KRAUSE & KOLLEGEN

Fresenius

Whitepaper

Rechtskonforme Durchführung von Penetrationstests im Konzern

Dr. Arne Klaas, Krause & Kollegen

Marius Fetzberger, Fresenius SE & Co. KGaA

Fabian Zenner, Fresenius SE & Co. KGaA

Malcolm Kögler, Fresenius SE & Co. KGaA

A. Zusammenfassung

- **Ausgangspunkt**: Penetrationstest („PenTest“) weisen ein straf-, datenschutz- und zivilrechtliches (Haftungs-)Risiko auf. Das gilt insbesondere für zentral gesteuerte, gesellschaftsübergreifende IT-Sicherheitstests im Konzern.

- **Zulässigkeit von PenTests**: Pflicht *und Recht* zum Ergreifen technischer und organisatorischer Maßnahmen („TOMs“, Art. 32 Abs. 1 DSGVO, § 165 Abs. 1 Satz 1 TKG, § 19 Abs. 4 Satz 1 TDDDG, § 8a Abs. 1, 1a BSIG, § 30 Abs. 1 BSIG-E).

    - Unternehmen sind dazu verpflichtet TOMs zu ergreifen, mit denen ein unberechtigter Zugriff auf bzw. das Kompromittieren der eigenen technischen Systeme verhindert werden kann. Diese Pflichten begründen ein spiegelbildliches Recht zur Umsetzung dieser TOMs. Soweit sich die einzelnen, konkreten (Angriffs-)Maßnahmen eines PenTests auf diese Rechte stützen, werden Straftat- und Bußgeldbestände nicht verwirklicht.

    - Dieses Recht kann – je nach Struktur der Konzern-IT sowie den individuellen Vereinbarungen – sowohl ein Recht der Konzerngesellschaften als auch der Konzernmutter begründen.

    - Auch bei erlaubter bzw. tolerierter Privatnutzung schränkt die Auffassung der Datenschutzaufsichtsbehörden die Zulässigkeit des Zugriffs auf (Beschäftigten-)Daten nicht wie bei anderen Compliance-Maßnahmen ein.

    - Gute Nachricht für das IT-Department: Ob eine Angriffsmaßnahme eine legitime TOM ist, bestimmt sich nach technischen Kriterien. Die juristische und technische Bewertung laufen hier gleich. D.h. auch der Durchführende kann selbst in der konkreten Situation beurteilen, ob der PenTest sich noch im Rahmen des Zulässigen bewegt oder nicht.

- **Rechtsgestalterische Risikominimierungsmaßnahmen**: Mit rechtsgestalterischen Maßnahmen lassen sich die (straf-)rechtlichen Grenzlinien zugunsten des Unternehmens verschieben. Hierzu müssen – in einem ersten Schritt – die individuellen Betroffenen und (Verfügungs-)Berechtigten identifiziert werden.

    - Begründen vertraglicher Zugangs- und Verarbeitungsrechte mit Beschäftigten und (Konzern-)Gesellschaften und Dritten;

    - Einholen von Einverständnis-/Einwilligungserklärungen von Beschäftigten, (Konzern-)Gesellschaften und Dritten;

    - Einholen von Bestimmungserklärungen von Beschäftigten, (Konzern-)Gesellschaften und Dritten;

    - Transparente Kommunikation gegenüber datenschutzrechtlich betroffenen Personen

    - Abschluss von (Konzern-/Gesamt-)Betriebsvereinbarungen

B. Inhaltsverzeichnis

C. Überblick

Ein PenTest beschreibt die Simulation eines Angriffs auf die informationstechnische Infrastruktur einer Organisation unter Realbedingungen. Das Ziel liegt in der präventiven Identifizierung sowie anschließenden Behebung von Schwachstellen. Die Cyber-Resilienz der jeweiligen Organisation wird damit (fortlaufend) gestärkt.

Die Thematik gewinnt mit der für Oktober 2024 geplanten[1] Umsetzung der „NIS-2-Richtlinie“[2] durch das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz („NIS2UmsuCG“)[3] weiter an Relevanz. Hiermit wird die Pflicht zur Gewährleistung eines ausreichenden IT-Sicherheitsniveaus ausgeweitet. Das zu gewährleistende Schutzniveau als auch die erfassten Unternehmen werden angehoben. Neben Betreibern kritischer Anlagen sollen nun auch „besonders wichtige Einrichtungen“ und „wichtige Einrichtungen“ verpflichtet werden (§ 30 Absatz 1 BSIG-E).[4] Gleichzeitig sollen Verstöße schärfer sanktioniert werden (§ 60 Abs. 2 Nr. 2 BSIG-E).[5]

Für den Finanzsektor hält der Digital Operational Resilience Act („DORA“)[6] sogar die ausdrückliche Verpflichtung zu „bedrohungsorientierte Penetrationstests“ (TLPT – Threat-Led Penetration Testing)“ bereit. Die EU-Verordnung gilt ab dem 17. Januar 2025.

Nach wie vor herrscht große Unsicherheit im Markt, in welchen Situationen und auf welche Art und Weise PenTests rechtskonform durchgeführt werden können. Auch die NIS-2-Richtlinie[7] und der zweite Referentenentwurf zum NIS2UmsuCG[8] greifen „Penetrationstests“ bzw. „Penetrationsanalysen“ auf, ohne jedoch – anders als der für den Finanzsektor geltende DORA –

---

[1] Zum gegenwärtigen Zeitpunkt ist noch nicht absehbar, ob eine richtliniengemäße Umsetzung zum 17. Oktober 2024 (Art. 41 Abs. 1 NIS-2-RL) erfolgen wird. Siehe zum aktuellen Stand vom 24. Juni 2024: NIS2UmsuCG_Verb_ndeanh_rung_1717530796.pdf (intrapol.org) (zuletzt abgerufen am 28. Juni 2024).
[2] Richtlinie 2022/2555 vom 14. Dezember 2022.
[3] Aktueller Stand: Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (zuletzt abgerufen am 28. Juni 2024).
[4] Referentenentwurf vom 24. Juni 2024 zum NIS2UmsuCG, S. 152 f.
[5] Bei *„wichtigen Einrichtungen“*: Geldbuße bis zu 7 Millionen Euro oder mit einem Höchstbetrag von mindestens 1,4 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens (§ 60 Abs. 6 BSIG-E). Bei *„Betreiber[n] kritischer Anlagen oder (…) besonders wichtige[r] Einrichtung“*: Geldbuße bis zu 10 Millionen Euro oder mit einem Höchstbetrag von mindestens 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens (§ 60 Abs. 7 BSIG-E).
[6] VO 2022/2554 vom 14. Dezember 2022, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2554 (zuletzt abgerufen am: 27. April 2024).
[7] Erwägungsgründe 86, 87 NIS-2-RL.
[8] § 41 Abs. 5 Nr. 3 NIS2UmsuCG („Penetrationsanalysen“ als Kriterium der Vertrauenswürdigkeit des Herstellers einer kritischen Komponente)

konkretere Aussagen zu Grund und Grenzen ihrer Zulässigkeit zu machen. Als größte Sorgenfelder werden regelmäßig das Straf- und Datenschutzrecht identifiziert. Straf- und datenschutzrechtliche Verstöße bilden ihrerseits Anknüpfungspunkte für mögliche zivilrechtliche Schadensersatzansprüche gegen Gesellschaften und Leitungspersonen.

An diesem Punkt setzt das Whitepaper an. Mit diesem soll ein besseres Verständnis für die rechtlichen Rahmenbedingungen geschaffen werden. Denn erst mit Kenntnis der sich aus dem Straf- und Datenschutzrecht ergebenden *Außengrenzen* können die *innerhalb* dieses Rechtsrahmens liegenden Gestaltungsmöglichkeiten bestimmt und genutzt werden. Das Whitepaper richtet sich daher primär an die unternehmens- bzw. konzerninternen IT-(Sicherheits-)Abteilungen, die mit der tatsächlichen Durchführung von PenTests befasst sind. Zielgruppe sind aber auch externe IT-Sicherheitsunternehmen, die von Unternehmen und Konzernen mit der Überprüfung der eigenen IT-Sicherheit beauftragt werden.

Das Whitepaper berücksichtigt insbesondere auch die Besonderheiten im Konzern. Denn hier werden die Angriffssimulationen nicht ausschließlich innerhalb der eigenen Gesellschaft, sondern auch in Konzerngesellschaften durchgeführt. Hier agiert bspw. die Konzernmutter als außerhalb der untersuchten Organisation stehende Dritte.

Der Fokus liegt auf den organisatorischen Maßnahmen, die beim Aufsetzen der Prozesse ergriffen werden können, um Rechtsverstöße proaktiv und präventiv zu verhindern.

Dabei zeigt sich: Die technische Bewertung der Erforderlichkeit einzelner Angriffssimulationen bestimmt die Bewertung ihrer rechtlichen Zulässigkeit entscheidend mit. D.h.: Die Welt der Juristen auf der einen Seite und die der IT-Sicherheitstechniker auf der anderen Seite liegt sehr viel näher als regelmäßig angenommen wird. Dieser Blickwinkel hilft bei der Organisation sowie Durchführung von PenTests. Er erleichtert auch die Zusammenarbeit von Rechts- sowie IT-(Sicherheits-)Abteilungen. Daher nimmt auch dieses Whitepaper diesen Blickwinkel ein und wählt den Schulterschluss zwischen rechtlicher (Dr. Arne Klaas, Krause & Kollegen) und technischer (Marius Fetzberger, Malcolm Kögler, Fabian Zenner, jeweils Group Cybersecurity Office, Fresenius SE & Co. KGaA) Perspektive.

Das Whitepaper schließt mit einem konkreten Praxisbeispiel. Hier wird eine konkrete Angriffssimulation aus der Perspektive einer PenTesterIn Schritt für Schritt begleitet. Der PenTesterIn wird beispielhaft aufgezeigt, wie er die rechtliche (Un-)Zulässigkeit seiner einzelnen

Angriffsschritte in der konkreten Situation selbst bestimmen und damit die Angriffssimulation eigenständig durchführen kann.

Im **Annex** werden die acht Phasen eines PenTests übersichtlich dargestellt. Die Übersicht hilft bei der erstmaligen Konzeptionierung und Umsetzung eines PenTests in der eigenen Organisation.

D. Scope

Die folgenden Ausführungen beziehen sich auf die Durchführung von PenTests im privatrechtlichen Bereich, d.h. insbesondere in privat-rechtlich organisierten Unternehmen. Die Durchführung von PenTests im öffentlich-rechtlichen Bereich (d.h. sowohl *durch* Behörden in privaten Unternehmen[9] oder *im* Organisationsbereich von Behörden) folgt anderen Regeln und ist nicht Gegenstand des Whitepapers.

In technischer Hinsicht bezieht sich die Betrachtung auf die Identifizierung systemischer Schwachstellen in Software, Konfigurationen und dem infrastrukturellen Setup. Nicht umfasst sind rein physische Angriffe und social-engineering-Maßnahmen.

E. (Straf-)Rechtliche Rahmenbedingungen

Unter I. findet sich ein Überblick über die relevanten Straftatbestände mitsamt einer verständlichen (Kurz-)Erläuterung. Hiermit werden die Außengrenzen skizziert, die bei der Durchführung von PenTests nicht überschritten werden dürfen.

Unter II. wird eine einheitliche Handlungslinie vorgegeben, auf deren Grundlage diese Außengrenzen insgesamt nicht übertreten werden.

Unter III. werden weitere Maßnahmen dargestellt, mit denen das Strafbarkeitsrisiko zusätzlich gemindert wird.

[9] Vgl. Erwägungsgrund 87 NIS-2-Rl.

I. Überblick

Die (straf-)rechtlichen Grenzlinien bei der Durchführung eines PenTests werden durch die folgenden Straftatbestände abgesteckt.

Wichtig zu wissen: Der Verlauf dieser Grenzlinien kann durch den Abschluss von Verträgen, das Einholen von Einverständnis-/Einwilligungserklärungen aber auch durch faktische, äußere Umstände (bspw. eine plötzlich bekanntwerdende Sicherheitslücke) individuell verschoben werden. Hiermit befasst sich der Abschnitt ab Seite 17 ff.

- **§ 202a StGB („Ausspähen von Daten“)**: Dieser Tatbestand – auch „Hacker-Paragraph“ – genannt, ist mit am Relevantesten. Er erfasst das Überwinden von sog. Zugangssicherungen (bspw. Passwörter, Verschlüsselungen, Firewalls etc.), die PenTesterInnen von dahinter liegenden Daten trennen. Strafbar ist dies jedoch nur, soweit das Überwinden „unbefugt“ geschieht und die hierdurch geschützten Daten nicht für die PenTesterInnen „bestimmt“ sind.

- **§ 202b StGB („Abfangen von Daten“)**: Der Tatbestand weist Ähnlichkeiten zum „Hacker-Paragraphen“ auf. Abweichend hierzu muss jedoch keine Zugangssicherung überwunden werden, sondern auf Daten während eines Übertragungsvorgangs bzw. aus der elektromagnetischen Abstrahlung zugegriffen werden. Anders als bei § 202a StGB müssen die Daten tatsächlich erlangt werden. Aber auch hier gilt: Strafbar ist dies jedoch nur, soweit das Überwinden „unbefugt“ geschieht und die hierdurch geschützten Daten nicht für die PenTesterInnen „bestimmt“ sind.

- **§ 202c StGB („Vorbereiten des Ausspähens und Abfangens von Daten“)**: Der Straftatbestand bezieht sich auf die *Vorbereitung* von Handlungen, die von §§ 202a und 202b StGB erfasst werden. Die Vorbereitung kann u.a. in einem Zugänglichmachen von „Computerprogrammen“ liegen, deren Zweck die Begehung einer solchen Tat ist. Soweit die geplanten PenTesting-Maßnahmen bereits von §§ 202a, 202b StGB nicht erfasst werden, sind auch alle vorbereitenden Maßnahmen nicht nach § 202c StGB strafbar. Die von den PenTesterInnen verwendete (Hacking-)Software ist kein von § 202c StGB erfasstes „Computerprogramm“, wenn die illegale Zweckbestimmung dem Programm nicht „auf die Stirn geschrieben steht“. Besonders sicher sind solche Tools, deren

Verwendungsvorschläge/das Marketing seitens der Entwickler auf die Gewährleistung der IT-Sicherheit abzielen.

- **§ 202d StGB („Datenhehlerei")**: Die sog. „Datenhehlerei" reguliert nicht den erstmaligen Zugriff auf, sondern den nachgelagerten Umgang mit durch Straftaten erlangten Daten. D.h.: Wird bereits nicht gegen bspw. §§ 202a, 202b StGB oder § 42 BDSG verstoßen, fehlt es an einer sog. „Anknüpfungstat". Liegt ein solcher Verstoß jedoch vor und werden die dabei erlangten Daten (weiter-)verarbeitet – bspw. um weitere Schwachstellen zu finden, Systeme zu trainieren oder im Rahmen der Auswertung/Analyse –, können diese nachgelagerten Schritte von § 202d StGB erfasst werden. Damit beinhaltet § 202d StGB das Potenzial, einen gesamten PenTest sowie die nachgelagerte Auswertung zu „infizieren".

- **§ 203 StGB („Verletzung von Privatgeheimnissen")**: Dieser Straftatbestand ist insbesondere dann relevant, wenn innerhalb der Organisation Berufsgeheimnisträger beschäftigt werden (bspw. Ärzte, Wirtschaftsprüfer, Rechtsanwälte etc.). Diese dürfen die ihnen anvertrauten oder sonst bekanntgeworden Geheimnisse nicht unbefugt offenbaren. Diese Pflicht trifft auch die sog. „mitwirkenden Person". Die PenTesterInnen können u.U. als „mitwirkende Personen" angesehen werden. Denn die Durchführung der PenTests ist ein Beitrag zur Gewährleistung der gesetzlichen Verschwiegenheitspflicht durch die Ergreifung von TOMs.

- **§ 206 StGB („Verletzung des Post- und Fernmeldegeheimnisses")**: Der Tatbestand reguliert den Umgang mit Informationen, die dem Fernmeldegeheimnis unterliegen. Voraussetzung ist, dass die Organisation, welche den PenTest durchführt, „geschäftsmäßig Telekommunikationsdienste" erbringt und damit durch das Fernmeldegeheimnis verpflichtet wird. Nach einer älteren Auffassung der Datenschutzaufsichtsbehörden ist das der Fall, wenn ein Unternehmen seinen Beschäftigten die Privatnutzung des Internets bzw. betrieblichen Kommunikationsmitteln wie E-Mails/Messenger-Diensten erlaubt bzw. jedenfalls toleriert/duldet.[10] In diesem Fall wird bspw. die unbefugte Mitteilung von

[10] Siehe hierzu: DSK, Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz, S. 1 ff. (abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/201601_oh_email_und_internetdienste.pdf (zuletzt abgerufen am: 16. November 2023); LfDI Baden-Württemberg, Ratgeber Beschäftigtendatenschutz vom 1.4.2020, S. 17 f., 51 (abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/wp-

entsprechenden Inhalten oder das Einwirken auf den Übertragungsvorgang im beherrschbaren Bereich des Unternehmens von § 206 StGB erfasst.

- **§ 27 Abs. 1 Nr. 1 TDDDG (Abhörverbot nach dem TDDDG)**: Der Tatbestand erfasst das Abhören einer nicht für die PenTesterInnen bestimmten Nachricht mit einer Funkanlage. Eine „Funkanlage" ist u.a. ein Computer/Laptop, der *kabellos* mit dem Internet verbunden werden kann. „Nachrichten" sind u.a. E-Mails bzw. Messengernachrichten sowie deren kommunikativen Begleitumstände. Diese müssen unter Nutzung dieser Funkfunktion zur Kenntnis genommen werden.

- **§ 27 Abs. 2 Satz 1 TDDDG (Mitteilungsverbot nach dem TDDDG)**: Der Tatbestand stellt das Mitteilen des Inhalts von Nachrichten, die unter (1) Verstoß gegen das Abhörverbot erlangt oder (2) unbeabsichtigt empfangen wurden unter Strafe. Erfasst wird jedoch nur die Mitteilung an einen „Dritten", d.h. an eine Person die sich *nicht* am erstmaligen Zugriff auf diese Nachricht in irgendeiner Form beteiligt hat.

- **§ 303a StGB („Datenveränderung")**: Auch dieser Straftatbestand ist bei der Durchführung von PenTests besonders bedeutsam. Er stellt das Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von Daten unter Strafe. Erfasst werden im Ausgangspunkt alle Daten, über die die PenTesterInnen nicht *alleine* verfügen können. Das ist bei den sich im TOE befindlichen Daten regelmäßig der Fall. Typischerweise sind die Beschäftigten und (Konzern-)Gesellschaften mitverfügungsbefugt. Strafbar ist das Einwirken auf diese Daten jedoch nur, wenn dies „rechtswidrig" erfolgt.

---

content/uploads/2020/04/Ratgeber-Besch%C3%A4ftigtendatenschutz.pdf (zuletzt ab-gerufen am 16. November 2023). So auch: Deusch/Eggendorfer, Taeger/Pohle, Computerrechts-Handbuch, 37. EL Mai 2022, Teil 5, 50.1 Rn. 419; Mengel, NZA 2017, 1494 (1496); Kühling/Buchner/Maschmann, 3. Aufl. 2020, BDSG § 26 Rn. 50; Wolf/Mulert, BB 2008, 442 (445); Dann/Gastell, NJW 2008, 2945 (2946); Hoppe/Braun, MMR 2010, 80; Vogel/Glas, DB 2009, 1747 (1752); Schmidl, MMR 2005, 343 (344); Ernst, NZA 2002, 585 (587).

A.A.: LG Erfurt, Urteil vom 28.4.2021 – 1 HK O 43/20; vgl. LAG Köln, ZD 2020, 262 (263 Rn. 30); ArbG Weiden BeckRA 2017, 120365; LAG Berlin-Brandeburg, BB 2011, 2298; LAG Niedersachsen, NZA-RR 2010, 406. HdB DatenschutzsanktionenR/Eisele/Bechtel, 1. Aufl. 2023, § 206 Rn. 9; Wünschelbaum, NJW 2022, 1561 (1561 f. Rn. 4; 1563 ff. Rn. 10–21, 31, 34 f., 39); Aufhauser, PinG 2021, 224 (224 ff.); ders., 2021, 188 (190 f.); Rossow, DuD 2022, 93 (97); Herrmann/Zeidler, NZA 2017, 1499 (1500); Kort, ZD 2016, 555 (559); Fülbier/Splittgerber, NJW 2012, 1995 (1999 f.); Scheben/Klos/Geschonneck, CCZ 2012, 13 (16); Wybitul, ZD 2011 69 (71); Haußmann/Krets, NZA 2005 259 (260); Schimmelpfennig/Wenning, DB 2006, 2290 (2290 f.).

- **§ 303b StGB („Computersabotage“)**: Dieser Straftatbestand bezieht sich auf das Stören von Datenverarbeitungen, die für einen anderen von wesentlicher Bedeutung sind. Betroffen können insbesondere Beschäftigte sein. In Konzernsachverhalten sind es auch die Konzerngesellschaften selbst. An die „Wesentlichkeit“ einer unternehmensinternen Datenverarbeitung werden teils nur sehr niedrige Anforderungen aufgestellt. Erfasst werden in jedem Fall die Funktionsfähigkeit des Internets sowie Kommunikationsmitteln (E-Mail, Messenger, Telefon) sowie der Zugriff auf dienstliche Daten.

- **§ 269 StGB („Fälschung beweiserheblicher Daten“)**: Der Straftatbestand erfasst das Speichern bzw. Ändern von Daten, anhand derer vorgespiegelt wird, dass eine beweiserhebliche Gedankenerklärung von einer anderen Person als dem tatsächlichen Erklärenden stammt. Erfasst werden können daher im Rahmen von PenTests insbesondere Datenverarbeitungen unter der Nutzung fremder Zugangsdaten und daraus folgenden technischen Modifikationsbefugnissen.

- **§ 274 Abs. 1 Nr. 2 StGB („Urkunden-/Datenunterdrückung“)**: Der Straftatbestand erfasst das Einwirken (d.h. löschen, unterdrücken, unbrauchbarmachen, verändern) auf Daten, die zum Beweis eines Umstands bestimmt oder geeignet sind. Voraussetzung ist, dass zumindest auch eine andere Person als die PenTesterInnen ein Mitverfügungsrecht an den Daten hat. Typischerweise haben Beschäftigte an elektronisch gespeicherten Vertragsdokumenten, Zeiterfassungsinformationen oder an Log-Daten ein (Mit-)Verfügungsrecht. Die zusätzliche „Nachteilszufügungsabsicht“ liegt bereits dann vor, wenn den PenTesterInnen *sicher bekannt ist*, dass sich die Einwirkung auf einzelne Daten bei einzelnen Beschäftigten nachteilig auswirkt (bspw. weil ein bestimmter Nachweis der Arbeitsleistung nicht erbracht werden kann).

- **§ 23 GeschGehG („Verletzung von Geschäftsgeheimnissen“)**: Der Tatbestand stellt das nicht erlaubte Erlangen sowie das Nutzen/Offenlegen von Geschäftsgeheimnissen unter Strafe. Typischerweise qualifizieren sich eine Vielzahl an Informationen als Geschäftsgeheimnisse – nicht nur die besonders wertvollen „Kronjuwelen“ der (Konzern-)Gesellschaft.

- **§ 42 BDSG („Strafbare Datenschutzverstöße“)**: Der Tatbestand stellt die unberechtigte Verarbeitung von nicht allgemein zugänglichen personenbezogenen Daten unter Strafe,

wenn hierbei entweder (1) gegen Entgelt, (2) mit (Dritt-)Bereicherungsabsicht oder mit (3) Schädigungsabsicht gehandelt wird. Erfasst werden daher die meisten sich in der Testumgebung befindlichen Informationen zu Beschäftigten/Geschäftspartnern. Ob und wann eine Verarbeitung „unberechtigt" erfolgt, hängt u.a. davon ab, ob der Arbeitgeber mit dem Angebot/dem Tolerieren der Privatnutzung des Internets/E-Mail-Postfachs durch den Beschäftigten zur Wahrung des Fernmeldegeheimnisses verpflichtet wird. Soweit dies – mit den Aufsichtsbehörden – bejaht wird, richtet sich die nach den (engeren) Voraussetzungen des TDDDG und nicht nach der DSGVO/dem BDSG. Nach einer Entscheidung des BGH aus dem Jahr 2012[11] besteht das Risiko, dass der mit den PenTesterInnen vereinbarte Arbeitslohn ein „Handeln gegen Entgelt" begründet.

- **Art. 83 DSGVO („Geldbußen wegen Datenschutzverstößen")**: Daneben halten Datenschutzverstöße im Rahmen eines PenTests auch ein Bußgeldrisiko für das jeweils datenschutzrechtlich Verantwortliche Unternehmen bereit.

II. Zulässigkeit von PenTests

Alle diese Tatbestände setzen ein „unbefugtes" jedenfalls aber ein „rechtswidriges" Handeln voraus. Interessant sind daher alle rechtlichen Argumentationsansätze, auf deren Grundlage die PenTesterInnen „befugt" bzw. „gerechtfertigt" handelt. Hiermit wird direkt am kleinsten gemeinsamen Nenner angesetzt und eine (General-)Antwort auf die oben skizzierten strafrechtlichen Risiken gefunden.

1. PenTests als technische und organisatorische Maßnahmen

Der Schlüssel zum Erfolg nennt sich technische und organisatorische Maßnahmen („TOMs").

Unternehmen sind bereits gegenwärtig dazu verpflichtet TOMs zu ergreifen, mit denen ein unberechtigter Zugriff auf bzw. das Kompromittieren der eigenen technischen Systeme verhindert

[11] BGH, NJW 2013, 2530 (2533 Fn. 50).

werden kann.[12] Diese – inhaltlich gleichbleibende[13] – Pflicht folgt aus unterschiedlichen Rechtsquellen und dient dem Schutz unterschiedlicher Informationen/Interessen/Rechtsgüter[14], konkret zum Schutz

- personenbezogener Daten (**Art. 32 Abs. 1 DSGVO**),

- des Fernmeldegeheimnisses und personenbezogener Daten (**§ 165 Abs. 1 Satz 1 TKG**),

- vor einem unerlaubten Zugriff auf bzw. eine Störung der für von ihnen angebotenen Digitale Diensten genutzten technischen Einrichtungen, auch durch äußere Angriffe (**§ 19 Abs. 4 Satz 1 TDDDG**) sowie

- vor Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind (**§ 8a Abs. 1, 1a BSIG**).

> Zukünftig wird sich diese Pflicht auch für „besonders wichtige Einrichtungen“ und „wichtige Einrichtungen“ auch aus § 30 Abs. 1 BSIG-E[15] ergeben, um Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen auf ihre oder andere Dienste zu verhindern oder möglichst gering zu halten.

Diese Pflichten begründen ein spiegelbildliches Recht zur Umsetzung dieser TOMs. D.h.: Soweit sich die einzelnen, konkreten (Angriffs-)Maßnahmen eines PenTests auf diese Rechte stützen, werden die o.g. Straftatbestände nicht verwirklicht. Die PenTesterInnen handeln in diesem Fall befugt bzw. gerechtfertigt.

---

[12] Vgl. Deusch/Eggendorfer, Taeger/Pohle, Computerrechts-Handbuch, 37. EL Mai 2022, Teil 5, 50.1 Rn. 1, 284; Poncza, ZD 2023, 8 (8 ff.).
[13] Deusch/Eggendorfer, Taeger/Pohle, Computerrechts-Handbuch, 37. EL Mai 2022, Teil 5, 50.1 Rn. 284 ff., 305, 313, 406.
[14] Deusch/Eggendorfer, Taeger/Pohle, Computerrechts-Handbuch, 37. EL Mai 2022, Teil 5, 50.1 Rn. 6, 30.
[15] In Umsetzung von Art. 21 Abs. 1, 2 NIS-2-RL („Risikomanagementmaßnahmen im Bereich der Cybersicherheit).

Zugriff auf (Beschäftigten-)Daten bei erlaubter/tolerierter Privatnutzung?

Das Schöne ist: Im Rahmen von PenTests schränkt die Auffassung der Datenschutzaufsichtsbehörden – nach der die Erlaubnis bzw. Toleranz der Privatnutzung von betrieblichen Kommunikationsmitteln die Anwendbarkeit des Fernmeldegeheimnisses (§ 3 Abs. 1 TDDDG) und den Ausschluss der DSGVO/des BDSG begründen – die Möglichkeit des Zugriffs auf (Beschäftigten-)Daten nicht wie bei anderen Compliance-Maßnahmen ein.

Denn diese Einschränkung folgt aus § 3 Abs. 3 Satz 3 TDDDG. Danach darf sich der Arbeitgeber die dem Fernmeldegeheimnis unterfallenden Informationen nur dann verwenden, wenn das TDDDG oder eine andere gesetzliche Vorschrift – die sich ausdrücklich auf Telekommunikationsvorgänge bezieht – das vorsieht.

Diese Anforderungen werden im Rahmen von PenTests durch § 3 Abs. 3 Satz 1 TDDDG und § 165 Abs. 1 Satz 1 TKG erfüllt. Danach darf der Arbeitgeber auf den (Kommunikations-)Inhalt sowie Informationen zu den Begleitumständen (bspw. die Uhrzeit) zugreifen, soweit dies zum Schutz der Hard- und Software, mithilfe derer der Telekommunikationsdienst angeboten wird, erforderlich ist.[16]

Die Durchführung von PenTests ist *im Abstrakten* sowohl eine technische als auch eine organisatorische Maßnahme.[17] Mit dieser werden informationstechnische Systeme – und damit auch die Umgebung, in der die personenbezogenen Daten/zum Fernmeldegeheimnis gehörende Umstände/das Angebot Digitaler Dienste zum größten Teil verarbeitet werden – auf potentielle Schwachstellen untersucht. Dies geschieht in einem geregelten Verfahren, mit vorab definierten Zuständigkeiten, Vorgehensweisen und Berichtslinien. Auf diese Art und Weise können etwaige Sicherheitslücken aufgespürt werden, *bevor* diese von fremden Dritten mit unlauteren Absichten entdeckt werden. Nur eine – möglichst frühzeitig – entdeckte Schwachstelle bietet der betroffenen

[16] Vgl. Geppert/Schütz/Hadidi, 5. Aufl. 2023, TDDDG § 3 Rn. 24; Deusch/Eggendorfer, Taeger/Pohle, Computerrechts-Handbuch, 37. EL Mai 2022, Teil 5, 50.1 Rn. 419; vgl. Fetzer/Scherer/Graulich/Graulich, TKG § 88 Rn. 80.

[17] Poncza, ZD 2023, 8 (10 f.). Vgl. zu Art. 32 Abs. 1 DSGVO auch: EG 49, 78 Satz 3 DSGVO.

(Konzern-)Gesellschaft die Chance, diese rechtzeitig (d.h. vor einem Ausnutzen durch einen Dritten) zu beheben. Die Durchführung systematischer PenTests ermöglicht nicht nur die rechtzeitige Schließung spezifischer Sicherheitslücken, sondern bietet gleichzeitig der Gesellschaft die Chance, die IT-Infrastruktur aufgrund der systematisch gewonnen Erkenntnisse insgesamt zu verbessern und widerstandsfähiger aufzustellen.

Bei der Umsetzung der TOMs soll der „Stand der Technik" berücksichtigt werden.[18] Dies setzt voraus, dass (1) eine bestimmte Maßnahme existiert und (2) deren „*Anwendung in der Praxis mit nachweislich positiven Effekten für die IT-Sicherheit*" einhergeht.[19] Dies ist bei der Durchführung interner sowie externer PenTests der Fall. Das Bundesamt für Sicherheit in der Informationstechnik („BSI") empfiehlt die Durchführung von PenTests als „bewährtes Mittel" und veröffentlicht hierzu Praxis-Leitfäden.[20] Dies wird nunmehr durch die Aufnahme der Verfahren in die Erwägungsgründe der NIS-2-RL[21] sowie in den Normtext von § 40 Abs. 5 Nr. 3 BSIG-E („Penetrationsanalysen") und dem DORA[22] normativ bestätigt.

Daraus folgt:

- Die Simulation eines IT-Angriffs unter Realbedingungen zur präventiven Identifizierung und anschließenden Behebung von Schwachstellen ist eine solche TOM.

- Soweit sich die einzelnen, konkreten (Angriffs-)Maßnahmen eines PenTests auf diese Rechte stützen, werden die o.g. Straftatbestände nicht verwirklicht. Die PenTesterInnen handeln in diesem Fall befugt bzw. gerechtfertigt.

[18] Art. 32 Abs.1 DSGVO, § 165 Abs. 1 Satz 2 TKG, § 19 Abs. 4 Satz 2 TDDDG, § 8a Abs. 1 Satz 2 BSIG; § 30 Abs. 2 Satz 1 BSIG-E.
[19] Deusch/Eggendorfer, Taeger/Pohle, Computerrechts-Handbuch, 37. EL Mai 2022, Teil 5, 50.1 Rn. 316; dieselb., K&R 2018, 223 (227).
[20] Siehe hierzu: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstest.pdf?__blob=publicationFile&v=10 (zuletzt abgerufen am: 27. April 2024). Siehe hierzu auch: Deusch/Eggendorfer, Taeger/Pohle, Computerrechts-Handbuch, 37. EL Mai 2022, Teil 5, 50.1 Rn. 317; Deusch/Eggendorfer, K&R 2018, 223 (227); Heidrich, DSRITB 2020, 391 (399).
[21] Erwägungsgründe 86, 87 NIS-2-RL.
[22] Erwägungsgründe EG 43, 44, 56, 59 DORA; Art. 3 Nr. 17, Art. 25, Art. 26 Abs. 2, 7, Art. 27 Abs. 1 lit. b) DORA.

a) <u>Konkrete Anforderungen an einen zulässigen PenTest</u>

Ein befugtes bzw. gerechtfertigtes und damit strafloses Handeln liegt vor, wenn die PenTesterInnen sich (1) auf das bzw. die Rechte zum Ergreifen von TOMs berufen kann (2) die getesteten IT-Systeme der Pflicht zur Ergreifung von TOMs unterfallen und (3) die Grenzen des bzw. der Rechte eingehalten werden.

1) **Rechtsinhaber** ist der datenschutzrechtlich Verantwortliche (Art. 32 Abs. 1 DSGVO), bzw. die Organisationseinheiten, die Telekommunikationsdienste (§ 165 Abs. 1 Satz 1 TKG) bzw. eigene oder fremde digitale Dienste (§ 19 Abs. 4 Satz 1 TDDDG) erbringen oder daran mitwirken bzw. Betreiber einer kritischen Infrastruktur sind (§§ 8 Abs. 1, 1a BSIG).

   Zukünftig sind auch die sog. „besonders wichtigen" Einrichtungen" und die „wichtigen Einrichtungen" aus § 30 Abs. 1 BSIG-E berechtigt.

   Konzernsachverhalte: Im Ausgangspunkt ist davon auszugehen, dass die zu untersuchenden Organisationseinheit (in der Regel eine Konzerngesellschaft) Rechtsinhaberin ist. Diese kann andere (Konzern-)Gesellschaften – bspw. die Konzernmutter – mit der Wahrnehmung des Rechts ermächtigen. Im Falle einer gemeinsamen datenschutzrechtlichen Verantwortlichkeit (Art. 26 DSGVO), steht das Recht auch den miteinbezogenen Konzerngesellschaften zu. Es sprechen gute Argumente dafür, dass § 165 Abs. 1 Satz 1 TKG und § 19 Abs. 4 Satz 1 TDDDG regelmäßig ein konzerndimensionales und damit ein eigenes Recht der Konzerngesellschaften/Konzernmutter begründen.

2) Der **räumliche Anwendungsbereich** erstreckt sich auf die gesamte technische Einrichtung (Hard- und Software), soweit diese über Schnittstellen (funk- oder kabelgebunden) miteinander verbunden sind und damit Seitwärtsbewegungen im Netzwerk ermöglichen.

Konzernsachverhalte: Hier erstreckt sich das Recht daher typischerweise – gesellschaftsübergreifend – auf die gemeinsam genutzte IT-Infrastruktur.

3) **Inhaltliche Reichweite**: Die Kenntnisnahme von personenbezogenen Daten/Tatsachen die dem Fernmeldegeheimnis unterfallen bzw. die Veränderung von Daten muss zur Aufklärung von potentiellen Schwachstellen **erforderlich** sein. Dies gilt sowohl für (private/dienstliche) Daten der Beschäftigten als auch der (Konzern-)Gesellschaft.

Wann ist die Kenntnisnahme bzw. die Veränderung von Daten für die Aufklärung von potentiellen Schwachstellen „erforderlich"?

Abstrakte Kontrollfrage: Kann die potentielle Schwachstelle ebenso effektiv aufgeklärt werden, wenn auf die Kenntnisnahme/Veränderung von Daten verzichtet wird?

Genau an dieser Schnittstelle wird der Staffelstab von der Rechtsabteilung an das IT-Department übergeben. Diese abstrakten rechtlichen Vorgaben lassen sich nur mit technischem Sachverstand in der jeweiligen individuellen Situation des PenTests entscheiden.

- Die **gute Nachricht** ist: Die juristische und technische Bewertung laufen hier gleich. D.h. auch der Durchführende kann selbst in der konkreten Situation beurteilen, ob der PenTest sich noch im Rahmen des Zulässigen bewegt oder nicht.

- Die **schlechte Nachricht** ist: Es gibt keine universelle Antwort und keine „one size fits all". Aber wann gibt es das schon in der Implementierung von Cybersecurity-Maßnahmen?

b) Checkliste

Mit der folgenden Prüfungsschema soll PenTesterInnen eine Checkliste an die Hand gegeben werden, mit denen diese im „ticking boxes"-Stil die Zulässigkeit einzelner Angriffssimulationen überprüfen können.

Erforderlichkeit wird bejaht	**Zugriff auf Daten:** Darf erfolgen. (+)
	Veränderung von Daten: Abwägung, ob der damit im System angerichtete technische/immaterielle Schaden im Verhältnis zu den dabei gewonnen Erkenntnissen steht. (+/-) Zu berücksichtigen ist, - (1) ob der Test in der operativen oder in einer Testumgebung durchgeführt wird, - (2) der Schaden durch ein Back-Up schnell behoben werden kann oder irreversible Schäden begründet werden, - (3) welche Daten bzw. Infrastruktur durch die mögliche Schwachstelle bedroht sind.

Erforderlichkeit wird verneint	**Zugriff auf Daten:** Darf nicht erfolgen. (-)
	Veränderung von Daten: Darf nicht erfolgen. (-)

Erforderlichkeit kann erst nach Zugriff/Veränderung beurteilt werden	**Zugriff auf Daten:** - Darf in einem ersten Schritt erfolgen. (+) - Sobald sich die fehlende Erforderlichkeit im Anschluss ergibt, muss die weitere Verarbeitung unverzüglich eingestellt werden. (-)
	Veränderung von Daten: Die ungewisse Erfolgsaussicht ist in der Abwägung zu berücksichtigen. (+/-)

2. Besonderheiten im Finanzsektor

Ab dem 17. Januar 2025 sind bestimmte Unternehmen aus dem Finanzsektor zur Durchführung „bedrohungsorientierter Penetrationstests“[23] verpflichtet.[24] Werden die dort aufgestellten Voraussetzungen eingehalten handeln die Verpflichteten auch aus diesem Grund befugt/rechtmäßig. Dieses Recht besteht zusätzlich und neben den o.g. Rechten zur Ergreifung von TOMs.

3. Doppelter Boden: Notstandsrecht

Darüber hinaus kann sich die Rechtmäßigkeit eines PenTests über den sog. Notstand (§ 34 StGB) als gerechtfertigt erweisen. Dieser dient jedoch im Wesentlichen als „doppelter Boden“. Die hier dargestellten Anforderungen an TOMs spiegeln sich in ähnlicher Form auch in den Voraussetzungen von § 34 StGB wider.

III. Maßnahmen, mit denen Strafbarkeitsrisiken vermieden werden

Ein PenTest kann strafrechtlich in zwei Phasen unterteilt werden:

- Erste Phase – Einwirken auf die IT-Infrastruktur/Datenbestand[25]
- Zweite Phase – Nachgelagertes Auswerten/Verwenden von Informationen[26]

Auf beiden Ebenen kann mit den folgenden Maßnahmen das Strafbarkeitsrisiko zusätzlich gemindert werden.

1. Erste Phase – Einwirken auf die IT-Infrastruktur/Datenbestand

Vorbereitung ist das halbe Leben. Vor der Durchführung des ersten PenTests sollte präzise analysiert werden, wer und wessen Daten hiervon betroffen sind. Basierend darauf können mit

[23] Art. 3 Nr. 17 DORA.
[24] Art. 24 Abs. 1, 2 i.V.m. 25 Abs. 1, Art. 26 Abs. 1, 2 DORA.
[25] Das umschließt die Phasen zwei bis fünf der im Annex dargestellten acht Phasen eines PenTests.
[26] Das umschließt die Phasen sechs bis acht der im Annex dargestellten acht Phasen eines PenTests.

- dem Abschluss individueller Vereinbarungen
- dem Einholen von Erklärungen der Betroffenen sowie
- einer transparenten Kommunikation,

die (straf-)rechtlichen Grenzlinien zugunsten des Unternehmens verschoben werden. Darüber hinaus wird durch den aktiven Einbezug und Information der Betroffenen mehr Verständnis innerhalb der Belegschaft erreicht und eine insgesamt fairere Ausgestaltung begründet.

Der Betriebsrat kann hier als vermittelnde Instanz und Vertreter der Interessen der betroffenen Arbeitnehmerschaft hinzugezogen werden um die oben beschriebenen Abmilderungsmaßnahmen, beispielsweise im Rahmen von Kollektivrechtlichen Verhandlungen, durchzuführen. (Beispiel: Schaffung Betriebsvereinbarung zur privaten Nutzung von IT Einrichtung)

a) <u>Einholen von Einwilligungen/Einverständnissen</u>

Einwilligungen (bzw. ein sog. „Einverständnis“) sind ein wichtiger Baustein. Eine wirksame „Zustimmung“ der Inhaber der zu schützenden Rechtsgüter begründet sowohl auf der datenschutzrechtlichen Ebene (§ 42 BDSG/Art. 83 DSGVO) als auch auf der rein strafrechtlichen Ebene ein befugtes/gerechtfertigtes und damit strafloses Handeln.

- **Einwilligungen/Einverständnisse von Beschäftigten**: Relevant bzgl. aller sich im TOE befindlichen Daten, an denen Beschäftigte ein (Mit-)Verfügungsrecht haben oder die einen Personenbezug aufweisen.

> **Vorbild Datenschutzrecht**: Die Erklärung sollte sich nach den Anforderungen des Datenschutzrechts richten. Diese sind strenger als die Voraussetzungen, die das Strafrecht an ein wirksames Einverständnis/eine Einwilligung stellt. D.h.: Selbst wenn die Einwilligung datenschutzrechtlich unwirksam sein sollte, kann dies durch eine strafrechtlich wirksame Einwilligung/ein Einverständnis „aufgefangen“ werden.
>
> **Doppelte Einwilligung bei Minderjährigen**: Soweit sich im TOE auch Daten von minderjährigen Beschäftigten (bspw. Praktikanten oder Ferienjobbern) existieren, sollten sowohl die Eltern (grundsätzlich gemeinschaftlich) als auch der Minderjährige ihre Einwilligung erteilen. Im Idealfall wird die Einwilligung des Minderjährigen in regelmäßigen Abständen neu eingeholt.

Sperrwirkung nach nicht erteilter Einwilligung?

Setzt das Unternehmen (auch) auf Einwilligungen von Betroffenen, entsteht jedoch ein datenschutzrechtliches Risikofeld.

Nach der Auffassung der Datenschutzaufsichtsbehörden[27] kann eine erbetene aber verweigerte Einwilligungserteilung dazu führen, dass ein Rückgriff des datenschutzrechtlich Verantwortlichen auf andere gesetzliche Erlaubnistatbestände gesperrt ist.[28]

Diese Auslegung ist mit Blick auf die grundsätzliche Gleichberechtigung der Erlaubnistatbestände[29] umstritten, lässt sich jedoch im Einzelfall dogmatisch mit der Bildung eines die weitere Datenverarbeitung ausschließenden Vertrauenstatbestand begründen.[30] Denn dem angesprochenen Betroffenen könnte damit suggeriert werden, dass er es alleine „in der Hand habe" über die Durchführung der Datenverarbeitung zu entscheiden.[31] Aufgrund des Transparenzgrundsatzes[32] ist das jedoch nur der Fall, wenn es sich bei dieser Annahme um eine „vernünftige Erwartung" handelt. Das Entstehen einer „vernünftigen" Erwartungshaltung kann mit der Aufnahme des folgenden Hinweises eingeschränkt werden:

> *„Verweigert der Betroffene die Einwilligung, behält sich der [Verantwortliche] hiermit ausdrücklich vor, den Zugriff auf personenbezogene Daten im Rahmen von Penetrationstests auf der Grundlage anwendbarer gesetzlicher Erlaubnistatbestände [ggf. einfügen des konkreten gesetzlichen Erlaubnistatbestands[33]] unabhängig vom Willen des Betroffenen durchzuführen."*[34]

[27] DSK Kurzpapier Nr. 20, S. 3, abrufbar unter: dsk_kpnr_20.pdf (datenschutzkonferenz-online.de) (zuletzt abgerufen am 27. April 2024).
[28] NK-BDSG/Scholz/Sokol § 4 Rn. 6; vgl. Kühling/Buchner/Buchner/Petri DSGVO Art. 7 Rn. 18; vgl. Gola, RDV 2002, 109 (110). A.A Gola/Heckmann/Schulz, 3. Aufl. 2022, DS-GVO Art. 6 Rn. 11; Veil, NJW 2018, 3337 (3342).
[29] Gola/Heckmann/Schulz, 3. Aufl. 2022, DS-GVO Art. 6 Rn. 10; vgl. Paal/Pauly/Frenzel, 3. Aufl. 2021, DS-GVO Art. 6 Rn. 10.
[30] Momsen/Grützner/Klaas/Wybitul, 2. Aufl. 2020, Kapitel 4 Rn. 220; vgl. Gola/Heckmann/Schulz, 3. Aufl. 2022, DS-GVO Art. 6 Rn. 12.
[31] Gola/Heckmann/Schulz, 3. Aufl. 2022, DS-GVO Art. 6 Rn. 12.
[32] Vgl. zur Konkretisierung des Transparenzgrundsatzes im spezifischen Kontext von Art. 6 Abs. 1 S. 1 lit. f) DSGVO: Erwägungsgrund 47 S. 1, 3 f. DSGVO.
[33] Kühling/Buchner/Buchner/Petri DSGVO Art. 7 Rn. 18.
[34] Momsen/Grützner/Klaas/Wybitul, 2. Aufl. 2020, Kapitel 4 Rn. 220; vgl. Gola/Heckmann/Schulz, 3. Aufl. 2022, DS-GVO Art. 6 Rn. 12.

- **Einwilligungen/Einverständnisse von (Konzern-)Gesellschaften**: Relevant bzgl. aller sich im TOE befindlichen Daten, an denen die (Konzern-)Gesellschaft ein (Mit)Verfügungsrecht haben. Das schließt auch Geschäftsgeheimnisse ein, bei denen die (Konzern-)Gesellschaft als (Mit-)Inhaberin anzusehen ist.

Wer kann und sollte einwilligen?

Soweit praktikabel und umsetzbar, sollte bei (Kapital-)Gesellschaften die Einwilligung/das Einverständnis stets durch die **Gesellschafter-/Hauptversammlung** erklärt werden.

Die **Gesellschafter-/Hauptversammlung** kann als „oberstes Willensbildungsorgan" bzw. als „zentrales Willensbildungsorgan" in die Preisgabe von Rechtsgütern der Gesellschaft einwilligen.[35] Erforderlich ist zumindest ein (Mehrheits-)Beschluss des die Gesamtheit der Gesellschafter repräsentierenden Gesellschaftsorgans[36], bei dem auch die Minderheitsgesellschafter mit der Frage der Billigung befasst wurden[37].

Ob – und inwieweit – auch der Vorstand bzw. Geschäftsführer auf ein strafrechtliches Individualrechtsgut verzichten können, ist dagegen nicht vollends geklärt.[38] Das lässt sich mit Blick auf die Leitungskompetenz aus § 43 Abs. 1 GmbHG/§ 76 Abs. 1 AktG bejahen.[39] Als Voraussetzungen werden hierbei genannt, dass der Geschäftsführer/Vorstand nicht seine eigene Handlung „genehmigt" und er mit der Einwilligungserteilung nicht selbst gegen ihm obliegende Pflichten (insbesondere: „die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters") verstößt.[40]

[35] BGH, NJW 2010, 3458 (3461 Rn. 34, 35); BGH, NJW 2003, 2996 (2998); BGH, NJW 2000, 154 (155); BGH, NStZ 1989, 23; BeckOK StGB/Wittig, 58. Ed. 1.8.2023, StGB § 266 Rn. 33.1, 33.2; MüKoStGB/Dierlamm/Becker, 4. Aufl. 2022, StGB § 266 Rn. 159, 161, 165.
[36] BGH, NStZ 2006, 214 (216 Rn. 12); BGH, NJW 2010, 3458 (3461 Rn. 36).
[37] BGH, NJW 2010, 3458 (3461 Rn. 36); BeckOK StGB/Wittig, 58. Ed. 1.8.2023, StGB § 266 Rn. 33.1.
[38] Satzger NStZ 2009, 297 (301).
[39] Schönke/Schröder/Perron, 30. Aufl. 2019, StGB § 266 Rn. 21; vgl. BGH, NJW 2010, 3458 (3461 f. Rn. 39); vgl. BGH, NStZ 2009, 95 (98 Rn. 40); vgl. BeckOK StGB/Wittig, 58. Ed. 1.8.2023, StGB § 266 Rn. 33.3. vgl. Knauer NStZ 2009, 151 (152); Knierim, CCZ 2009, 38 (38 Fn. 2).
[40] BGH, NJW 2010, 3458 (3461 f. Rn. 39); BeckOK StGB/Wittig, 58. Ed. 1.8.2023, StGB § 266 Rn. 33.3. Vgl. auch: BGH, NJW 1988, 1397 (1398); Satzger NStZ 2009, 297 (301); Knierim, CCZ 2009, 38 (38 Fn. 2).

b) <u>Einholen von Bestimmungserklärungen</u>

Parallel hierzu können sog. „Bestimmungserklärungen" eingeholt werden. Hintergrund: Ein Strafbarkeitsrisiko aus

- § 202a StGB („Ausspähen von Daten");
- § 202b StGB („Abfangen von Daten");
- § 202c StGB („Vorbereiten des Ausspähens und Abfangens von Daten")

besteht nicht, wenn die Daten für die PenTesterInnen „bestimmt" sind.

Die Bestimmung kann nur durch den sog. Verfügungsberechtigten getroffen werden. In Betracht kommen regelmäßig Beschäftigte sowie die (Konzern-)Gesellschaften. Bei mehreren (Mit-)Verfügungsberechtigten müssen alle übereinstimmend die Daten für die PenTesterInnen bestimmen.

Anforderungen an eine Bestimmungserklärung:

- **Adressaten**: Bestimmt werden können Einzelpersonen oder Personenmehrheiten
- **Zeitpunkt**: Die „Bestimmung" muss zum Zeitpunkt der Tathandlung vorliegen
- **Form:** Keine bestimmte Form erforderlich – die Bestimmung muss innerlich gefasst sein, nicht jedoch nach außen erkennbar kundgetan werden. Zu Dokumentations-/Beweiszwecken sollte die Bestimmungserklärung jedoch stets in Textform festgehalten werden.
- **Bedingungen**: Die Bestimmung kann von aufschiebenden oder auflösenden Bedingungen abhängig gemacht oder zeitlich befristet werden.[41]
- **<u>Keine</u> „Zweckbindung"**: Die Bestimmung bezieht sich stets auf die *Daten an sich*. Eine Beschränkung des Zugriffsrechts auf einen konkreten Verarbeitungszweck berührt den Tatbestandausschluss selbst bei zweckwidrigem Handeln nicht.[42]

[41] MüKoStGB/Graf, 4. Aufl. 2021, StGB § 202a Rn. 23; NK-StGB/Kargl, 6. Aufl. 2023, StGB § 202a Rn. 19; vgl. Schönke/Schröder/Eisele, 30. Aufl. 2019, StGB § 202a Rn. 10.
[42] OLG Celle, BeckRS 2016, 18380 Rn. 34; MüKoStGB/Graf, 4. Aufl. 2021, StGB § 202a Rn. 24; Schönke/Schröder/Eisele, 30. Aufl. 2019, StGB § 202a Rn. 11; NK-StGB/Kargl, 6. Aufl. 2023, StGB § 202a Rn. 20; BeckOK StGB/Weidemann, 58. Ed. 1.8.2023, StGB § 202a Rn. 10.

- **Erklärungsberechtigter**: Bei (Kapital-)Gesellschaften liegt die Erklärungsmacht – jedenfalls im Außenverhältnis – bei den organschaftlichen Vertretern (§ 35 Abs. 1 Satz 1 GmbHG, § 78 Abs. 1 Satz 1 AktG).

c) Abschluss vertraglicher Vereinbarungen

Die o.g. Straftatbestände sind stark zivilrechtlich geprägt. Vertraglich begründete Zugriffs- und Untersuchungsrechte können ein eigenständiges Recht für ein befugtes/gerechtfertigtes Handeln bilden.

- **(Konzern-)Gesellschaften**: Gerade bei der Durchführung von PenTests in Konzernstrukturen ist die präzise Bestimmung der Rechte und Pflichten zwischen der untersuchenden und untersuchten Gesellschaft zwingend auf eine vertragliche Grundlage zu stellen. In diesem Rahmen können – und sollten – auch Zugriffs- und Untersuchungsrechte der untersuchenden Gesellschaft begründet werden. Vertretungsberechtigt hierzu sind auch hier – jedenfalls im Außenverhältnis – Geschäftsführer/Vorstände (§ 35 Abs. 1 Satz 1 GmbHG, § 78 Abs. 1 Satz 1 AktG).

Einheitliches (Vertrags-)Werk:

Es bietet sich an, dass (1) die Einwilligung (2) die Bestimmung sowie (3) die vertragliche Auftragserteilung/Begründung vertraglicher Zugangs-/Untersuchungsrechte in einem einheitlichen Vertragswerk abgebildet werden. Hier bietet sich folgende Struktur an:

Der Vertrag wird zweiseitig zwischen der (Mutter-)Gesellschaft und der jeweiligen Konzerngesellschaft, handelnd jeweils durch den Geschäftsführer/Vorstand, geschlossen.

- Dieser wird unter die aufschiebende Bedingung der Fassung eines vorzulegenden und als Annex zum Vertragswerk zu nehmenden zustimmenden Gesellschafter-/Hauptversammlungsbeschlusses der zu untersuchenden Gesellschaft gestellt.

- Der Bedingungseintritt wird davon abhängig gemacht, dass dem Gesellschafterbeschluss entnommen werden kann, dass (1) den Gesellschaftern

der Umfang/die Auswirkungen des PenTests bekannt war und (2) auch – soweit vorhanden – die Minderheitsgesellschafter mit der Beschlussfassung befasst wurden.

Ein drei- bzw. mehrseitiger Vertrag unter Einbezug der Mitglieder der Gesellschafter-/Hauptversammlung ist nicht zu empfehlen. Eine wirksame Einwilligung setzt lediglich voraus, dass die Anteilseigner mehrheitlich und unter Beteiligung etwaiger Minderheitsgesellschafter ihr Einverständnis erklären. Eine Einbindung in gegenseitige Rechte und Pflichten ist nicht erforderlich und erhöht den Verwaltungsaufwand.

- **Beschäftigte**: In Arbeitsverträgen und Nebenvereinbarungen können (zweckgebundene) Zugriffs- und Untersuchungsrechte des Arbeitgebers geregelt werden. Für mehr Flexibilität (und gerade in Konzernstrukturen) sollte vereinbart werden, dass auch Dritte (bspw. andere Konzerngesellschaften) mit der Wahrnehmung dieser Rechte ermächtigt werden können.

d) Abschluss von (Konzern-/Gesamt-)Betriebsvereinbarungen

Anstelle einer individualvertraglichen Vereinbarung können Zugriffs- und Untersuchungsrechte im Verhältnis zu den meisten Beschäftigten[43] im Rahmen einer (Konzern-/Gesamt-)Betriebsvereinbarung (kollektivrechtlich) geregelt werden. Diese haben normativen Charakter, § 77 Abs. 4 Satz 1 BetrVG („unmittelbar und zwingend“)[44] und begründen ein befugtes/gerechtfertigtes Handeln.

- **Vorteil**: Einheitliche – ggf. auch konzernweite – Regelung, d.h. (1) kein „Flickenteppich“ an individualvertraglichen Regelungen, (2) geringerer Verwaltungsaufwand vor der Durchführung einzelner PenTests, (3) größeres Verständnis/Zustimmung im Betrieb

- **Nachteil**: Verlust an Flexibilität. Die (Konzern-/Gesamt-)Betriebsvereinbarung setzt einen Mindeststandard, der nicht durch ergänzende individualvertragliche Regelungen

[43] Nicht aber den in § 5 Abs. 2 BetrVG aufgezählten Arbeitnehmern und Leitenden Angestellten (§ 5 Abs. 3 BetrVG).
[44] ErfK/Kania, 23. Aufl. 2023, BetrVG § 77 Rn. 5, 32.

unterlaufen werden kann. Der „Flickenteppich“ lässt sich insbesondere bei älteren Arbeitsverträgen wegen der „Günstigkeitsprinzip“ nicht ausschließen.

Günstigkeitsprinzip:
Gegenläufig ist stets zu berücksichtigen, ob dem konkreten in einer (Konzern-/Gesamt-)Betriebsvereinbarung geregelten Zugangsrecht eine für den Beschäftigten günstigere Regelung im individuellen Arbeitsvertrag entgegensteht („Günstigkeitsprinzip“).[45]

e) Information der datenschutzrechtlich betroffenen Personen

Die datenschutzrechtliche Zulässigkeit der Maßnahmen wird durch die vorherige Ankündigung der Maßnahme ggü. den Beschäftigten, deren personenbezogene Daten sich im TOE befinden und daher ggf. betroffen sind, positiv beeinflusst werden (Transparenzgrundsatz/“vernünftige Erwartungen“). Dies kann bspw. im Intranet bzw. über einen E-Mail-Verteiler erfolgen.

f) Verwendung kabelgebundener Hardware

Klingt zunächst realitätsfern, hat aber einen (rechts-)realen Hintergrund: Erst der Einsatz einer sog. „Funkanlage“ eröffnet den Anwendungsbereich für das strafbewehrte Abhörverbot nach dem TDDDG. Eine Funkanlage ist nicht nur ein anachronistisches Kommunikationsmittel aus dem Polizeiwagen, sondern im Prinzip jedes Elektronikgerät, das Funkwellen zum Zweck der Funkkommunikation aussendet/empfängt. Eine Funkanlage ist daher auch ein, Laptop der sich per Wlan mit dem Internet verbinden lässt oder aber Bluetooth-Tastaturen und -Mäuse.

D.h. Soweit im Rahmen des PenTestings auf Hardware zurückgegriffen wird, die *ausschließlich* kabelgebunden auf das Internet zugreift und auch die einzelnen Angriffssimulationen nicht auf weiteren Funktechniken (Bluetooth etc.) basieren, scheidet eine Strafbarkeit nach §§ 27 Abs. 1 Nr. 1, 5 Abs. 1 TDDDG aus.

Hinweis:

Das Ausklammern von Wireless-Geräten wirkt im Jahr 2024 kaum zeitgemäß. Es handelt sich lediglich um eine mögliche, *zusätzliche* (Sicherheits-)Maßnahme. Mit Blick auf die weiteren o.g.

[45] ErfK/Kania, 23. Aufl. 2023, BetrVG § 77 Rn. 6.

rechtsgestalterischen Maßnahmen und Argumentationsansätzen muss nicht zwangsläufig auf die Bluetooth-Tastatur verzichtet werden.

g) Testumgebung/Back-Ups

Einige der o.g. Tatbestände[46] sehen die Merkmale der „Nachteilszufügungs-“ bzw. „Schädigungsabsicht“ vor. Zum Teil reicht bereits das sichere Wissen aus, dass mit der Angriffssimulation bestimmte Beeinträchtigungen einhergehen.

Dieses Risiko wird mit der Durchführung der Angriffssimulation in einer vom operativen System entkoppelten **Testumgebung** stark reduziert.

Soweit die Angriffssimulation in der **operativen Umgebung** durchgeführt wird, sollte vor dem Beginn der Maßnahme ein möglichst zeitnahes und damit aktuelles Back-Up des TOE erstellt und die Personen, die den PenTest durchführen, hierüber in Kenntnis gesetzt werden.

2. Zweite Phase – Nachgelagertes Auswerten/Verwenden von Informationen

An diese erste Phase – das Einwirken auf die IT-Infrastruktur und den Datenbestand – schließt sich die zweite Phase an. Diese besteht primär aus der Analyse/Auswertung der in der ersten Phase erlangten Informationen.

In dieser Phase sind insbesondere die sog. „Anschlussdelikte“ zu berücksichtigen, wie bspw. die Datenhehlerei gem. § 202d StGB oder das Mitteilungsverbot gem. § 27 Abs. 1 Nr. 2 TDDDG.

a) Einsatz einheitlicher Teams

Der Einsatz eines einheitlichen Teams in Phase 1 und 2 reduziert diese Strafbarkeitsrisiken.

[46] § 42 BDSG („Strafbare Datenschutzverstöße“), § 303b StGB („Computersabotage“), § 202d StGB („Datenhehlerei“), § 23 GeschGehG („Verletzung von Geschäftsgeheimnissen“), § 274 StGB („Urkundenunterdrückung“).

Das Mitteilungsverbot (§ 27 Abs. 1 Nr. 2 TDDDG) setzt das Mitteilen an einen „Dritten" voraus. Alle die sich am erstmaligen Zugriff auf diese Nachricht in irgendeiner Form beteiligt haben, sind keine Dritten.

Der Anwendungsbereich der Datenhehlerei ist nur eröffnet, soweit bei der Erhebung dieser Informationen gegen einen Straftatbestand verstoßen wurde. Der Täter dieser sog. Anknüpfungstaten kann kein Datenhehler sein.

b) Auswertung/Analyse ausschließlich zum Zweck der Gewährleistung der IT-Sicherheit

Die Datenhehlerei erfasst keine Handlungen, „*die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen*" (§ 202d Abs. 3 Satz 1 StGB). Die Durchführung von PenTests sowie die sich daran anschließende Analyse/Auswertung von Daten ist eine solche berufliche Pflicht.[47] Die Pflicht zur Gewährleistung der IT-Sicherheit folgt aus den o.g. Normen sowie für Vorstände und Geschäftsführer aus § 93 Abs. 1 Satz 1, 91 Abs. 2 AktG, § 43 Abs. 1 GmbHG. Der Tatbestandsausschluss erstreckt sich auch auf den Beauftragten, der für die Erfüllung dieser beruflichen Pflichten herangezogen wird.[48]

Vorausgesetzt wird jedoch, dass die Entgegennahme der erhobenen Daten „ausschließlich" der Erfüllung dieser Pflichten dient. Die Gewährleistung der IT-Sicherheit – und damit die Erfüllung der vorgenannten Pflichten – darf daher der einzige Zweck der Auswertung/Analyse der Daten sein.[49] Eine parallele Auswertung des Leistungsverhaltens von Arbeitnehmern o.ä. ist nicht zulässig.

Unabhängig davon, ob einheitliche oder getrennte Teams zum Einsatz kommen gilt: Soweit die Entgegennahme der Daten durch einen Unternehmensangehörige alleine den Zweck verfolgt, die IT-Sicherheit der jeweiligen (Konzern-)Gesellschaft durch eine Analyse/Verwertung der Daten zu gewährleisten/zu verbessern, greift der Tatbestandsausschluss aus § 202d Abs. 3 Satz 1 StGB.

[47] Vgl. NK-StGB/Kargl, 6. Aufl. 2023, StGB § 202d Rn. 27: *„(…) Daran ist insofern Kritik geübt worden, als die Vorschrift nur die „berufliche" Mitwirkung von Personen an der Datenweitergabe von Strafe freistellt: Nebenberufliche Journalisten, Blogger und IT-Fachleute seien nicht erfasst."*

[48] BT-Drs. 18/5088 S. 48; Schönke/Schröder/Eisele, 30. Aufl. 2019, StGB § 202d Rn. 15; BeckOK StGB/Weidemann, 58. Ed. 1.8.2023, StGB § 202d Rn. 19.

[49] NK-StGB/Kargl, 6. Aufl. 2023, StGB § 202d Rn. 27; Spindler/Schuster/Gercke, 4. Aufl. 2019, StGB § 202d Rn. 6; Schönke/Schröder/Eisele, 30. Aufl. 2019, StGB § 202d Rn. 15. Vgl. BT-Drs. 12/4883, 8.

F. Praxisbeispiel: Bestimmung der Erforderlichkeit von Angriffsszenarien

Die Silas Sorglos GmbH & Co KG, hatte im letzten Jahr einen schwerwiegenden Cybervorfall mit mehreren Tagen Produktionsausfall. Die Sicherheitslücke befand sich an einer Schnittstelle des Warenwirtschaftssystems. Die Wettbewerberin Dieter Dichtring AG nutzt dasselbe Warenwirtschaftssystem. Auch nachdem die Sicherheitslücke geschlossen wurde, sorgt der Vorfall bei ihr für Unbehagen. Daher beauftragt sie die Petra Pentest GmbH mit der Durchführung eines konzernweiten Penetrationstest. Ziel ist es herauszufinden, ob es möglich ist von außen in das (Konzern-)Netzwerk einzudringen und welchen potentiellen Schaden ein Angreifer innerhalb des Netzwerkes anrichten könnte.

Die IT-Experten der Petra PenTest GmbH ergreifen die folgenden Maßnahmen:

Maßnahme 1: OSINT-Recherche
Die IT-Experten besuchen die Social-Media-Profile des IT-Personal der Dieter Dichtring AG auf LinkedIn („Open Source Intelligence"-Recherche, „OSINT"). Über die gelisteten Kenntnisse und Erfahrungen mit Produkten der Mitarbeitenden lassen sich oftmals Rückschlüsse auf aktuell eingesetzte Sicherheitslösungen treffen. Daneben bemühen die IT-Experten Datenbanken wie *Shodan*, *ZoomEye* oder *FOFA*. In diesen werden Geräte/Systeme gelistet, die mit dem Internet verbunden sind. Die Datenbanken lassen sich nach Schlagwörtern filtern und zeigen an, welche IP-Adressen und Ports den jeweiligen Geräten/Systemen zugeordnet sind. Auf diese Weise können die IT-Experten im Internet exponierte Systeme der Dieter Dichtring AG zu finden und einen Überblick über die potentielle Angriffsoberfläche gewinnen. Im konkreten Fall bringen die IT-Experten über das LinkedIn-Profil eines bei der Dieter Dichtring AG angestellten IT-Administrator in Erfahrung, welche *Web Application Firewall* mit hoher Wahrscheinlichkeit genutzt wird, um die Webseiten oder öffentlichen Schnittstellen der Dieter Dichtring AG abzusichern. Über die Shodan-Datenbankabfrage wurde eine Schnittstelle zu einem Warenwirtschaftssystem verifiziert. Außerdem wurde ein E-Mail-Webportal entdeckt, das wohl aufgrund kurzfristig gestiegener Remote-Work Anforderungen installiert wurde und sich nicht in der Dokumentation der Dieter Dichtring AG wiederfindet.
Bewertung: Die Zugriffe auf die LinkedIn-Profile der Beschäftigten sind primär am Datenschutzrecht zu messen. Als Erlaubnistatbestand kommt u.a. Art. 6 Abs. 1 Satz 1 lit. f) DSGVO in Betracht.[50]

[50] Poncza, ZD 2023, 8 (10).

- **Berechtigtes Interesse**: Die Dieter Dichtring AG hat das berechtigte Interesse an der Gewährleistung einer hinreichenden technischen und organisatorischen Datensicherheit (vgl. die *Pflicht* aus Art. 32 DSGVO). Erwägungsgrund 49 der DSGVO bestätigt das.[51]

- **Erforderlichkeit**: Zur Gewährleistung der IT-Sicherheit ist ein Test der IT-Infrastruktur unter Realbedingungen notwendig. Dies setzt – in einem ersten Schritt – die Identifizierung möglicher Angriffspunkte voraus. Hierzu ist die Kenntnisnahme der auf LinkedIn geteilten Informationen ein effektives und vergleichsweise eingriffsarmes Mittel. Mit Kenntnis der wahrscheinlich genutzten Web Application Firewall kann gezielt nach Umgehungsmöglichkeiten bzgl. der Schutzmechanismen gesucht werden. Die Verarbeitung der personenbezogenen Daten des IT-Administrators ist ein zur Gewährleistung der IT-Sicherheit der Dieter Dichtring AG notwendiger „Baustein" und damit erforderlich.

- **Abwägung**: In der Abwägung mit dem gegenläufigen Interesse des IT-Administrators am Schutz seiner personenbezogenen Daten ist zu berücksichtigen, dass

    - es sich bei LinkedIn um ein berufliches Netzwerk handelt[52],
    - die Informationen öffentlich einsehbar waren (Art. 11 Abs. 1 S. 1 GRCh; Art. 5 Abs. 1 Satz 1 GG,)[53];
    - über die Angabe der Beschäftigung bei der Dieter Dichtring AG ein unmittelbarer Bezug zum Arbeitgeber hergestellt wurde;
    - ein IT-Administrator „vernünftigerweise" erwartet, dass im Rahmen eines PenTests seine öffentlich einsehbaren Informationen ausgewertet werden (Erwägungsgrund 47 Satz 3 DSGVO; Art. 5 Abs. 1 lit. a) DSGVO).

Tipp 1: Im Rahmen der Dokumentation der Maßnahme sollte der Klarname des IT-Administrators pseudonymisiert werden. Eine Anonymisierung – also der endgültige Ausschluss des Personenbezugs – sollte nicht erfolgen. Ggf. soll der IT-Administrator nach Abschluss der Maßnahme zu einer restriktiveren Informationsweitergabe auf LinkedIn angehalten werden.

[51] Poncza, ZD 2023, 8 (10).
[52] Kramer, IT-Arbeitsrecht/*Schulze/Zumkley*, 3. Auflage 2023 § 2 Individualarbeitsrecht Rn. 1071; BeckOK DatenschutzR/Riesenhuber, 47. Ed. 1.2.2024, BDSG § 26 Rn. 101.
[53] BeckOK DatenschutzR/Riesenhuber, 47. Ed. 1.2.2024, BDSG § 26 Rn. 99.

Tipp 2: Informationspflichten aus den Art. 13, 14 DSGVO beachten und ggf. Ausnahmetatbestände prüfen.

Die Datenbankabfrage bewegt sich nicht im strafrechtlichen Bereich:

- **Kein Ausspähen von Daten (§ 202a Abs. 1 StGB)**: Die in der Datenbank hinterlegten Informationen werden entweder (1) nicht durch Zugangshürden geschützt bzw. (2) sind nach dem Einrichten eines Accounts für die PenTester bestimmt bzw. (3) Zugriffe erfolgen befugt.

- **Kein Vorbereiten des Ausspähens/Abfangens von Daten (§ 202c Abs. 1 StGB)**: Die Informationen zur Existenz eines Systems bzw. eines offenen Ports ermöglichen *für sich genommen* noch nicht den Zugang zu Daten in einer von § 202a StGB/§ 202b StGB unter Strafe gestellten Form. Die Datenbanken sind auch keine „Computerprogramme" im Sinne von § 202c StGB. Das ist bei sog. „dual-use-Programmen" nur der Fall, wenn „*deren funktionaler Zweck (…) eindeutig einer krimineller ist*"[54] bzw. wenn die illegale Zweckbestimmung dem Programm „auf die Stirn geschrieben steht" (siehe oben).[55]

- **Keine Datenhehlerei (§ 202d Abs. 1 StGB)**: Soweit die in den Datenbanken gespeicherten Informationen ihrerseits – zuvor – rechtmäßig erhoben wurden, fehlt es an einer Anknüpfungstat.

[54] BT-Drs. 16/3656, S. 19.
[55] BVerfG, BeckRS 2009, 35013 Rn. 48. Ausführlich: Klaas/Momsen/Wybitul/Klaas, HdB Datenschutzsanktionenrecht § 202c StGB Rn. 16 ff.

Maßnahme 2: Netzwerkscans

Im Folgeschritt versuchen die PenTesterInnen mit gezielten Netzwerkscans die Erkenntnisse aus der vorgelagerten OSINT-Recherche zu verifizieren. Darüber hinaus sollen verbundene Systeme identifiziert werden. Auf dieser Grundlage können die IT-Experten die konkrete „Angriffsfläche" bestimmen und analysieren.

Bei einem Netzwerkscan erfolgt eine systematische Erkundung der Netzwerkinfrastruktur, wobei verschiedene Schnittstellen angesprochen werden. Typischerweise werden Ports und Dienste auf Zielrechnern überprüft, um potenzielle Schwachstellen zu identifizieren.

Ergebnis:

- Aufgrund der Web Application Firewall sind bzgl. der Website der Dieter Dichtring AG nur die notwendigen Netzwerkports 80 und 443 exponiert.

- Das in der Datenbank entdeckte Remote-Work-System entpuppte sich als kurzfristig installierte E-Mail Web-Applikation damit Mitarbeitende auf ihre E-Mails zugreifen können, auch wenn Sie nicht im Büro sind.

- Daneben konnten die IT-Experten nur das übliche E-Mail-Gateway zum Empfang und Versenden von E-Mails und einen DNS-Server finden.

Anschließend werden HTTP-GET-Requests an den eingesetzten Webserver gesendet. Aus dem vom Server zurückgelieferten Antwortheader können die genauen Softwareversionen der eingesetzten Webserver („Bannergrabbing") bestimmt werden.

Ergebnis: Es werden keine verwundbaren Softwareversionen festgestellt, die einen einfachen Angriff über einen Exploit ermöglichten.

Anschließend werden mithilfe von *FFUF* („Fast Web Fuzzer“) und einer dazugehörigen Wörterliste weitere Anfragen an den Webserver gesendet, um potentiell sensible Pfade auf den einzelnen Webservern zu entdecken („Pfad-Enumeration“).

Ergebnis:

- Auf der Unternehmenswebseite und der Schnittstelle des Warenwirtschaftssystems werden die IT-Experten von der Web Application Firewall gestoppt.

- Bei der E-Mail Web Applikation, die nicht durch die Web Application Firewall abgesichert wurde, wird aufgrund der Rückantworten des Webservers die dazugehörige Login-Seite entdeckt.

Bei einer anschließenden Analyse der Unternehmenswebseite wurde eine Suchfunktion entdeckt. Mit dieser können die von der Dieter Dichtring AG hergestellten Produkte und die verfügbaren Lagerbestände durchsucht werden. Dies legt eine Schnittstelle oder eine gemeinsame Datenbank mit dem Warenwirtschaftssystem nahe.

Auf der Grundlage dieses Netzwerkscans wurden

- die Suchfunktion der Unternehmenswebseite und
- die entdeckte Login-Seite der E-Mail Web Applikation

in die Liste der potentiellen Ziele aufgenommen.

Bewertung:

Netzwerkscans zeichnen sich in aller Regel durch ein *nicht invasives* Vorgehen aus. In diesem Beispiel werden im Rahmen der Informationsbeschaffung ebenfalls keine Zugangshürden überwunden. Eine Strafbarkeit nach § 202a Abs. 1 StGB kommt nicht in Betracht.

Relevanter sind in diesem Abschnitt die Grenzlinien aus § 202c Abs. 1 StGB. Denn bei einem Streifzug durch die Netzwerkinfrastruktur können auch aus Nachlässigkeit dokumentierte Passwörter oder sonstige Sicherungscodes entdeckt werden, die anschließend ausgenutzt werden.[56] In diesem Fall gilt: Soweit die geplante Ausnutzung solcher entdeckten Passwörter nicht von §§ 202a, 202b StGB erfasst wird (siehe hierzu im nächsten Schritt), ist auch das vorbereitende „Verschaffen" nicht nach § 202c StGB strafbar. Die in diesem Beispiel erlangten Informationen fallen nicht in den Anwendungsbereich von § 202c Abs. 1 StGB – ein Strafbarkeitsrisiko besteht nicht.

Maßnahme 3: Password-Cracking-Tool

Die IT-Experten starten auf der Login-Seite der E-Mail-Web-Applikation mit einem „Password Cracking Tool" einen sog. „Brute-Force Angriff". Das Programm greift auf ein Wörterbuch mit den gängigsten Benutzernamen und Passwort Kombinationen zurück. Da die E-Mail-Web Applikation nicht durch die Web Application Firewall geschützt wird, können problemlos automatisierte hunderte Versuche pro Minute durchgeführt werden. Hierdurch erlangen die PenTesterInnen den Zugriff auf einige E-Mail-Postfächer von Mitarbeitenden der Dieter Dichtring AG. Diese dürfen nach den Vorgaben des Arbeitgebers auch zu privaten Zwecken genutzt werden.

Bewertung:

Brute-Force-Angriff: Das Überwinden des Passwortschutz ist ein invasives Vorgehen und fällt in den Anwendungsbereich von § 202a Abs. 1 StGB. Da die Mitarbeiter das E-Mail-Postfach auch privat nutzen dürfen, sind diese (auch) Verfügungsberechtigte. Die Mitarbeiter haben von den Maßnahmen keine Kenntnis und daher auch keine Einverständnis- oder Bestimmungserklärungen abgegeben.

[56] Klaas, MMR 2019, 187 (189).

Die IT-Experten handeln jedoch „befugt“, wenn die Überwindung des Passwortschutzes sich als „technische und organisatorische Maßnahme“ im Sinne von Art. 32 Abs. 1 DSGVO[57] bzw. § 165 Abs. 1 Satz 1 TKG[58] darstellt. Das ist der Fall, wenn die Überwindung der Zugangssicherung zum Schutz der Hard- und Software der Dieter Dichtring AG bzw. der von ihr hiermit verarbeiteten personenbezogenen Daten **erforderlich** ist.

- Kontrollfrage: Kann die potentielle Schwachstelle ebenso effektiv aufgeklärt werden, wenn auf ein Überwinden der Zugangssicherung verzichtet wird?

- Antwort: Nein.

    - Erst in dem Moment, in dem das Password-Cracking-Tool „erfolgreich“ ist, wird die Schwachstelle entdeckt. Damit steht fest, dass dieser Weg auch (böswilligen) Dritten offensteht, die auf dieselben tools zurückgreifen können.

    - Daneben ist das Überwinden der Zugangssicherung eine notwendige Vorbedingung, um in einem Folgeschritt zu testen, ob – und wenn ja, mit welchen Funktionsmöglichkeiten – eine Web-Shell hinterlegt werden kann.

  D.h.: Das Überwinden der Zugangssicherung ist erforderlich, um die Schwachstellen im System zu identifizieren. Erst auf dieser (Informations-)Grundlage können gezielte und effektive Gegenmaßnahmen ergriffen werden um das System und die personenbezogenen Daten zukunftsgerichtet zu schützen. Damit erweist sich der „Brute Force-Angriff“ insgesamt als erforderlich. Die IT-Experten handeln „befugt“ und machen sich nicht nach § 202a Abs. 1 StGB strafbar.

[57] Soweit der überwiegenden Ansicht in der Rechtsprechung und in der Literatur zur Anwendbarkeit der DSGVO/BDSG auch bei erlaubter Privatnutzung dienstlicher (Tele-)Kommunikationsmittel gefolgt wird.
[58] Soweit der Ansicht der Datenschutzaufsichtsbehörden zur Anwendbarkeit des TDDDG bzw. des TKG gefolgt werden soll.

Maßnahme 4: SQL-Injection
Zurück zur Unternehmenswebsite: Die IT-Experten vermuten, dass die Suchmaske mit einer an das Warenwirtschaftssystem gekoppelten Datenbank über SQL (Structured Query Language) kommuniziert. Deshalb werden gezielt Sonderzeichen in die Suchmaske eingegeben, um zu überprüfen, ob aufgrund fehlender Sicherheitsmaßnahmen mit SQL-Befehlen Reaktionen der Datenbank ausgelöst werden können (sog. „SQL-Injection“).[59] Im konkreten Fall wird durch das open source erhältliche Programm „SQLMap“ die Datenbank dazu gebracht, weite Teile der hinter der Suchmaske liegenden Datenbank – inklusive verschlüsselter Zugangsdaten – offenzulegen. Dabei wird festgestellt, dass in der Datenbank einzelne Unterseiten der Unternehmenswebseite gespeichert sind. Mittels weiterer Eingabebefehle in der Suchmaske können Einträge in der Datenbank geändert oder hinzugefügt werden. Die IT-Experten hinterlegen auf diese Weise auf einem entdeckten Website-Pfad eine eigens entwickelte (passwortgeschützte) Web-Shell in der Datenbank. Über diesen erlangen sie den vollständigen Zugriff auf den Webserver.
Bewertung: **SQL-Injection:** Der Zugriff auf die hinter der Suchmaske liegenden Datenbank spielt im Anwendungsbereich von § 202a Abs. 1 StGB. Die Dieter Dichtring AG ist für die Datenbank die Verfügungsberechtigte. In der Auftragserteilung an die PenTesterInnen liegt eine darauf bezogene Einverständnis-/Bestimmungserklärung. Bereits aus diesem Grund ist der Zugriff auf die Datenbank straflos. Bei den einzelnen Einträgen in den Datenbanken kann es schon anders aussehen: Die IT-Experten wissen im Zeitpunkt des Zugriffs nicht, welche Daten in der Datenbank hinterlegt sind und welche weiteren Personen bzgl. dieser (mit-)verfügungsbefugt sind. Hier können sich die IT-Experten nicht darauf verlassen, dass die alleinige Einverständnis-/Bestimmungserklärungen

[59] Klaas, MMR 2022, 187 (188).

der Dieter Dichtring AG zur Straflosigkeit führen. Aus diesem Grund ist auch hier die Kontrollfrage zu stellen.

- Kontrollfrage: Kann die potentielle Schwachstelle ebenso effektiv aufgeklärt werden, wenn auf die Eingabe der Sonderzeichen in der Suchmaske verzichtet wird?

- Antwort: Nein.

    - Maßgeblich ist die ex-ante Perspektive im Zeitpunkt der Eingabe. Die Suchmaske ist eine offen zugängliche Schnittstelle und SQLMap ein Open Source-Programm. Jedem (böswilligen) Angreifer steht diese Möglichkeit ebenfalls offen. Um festzustellen, ob – und in welchem Umfang – Schwachstellen existieren, ist die Eingabe aller theoretisch denkbaren SQL-Befehle erforderlich.

    - Der anschließende Umgang mit den dabei gewonnen Informationen bzw. dem dabei erlangten Zugriff auf weitere Daten ist gesondert zu betrachten. Siehe hierzu der nächste Punkt („Installation der Web-Shell“).

Installation der Web-Shell: Die Installation der Web-Shell birgt ein Strafbarkeitsrisiko aus § 303a Abs. 1 StGB und § 303b Abs. 1 Nr. 1, 2 StGB. Soweit mit dieser auch weitere systeminterne Zugangshindernisse überwunden werden sollen, ist erneut § 202a Abs. 1 StGB im Blick zu behalten.

Auch hier gilt: Soweit die Dieter Dichtring AG bzgl. der Datenbank verfügungsberechtigt ist, erfolgt der weitere Eintrag in der Datenbank aufgrund des entsprechenden Auftrags rechtmäßig (§ 303a Abs. 1 StGB, § 303b Abs. 1 Nr. 1 StGB) bzw. gerechtfertigt (§ 303b Abs. 1 Nr. 2, 3 StGB).

Darüber hinaus handelt es sich auch um eine erforderliche TOM:

- Kontrollfrage: Können potentielle Schwachstellen ebenso effektiv aufgeklärt werden, wenn auf die Installation der Web-Shell verzichtet wird?

- Antwort: Nein.
    - Mit dem anschließenden Ausnutzen der mithilfe der SQL-Injection erlangten Informationen bzw. des erlangten Datenbankzugriffs wird überprüft, wie tief ein (böswilliger) Angreifer anhand dieser – hypothetisch auch für ihn über die Suchmaske erreichbaren Informationen – in das System eindringen könnte. Daneben wird mit der installierten Web-Shell der Grundstein für potentielle weitere Seitwärtsbewegungen gelegt. Durch einen (wirksamen) Passwortschutz wird verhindert, dass die Web-Shell selbst zu einer eigenständigen Schwachstelle wird, welche ihrerseits unberechtigten Dritten den Zugriff auf den Webserver ermöglicht bzw. erleichtert.

    - Als mildere, gleich geeignete Alternative könnte der Abbruch des „live-pentesting“ und die Installation der Web-Shell in einer nicht aktiven Testumgebung in Betracht kommen.

        - **Milderes Mittel**: Das ist bzgl. in der Datenbank gespeicherten personenbezogenen (Mitarbeiter-)Daten der Fall. Klammert die Testumgebung diese aus, werden diese nicht verarbeitet. Ebenso wird der zukunftsgerichtete Zugriff auf die Mitarbeiterdaten auf der Grundlage der Web-Shell-Funktionen ausgeschlossen.

        - ***Nicht* gleich effektiv**: Aus dem letzten Grund handelt es sich nicht um ein ebenso effektives Mittel. Das (Gesamt-)Ziel des PenTests liegt in der Aufklärung aller Schwachstellen der im scope liegenden IT-Systeme. Zu diesem Zweck muss die Web-Shell in der aktiven Umgebung installiert werden. Nur auf diese Weise können ergänzende Seitwärtsbewegungen im IT-System vorbereitet werden – ansonsten endet der Weg schnell an den Grenzen der Testumgebung.

Die Installation der Web-Shell in der aktiven Umgebung erweist sich als erforderlich.

Zu beachten ist:

Soweit auf dem Webserver auch Daten von weiteren Verfügungsberechtigten (bspw. Mitarbeitern) gespeichert sind, könnte in der Web-Shell-Installation eine Vorbereitungshandlung im Sinne von § 202c Abs. 1 StGB (i.V.m. § 303a Abs. 3 StGB bzw. § 303b Abs. 5 StGB) gesehen werden. Diese wären jedoch straflos, wenn sich die hiermit vorbereiteten (Angriffs-)Maßnahmen wiederum als zulässige – d.h. vor allem: erforderliche – TOM und damit als „befugt"/„rechtmäßig"/„gerechtfertigt" erweisen.

Maßnahme 5: Manipulation eines E-Mail-Postfachs

Auf der Grundlage der auf dem Webserver installierten Web-Shell, können die IT-Experten auf das E-Mail-Postfach des Mitarbeiters X zugreifen. Sie modifizieren das E-Mail-Postfach dergestalt, dass der Nachrichteninhalt der dort eingehenden und ausgehenden E-Mails verändert werden kann. Das auf diese Weise kompromittierte E-Mail-Postfach des Mitarbeiters X wird anschließend nicht weiter untersucht.

Bewertung:

Der Zugriff auf bzw. die Modifikation des E-Mail-Postfachs des Mitarbeiters X: Auch hierbei handelt es sich um ein invasives Vorgehen. Falls im Rahmen der Installation weitere technische Zugangshindernisse überwunden werden mussten, steht erneut eine Strafbarkeit wegen § 202a Abs. 1 StGB in Frage. Durch die Installation des (Manipulations-)Programms kommt eine Strafbarkeit wegen § 303a Abs. 1 StGB oder § 303b Abs. 1 Nr. 1 ,2 StGB in Betracht. Die IT-Experten handeln in allen Fällen „befugt" – und damit straflos – wenn der Zugriff auf bzw. die Modifikation des E-Mail-Postfachs des Mitarbeiters X zum Schutz der Hard-/Software und den dort gespeicherten personenbezogenen Daten **erforderlich** ist.

- Kontrollfrage: Kann die potentielle Schwachstelle ebenso effektiv aufgeklärt werden, wenn auf ein Überwinden der Zugangssicherung verzichtet wird?

- Antwort: Es kommt darauf an.

- Umfasst der Scope des PenTests auch die Durchführung von social-engineering-Angriffen, kann die Modifikation der Vorbereitung dieser Maßnahme dienen. Sollen die Mitarbeiter der Dieter Dichtring AG mit scheinbar authentischen E-Mails ihrer (vorgeblichen) Kollegen bzw. Geschäftspartnern – die sich scheinbar in die vorherige Kommunikationskette einfügen – zur Preisgabe von vertraulichen Informationen/Unterlagen bewegt werden, kann sich die Installation als erforderlich erweisen.

- Soll dagegen lediglich geprüft werden, ob eine solche Maßnahme für einen potentiellen Angreifer praktisch möglich wäre, so existiert eine für den betroffenen Mitarbeiter mildere (d.h. weniger eingriffsintensive) Maßnahme. Die rein technische Möglichkeit muss nicht „live" und in einem realen, aktiv genutzten E-Mail-Postfach eines Mitarbeiters simuliert werden. Der Test kann ebenso effektiv in einem Test-E-Mail-Account durchgeführt werden.

D.h.: Der Zugriff auf bzw. die Modifikation des E-Mail-Postfachs ist erforderlich, soweit die IT-Experten die o.g. spezifische Social Engineering-Maßnahme in einer Realsituation simulieren wollen. Die rein technische „Machbarkeits"-Prüfung ist dagegen nicht erforderlich. Nur im ersten Fall handeln die IT-Experten „befugt" und machen sich nicht nach §§ 202a Abs. 1, 303a Abs. 1, 303b Abs. 1 Nr. 1, 2 StGB strafbar.

Annex 1: „Best practice“ – Ausgestaltungsformen von PenTests

In der Praxis haben sich unterschiedliche Ausgestaltungsformen von PenTests herausgebildet. Der Unterschied liegt primär im Umfang der Informationen sowie Zugänge, die den PentesterInnen im Vorfeld zur Verfügung gestellt werden. Wie ein konkreter PenTest ausgestaltet wird, bestimmt sich regelmäßig nach den zeitlichen, personellen und finanziellen Ressourcen.

Bezeichnung	Bedeutung
White-Box	Bei einem White-Box PenTest erhalten die PenTesterInnen zusätzliche Informationen oder Zugänge zum System. Diese Vorgehensweise empfiehlt sich, wenn ein sehr spezifisches System getestet oder der Aufwand geringgehalten werden soll bzw. wenig Zeit zur Verfügung steht.
Black-Box	Bei einem Black-Box PenTest werden keine bzw. wenige Informationen/Zugänge vom Auftraggeber zur Verfügung gestellt. Diese Variante entspricht einem realistischen Angriff nimmt, aber unter Umständen mehr Zeit in Anspruch.
Grey-Box	Bei einem Grey-Box Pentest werden ebenfalls keine bzw. wenige Informationen/Zugänge vom Auftraggeber zur Verfügung gestellt. Die PenTesterInnen haben aber die Möglichkeit ihre Erkenntnisse im laufenden Test über den Auftraggeber zu verifizieren.
Red-Team Engagement	Bei der Sonderform des Red-Team Engagements ist auf Auftraggeberseite nur ein sehr kleiner Personenkreis involviert. Hierbei möchte man neben technischen Schwachstellen und Verwundbarkeiten auch in Erfahrung bringen ob interne Incident Response Prozesse und Kommunikationswege auch im (simulierten) Ernstfall funktionieren.

Annex 2: „Best practice“ – Die acht Phasen eines PenTests

Die folgende Übersicht hilft bei der erstmaligen Konzeptionierung und Umsetzung eines PenTests in der eigenen Organisation.

Phase	**Maßnahmen**
1 - Planung („Planning“)	Abstimmung mit dem Auftragsgeber – definieren von - Art, - Umfang und - Ziel der Testmaßnahmen. Der „Umfang“ sollte eine Auflistung der Netzsegmente oder einzelner Geräte („Testumgebung“) als auch die vom Redteam zu verwendenden Methoden beinhalten. In der Praxis bewährt sich auch eine negative Abgrenzung: welche Systeme sollen ausgespart und welche Methoden sollen nicht zur Anwendung gelangen? Schriftliche Fixierung der Vereinbarung und Beauftragung.
2 - Informationsbeschaffung („Reconnaissance“)	Zwei Kategorien: - **Passive Informationsbeschaffung**: Sammeln von Informationen ohne direkten Kontakt oder Interaktion mit dem Ziel. Bspw. werden Informationen aus öffentlichen oder nicht zugangsbeschränkten Quellen extrahiert.

	- **Aktive Informationsbeschaffung**: Sammeln von Informationen durch direkten Kontakt und Interaktion mit den möglichen Zielen. Bspw. werden Netzwerke gescannt. Dabei könnten Systeme und Schutzmaßnahmen zur Angriffserkennung erste Indikatoren liefern, dass ein möglicher Angriff bevorsteht. Hierbei können Informationen, die durch passive Methoden ermittelt wurden, verifiziert werden. Praxistipp: klare Dokumentation und Protokollierung, um die Nachvollziehbarkeit und Transparenz der durchgeführten Handlungen sicherzustellen.
3 - Schwachstellenerkennung („Vulnerability Discovery“)	Verwendung der zuvor gesammelten Informationen, um potentielle Schwachstellen oder Fehlkonfigurationen zu identifizieren, die es ermöglichen, in eines der Ziele einzudringen (bspw. durch aktive Schwachstellenscans, einschließlich der Identifikation von verwundbaren Netzwerkprotokollen und -kommunikation. Hiermit werden mögliche Angriffsvektoren identifiziert und der **Grundstein für die nachfolgenden Phasen** gelegt.
4 - Zugangserlangung („Gaining Access“ bzw. „Exploitation Phase“)	Ausnutzen der erkannten Schwachstellen: - Typischerweise werden zunächst die identifizierten verwundbaren Netzwerkprotokollen und -kommunikation angegriffen. Sofern die Ziele mit angemessenen Maßnahmen zur Angriffserkennung ausgestattet sind, sollten diese spätestens in dieser Phase entsprechende Alarme auslösen.

	- Daneben können Netzwerkdaten von BenutzerInnen abgefangen und umgeleitet werden, die auf den Zielsystemen Zugangsberechtigungen besitzen. Nach erfolgreichem Zugang zu einem der Zielsysteme können die PenTesterInnen auf dessen Daten und Informationen zugreifen. Falls vom Untersuchungsauftrag umfasst, werden die hierbei erlangten Daten/Informationen für den Angriff auf weitere Ziele genutzt. Mit Blick auf das „Acht Phasen"-Modell initiieren die PenTesterInnen auf jedem System, das sie unter ihre Kontrolle gebracht haben, eine **neue** (2) Reconnaissance- und (3) Vulnerability-Discovery-Phase, um zusätzliche potenzielle Angriffsvektoren zu identifizieren und gegebenenfalls weitere Ziele anzugreifen („Lateral Movement").
5 - Zugriff aufrechterhalten („Maintaining Access" bzw. „Persistence")	Anschließend wird der Zugang „verankert" – bspw. durch die Installation von Fernsteuerungssoftware, den missbräuchlichen Einsatz bereits vorhandener Software oder die Schaffung neuer Zugangsmöglichkeiten. Hintergrund: Hiermit kann jederzeit auf das Ziel zugegriffen werden, ohne dass gegebenenfalls Teile des Angriffs wiederholt werden müssen. Gleichzeitig simuliert es realistisches Angreiferverhalten. Oftmals werden durch echte Angreifer zwei bis drei Hintertüren oder Zugänge pro kompromittiertem System eingerichtet.

6 – Analysephase („Analysis“)	Analyse der erlangten Informationen, Daten und technischen Zugänge bzgl. (1) Kritikalität und (2) Tragweite für die Organisation. Parameter der Risikobewertung: - Wie herausfordernd – oder einfach – war es, entsprechende Informationen oder Zugänge zu erlangen? - Welches sind die kritischsten Systeme im Kontext der vereinbarten Zielstellung? - Welche Daten oder Informationen wurden erlangt und welche potentiellen Auswirkungen hat dies auf die Organisation? Darauf aufbauend können mögliche Gegenmaßnahmen für die identifizierten Sicherheitsrisiken erarbeitet werden.
7 - Berichterstattung („Reporting“)	Zusammenstellung der Erkenntnisse und Bewertungen in einem umfassenden Bericht. Struktur: - Informationen über den vorher festgelegten Rahmen, die Zielsetzung und die freigegebenen Angriffstechniken sowie -werkzeuge - Detaillierte zeitliche Auflistung der von den PenTesterInnen durchgeführten Aktivitäten und der

	dabei gewonnenen Erkenntnisse, Informationen und Zugänge - Dokumentation der identifizierten Schwachstellen - Empfehlung von Gegenmaßnahmen in verständlicher Sprache, klarer Priorisierung und Darstellung des Ressourcenbedarfs und Zeitrahmen. Kritische Schwachstellen, die sofortiges Handeln erforderten, werden besonders hervorgehoben. - Zusammenfassung des gegenwärtigen Sicherheitsniveaus, potentiellen Auswirkungen der identifizierten Schwachstellen und Hinweis auf mögliche Schwachstellen, die trotz der noch umzusetzenden Maßnahmen noch bestehen könnten.
8 - Aufräumphase („Cleanup“)	Anschließend werden die Systeme oder Anwendungen in ihren ursprünglichen Zustand zurückversetzt. Dieser Schritt ist für die Gewährleistung der Systemintegrität von überragender Bedeutung. Typischerweise umfasst dieser Prozess - das Entfernen eingerichteter Seitenkanalzugangsmöglichkeiten, - die Vergabe neuer Passwörter und - das Zurücksetzen veränderter Konfigurationseinstellungen.

	Die einzelnen Schritte sollten umfassend dokumentiert werden.