Rechenkapazität des IT-Systems derart belegt, dass sie für andere Anwendungen nicht mehr zur Verfügung steht. Das kann zur Folge haben, dass notwendige Abfragen oder Zugriffe anderer Programme nicht mehr oder nur noch verzögert durchgeführt werden können.

Innerhalb dieses Haftungsszenarios wird danach unterschieden, ob der Betreiber der Kritischen Infrastruktur, in der das IT-Sicherheitsbewusstsein gemessen werden soll, die Software selbst verwendet (1.) oder, ob ein externes Unternehmen mit der Durchführung der Tests und der Verwendung der Software beauftragt wird (2.).

a) Verwendung der ITS.APT-Lösung durch den KRITIS-Betreiber selbst

Zunächst wird der Fall betrachtet, in dem die Software durch den KRITIS-Betreiber selbst verwendet wird. Hierbei können sowohl vertragliche (aa) als auch deliktische Ansprüche entstehen (bb).

aa) Vertragliche Haftung

Eine vertragliche Haftung des Betreibers gegenüber etwaigen Vertragspartnern ergibt sich aus § 280 Abs. 1 BGB, wenn der KRITIS-Betreiber eine Pflichtverletzung zu vertreten hat und ein kausaler Schaden entstanden ist.

Die Pflichtverletzung gründet in dieser Konstellation darauf, dass die interne Nichtverfügbarkeit von Anwendungen dazu führt, dass Leistungen gegenüber Vertragspartnern nicht oder nur verspätet erbracht werden. Welche Leistungen das sein können, wird später noch beispielhaft besprochen (siehe unten 1-3).

Die Pflichtverletzung muss nicht zwingend vorsätzlich begangen werden. Ausreichend ist bereits leichte Fahrlässigkeit (§ 276 Abs. 1 S. 1 BGB). Hierbei gilt, dass der Arbeitgeber sich ein Verschulden seiner Arbeitnehmer nach § 278 BGB zurechnen lassen muss und das Vertretenmüssen gemäß § 280 Abs. 1 S. 2 BGB vermutet wird. Eine Widerlegung dieser Vermutung wird dem Betreiber in aller Regel nicht gelingen, da die Nichtverfügbarkeit von Anwendungen oft auf einen Organisationsfehler zurückzuführen sein wird. Der Betreiber ist dementsprechend dazu verpflichtet, innerbetrieblich die organisatorischen Voraussetzung dafür zu schaffen, dass eine Nichtverfügbarkeit von Anwendungen erst gar nicht auftreten kann.

Ein weiteres finanzielles Risiko besteht darin, dass der Arbeitgeber nur bedingt Regressansprüche gegen den Arbeitnehmer hat, der die Nichtverfügbarkeit verursacht hat. Handelte der Arbeitnehmer aufgrund einer betrieblich veranlassten Tätigkeit und nur leicht fahrlässig scheiden Ansprüche gegen den Arbeitnehmer aus. Das erklärt sich durch die arbeitsrechtliche Haftungsbegrenzung zugunsten von Arbeitnehmern (sog. innerbetrieblicher Schadensausgleich). Demnach haftet der Arbeitnehmer nur bei Vorsatz oder grober Fahrlässigkeit voll. Bei mittlerer Fahrlässigkeit erfolgt eine Schadensaufteilung zwischen ihm und dem Arbeitgeber. Verschärft wird dieses Ausfallrisiko dadurch, dass im Arbeitsverhältnis ein Verschulden des Arbeitnehmers nicht vermutet wird, sondern vom Arbeitgeber nachzuweisen ist (§ 619a BGB).

Welche konkreten Pflichtverletzungen erfolgen und welche Schäden entstehen können, ist dabei abhängig von der Kritischen Infrastruktur in der die Software verwendet wird. Im Folgenden werden drei Bereiche beispielhaft behandelt.

(1) Energie

Im Bereich der Energieversorgung besteht die Pflichtverletzung des Energieversorgungsunternehmens darin, den Vertragspartner nicht mehr ausreichend mit Elektrizität, Gas oder anderen Energieformen zu versorgen. Denkbar wäre, dass im Zuge der Verwendung der ITS.APT-Software notwendige Computerprogramme zur Steuerung der Anlagen zur Stromerzeugung und Weiterleitung nicht verfügbar sind, was zu einer Unterbrechung oder Störung der Versorgung der Vertragspartner führen würde.

Exemplarisch kann hier auf den durch einen Cyber-Angriff ausgelösten Stromausfall in der Ukraine im Jahr 2015 verwiesen werden. Mindestens 225.000 Einwohner der Ukraine waren von einem mehrstündigen Ausfall der Stromversorgung betroffen. Aufgrund der Sabotage der im Regelbetrieb für die Fernsteuerung der Umspannwerke genutzten Leittechnik, mussten die

Schaltvorgänge vor Ort in den Umspannwerken manuell ausgelöst werden. Dadurch wurde die Wiederherstellung der Stromversorgung deutlich verzögert.[68]

(2) Informationstechnik und Telekommunikation

Bei Betreibern von Informationstechnik- und Telekommunikationseinrichtungen kann die Pflichtverletzung in Anschlussunterbrechungen liegen.

So hatten beispielsweise im Jahr 2016 zahlreiche DSL-Kunden der Deutschen Telekom keinen Zugang mehr zum Internet. Nach offiziellen Angaben waren bundesweit ca. 900.000 Internetanschlüsse betroffen.[69] Da die Verfügbarkeit des Internets für die private sowie wirtschaftliche Lebensgestaltung von zentraler Bedeutung ist, stellt nach der Rechtsprechung bereits die unterbliebene Möglichkeit, den Anschluss zu nutzen einen ersatzfähigen Schaden dar.

(3) Gesundheit

In den Sektor der Gesundheit fallen insbesondere Krankenhäuser, Apotheken und Labore. Können diese ihre Leistung gegenüber ihren Vertragspartnern – also bspw. den Patient*innen – nicht ordnungsgemäß erfüllen, sind Schäden für Leib, Leben und Gesundheit nicht auszuschließen. Besonders gravierend wäre in dem Zusammenhang ein Ausfall der IT-Infrastruktur auf der Intensivstation eines Krankenhauses, infolgedessen seine Patient*innen nicht adäquat versorgen kann.

Als Beispiel kann hier auf den Cyber-Angriff auf ein Neusser Krankenhaus im Jahr 2016 verwiesen werden, der zu Störungen in den IT-Systemen führte und auch die Behandlung von Patienten behinderte. Alleine die Kosten für die Wiederherstellung des IT-Betriebs wurden auf ca. eine Million Euro beziffert.[70]

Diese Fälle zeigen, dass KRITIS-Betreiber, die auf ihre IT-Systeme nicht mehr zugreifen können, ihre vertraglichen Leistungen nicht mehr oder nur mit Verzögerungen erfüllen und, welche Schäden dadurch entstehen können.

---

[68] Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2016, S. 40 (abrufbar unter: www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/2016_16_11_Lagebericht2016.pdf?__blob=publicationFile, zuletzt aufgerufen am 16.10.2017).

[69] Bundesamt für Sicherheit in der Informationstechnik, Pressemeldung, Cyber-Angriffe auf Telekom: BSI fordert Umsetzung geeigneter Schutzmaßnahmen (abrufbar unter: www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2016/Angriff_Router_28112016.html, zuletzt aufgerufen am 16.10.2017).

[70] Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2016, S. 39 (abrufbar unter: www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/2016_16_11_Lagebericht2016.pdf?__blob=publicationFile, zuletzt aufgerufen am 16.10.2017).

bb) Deliktische Haftung nach § 823 Abs. 1 BGB

Neben die vertragliche tritt die deliktische Haftung. Diese Haftungsmöglichkeit besteht sowohl gegenüber Vertragspartnern, als auch gegenüber Dritten. Eine Haftung nach § 823 Abs. 1 BGB kommt dann in Betracht, sofern ein geschütztes Recht oder Rechtsgut durch eine zurechenbare Handlung rechtswidrig und schuldhaft verletzt wird.

(1) Verkehrspflichten des KRITIS-Betreibers

Als unerlaubte Handlungen kommen neben solchen, die unmittelbar ein Recht oder Rechtsgut verletzen, auch solche in Betracht, die nur mittelbar verletzend sind, sofern eine Verkehrspflicht verletzt wird. Verkehrspflichten beruhen auf dem Gedanken, dass derjenige, der eine Gefahrenquelle schafft oder unterhält, Maßnahmen zu treffen hat, um andere vor der Gefahr zu schützen. Eine absolute Sicherheit wird allerdings nicht gefordert. Vielmehr werden Verkehrspflichten durch die Grenze des Möglichen und Zumutbaren beschränkt. Was möglich und zumutbar ist, wird anhand mehrerer Kriterien bestimmt.

Relevant sind dabei zunächst die Größe der jeweiligen Gefahr und ihre Eintrittswahrscheinlichkeit. Sind besonders schützenswerte Rechtsgüter wie das Leben oder die körperliche Unversehrtheit betroffen, sind strengere Anforderungen an die zu treffenden Sicherheitsmaßnahmen zu stellen, als in Fällen, in denen nur das Eigentum bedroht ist. Darüber hinaus sind auch die Kosten und Nutzen einer bestimmten Sicherheitsmaßnahme zu berücksichtigen. Können gravierende Schäden durch kostenintensive Maßnahmen verhindert werden, sind diese eher zuzumuten, als in dem Fall, in dem kostenintensive Maßnahmen nur einen minimalen Sicherheitsgewinn versprechen. Außerdem hängt der geforderte Sicherheitsmaßstab von den Erwartungen des betroffenen Verkehrskreises ab. Innerhalb des Verkehrskreises sind stets die Erwartungen der schutzbedürftigsten Personen maßgeblich. Daher gilt insbesondere für Betreiber von Krankenhäusern oder sonstigen Kritischen Infrastrukturen für kranke, behinderte oder in sonstiger Weise hilfsbedürftige Menschen ein außerordentlich strenger Sorgfaltsmaßstab.

Auch sonst ergibt sich aus diesen Kriterien ein besonders strenger Maßstab für den Betreiber einer Kritischen Infrastruktur. Dafür spricht zunächst, dass ihr ordnungsgemäßes Funktionieren unerlässlich für das gesellschaftliche Zusammenleben und eine funktionierende Wirtschaft ist und der Verkehr entsprechend hohe Sicherheitserwartungen hat. Es wird schlechthin erwartet, dass eine Kritische Infrastruktur funktioniert. Für einen besonders strengen Maßstab spricht außerdem, dass im Falle eines Versorgungsausfalls besonders

gravierende Schäden zu erwarten sind. Das zeigen die schon oben angesprochenen Branchenbeispiele.

Aufgrund dieses strengen Maßstabs hat ein KRITIS-Betreiber, der die ITS.APT-Methode in seinem Unternehmen anwenden will, spezielle Verkehrspflichten. Demnach sind die betrieblichen Abläufe so zu organisieren, dass Schädigungen vermieden werden. Hierbei kann sich der einzelne Betreiber insbesondere an Industriestandards orientieren. Zum Beispiel zeigt die ISO-Norm 27001 auf, wie Informationssicherheit in privaten, öffentlichen oder gemeinnützigen Organisationen gewährleistet werden kann. Sie beschreibt die Anforderungen an ein Informationssicherheits-Managementsystem. Darüber hinaus bietet das Bundesamt für Informationssicherheit Anleitungen zum Schutz Kritischer Infrastrukturen an, die in Zusammenarbeit mit Betreibern solcher Infrastrukturen erstellt wurden.[71] Zwar haben sowohl solche DIN-Normen, als auch die erwähnten Anleitungen keine Bindungswirkung. Sie normieren allerdings ein Sicherheitsniveau, das dem Verkehrspflichtigen bekannt sein sollte und von Branchenexperten als zumutbar und möglich beschrieben wurde und daher eingehalten werden sollte. Außerdem zeigen sie hilfreiche Leitlinien auf und geben praktische Unterstützung. Darüber hinaus ist es dem Betreiber einer Kritischen Infrastruktur anzuraten, bei dem Einsatz der ITS.APT-Lösung die unter Abschnitt B. genannten Handlungen vorzunehmen, bevor er das IT Sicherheitsbewusstsein seiner Mitarbeiter testet.

Als maßgeblicher Beurteilungszeitpunkt wird primär auf den Zeitpunkt der Verletzung der Verkehrspflicht abgestellt. Dies entbindet aber weder von einer Kontrolle noch einer gegebenenfalls erforderlichen Anpassung der internen Organisation. Allerdings wird dem Verpflichteten eine angemessene Übergangszeit zuerkannt, um seine Organisationsstrukturen anzupassen. Wie lang diese Zeit ist, hängt von den jeweiligen Umständen des Einzelfalls ab. Aus diesem Grund kann jedoch nicht davon ausgegangen werden, dass die hier vorgeschlagenen Maßnahmen zur Verringerung von Haftungsrisiken auch in Zukunft den Maßstab des Möglichen und Zumutbaren definieren. Vielmehr hat ein KRITIS-Betreiber die weitere Entwicklung auf diesem Gebiet zu beobachten und seine Maßnahmen ggf. anzupassen.

(2) Zurechnung der Handlung

Der Betreiber ist häufig als juristische Person organisiert und muss sich daher die Handlungen seiner Organe, also beispielsweise seines Geschäftsführers, entsprechend § 31 BGB

[71] Siehe www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Schutz-Kritischer-Infrastrukturen-ITSig-u-UP-KRITIS.pdf?__blob=publicationFile&v=5.

zurechnen lassen. Eine Haftung des Betreibers für schädigende Handlungen der einfachen Arbeitnehmer ist über diese Norm zwar nicht direkt möglich. Sind diese aber auf organisatorische Mängel des Geschäftsführers zurückzuführen, so muss dieser und damit der KRITIS-Betreiber dafür über § 31 BGB einstehen. Eine besondere Selbstständigkeit des Arbeitnehmers kann jedoch dessen deliktische Haftung gegenüber Dritten begründen (zur Zurechnung von Fehlverhalten externer Dienstleister siehe unter 2.).

(3) Rechtswidrigkeit und Schuld

Die Rechtswidrigkeit einer Verkehrspflichtverletzung wird durch die Tatbestandsmäßigkeit indiziert. Nur wenn das mittelbar ursächliche Verhalten von einem Rechtfertigungsgrund gedeckt ist, bestand auch keine Pflicht, sich anders zu verhalten. Ein Verschulden liegt erst vor, wenn der Verkehrspflichtige der im konkreten Fall bestehenden Pflicht fahrlässig oder vorsätzlich nicht nachgekommen ist. Damit ist die persönliche Vorwerfbarkeit des ursächlichen Verhaltens angesprochen. Ein solcher Vorwurf entfällt, wenn die Gefahr nicht zu erkennen war oder der Verkehrspflichtige keine Möglichkeit hatte, sie abzuwenden.

(4) Schaden

Im Rahmen der Haftung nach § 823 Abs. 1 BGB kommen grundsätzlich dieselben Schäden in Betracht, die auch schon im Zusammenhang mit der vertraglichen Haftung genannt wurden. Zu beachten ist jedoch, dass reine Vermögensschäden nicht nach § 823 Abs. 1 BGB ersatzfähig sind. Solche können im Deliktsrecht nur über § 823 Abs. 2 BGB oder über § 826 BGB ersetzt werden. Also entweder wenn ein speziell das Vermögen schützendes Schutzgesetz verletzt wurde oder im Falle einer vorsätzlichen sittenwidrigen Schädigung.

cc) Sonstige deliktische Haftung

Im zuletzt genannten Fall einer Haftung nach § 826 BGB müsste die Durchführung des Tests allerdings gegen das Anstandsgefühl aller billig und gerecht Denkenden verstoßen, um eine Sittenwidrigkeit anzunehmen. Davon kann angesichts der bezweckten Verbesserung des IT Sicherheitsbewusstseins der Mitarbeiter nicht ausgegangen werden.

b) Verwendung der ITS.APT-Lösung durch einen externen IT-Dienstleister

Gegenüber der Konstellation, dass der Betreiber einer Kritischen Infrastruktur die ITS.APT-Software selbst verwendet, ist auch denkbar, dass er sich dazu eines externen Unternehmens bedient. Hierbei ist zwischen der Haftung des KRITIS-Betreibers und der Haftung des IT-Dienstleisters zu differenzieren.

aa) Haftung des KRITIS-Betreibers

Als erstes wird hier die Haftung des KRITIS-Betreibers behandelt.

(1) Vertragliche Haftung

Hinsichtlich der vertraglichen Haftung aus § 280 Abs. 1 BGB kommt dieselbe Pflichtverletzung in Betracht, die schon oben genannt wurde, also die unzureichende Vertragsleistung aufgrund einer Nichtverfügbarkeit der IT-Systeme. Auf welche Weise ein KRITIS-Betreiber das IT-Sicherheitsbewusstsein seiner Mitarbeiter testet, hat keinen Einfluss auf die jeweiligen Pflichten gegenüber seinen Vertragspartnern.

Der entscheidende Unterschied zur obigen Konstellation liegt in der Frage, unter welchen Umständen der KRITIS-Betreiber eine solche Nichtverfügbarkeit zu vertreten hat. In Betracht kommt sowohl ein eigenes Verschulden (bzw. das seiner Angestellten, das sich der KRITIS-Betreiber in jedem Fall zurechnen lass muss, vgl. Abschnitt 1. a), als auch ein Verschulden des externen Dienstleisters, das sich der KRITIS-Betreiber eventuell zurechnen lassen muss.

Ein eigenes Verschulden könnte darin begründet sein, den externen Dienstleister unzureichend auszuwählen oder zu überwachen. Grundsätzlich kann der KRITIS-Betreiber jedoch darauf vertrauen, dass ein externer Dienstleister, der die ITS.APT-Methode anwendet, die erforderliche Sachkunde besitzt. Sollten aber Anzeichen für eine Unzuverlässigkeit auftreten, beispielsweise weil der Dienstleister grundlegende IT-Kenntnisse vermissen lässt oder weil der Betreiber besonders häufig negativ bewertet wurde, kann das ein eigenes Auswahlverschulden begründen. Gleichermaßen hat der KRITIS-Betreiber den Dienstleister nicht dauerhaft persönlich zu überwachen. Er muss ihn aber regelmäßig und erst Recht bei hinreichendem Verdacht kontrollieren. Wählt der KRITIS-Betreiber den Dienstleister jedoch sorgfältig aus und überwacht ihn, so trifft ihn kein eigenes Verschulden.

Allerdings könnte dem KRITIS-Betreiber ein Verschulden des externen Dienstleisters zuzurechnen sein. Maßgebliche Vorschrift ist dabei § 278 BGB. Sie setzt voraus, dass ein Erfüllungsgehilfe im Pflichtenkreis des Geschäftsherrn gegenüber einem Vertragspartner tätig wird und ihn dabei ein Verschulden trifft. Erfüllungsgehilfe ist, wer mit Wissen und Wollen des Geschäftsherrn tätig wird. Verpflichtet der KRITIS-Betreiber also einen externen Dienstleister mit der Anwendung der ITS.APT-Methode, so müsste der im Pflichtenkreis gegenüber den Vertragspartnern des KRITIS-Betreibers tätig werden. Das ist allerdings nicht der Fall. Denn das Testen des IT-Sicherheitsbewusstseins der Mitarbeiter ist niemals Gegenstand einer vertraglichen Leistungspflicht des KRITIS-Betreibers gegenüber seinen sonstigen Vertragspartnern. Beispielsweise schuldet ein Krankenhaus dem Patienten aus dem

Behandlungsvertrag eine fehlerfreie medizinische Behandlung. Ein Telekommunikationsunternehmen schuldet seinen Vertragspartnern eine einwandfreie Nutzung der zugesicherten Telekommunikationsdienste. Zur Erfüllung solcher Verbindlichkeiten wird der externe Dienstleister nicht herangezogen, wenn er das IT-Sicherheitsbewusstsein testet. Dementsprechend muss sich der KRITIS-Betreiber kein fremdes Verschulden des externen Dienstleisters zurechnen lassen.

(2) Deliktische Haftung

Hinsichtlich der deliktischen Haftung des KRITIS-Betreibers kann zunächst auch auf die Ausführungen von oben verwiesen werden. Die entscheidende Frage ist abermals, unter welchen Umständen der KRITIS-Betreiber für ein Fehlverhalten des externen Dienstleisters verantwortlich ist.

Eine solche Verantwortlichkeit kann sich zunächst aus § 831 BGB ergeben. Haftungsgrund ist hierbei jedoch nicht das Verschulden des Dritten, sondern das Verschulden des Betreibers hinsichtlich der Bereitstellung von Arbeitsmitteln oder der Auswahl bzw. Kontrolle des externen Dienstleisters. Voraussetzung für die Anwendbarkeit des § 831 BGB ist, dass der externe Dienstleister ein Verrichtungsgehilfe ist, also von den Weisungen seines Geschäftsherrn abhängig und in seine Organisation eingegliedert ist. Soweit aber ein externer Dienstleister als selbständiger Unternehmer tätig wird, ist diese Voraussetzung nicht erfüllt.

Daneben kommt eine Verantwortlichkeit des KRITIS-Betreibers aus § 823 Abs. 1 BGB in Betracht, soweit er eine Verkehrspflicht verletzt hat. Dabei bestehen grundsätzlich dieselben Verkehrspflichten, die bereits im Rahmen der Verwendung der ITS.APT-Methode durch den KRITIS-Betreiber selbst erwähnt wurden. Im Unterschied zur dortigen Situation kann er manche der Pflichten aber auch erfüllen, indem er dazu einen zuverlässigen externen Dienstleister einsetzt und diesen sorgfältig auswählt und überwacht. Bezüglich der Auswahl und Kontrolle gilt dasselbe wie im Rahmen der vertraglichen Haftung. Bei den Pflichten, die übertragen werden können, ist zu beachten, dass dafür nur solche in Betracht kommen, die auch durch den externen Dienstleister erfüllt werden können. Daher ist stets zu hinterfragen, ob die verursachte Nichtverfügbarkeit eher der Risikosphäre des KRITIS-Betreibers zuzurechnen ist oder der des externen Dienstleisters. Letzterer kann beispielsweise nicht in jedem Fall festlegen, in welchem Bereich Mitarbeiter überhaupt getestet werden dürfen. In der Regel wird er nicht beurteilen können, wie essentiell die Tätigkeit bestimmter Mitarbeiter für das ordnungsgemäße Funktionieren der Kritischen Infrastruktur ist. Auch in Bezug auf die

sonstige Nutzung der ITS.APT-Methode wird es darauf ankommen, wer die Durchführung der Tests beherrschend „in den Händen hält“.

bb) Haftung des externen IT-Dienstleisters

Nachdem die Haftung des KRITIS-Betreibers untersucht wurde, wird im Folgenden die Haftung des externen Dienstleisters begutachtet.

(1) Vertragliche Haftung

Gegenüber demjenigen, der die Leistungen einer Kritischen Infrastruktur nutzt, und dem externen Dienstleister, ist eine vertragliche Haftung des Dienstleisters mangels einer vertraglichen Beziehung ausgeschlossen.

Muss der KRITIS-Betreiber aber für ein Fehlverhalten des externen Dienstleisters einstehen, kommt ein Regress des KRITIS-Betreibers in Betracht. Ein solcher Schadensersatzanspruch würde sich dann aus dem zwischen den Parteien geschlossenen Vertrag ergeben.

(2) Deliktische Haftung

Inwiefern der externe Dienstleister deliktisch haftet, hängt wesentlich davon ab, wessen Risikosphäre der Fehler zuzurechnen ist (siehe bereits deliktische Haftung beim KRITS-Betreiber). Nimmt der externe Dienstleister nicht bloß eine Hilfsfunktion, sondern eine das System beherrschende Stellung ein, ist die Nichtverfügbarkeit ihm zuzurechnen. Hat er daraus folgende Rechts- und Rechtsgutsverletzung auch zu verschulden und ist sein Verhalten nicht gerechtfertigt, besteht eine deliktische Haftung aus § 823 Abs. 1 BGB.

2. Verletzung des Allgemeinen Persönlichkeitsrechts des Arbeitnehmers

In einem zweiten Szenario werden die Haftungsrisiken aufgrund einer Beeinträchtigung des Allgemeinen Persönlichkeitsrechts der Arbeitnehmer betrachtet. Dieses Recht gewährleistet dem Arbeitnehmer insbesondere über die Preisgabe und Verwendung seiner persönlichen Daten selbst zu bestimmen (Recht auf informationelle Selbstbestimmung), vgl. oben, Teil B II. Dabei ist anerkannt, dass sich der Schutz des Allgemeinen Persönlichkeitsrechts auch auf das Arbeitsverhältnis erstreckt.

Eine Beeinträchtigung des Allgemeinen Persönlichkeitsrechts liegt vor, wenn mit Hilfe der ITS.APT-Software persönliche Daten heimlich auf den Rechnern der Arbeitnehmer erhoben werden oder auf anderem Weg in die Hände des Arbeitgebers gelangen. Zum Beispiel könnten solche Daten aufgrund einer Reaktion des Arbeitnehmers auf eine Phishing-Mail erhoben werden, die ihn zur Herausgabe seines E-Mail-Passworts auffordert. Aus dem Grund müssen die selbst anzupassenden Artefakte der ITS.APT-Lösung so konstruiert werden, dass

mit Ausnahme der Art der Reaktion keine sonstigen personenbezogenen Daten erhoben und verarbeitet werden. Sollte das doch der Fall sein, könnte die betroffene Person Schadensersatzansprüche gegen den KRITIS Betreiber oder, falls die Software von einem externen IT-Dienstleister verwendet wird, auch gegen diesen haben.

Im Folgenden wird daher wie im ersten Haftungsszenario danach unterschieden, ob der KRITIS-Betreiber die Software selbst verwendet (1.) oder, ob ein externes Unternehmen mit der Durchführung der Tests und damit auch mit der Verwendung der Software beauftragt wird (2.).

a) Verwendung der ITS.APT-Lösung durch KRITIS-Betreiber selbst

Zunächst erfolgt eine Betrachtung des Falls, in dem die Software durch den Betreiber selbst verwendet wird. Möglich sind hierbei vertragliche (a) sowie deliktische (b) Ansprüche.

aa) Vertragliche Haftung

Der KRITIS-Betreiber der Software haftet seinen Arbeitnehmern gegenüber im Rahmen seiner vertraglichen Beziehung als Arbeitgeber nach § 280 Abs. 1 BGB für Pflichtverletzungen, die er zu vertreten hat. Der Arbeitgeber hat insbesondere die Pflicht, Rücksicht auf die Rechte, Rechtsgüter und Interessen seines Arbeitnehmers zu nehmen (§ 241 Abs. 2 BGB). Diese Schutzpflicht umfasst auch, das Allgemeine Persönlichkeitsrecht des Arbeitnehmers zu wahren.

Bezüglich des Verschuldens des Betreibers gelten die Ausführungen des ersten Haftungsszenarios. Auch hier muss sich der Betreiber das Fehlverhalten der Angestellten, die für die Implementierung der ITS.APT-Methode zuständig sind, gegenüber dem betroffenen Arbeitnehmer gemäß § 278 BGB zurechnen lassen. Da für eine vertragliche Haftung bereits leichte Fahrlässigkeit ausreicht (§ 276 Abs. 1 S. 1 BGB), ist nicht erforderlich, dass der Arbeitgeber vorsätzlich auf die Daten des Arbeitnehmers zugreift. Eine Speicherung der Arbeitnehmerdaten aufgrund einer beispielsweise nicht sorgfaltsgemäßen Anpassung der Software an die eigene Infrastruktur begründet daher bereits ein Verschulden des Arbeitgebers.

Bei einer Verletzung des Allgemeinen Persönlichkeitsrechts besteht die Besonderheit, dass in der Regel keine materiellen Schäden entstehen. Die Ersatzfähigkeit eines immateriellen Schadens erfordert gemäß § 253 Abs. 1 BGB grundsätzlich eine gesetzliche Regelung. Eine solche Regelung findet sich für immaterielle Schäden aufgrund einer Verletzung des Allgemeinen Persönlichkeitsrechts jedoch nicht. Handelt es sich aber um eine besonders

schwerwiegende Verletzung, leitet die Rechtsprechung aus Art. 2 Abs. 1 GG, Art. 1 Abs. 1 GG eine Ausnahme von diesem Grundsatz ab und gewährt eine billige Geldentschädigung. Der Umfang der Ersatzpflicht hängt u.a. von Bedeutung und Tragweite des Eingriffs, Anlass und Beweggrund des Handelnden sowie dem Grad des Verschuldens ab. Bei einer Verletzung des Persönlichkeitsrechts kann also im Rahmen des Schadens für den Arbeitgeber begünstigend berücksichtigt werden, ob er bzw. einer seiner Angestellten lediglich fahrlässig gehandelt hat.

bb) Deliktische Haftung

Neben die vertragliche tritt die deliktsrechtliche Haftung. Hierbei sind im Wesentlichen zwei Anspruchsgrundlagen zu unterscheiden, zum einen § 823 BGB (aa) sowie
Art. 82 DSGVO (bb).

(1) § 823 BGB

(a) Rechts- oder Rechtsgutsverletzung

Als sonstiges Recht im Sinne des § 823 Abs. 1 BGB wird auch das Allgemeine Persönlichkeitsrecht anerkannt, sodass dessen Verletzung auch zu einer deliktsrechtlichen Haftung des Arbeitgebers gegenüber dem Arbeitnehmer führen kann. Schließlich kann der Arbeitgeber nach § 823 Abs. 2 BGB haften, wenn er gegen datenschutzrechtliche Normen verstößt und diese auch den Einzelnen schützen, was angesichts der Verwurzelung im Allgemeinen Persönlichkeitsrecht in der Regel der Fall sein dürfte. Auch eine Dienst-/Betriebsvereinbarung, die Bestimmungen bezüglich des Persönlichkeitsrechtsschutzes von Arbeitnehmern festlegt, kann ein Schutzgesetz im Sinne des § 823 Abs. 2 BGB sein und damit eine Haftung des Arbeitgebers begründen. Letzteres ist besonders hervorzuheben, da eine solche regelmäßig am besten geeignet ist, um die ITS-APT-Tests rechtskonform durchführen zu können, vgl. oben, Teil B IV. und Teil H.

(b) Die Zurechnung der Handlung

Bezüglich der Zurechnung der Handlung ist auf die Ausführungen zur Nichtverfügbarkeit von Anwendungen im Rahmen der deliktischen Haftung zu verweisen. Der Betreiber muss sich folglich das Handeln seiner Organe entsprechend § 31 BGB zurechnen lassen.

(c) Rechtswidrigkeit und Schuld

Die Rechtswidrigkeit einer Verletzung des Allgemeinen Persönlichkeitsrechts wird – anders als bei einer Verletzung der oben genannten Verkehrspflichten – nicht durch die Tatbestandsmäßigkeit indiziert. Sie muss in einer umfassenden Güter- und

Interessensabwägung positiv festgestellt werden. Es sind daher das Interesse des Betreibers, seine IT-Sicherheit zu verbessern und das Interesse des Arbeitnehmers an dem Schutz seiner personenbezogenen Daten abzuwägen. In der Regel wird dabei das Allgemeine Persönlichkeitsrecht des Arbeitnehmers überwiegen. Mit Hilfe der ITS.APT-Methode kann das IT-Sicherheitsbewusstsein schließlich gemessen werden ohne, dass übermäßige Beeinträchtigungen der Rechte des Arbeitnehmers notwendig sind. Dem Interesse des Arbeitgebers ist damit ausreichend Rechnung getragen und es sind keine Gründe ersichtlich, die eine weitergehende Verarbeitung rechtfertigen. Das Verschulden des KRITIS-Betreibers bestimmt sich hier nach denselben Maßstäben wie im ersten Haftungsszenario.

(d) Schaden

Hinsichtlich des Schadens gilt das zur vertraglichen Haftung Gesagte.

(2) Art. 82 DSGVO

Art. 82 DSGVO regelt, dass jeder Person, der wegen eines Verstoßes gegen DSGVO ein Schaden entstanden ist, ein Anspruch auf Schadensersatz gegen den Verantwortlichen oder den Auftragsverarbeiter zusteht. Obwohl es sich bei der DSGVO um einen Rechtsakt der Europäischen Union handelt, kann sich der Anspruchsberechtigte direkt auf sie stützen, um einen Anspruch vor einem deutschen Gericht durchzusetzen. Das liegt darin begründet, dass Verordnungen der Europäischen Union in den Mitgliedsstaaten unmittelbare Geltung entfalten gemäß Art. 288 Abs. 2 AEUV.

Der Anspruch setzt demnach die Anspruchsberechtigung (1), einen tauglichen Anspruchsgegner (2) und einen Verstoß gegen die DSGVO (3) voraus. Unter diesen Voraussetzungen besteht grundsätzlich ein Schadensersatzanspruch, wenn nicht ein Ausschlussgrund greift (4). Auf Rechtsfolgenseite ist insbesondere die Ersatzfähigkeit des Schadens in den Blick zu nehmen (5).

(a) Anspruchsberechtigung

Anspruchsberechtigt ist „jede Person“, die von dem Datenschutzrechtsverstoß betroffen ist. In diesem Haftungsszenario meint das die Person, deren Allgemeines Persönlichkeitsrecht verletzt wurde, also den Arbeitnehmer.

(b) Anspruchsgegner

Anspruchsgegner kann sowohl der Verantwortliche als auch der Auftragsverarbeiter sein.[72] Im Verhältnis des KRITIS-Betreibers zum Arbeitnehmer ist der Betreiber als Verantwortlicher zu qualifizieren. Nach Art. 82 Abs. 2 S. 1 DSGVO reicht bereits seine bloße Beteiligung an dem Datenschutzrechtsverstoß aus. Zudem muss sich der Verantwortliche auch das Handeln seiner Mitarbeiter zurechnen lassen.

(c) Verstoß gegen die DSGVO

Der Verantwortliche oder der Auftragsverarbeiter muss gegen die DSGVO verstoßen haben. Aus EG 146 S. 5 ergibt sich, dass darunter auch Verstöße gegen nationales Recht der Mitgliedstaaten zur Umsetzung bzw. Konkretisierung der DSGVO fallen. Daher müssen bei der Anwendung der ITS.APT-Software auch auf die Vorgaben aus dem Bundesdatenschutzgesetz geachtet werden, die auf Öffnungsklauseln der DSGVO zurückzuführen sind.

Hinsichtlich der Frage, welche Normenverstöße konkret in Betracht kommen, ist vertiefend auf den datenschutzrechtlichen Teil dieses Gutachten zu verweisen.

(d) Kein Ausschluss

Der KRITIS-Betreiber wird von der Haftung gemäß Art. 82 Abs. 3 DSGVO frei, wenn er nachweist, dass er für den Umstand, durch den der Schaden eingetreten ist, nicht verantwortlich ist, also alle relevanten Datenschutzvorschriften eingehalten hat. Aus dem Grund ist zum einen die strenge Beachtung der im Datenschutzteil genannten Maßnahmen anzuraten und zum anderen deren umfassende Dokumentation.

(e) Rechtsfolge

Ersetzt werden sowohl materielle als auch immaterielle Schäden. In diesem Haftungsszenario ist insbesondere der Ersatz immaterieller Schäden in Form einer Geldentschädigung relevant. Auch insofern dürfte die Art und Intensität des Eingriffs maßgeblich sein. Als unionsrechtliche Besonderheit ist in dem Zusammenhang noch hervorzuheben, dass der Schadensersatzanspruch aus Art. 82 DSGVO nach EG 146 S. 3 „im Lichte der Rechtsprechung des Gerichtshofs weit auf eine Art und Weise ausgelegt werden [muss], die den Zielen dieser Verordnung in vollem Umfang entspricht." Nach der Rechtsprechung des EuGH muss der Schadenersatz eine abschreckende Wirkung erzielen. Die soll den Schädiger im Vorhinein davon abhalten, sich überhaupt schädigend zu verhalten. Berücksichtigt man die

[72] Siehe zum Begriff des Verantwortlichen und des Auftragsverarbeiters unter Rechtslage des BDSG und des LDSG: ITS.APT Dokument D2.3 S. 10 ff.

zurückhaltende Position der deutschen Gerichtsbarkeit gegenüber der Gewährung immateriellen Schadensersatzes nach § 823 BGB, ist es demnach geboten, bei einem Anspruch aus Art. 82 DSGVO deutlich höhere Beträge anzusetzen.

b) Verwendung der ITS.APT-Lösung durch externen IT-Dienstleister

Wird die ITS.APT-Lösung durch einen externen IT-Dienstleister implementiert, ist wieder zwischen der Haftung des KRITIS-Betreibers (a) und der Haftung des IT-Dienstleisters (b) zu differenzieren.

aa) Haftung des KRITIS-Betreibers

Zunächst wird auf die Haftung des KRITIS-Betreibers eingegangen.

(1) Vertragliche Haftung

Die vertragliche Haftung des KRITIS-Betreibers ergibt sich aus derselben Pflichtverletzung, die bereits im Rahmen der Verwendung der ITS.APT-Lösung durch ihn selbst erläutert wurde. Sie besteht in der Verletzung des Allgemeinen Persönlichkeitsrechts, indem beispielsweise die Software fehlerhaft an die Netzinfrastruktur des Betreibers angepasst wird oder indem auf unzulässige Weise personenbezogene Daten des Arbeitnehmers erhoben werden.

Es stellt sich jedoch abermals die Frage, inwiefern der Betreiber diese Pflichtverletzung zu vertreten hat. Wie auch im ersten Haftungsszenario, ist hier ein Verschulden des KRITIS-Betreibers oder ein Verschulden des externen Dienstleisters möglich, das dem Betreiber zugerechnet wird. Letzteres scheidet jedoch auch in diesem Haftungsszenario aus, da der Externe nicht als Erfüllungshilfe des Betreibers im Sinne des § 278 BGB zur Erfüllung einer Verbindlichkeit aus dem Arbeitsvertrag tätig ist. Es kann demnach nur noch ein eigenes Verschulden des Betreibers haftungsbegründend wirken. Das könnte sich abermals aus einer unzureichenden Auswahl oder Kontrolle des Dienstleisters ergeben. Insofern gelten die schon im ersten Haftungsszenario herausgearbeiteten Grundsätze.

(2) Deliktische Haftung

Hinsichtlich der deliktischen Haftung des KRITIS-Betreibers ist zunächst auf die Ausführungen im ersten Haftungsszenario zu verweisen. Auch in diesem Haftungsszenario ist maßgeblich, in welchem Rahmen der KRITIS-Betreiber für ein etwaiges Fehlverhalten des externen Dienstleisters haften muss.

Eine Verantwortlichkeit lässt sich auch in diesem Fall nicht aus § 831 BGB herleiten, soweit der Externe als selbstständiger Unternehmer tätig wird. In dem Fall unterliegt er nicht den

Weisungen des Betreibers und ist daher kein Verrichtungsgehilfe i.S.d. § 831 BGB. Hat der Betreiber einen zuverlässigen Dienstleister sorgfältig ausgewählt und überwacht, so scheidet aus den gleichen Gründen wie im ersten Haftungsszenario eine Haftung nach § 823 Abs. 1 BGB aus.

Daneben kann ebenfalls ein Anspruch aus Art. 82 DSGVO bestehen (ausführlich dazu oben). Dabei haftet der KRITIS-Betreiber als Verantwortlicher dem Arbeitnehmer gegenüber voll, selbst wenn das schadensursächliche Verhalten vom externen Dienstleister ausgeht. Art. 82 Abs. 4 DSGVO sieht in dem Fall vor, dass beide als Gesamtschuldner haften. Für das Innenverhältnis regelt Art. 82 Abs. 5 DSGVO einen Regressanspruch des Betreibers gegen den externen Dienstleister. Der scheidet jedoch aus, wenn der Auftragsverarbeiter keine Verpflichtung aus der DSGVO verletzt hat oder keine Anweisung des Verantwortlichen missachtet hat (Art. 82 Abs. 2 S. 2 DSGVO). Entscheidend ist daher im Innenverhältnis der Verursachungsanteil bezüglich der unzulässigen Datenverarbeitung.

aa) Haftung des externen Dienstleisters

(1) Vertragliche Haftung

Mangels einer vertraglichen Beziehung zwischen dem Arbeitnehmer und dem externen Dienstleister ist eine vertragliche Haftung des Dienstleisters dem Arbeitnehmer gegenüber ausgeschlossen. Allerdings könnte sich der Dienstleister einem Regressanspruch ausgesetzt sehen, sollte der KRITIS-Betreiber seinem Arbeitnehmer gegenüber haften und die Schadenursache in der Sphäre des externen Dienstleisters liegen.

(2) Deliktische Haftung

Der externe Dienstleister kann durch die Ausführung seines Dienstes auch die Verletzung des Allgemeinen Persönlichkeitsrechts des Arbeitnehmers verursachen. Insofern kommt auch in dieser Beziehung ein Anspruch aus § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1, 1 Abs. 1 GG in Betracht.

Wie oben bereits hervorgehoben, muss berücksichtigt werden, wessen Risikosphäre das schadensursächliche Verhalten zuzurechnen ist. Das hängt wiederum von den Umständen des Einzelfalls ab. Werden beispielsweise Daten des Arbeitnehmers erhoben, weil der KRITIS-Betreiber dem externen Dienstleister keine ordnungsgemäße Anleitung bezüglich der Netzinfrastruktur bereitgestellt hat, trifft den Dienstleister kein Verschulden. Auch eine Zurechnung des Fehlverhaltens des KRITIS-Betreibers kommt nicht in Betracht. Eine Haftung des externen Dienstleisters ist damit ausgeschlossen. Ist die Rechtsverletzung jedoch

beispielsweise darauf zurückzuführen, dass der Dienstleister die Tests mit einer eigens bereit gestellten, aber veralteten und daher für die Verwendung der ITS.APT-Software unbrauchbaren Hardware durchführt, kommt eine Haftung sehr wohl in Betracht.

Außerdem könnte der externe Dienstleister aus Art. 82 DSGVO haften. Dies gilt nach Art. 82 Abs. 2 S. 2 DSGVO allerdings nur, wenn er seinen eigenen Pflichten aus der DSGVO nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des KRITIS-Betreibers gehandelt hat.

3. Datenverluste

Schlussendlich ist denkbar, dass im Rahmen der Messung des IT-Sicherheitsbewusstseins der Mitarbeiter Daten gelöscht oder verändert werden. Hierbei könnten Daten der Arbeitnehmer, Vertragspartner oder unbeteiligter Dritten betroffen sein. Auch in diesem Szenario ist abermals zwischen der Haftung des KRITIS-Betreibers (1.) und der des externen Dienstleisters (2.) zu differenzieren.

a) Verwendung der ITS.APT Lösung durch den KRITIS-Betreiber selbst

Im Rahmen einer Vertragsbeziehung stellt sich die schuldhafte Verursachung eines Datenverlusts beim Vertragspartner des KRITIS-Betreibers als Pflichtverletzung dar. Insofern ist das Haftungsrisiko mit dem in den anderen Szenarien vergleichbar.

Deliktsrechtlich bedürfte es allerdings einer Rechts- bzw. Rechtsgutsverletzung. Bei bloßen Datenverlusten ist umstritten, ob diese bereits eine Eigentumsverletzung darstellen können. Denn ein Datenträger wird nicht in seiner Substanz oder Funktionsfähigkeit beeinträchtigt, soweit ein Datenverlust erfolgt. Da jedoch in der Rechtsprechung auch ein Datenverlust bereits als Eigentumsverletzung qualifiziert worden ist, kann ein Haftungsrisiko insofern nicht gänzlich ausgeschlossen werden.

Sofern bereits materielle Schäden eingetreten sind, ist der Sachverhalt vergleichbar mit dem des ersten Haftungsszenarios. Der KRITIS-Betreiber muss daher die Kosten für eine Wiederherstellung der Daten tragen.

Gegenüber der deliktischen Haftung hervorzuheben ist, dass der Datenverlust an sich bereits einen Verstoß gegen die DSGVO darstellt und somit eine Haftung nach Art. 82 DSGVO verursachen kann. Dies betrifft jedoch nicht solche Daten, die keinen Personenbezug aufweisen. Insofern wäre der Anwendungsbereich der DSGVO bereits nicht eröffnet, Art. 2 DSGVO. Gemäß Art. 5 Abs. 1 lit. f DSGVO müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit dieser Daten gewährleistet,

einschließlich Schutz vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Schädigung („Integrität und Vertraulichkeit“). Bei Vorliegen der übrigen Voraussetzungen (siehe dazu bereits oben) ergibt sich also ein Anspruch aus Art. 82 DSGVO gegen den Betreiber als Verantwortlichen.

b) Verwendung der ITS.APT-Lösung durch einen externen IT-Dienstleister

aa) Haftung des KRITIS-Bertreibers

Auch in dieser Konstellation gilt das gleiche wie im Rahmen der anderen Szenarien. Der KRITIS-Betreiber haftet demnach, sofern er den externen Dienstleister unsorgfältig auswählt oder überwacht hat oder sofern der schadensursächliche Umstand in seine Risikosphäre fällt. Hervorzuheben ist abermals die Haftung aus Art. 82 DSGVO. Der Verantwortliche bleibt in dem Fall weiterhin im Außenverhältnis verantwortlich, auch wenn der externe Dienstleister den Schaden verursacht hat. Erst wenn er nachweisen kann, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist, scheidet die Haftung aus.

bb) Haftung des externen Dienstleisters

Erkennt man den Datenverlust bereits als Eigentumsverletzung an oder ist es aufgrund des Datenverlusts in der Folge zu einer Rechts- oder Rechtsgutsverletzung im Sinne des § 823 Abs. 1 BGB gekommen, kann eine deliktische Haftung nach den o.g. Grundsätzen bestehen. Im Übrigen besteht ein Anspruch aus Art. 82 DSGVO unter den oben genannten Voraussetzungen.

II. Handlungen zur Haftungsreduzierung

Im ersten Abschnitt dieses Dokuments wurden die Risiken einer Haftung aufgezeigt. Daran anknüpfend wird im Folgenden aufgezeigt, wie diese Risiken minimiert werden können. Aus dem oben Gesagten, insbesondere den unterschiedlichen Haftungsszenarien, ergeben sich dabei vier grundlegende Handlungsempfehlungen. Durch Befolgung dieser Empfehlungen können sowohl der KRITIS-Betreiber als auch ein externer Dienstleister dafür Sorge tragen, dass ein Schadenseinritt weniger wahrscheinlich wird. Dabei gilt stets zu beachten, dass nicht nur Schäden aufgrund eigenen Fehlverhaltens, sondern, wegen entsprechender Zurechenbarkeit, auch das Fehlverhalten Anderer vermieden werden muss.

Die folgenden Grundregeln knüpfen zunächst an der internen Organisation eines Betriebs an (I.). Sodann wird die Bedeutung von der Definition geeigneter Testbereiche (II.) und von

der Durchführung von Testläufen (III.) beleuchtet. Zuletzt wird das zentrale Thema des Arbeitnehmerdatenschutzes angeführt (IV.).

1. Organisationspflichten

Aufgrund der aufgezeigten Haftungsrisiken ist zunächst zu empfehlen, die Messung des IT-Sicherheitsbewusstseins sorgfältig zu organisieren. Dies betrifft in erster Linie den KRITIS-Betreiber, da schließlich in seinem Betrieb getestet wird. Eingeschränkt gilt es aber auch für den externen Dienstleister. Insbesondere können ihn Aufklärungspflichten hinsichtlich anzusprechender Risiken treffen.

Daher ist die innerbetriebliche Organisation derart zu strukturieren, dass Schädigungen Dritter möglichst vermieden werden. Dies umfasst zunächst die Obliegenheit, die Personen sorgfältig auszuwählen, die mit der Durchführung des Tests betraut sind. Darüber hinaus muss sichergestellt werden, dass diese Personen auch weiterhin verlässlich sind. Daher geht die Pflicht einer ordnungsgemäßen Auswahl in die Pflicht einer ordnungsgemäßen Leitung und Überwachung über.

Wie umfassend die jeweiligen Auswahl-, Überwachungs- und Leitungspflichten gestaltet sind, hängt wiederum vom Grad der Komplexität, der erforderlichen Verlässlichkeit und der Gefährlichkeit einer Tätigkeit ab. Da sich das ITS.APT-Framework an Fachpersonal richtet, ist ein vertieftes Wissen in den entsprechenden Bereichen (Netzwerkadministration etc.) zu verlangen. Diese Sachkunde und die erforderliche Zuverlässigkeit sollte mit Hilfe von geeigneten Nachweisen überprüft werden. Des Weiteren müssen die Personen, die den Test durchführen, hinreichend kontrolliert werden. Dabei bezieht sich die Kontrolle sowohl auf die Testphase als auch auf eventuelle Vor- und Nachbereitungsphasen. Außerdem müssen diese Personen derart instruiert werden, dass keine Schäden entstehen. Da die Anwendung der ITS.APT-Software auf die konkrete IT Umgebung angepasst werden muss, sind den Testern in dem Zusammenhang insbesondere alle dafür notwendigen Informationen zur Verfügung zu stellen. Um nachzuweisen, dass solche Kriterien erfüllt wurden, empfiehlt sich eine entsprechende schriftliche Protokollierung. Ergänzende Hinweise, wie die Anforderungen an die interne Organisation konkret umzusetzen sind, können der ISO-Norm 27001 sowie Best-Practice Katalogen des BSI entnommen werden, vgl. oben, Teil J I. 1. a) bb) (1).

Neben dieser personellen Perspektive fällt es aber – wie im Haftungsszenario der Nichtverfügbarkeit von Anwendungen erläutert – ebenfalls unter den Begriff der Organisationspflicht, die nötigen technischen Voraussetzungen zu schaffen. Dazu zählt insbesondere das Bereitstellen der erforderlichen aktuellen Hard- und Software.

2. Definition geeigneter Testbereiche

Ein Schadenseintritt ist auch bei Einhaltung aller Organisationspflichten gelegentlich unvermeidlich. Für diesen Fall sollte jedoch von vornherein gewährleistet sein, dass von einem möglichen Schaden nur solche Unternehmensbereiche betroffen sein können, die nicht systemrelevant sind. Der Test ist daher so zu gestalten, dass er nur solche Unternehmensbereiche berührt, die strukturell nicht essentiell für den Betrieb sind. Aufgrund des Wissensvorsprung richtet sich diese Empfehlung insbesondere an KRITIS-Betreiber, unabhängig davon, ob dieser selbst die Tests durchführt oder von einem Externen durchführen lässt. Für den externen Dienstleister besteht jedoch die Pflicht, den Betreiber auf solche Risiken hinzuweisen und ihm die hier genannten Maßnahmen zu empfehlen.

Die Testbereiche sollten anhand ihres jeweiligen Gefahrenpotenzials definiert werden. Dabei sind zum einen die genannten Haftungsszenarien zu berücksichtigen aber auch sonstige Umstände wie die allgemeine Ablenkung der Mitarbeiter durch die Tests. Wird das IT-Sicherheitsbewusstsein beispielsweise in einem Wasserwerk gemessen, ist zu gewährleisten, dass Phishing-Mails niemals an Personen gesendet werden, die in der Steuerzentrale arbeiten. Entsprechend ist in einem Krankenhaus zu gewährleisten, dass das oben angeführte Szenario der „Nichtverfügbarkeit“ niemals das IT-System betrifft, das für lebenserhaltende Maßnahmen verantwortlich ist. Gleichzeitig sollten auch nicht solche Computer von dem Test erfasst werden, die von Personen benutzt werden, die eine zentrale Position im Unternehmen bekleiden und auf die ständige Verfügbarkeit des Computers angewiesen sind.

Aus diesen Überlegungen ergibt sich, dass die Testbereiche nicht nur abstrakt definiert werden müssen, sondern auch, dass diese Definition technisch umgesetzt werden muss.

3. Sicherheitsmaßnahmen im Vorfeld der Testdurchführung

Sind die Testbereiche festgelegt worden, sollten vor der tatsächlichen Testdurchführung Sicherheitsmaßnahmen erfolgen, um etwaige Risiken zu entdecken und solchen vorzubeugen.

Zu diesen gehören insbesondere entsprechende Testläufe. Diese können so gestaltet werden, dass vorerst nur vereinzelte Artefakte an einen Arbeitnehmer bzw. an einen Test-Rechner gesendet werden. Insoweit kann überprüft werden, ob der ITS.APT-Test bereits technisch funktioniert. Auch sollten verschiedene Systemkonfigurationen überprüft werden. Zu bedenken sind außerdem „irrationale“ Reaktionen der getesteten Mitarbeiter. Beispielsweise ist es denkbar, dass diese den Computer nicht ordnungsgemäß herunterfahren, indem sie etwa den Stecker ziehen. Trotzdem muss die technische Funktionsfähigkeit beim nächsten Start gewährleistet werden.

Besitzt die Kritische Infrastruktur einen IT-Help Desk oder eine ähnliche Abteilung, die Mitarbeitern bei IT-Problemen hilft, ist diese zu informieren, um den getesteten Personen angemessen Ratschläge erteilen zu können. Schließlich sind die jeweiligen Sicherheitsmaßnahmen schriftlich festzuhalten.

4. Überwachung des Tests an sich, keine unzulässige Datenverarbeitung

Die konkrete Testdurchführung ist selbstverständlich durch geeignetes Personal ständig zu überwachen. Treten während des Tests Probleme auf, ist auf diese fachgerecht zu reagieren.

Auch ist zu gewährleisten, dass keine unzulässigen Daten verarbeitet werden. Demnach dürfen im Rahmen der Messung des IT-Sicherheitsbewusstseins keine personenbezogenen Daten erhoben werden, soweit dies nicht ausdrücklich durch eine Rechtsgrundlage gedeckt ist. Das bedeutet zum einen keine personenbezogenen Daten Dritter zu erheben und zum anderen personenbezogene Daten der getesteten Arbeitnehmer nur in dem Rahmen zu erheben wie dies die zu schließende Betriebs- bzw. Dienstvereinbarung erlaubt. Beispielsweise dürfen aus dem Grund keine Daten, insbesondere Reaktionsdaten, erhoben werden, die einen Rückschluss auf die private Lebensführung erlauben.

Bezüglich der spezifischen Anforderungen des Datenschutzrechts wird auf die detaillierten Ausführungen in diesem Dokumenten hingewiesen. Insbesondere ist in dem Zusammenhang auf die erforderliche Datenschutz-Folgenabschätzung hinzuweisen.

- Zur Reduzierung von Haftungsrisiken muss der KRITIS-Betreiber oder ggf. ein externer IT-Dienstleister seine sog. Organisationspflichten erfüllen, d.h. die mit der Testdurchführung betrauten Personen sorgfältig auswählen und überwachen.
- Die Tests sollten nur in Bereichen stattfinden, in denen keine gravierenden Schäden möglich sind, also bspw. nicht auf der Intensivstation einen Krankenhauses,
- Im Vorfeld sind Testläufe durchzuführen.
- Eine unzulässige Datenverarbeitung ist zu unterlassen.

Annex I – Muster-Dienst-/Betriebsvereinbarung

VEREINBARUNG

zwischen dem

[KRITS-Betreiber]

und

dem [Personalrat des KRITIS-Betreibers]

Präambel

Die vorliegende Vereinbarung ermöglicht die Durchführung eines IT-Sicherheits- und Datenschutz Penetration und Awareness Tests bei [KRITS-Betreiber]. Gegenstand dieser Methode ist die Erfassung des IT-Sicherheitsbewusstseins der Beschäftigten unter normalen Arbeitsbedingungen. Diese Dienstvereinbarung regelt die dafür notwendige Datenverarbeitung und -nutzung, sowie die Rechte der betroffenen Beschäftigten und dient dazu, die Mitbestimmungsrechte des unterzeichnenden Personalrats zu wahren.

§ 1 Geltungsbereich

Diese Dienstvereinbarung gilt

(1) in personeller Hinsicht für alle Beschäftigten des [KRITS-Betreibers] aus folgenden Dezernaten/Bereichen:

   (a) [Dezernat/Bereich]

   (b) [Dezernat/Bereich]

   Es werden nur Personen berücksichtigt, die aktiv eine [KRITS-Betreiber]-Benutzerkennung verwenden. Damit sind von dem Projekt ca. [Anzahl] Beschäftigte betroffen.

(2) In sachlicher Hinsicht für die Testdurchführung und das damit verbundene Erheben, Speichern, Übermitteln und Auswerten von Beschäftigtendaten sowie für die Durchführung von Schulungen.

§ 2 Technisch-organisatorischer Hintergrund

(1) Um das IT-Sicherheitsbewusstsein der Beschäftigten zu messen und zu verbessern, werden typische IT-sicherheits-relevante Vorfälle simuliert und ausgewählte Reaktionen der Beschäftigten im Sinne der §§ 3 und 6 Abs. 2 auf die Simulation erfasst, gespeichert und ausgewertet. Im Anschluss wird an die Beschäftigten ein Online-Fragebogen verschickt, in dem verschiedene persönliche Daten und Parameter zum jeweiligen IT-Sicherheitsbewusstsein abgefragt werden. Anhand der gewonnenen Ergebnisse und unter Zugrundelegung psychologischer Erkenntnisse werden die Beschäftigten in IT-sicherheitskonformem Verhalten geschult. Im Anschluss daran werden erneut Tests durchgeführt und ein Online-Fragebogen verschickt, um zu überprüfen, ob mit Hilfe der Schulung eine Verbesserung des IT-Sicherheitsbewusstseins erreicht werden konnte.

(2) In den Tests werden insbesondere folgende typische IT-sicherheits-relevante Vorfälle simuliert:
- Versand von Test-Phishing-Mails an die dienstliche E-Mail-Adresse der Beschäftigten
- Öffnen von Dateien unbekannter und damit nicht vertrauenswürdiger Herkunft
- Reaktion auf unvertrautes Verhalten des Computers etwa Pop-Ups bei der Anmeldung
- Zertifikatswarnungen bei der Benutzung von Internet-Browsern

(3) Sämtliche IT-Sicherheits-relevanten Vorfälle sind so konzipiert, dass sie die Beschäftigten nicht mehr als unbedingt notwendig von ihrer Arbeit ablenken.

§ 3 Ermittlung des IT-Sicherheitsbewusstseins

(1) Zur Ermittlung des IT-Sicherheitsbewusstseins werden Reaktionen der Beschäftigten auf die simulierten IT-Sicherheitsvorfälle erfasst. Anschließend werden sie danach ausgewertet, ob sie für einen potentiellen Angreifer hinderlich oder förderlich sind.

(2) Eine förderliche Reaktion auf IT-Sicherheits-relevante Vorfälle ist insbesondere anzunehmen, wenn der Beschäftigte:
- eine Test-E-Mail öffnet
- auf den Link in einer Test-E-Mail klickt
- einen Anhang einer Test-E-Mail öffnet
- Sicherheitswarnungen oder Pop-Ups ignoriert

Eine hinderliche Reaktion ist insbesondere anzunehmen, wenn der Beschäftigte:
- eine Test-E-Mail ignoriert
- den IT-Service Desk kontaktiert

§ 4 Zeitraum der Tests

(1) Die erste Testphase soll im [X. Quartal] stattfinden.
(2) Die zweite Testphase soll im [X. Quartal] stattfinden.
(3) Der Personalrat wird über das genaue Datum und die Zeit, in der die Tests stattfinden, vorab informiert.

§ 5 Schulungen

(1) Im Anschluss an die Testphase werden Schulungen von [Name] durchgeführt. Zuständig für die Organisation ist [Name].
(2) Die Schulungen sollen einen verantwortungsbewussten Umgang mit IT-Geräten vermitteln, um das IT-Sicherheitsbewusstsein der Beschäftigten zu verbessern.
(3) Die Kosten der Schulungen trägt der Arbeitgeber.
(4) Die Schulungen finden während der Arbeitszeit statt.
(5) Die Schulungen werden auf freiwilliger Basis stattfinden.
(6) Die Schulungen stehen allen Beschäftigen des [KRITS-Betreibers] zur Verfügung. Zur besseren Planung kann eine Anmeldepflicht eingeführt werden.

§ 6 Grundsätze der Datenverarbeitung und des Persönlichkeitsschutzes

(1) Das Erfassen, Speichern und Auswerten der Beschäftigtendaten dient ausschließlich der Projektdurchführung. Eine Weitergabe der Daten an den [Vorstand, Aufsichtsrat, Dezernatsleitungen, etc.] des [KRITIS-Betreibers] erfolgt nicht.
(2) Bei den erfassten Reaktionen der Beschäftigten auf die IT-sicherheits-relevanten Vorfälle handelt es sich lediglich um solche, die für einen potentiellen Angreifer hinderlich oder förderlich sind (vgl. § 3 Abs. 2).
(3) Die simulierten IT-Sicherheitsvorfälle sind so gestaltet, dass sie lediglich dienstliche oder neutrale Inhalte haben. Bei der Auswertung der Beschäftigtenreaktionen auf diese Vorfälle sind daher keine Rückschlüsse auf private Belange oder Interessen möglich.
(4) Inhaltsdaten werden nicht aufgezeichnet. Ebenso wenig erfolgt ein Zugriff auf persönliche Speicherbereiche. Insbesondere wird das E-Mail-Postfach der Beschäftigten nicht überwacht.
(5) Eine visuelle Überwachung der Beschäftigten erfolgt nicht.
(6) Die Ergebnisse werden nicht zur allgemeinen Leistungs- oder Verhaltenskontrolle der Beschäftigten genutzt.
(7) Disziplinarmaßnahmen oder Personalaktenvermerke dürfen aufgrund des Verhaltens in Bezug auf die simulierten IT-Sicherheitsvorfälle oder auf den Online-Fragebogen nicht erfolgen.

§ 7 Speicherung, Auswertung und Verwertung der Daten

(1) Zur Durchführung der Tests werden Verkehrsdaten „geloggt“, das heißt erfasst und gespeichert. „Verkehrsdaten“ sind solche Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Es werden nur Daten von Beschäftigten erfasst, die auch am Test teilnehmen. Im konkreten Zusammenhang handelt es sich um:
   - zur Identifizierung der/des Beschäftigten: IP-Adresse des genutzten PCs, interne Benutzerkennung, Zeitstempel, Daten über die Reaktion auf den simulierten IT-Sicherheitsvorfall, vgl. §§ 3 und 6 Abs. 2 dieser Dienstvereinbarung;
   - die Telefonanlage als Teil des IT-Systems. In diesem Zusammenhang werden folgende Daten geloggt: Apparat-Kennung, Verbindungsaufbau bzw. -versuch vom Telefonapparat des Arbeitsplatzes ausschließlich zum IT-Service Desk, Zeitpunkt des Verbindungsaufbaus bzw. -versuchs, Wartezeit. Die Daten werden nur geloggt, wenn es sich um eine Verbindung zum IT-Service Desk handelt.

(2) Das Logging erfolgt durch eine Software, die in die IT des KRITIS-Betreibers eingebracht wird. Die Software wird auf einem eigenen Server betrieben, der nur zur Durchführung der Tests mit der bestehenden IT des KRITIS-Betreibers verbunden wird. Die Installation und Durchführung erfolgt unter Anleitung von […], durch Beschäftigte der […].Andere Personen erhalten keinen Zugriff auf das für Test und Logging verwendete IT-System und die dort gespeicherten Daten.

(3) Für den KRITIS-Betreibersind die geloggten Verkehrsdaten personenbeziehbare Daten, da die Nutzung der Telekommunikationsmittel anhand der internen Benutzerkennung der/dem einzelnen Beschäftigten zugeordnet werden kann. Auch die Verkehrsdaten möglicher Telefonate sind personenbeziehbar.

(4) Der KRITIS-Betreiber fügt die geloggten Daten zu Profilen zusammen. Hierbei erfolgt zugleich eine teilweise Aggregation der Verkehrsdaten.

   Jedes Profil enthält folgende Informationen:

   - Nutzerkennung (im Folgenden: „Pseudonym“), die sich von der internen Nutzerkennung unterscheidet
   - Reaktion auf Präsentation des IT-sicherheits-relevanten Vorfalls
   - Zeitpunkt der Wahrnehmung des IT-sicherheitsrelevanten Vorfall und der Reaktion (Skalierung: stundenweise)

   Die [zuständige Abteilung] des KRITIS-Betreibers [Beispiel] hält die Zuordnungsfunktion unter Verschluss. Aus Sicht von Dritten sind die Profile damit pseudonym.

(5) Zur Entwicklung von Schulungskonzepten ist es von Vorteil, Aussagen über das IT-Sicherheitsbewusstsein bestimmter Gruppen treffen zu können. Daher werden über die

Verkehrsdaten hinausgehende Personaldaten und Auskünfte zum persönlichen IT-Sicherheitsbewusstsein erfasst und den Profilen hinzugefügt. Ihre Erhebung erfolgt direkt bei den Beschäftigten und ist freiwillig. Dazu wird ein Online-Fragebogen per E-Mail von der Stabstelle IT [Beispiel] an die Beschäftigten verschickt wird, die an dem Test teilgenommen haben. Darin befindet sich ein personalisierter Link, der unter Verwendung des Pseudonyms des Beschäftigten zu dem Online-Fragebogen führt. Durch das anschließende Ausfüllen des Online-Fragebogens werden die Personaldaten dem Profil des/der Beschäftigten hinzugefügt.

(6) Bei den Personaldaten gem. Abs. 5 handelt es sich um folgende Daten:

- Altersgruppe
- Geschlecht
- Arbeitsbereich/Position
- Dienstalter
- Ausreichende Sprachkenntnis
- Höchster Bildungsabschluss
- Häufigkeit der PC-Arbeitsplatz Nutzung (Ein-/Ausloggen pro Tag/Woche)

Bei den Auskünften zum IT-Sicherheitsbewusstsein handelt es sich um ca. 30 Fragen, mit dessen Hilfe das eigene IT-Sicherheitsbewusstsein eingeschätzt werden soll. Die Beantwortung dauert ca. 15 Minuten.

(7) Um zu erfassen, welche Testpersonen auch an der Schulung teilgenommen haben, wird der Schulungsakademie des KRITIS-Betreibers [Beispiel] eine Namensliste zur Verfügung gestellt. Die Akademie protokolliert, ob die aufgelisteten Personen an der Schulung teilgenommen haben und übergibt im Anschluss an die Schulung das Protokoll an die [zuständige Abteilung]. Diese fügt die Information, ob eine getestete Person an der Schulung teilgenommen hat, dem Profil hinzu.

(8) Ein Zugriff auf sämtliche personalisierten Daten, die im Rahmen des Projekts erhoben werden, darf ausschließlich durch die [zuständige Abteilung] erfolgen. Ein Zugriff darf nur zur technischen Störungsbeseitigung, zur Durchsetzung der Betroffenenrechte o erfolgen.

§ 8 Aufbewahrung und Löschung der Daten

(1) Alle aufgrund dieser Dienstvereinbarung erhobenen Daten werden zum frühestmöglichen Zeitpunkt anonymisiert; spätestens jedoch nach Ablauf des vorgesehenen Gesamtzeitraums für die Tests und die Schulungen. Technisch wird dies umgesetzt, indem die Zuordnungsfunktion gelöscht wird. Eine Zuordnung der Daten zu einer konkreten Person ist damit für Jedermann unmöglich.

(2) Das Recht der Betroffenen auf Löschung gem. [genaue datenschutzrechtliche Norm nennen] bleibt hiervon unberührt.

(3) Es werden technische und organisatorische Maßnahmen ergriffen, die sicherstellen, dass die Verfügbarkeit, Integrität und Vertraulichkeit der erhobenen Daten gewährleistet wird.
(4) Der Datenschutzbeauftragte des KRITIS-Betreibers führt ein Verzeichnis, in dem weitere Details zur Verarbeitung der Daten dokumentiert sind und das eingesehen werden kann.

§ 9 Rechte der Betroffenen

(1) Alle Betroffenen haben das Recht, Auskunft über ihre personenbezogenen Daten, die im Rahmen des Projekts erhoben wurde, zu erhalten.
(2) Alle Betroffenen haben das Recht ihre im Rahmen des Projekts gespeicherten personenbezogenen Daten berichtigen zu lassen.
(3) Alle Betroffenen haben das Recht ihre im Rahmen des Projekts erhobenen personenbezogenen Daten löschen zu lassen oder dessen weitere Verarbeitung zu untersagen. Macht eine betroffene Person von diesem Recht Gebrauch, wird der entsprechende Datensatz gem. § 8 Abs. 1 anonymisiert.
(4) Sämtliche Ansprüche der Betroffenen sind an die [zuständige Abteilung] zu richten.

§ 10 Rechte des Personalrats und des Datenschutzbeauftragten

(1) Der Personalrat hat das Recht eine Person zu bestimmen, die während der Durchführung der Tests und der Durchführung der Schulung anwesend ist.
(2) Der Datenschutzbeauftragte hat das Recht während der Durchführung der Tests anwesend zu sein.

§ 11 Bekanntmachung

Die Dienstvereinbarung ist allen betroffenen Beschäftigten zugänglich zu machen.

§ 12 Inkrafttreten und Geltungsdauer

(1) Diese Dienstvereinbarung tritt am … in Kraft. Sie endet am […]. Die Dienstvereinbarung kann mit einer Frist von 6 Monaten gekündigt werden.
(2) Bis zum Inkrafttreten einer neuen Dienstvereinbarung gilt die bisherige Dienstvereinbarung weiter.

Annex II – Musterverfahrensverzeichnis

Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 DSGVO

Aktenzeichen: _____ ☒ neues Verfahren ☐ Änderung

Erstellungsdatum des Verfahrensverzeichnisses _____

1 Name und Anschrift der Daten verarbeitenden Stelle

Name und Anschrift *KRITIS-Betreiber*
Fachbereich, Abteilung, ggf. Sachgebiet
Kontaktdaten für Betroffene

2 Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung

Zweckbestimmung *Durchführung eines Feldtests (sog. penetration test) bei [KRITIS-Betreiber] um das IT-Sicherheitsbewusstsein der Beschäftigten zu messen und zu verbessern. Es wird eine Simulation von [Maßnahmen, z.B. Phishing-Mails, Virenmeldungen, Zertifikatswarnungen (Internet-Browser) etc.] durchgeführt und die Reaktion der Beschäftigten auf diese erfasst, gespeichert und ausgewertet. Anhand der gewonnenen Ergebnisse und unter Zugrundelegung psychologischer Erkenntnisse werden die Beschäftigten in IT-sicherheitskonformem Verhalten geschult. Im Anschluss daran werden erneut Tests durchgeführt, um zu überprüfen, ob mit Hilfe der Schulung eine Verbesserung*

des IT-Sicherheitsbewusstseins erreicht werden konnte.
Rechtsgrundlage (ggf. nach Art der Datenverarbeitung unterscheiden) *Art. 88 Abs. 1 DSGVO i.V.m. § 26 BDSG gestattet die Verarbeitung von personenbezogenen Beschäftigtendaten*

3 Kreis der Betroffenen

lfd. Nr.	Betroffene Person oder Betroffenengruppen
1	*[Anzahl und betroffene Abteilungen]*

4. Kategorien der verarbeiteten Daten und deren Löschungs- bzw. Aufbewahrungsfristen

4.1 Kategorien der verarbeiteten Daten

lfd. Nr.	Kategorien	Daten nach Art. 9, 10 DSGVO (ja/nein)
1	• *IP-Adresse des genutzten PC,* • *interne Benutzerkennung,* • *Zeitstempel,* • *Daten über Aktivitäten im Zusammenhang mit der empfangenen Test-Phishing-Mail (öffnen, als gelesen markieren, weiterleiten, beantworten, löschen, es werden keine Inhaltsdaten erfasst)*	*nein*
2	*Daten der Telefonanlage, soweit sie von den ausgewählten Probanden genutzt werden, um den IT-Help-Desk während der Versuchszeit zu kontaktieren* • *Apparat-Kennung,* • *Verbindungsaufbau bzw. -versuch vom Telefonapparat des Arbeitsplatzes,* • *Zeitpunkt des Verbindungsaufbaus bzw. -versuchs,* •	*nein*
3	*Durch den freiwilligen Online-Fragebogen*	

	• *Altersgruppe* • *Geschlecht* • *Arbeitsbereich/Position* • *Dienstalter* • *Höchster Bildungsabschluss* • *Häufigkeit der PC-Arbeitsplatz Nutzung (Ein-/Ausloggen pro Tag/Woche)*	
4	*Teilnahme der Probanden an Schulungen zur IT-Sicherheit (Ja/Nein)*	*nein*

4.2 Löschungs- und Aufbewahrungsfristen

lfd. Nr. aus 4.1 (Daten-Kategorie)	**Wie lange werden die gespeicherten Daten aufbewahrt bzw. wann werden sie gelöscht?**
1-4	*Anonymisierung zum frühestmöglichen Zeitpunkt, spätestens jedoch nach Abschluss der Tests am [Datum]. Die Rechte der betroffenen Personen nach Art. 16-18 und 21 DSGVO bleiben hiervon unberührt. .*

4.3. Zugriffsberechtigte Personen oder Personengruppen

lfd. Nr. aus 4.1 (Daten-Kategorie)	**Welche Personen oder Personengruppen dürfen auf die gespeicherten Daten zugreifen?**
1-4	*[zuständige Abteilung des KRITIS-Betreibers]*

5. Datenübermittlung

5.1 Empfänger von zu übermittelnden Daten

lfd. Nr. aus 4.1 (Daten-Kategorie)	**An welche Stellen werden Daten übermittelt?**

1-4	*[ggf. IT-Dienstleister]*

5.2 Herkunft empfangener Daten

lfd. Nr. aus 4.1 (Daten-Kategorie)	**Von welchen Stellen werden Daten empfangen?**
2	
4	

6 Übermittlung an Stellen außerhalb der Mitgliedstaaten der Europäischen Union

☐	nein	☐	ja (aufgeführt in Punkt 5.2)

7 Allgemeine Beschreibung der nach den §§ 5 und 6 LDSG zur Einhaltung der Datensicherheit getroffenen Maßnahmen

-

8 Datenschutzrechtliche Beurteilung

8.1 Rechtsgrundlagen und Zweckbestimmung

8.2 Technisch-organisatorische Maßnahmen

Verfügbarkeit (Wie wird gewährleistet, dass Verfahren und Daten zeitgerecht zur Verfügung stehen?):

Vertraulichkeit (Wie wird gewährleistet, dass nur befugte Personen auf Daten und Verfahren zugreifen?):

Integrität (Wie wird gewährleistet, dass Daten unversehrt, vollständig, zurechenbar und aktuell bleiben?):

Transparenz (Wie wird gewährleistet, dass die automatisierte Verarbeitung von Daten mit zumutbaren Aufwand nachvollzogen, überprüft und bewertet werden kann):

Intervenierbarkeit (Wie kann die Daten verarbeitende Stelle nachweisen, dass sie den Betrieb ihrer informationstechnischen Systeme steuernd beherrscht und dass Betroffene die ihnen zustehenden Rechte ausüben können?):

Nicht-Verkettbarkeit (Wie wird sichergestellt, dass Daten nur zu dem ausgewiesenen Zweck automatisiert erhoben, verarbeitet und genutzt werden):

Literaturverzeichnis

Art. 29 Datenscschutzgruppe	Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. 4. April 2017, abrufbar unter: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=44137.
Brink, Stefan	Empfehlungen zur IuK-Nutzung am Arbeitsplatz, ZD 2015, 295-300 (Zitiert als: *Brink*, ZD 2015, 295)
Bundesamt für Sicherheit in der Informationstechnik, BSI (Hrsg.)	Schutz Kritischer Infrastrukturen durch IT-Sicherheitsgesetz und UP KRITIS, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Schutz-Kritischer-Infrastrukturen-ITSig-u-UP-KRITIS.pdf?__blob=publicationFile&v=5
Bundesamt für Sicherheit in der Informationstechnik, BSI (Hrsg.)	Die Lage der IT-Sicherheit in Deutschland 2016, abrufbar unter: www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/2016_16_11_Lagebericht2016.pdf?__blob=publicationFile, zuletzt aufgerufen am 16.10.2017 (Zitiert als: Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2016, S.)
Datenschutzkonferenz, DSK (Hrsg.)	„Das Standard-Datenschutzmodell - Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele." V1.0., 2016, abrufbar unter: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/
Datenschutzkonferenz, DSK (Hrsg.)	Kurzpapier Nr. 5, Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO, 2017, abrufbar unter:

	https://www.lda.bayern.de/media/dsk_kpnr_5_dsfa.pdf.
Däubler, Wolfgang / Klebe, Thomas / Wedde, Peter / Weichert, Thilo	Bundesdatenschutzgesetz, 4. Auflage, Frankfurt 2013 (Zitiert als: Däubler/Klebe/Wedde/Weichert/*Bearbeiter*, BDSG, § Rn.)
Friedewald, Michael / Bieker, Felix / Obersteller, Hannah, u.a.	White Paper Datenschutz-Folgenabschätzung – Ein Werkzeug für einen besseren Datenschutz, 3. Auflage 2017, abrufbar unter: https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum-Privatheit-WP-DSFA-3-Auflage-2017-11-29.pdf.
Geppert, Martin /Schütz, Raimund (Hrsg.)	Beck'scher TKG Kommentar, 4. Auflage, München 2013 (Zitiert als: BeckTKG/*Bearbeiter*, § Rn.)
Gersdorf, Hubertus / Paal, Boris (Hrsg.)	Beck'scher Online-Kommentar Informations- und Medienrecht, 15. Edition, München 2017 (Zitiert als: BeckOK InfoMedienR/*Bearbeiter*, Gesetz, § Rn.)
Gola, Peter (Hrsg.)	DS-GVO – Datenschutzgrundverordnung VO (EU) 2016/679 – Kommentar, 1. Aufl. 2017 (Zitiert Gola/*Bearbeiter*, DSGVO, Art. Rn.)
ITS.APT Projekt (Hrsg.)	ITS.APT-Projekt, Tim Hey, Robert Ortner, Meiko Jensen, Hannah Obersteller, Arbeitsrechtliche Risikoabschätung – Projekt ITS.APT Deliverable 2.1, 2016.
ITS.APT Projekt (Hrsg.)	ITS.APT-Projekt, Tim Hey, Robert Ortner, Meiko Jensen, Hannah Obersteller, Arbeitsrechtliche Risikoabschätung – Projekt ITS.APT Deliverable 2.1, 2016.
Kopp, Reinhold / Sokoll, Karen	Wearables am Arbeitsplatz – Einfallstore für Alltagsüberwachung?, NZA 2015, 1352-1359 (Zitiert als: *Kopp/Sokoll*, NZA 2015, 1352 (Fundstelle))

Kühling, Jürgen / Buchner, Benedikt (Hrsg.)	Datenschutz-Grundverordnung Kommentar, 1. Auflage, München 2017 (Zitiert als: Kühling/Buchner/*Bearbeiter*, DSGVO, Art. Rn.)
Paal, Boris / Pauly, Daniel (Hrsg.)	Beck'sche Kompakt- Kommentare Datenschutz-Grundverordnung, 1. Auflage, München 2017 (Zitiert als: Paal/Pauly/*Bearbeiter*, DSGVO, Art. Rn.)
Roßnagel, Alexander	Das IT-Sicherheitsgesetz, DVBl. 2015, 1206-1212 (Zitiert als: *Roßnagel*, DVBl. 2015, 1206)
Schaffland, Hans-Jürgen / Wiltfang, Noeme (Hrsg.)	Datenschutz-Grundverordnung (DSGVO)/Bundesdatenschutzgesetz (BDSG) Kommentar, Loseblattsammlung (Zitiert als: Schaffland/Wiltfang/*Bearbeiter*, DSGVO, Art. Rn.)
Spindler, Gerald / Schuster, Fabian	Recht der elektronischen Medien Kommentar, 3. Auflage, München 2015 (Zitiert als: Spindler/Schuster/*Bearbeiter*, Teil, Rn. in §)
Wolff, Heinrich Amadeus / Brink, Stefan (Hrsg.)	Beck'scher Online-Kommentar Datenschutzrecht, 19. Edition, München 2017 (Zitiert als: BeckOK/*Bearbeiter,* Gesetz, Rn. in § oder Art.)
Wybitul, Tim	Neue Spielregeln bei Betriebsvereinbarungen und Datenschutz – BAG schafft Klarheit zu Anforderungen an Umgang mit Arbeitnehmerdaten, NZA 2014, 225-232 (Zitiert als: *Wybitul*, NZA 2014, 225)
Wybitul, Tim	E-Mail-Auswertung in der betrieblichen Praxis, NJW 2014, 3605-3611 (Zitiert als: *Wybitul*, NJW 2014, 3605)