Bundesverband

Basisleitfaden

Investigation 4.0 – Digitale Forensik

Grundlageninformationen

Stand: 2. Juli 2021

Inhalt:

I. Kerninhalte der digitalen Forensik

Die immense Zunahme der Digitalisierung in Unternehmen und die ausgeprägte Komplexität von rasant zunehmenden Datenmengen, Datenarten, IT-Systemen sowie Geräten verstärken die Bedeutung der digitalen Forensik im Rahmen interner Ermittlungen.

Die digitale Forensik (auch IT-Forensik genannt) beschäftigt sich im Kern mit der systematischen Analyse von IT-Systemen und digitalen Daten. Ziel ist es vor allem, im Rahmen interner Ermittlungen Beweise gerichtsverwertbar zu finden und zu sichern. Die IT-Forensik gewährleistet die Nachvollziehbarkeit und Dokumentation von sachverhaltsrelevanten Ereignissen im digitalen Umfeld und ermöglicht die Identifizierung möglicher Verantwortlicher und eine individuelle Zurechenbarkeit von Verstößen und Straftaten.

Die IT-Forensik unterteilt sich in die Gebiete Daten-Forensik und Computer-Forensik:

- Die Daten-Forensik beschäftigt sich vor allem mit auf IT-Systemen gespeicherten Daten und Inhalten von Datenbanken.
- Die Computer-Forensik kümmert sich vor allem um die Analyse von Geräten.

Im Laufe einer IT-forensischen Analyse werden unterschiedliche digitale Spuren identifiziert, lokalisiert und gesichert. Hierzu zählen zum Beispiel:

- Anmeldungen und Zeitstempel
- Ausgeführte Anwendungen
- Downloads von Dateien aus dem Internet
- Aufrufe von Webseiten
- Ausgeführte Befehle
- Anschluss von externen Geräten
- Logfiles und darauf erfolgte Zugriffe beziehungsweise Modifikationen

Eine systematische Vorgehensweise einer IT-forensischen Analyse, die jeweils an internationalen beziehungsweise länderspezifischen Standards/ Rechtsnormen auszurichten ist, besteht aus einer Reihe an Elementen, wie das folgende Beispiel zeigt:

- Identifizierung: Im ersten Schritt erfolgt eine Bestandsaufnahme, indem insbesondere die Ausgangslage (Fall/Sachverhalt sowie Datenlage) identifiziert wird. Auf dieser Basis werden die zu klärenden Fragen definiert beziehungsweise festgelegt.
- Datensicherung: Alle im ersten Schritt identifizierten Informationen werden gesichert und eine forensische Kopie des zu untersuchenden IT-Systems angefertigt. Hierbei wird auch geklärt, ob das betroffene IT-System während der Analyse weiter betrieben werden kann.
- Analyse: In weiteren Schritten werden zu bestimmten Einzelthemen/Sachzusammenhängen digitale Spuren ermittelt, die zur Aufklärung des Sachverhalts beitragen können.
- Dokumentation und Aufbereitung: Nach der Analyse werden die Ergebnisse nachvollziehbar dokumentiert. Die Dokumentation soll Informationen enthalten, wie etwa ausgeführte Anwendungen, Aufrufe von Webseiten, Identitäten der Anwender sowie Zeiträume, in denen bestimmte Aktionen ausgeführt wurden.

II. Anwendungsfelder der digitalen Forensik

Ergänzend zu den eingangs genannten Kerninhalten der digitalen Forensik werden nachfolgend weitere wesentliche Anwendungsfelder dargestellt:

Die **Betriebssystem-Forensik** ist ein Teilgebiet der IT-Forensik, das sich mit der Auswertung von Betriebssystemen (zum Beispiel Windows, Mac, Unix) befasst.

Als **Browser-Forensik** wird ein Teilgebiet der IT-Forensik bezeichnet, das sich mit den Besonderheiten zu Webbrowser-Artefakten (beispielsweise Browserverlaufsforensik, Browserformularforensik, Cookie-Forensik) befasst.

Immer wieder werden Geschäftsgeheimnisse und sensible Informationen zum Opfer von Datendieben, die nicht selten aus der Organisation selbst kommen. Ein Werkzeug, um dagegen gewappnet zu sein, bietet **Data Leakage Prevention** (auch **Data Loss Prevention**, kurz **DLP**). Darunter lässt sich grob der Schutz vor ungewollten Datenabfluss beziehungsweise die Abwendung des Schadens, der dadurch entstehen kann, wenn sensible Informationen (z.B. Forschungsergebnisse, Rezepturen, Kundendaten, Bankverbindungen, Passwörter, etc.) in die Hände unbefugter Dritter fallen, verstehen. DLP verspricht Abhilfe, indem es die ausgehende E-Mail-Kommunikation auswertet und dadurch gegebenenfalls Spuren zu potenziellem Datendiebstahl ermittelt werden. Eine DLP-Strategie kann aus drei Elementen bestehen:

- Analyse: Datenströme werden in Echtzeit analysiert, um vertrauliche Inhalte sowie Verhaltensanomalien zu erkennen, zum Beispiel ein starker Anstieg ausgehender E-Mails eines einzelnen Users oder der Versand ungewöhnlich großer Datenmengen.
- Auswertung: Die Daten werden über ein webbasiertes Dashboard transparent visualisiert. Nur autorisierte Personen erhalten Zugriff.
- Blockade: Jede verdächtige Kommunikation wird vor Versand gestoppt. Nach einer individuellen Prüfung des Sachverhaltes ist eine manuelle Freigabe der Inhalte nach Unbedenklichkeitseinschätzung möglich.

Die **Datenträger-Forensik** ist ein Teilgebiet der IT-Forensik, das sich mit den Besonderheiten verschiedener Datenträger befasst. Dazu zählen die Festplattenforensik, SSD-Forensik, Speicherkartenforensik, RAM-Baustein-Forensik, Magnetbandforensik, Sicherungsmedien-Forensik, CD-/ DVD-Forensik etc.

Ein weiteres Teilgebiet der IT-Forensik ist die **digitale Multimedia-Forensik**. Diese hat eine systematische Analyse der Authentizität digitaler Mediendaten zum Ziel. Fragestellungen sind hierbei die Bestimmung des Ursprungs digitaler Mediendaten sowie die Erkennung des Ursprungs von Manipulationen an diesen.

Unter **eDiscovery** versteht man in der IT-Forensik bestimmte Software und Verfahren zur Identifikation relevanter Dokumente aus großen Dokumentmengen mittels computerunterstützter Suche und teilautomatisierter Verfahren. Software-Lösungen zur eDiscovery, typischerweise webbasiert, bieten hocheffizient die Möglichkeiten, relevante Dokumente überhaupt oder rascher zu identifizieren. eDiscovery macht zum Beispiel das Finden ähnlicher Dokumente nach Dokumentinhalt (semantisch bzw. konzeptbasiert), Dokumentfamilien oder anderen Eigenschaften möglich. Weitere Aktivitäten im Zuge der eDiscovery können die Suche nach Stichworten, inhaltliche Sichtung großer Dokumentmengen, Beurteilung von Dokumenten hinsichtlich ihrer Relevanz zu Sachverhalten, Schwärzung vertraulicher, privilegierter Dokumentpassagen oder auch Export und Bereitstellung relevanter Dokumente sein.

Das idealtypische Vorgehen der umfassenden zugehörigen Prozesse orientiert sich am sogenannten „Electronic Discovery Reference Model“ (EDRM; s. Abbildung 1).

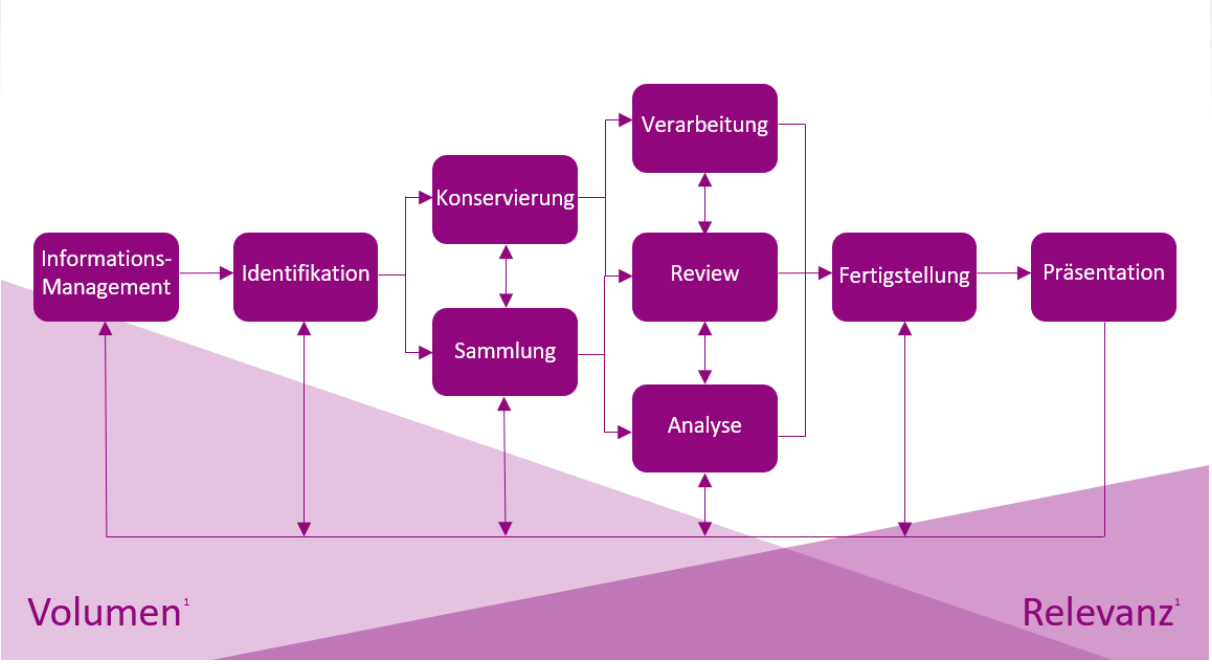

Abbildung 1: Electronic Discovery Reference Model (Eigene Darstellung in Anlehnung an edrm.net)
[1]Während der Verarbeitung großer Datenmengen (d.h. „das Volumen“) werden Informationen auf das reduziert, was relevant ist.

Endpoint-Forensik ist ein Teilgebiet der IT-Forensik, das sich mit bestimmten Endgeräten wie Notebooks und Smartphones befasst.

Live-/ Remote-Forensik ist ein Teilgebiet der IT-Forensik, das sich im Rahmen einer sogenannten „Cyber Incident Response“ mit den besonderen Bedingungen einer IT-forensischen Sicherung und Auswertung unter kritischen Zeitbedingungen befasst.

Die **Post-Mortem-Forensik** wiederum ist mit der Aufklärung eines Vorfalls im Nachhinein befasst. (Beispiel: Durchführung einer Datenanalyse mit Schwerpunkt auf der Datenwiederherstellung gelöschter Daten und gespeicherter Informationen).

Malware-Forensik mittels Reverse Engineering umfasst die Analyse von bösartiger Software (Malware) mit dem Ziel, ihren inneren Aufbau, ihre Struktur, zu erkennen und zu verstehen.

Netzwerk-Forensik bezeichnet das Teilgebiet der IT-Forensik, das sich mit den Besonderheiten der Konfiguration und von Datenverkehr in Computernetzwerken befasst. Dazu zählen das Mitschneiden von Netzwerkverkehr, die Auswertung von Datenverkehr zu Malware mit Wireshark, die Auswertung der Konfiguration von Routern, Switches, Servern etc.

III. Grundsätze elektronischer Datensichtung/ -auswertung

Zur Sichtung und Auswertung von Daten sind rechtliche und betriebliche Anforderungen vorab zu klären. Im ersten Schritt ist unter anderem die geplante Vorgehensweise und das Ziel einer Sichtung und Auswertung mit dem Datenschutzbeauftragtem abzustimmen, sodass die Ermittlungshandlungen (einschließlich der eingesetzten IT-Forensik-Tools) datenschutzkonform und damit auch verwertbar sind.

Im Zuge einer Ermittlung kann das Ermittlungsteam vorab bereits entsprechende Suchbegriffe festlegen, nach denen die Sichtung der Daten durchgeführt wird. Mit entsprechenden IT-Forensik-Tools ist insoweit sichergestellt, dass nur Daten in die Sichtung miteinbezogen werden, die diesen Kriterien entsprechen. Das kann eine größere Effizienz schaffen.

Dabei gelten bestimmte Vorgaben des Datenschutzes, beispielsweise eine dedizierte Privatfilterung. Dies gilt es insbesondere zu berücksichtigen, sofern die Privatnutzung von Hardware sowie E-Mails durch Mitarbeiter erlaubt ist und damit als privat gekennzeichnete Daten aus der Analyse zu entfernen sind. Damit werden die datenschutzrechtlichen Belange des Mitarbeiters gewährleistet.

Der Prozess der Datenauswertung ist nachvollziehbar und lückenlos zu dokumentieren. Dazu gehören beispielsweise die exakten Datenquellen, analysierte Datenbestände, angewandte Filter wie Suchbegriffe, Zeit- oder Dateitypfilter sowie die Ergebnisse der Analysen. Eine enge Zusammenarbeit zwischen Ermittlern und IT-Forensikern ist essenziell, um sicherzustellen, dass alle Beteiligten einen einheitlichen Sachstand beziehungsweise dasselbe Verständnis der Ermittlung und deren Ziele haben. Eine Formularvorlage kann helfen, den Start in die Dokumentation zu gestalten (s. Anhang).

Daneben sind die in der Auswertung genutzten Daten entsprechend zu archivieren, sodass eine mögliche Wiederherstellung zu einem späteren Zeitpunkt gewährleistet ist. Im Zuge der Archivierung von Daten und vor dem Hintergrund des datenschutzrechtlichen Grundsatzes der Datensparsamkeit sind entsprechende Löschfristen festzulegen. Bei der Implementierung der Löschfristen müssen die datenschutzrechtlichen Belange berücksichtigt werden. Insbesondere bei der externen Vergabe an einen Dienstleister von Ermittlungen sind Löschfristen entsprechend abzustimmen und auf vertraglicher Basis zu vereinbaren.

IV. Beispiele elektronischer Datensicherung/ -aufbereitung

Quell-Datenvolumen	**< 1 TB**	**< 10 TB**	**< 100 TB**	**> 100 TB**
Datensicherung	Forensische Datensicherung unter Verwendung eines entsprechenden Prozesses auf Festplatten (Target, Backup und Working Copy).		Forensische Datensicherung auf ein Netzlaufwerk (RAID 6[1]), sowie eine zusätzliche Kopie auf externer Festplatte.	Forensische Datensicherung in virtuellen Containern (bspw. Microsoft VHD) auf ein Netzlaufwerk (RAID 6), sowie Erstellung eines „Offsite-Backup Storage“[2].
Datensicherungen Besonderheiten	-		Der Aufbau einer eigenen Datensicherungsstraße mit entsprechendem Prozess zur Sicherung und Benamung von Quell-Daten ist sinnvoll.	

[1] RAID6 („Redundant Array of Independent Level 6“) bezeichnet einen Datenspeicher mit doppelter Ausfallsicherheit
[2] Datenspeicher, der sich physikalisch an einem gesonderten Lagerort befindet, um zum Beispiel Datenverlust durch einen Brand auszuschließen

Quell-Datenvolumen	< 1 TB	< 10 TB	< 100 TB	> 100 TB
Datenaufbereitung	Datenaufbereitung mittels eines Tools[3] wie EnCase, X-Ways, FTK oder NUIX als Pre-Processor für beispielsweise eDiscovery.			
Datenaufbereitung Besonderheiten	Direkter Aufbau eines maximalen Datenbestandes für die Analyse, beispielsweise durch das Entpacken von Archiven und Suche nach gelöschten Dateien und Dateiformaten.		Stufenweise und bedarfsorientierter Aufbau eines maximalen Datenbestandes für die Analyse, um die Datenmenge beherrschbar zu halten.	
Personalbedarf	Einzelplatzauswertung durch einen Analysten möglich.	Auswertung durch mehrere Analysten sinnvoll.	Aufteilung in funktionale Teams: Datensicherung, Datenaufbereitung und Sichtung.	Aufteilung in funktionale Teams: Datensicherung, Datenaufbereitung und Sichtung, wobei eine weitere sachverhaltsbezogene Aufteilung in mehrere Teams zur Sichtung sinnvoll sein kann.

V. Datenaustausch mit Behörden (Dos & Don‘ts)

Dos	Don‘ts
Beweisbeschluss Abstimmung mit den Behörden, um Art und Umfang der Daten klar zu definieren. Idealerweise sollte ein formeller Beweisbeschluss vorliegen, der die Anforderungen detailliert spezifiziert.	**Beeinträchtigung der Datenintegrität** Löschung/ Veränderung von Daten nach Beginn einer etwaigen Untersuchung oder anderweitige Veränderung von Beweismitteln (bspw. „Ansehen“ von Laptops durch die eigene IT, ohne Berücksichtigung, was rechtlich erlaubt ist).
Kommunikationsprotokoll Festlegung eines Kommunikationsprotokolls mit den Behörden, inklusive der Bestimmung der angemessenen Amtssprache (in Abhängigkeit des Gerichtsstandes).	**Kommunikationsprotokoll** Unabgestimmte Kommunikation zwischen Stakeholdern des Unternehmens mit Behörde(n).

[3] Beispielhafte Auswahl von forensischen Softwareprodukten, die zur Analyse (EnCase, FTK, X-Ways) oder zur Vorverarbeitung von Datenbeständen für eDiscovery genutzt werden können (NUIX)

Dos	Don'ts
Externer Rechtsbeistand Einbindung eines sachkundigen Rechtsbeistandes (intern oder extern) zur Begleitung des Prozesses des Datenaustausches, etwa zur Wahrung datenschutzrechtlicher Aspekte). Darüber hinaus sollte je nach Status (Zeuge versus Beschuldigter) eine entsprechende Datensicherungsstrategie besprochen werden.	**Fristenwahrung** Verspätete Identifikation der notwendigen Ressourcen, um behördliche Anfragen fristgerecht und mit der notwendigen Sorgfalt und unter Wahrung der in der Regel rigiden Anforderungen zu erfüllen.
Document Preservation Notice Hinweis zur Aufbewahrung von Dokumenten an betroffene Personen (Document Preservation Notice), sofern die Möglichkeit besteht, dass Dokumente/ Dateien gelöscht oder verändert werden können.	**Wahrung der Unabhängigkeit** Datensicherung und/ oder Übermittlung durch Personen die möglicherweise Gegenstand der Untersuchung sind.
Zusammenarbeit/ Kollaboration Abhängig von möglicher Verteidigungsstrategie, frühzeitige Kollaboration mit Behörden anbieten und etwa Erläuterung der diversen Daten anbieten. Auch kann das Anbieten der Nutzung der eigenen Infrastruktur speziell im Zeugenstatus hilfreich sein.	**Datenerfassung** Unsystematische Erfassung von Daten/ Datenerfassung, die forensischen Ansprüchen nicht genügt.
Datenübermittlung Frühzeitige Abstimmung des Formats und Datenträger/ technische Ausgestaltung der Datenübermittlung und eine Prüfung, ob die Übergabe im geforderten Format erfolgen kann.	**Datenübermittlung** Unsachgemäße Übermittlung von Daten, beispielsweise ohne angemessene Verschlüsselung sensibler Daten. Die Übermittlung von „zu viel" und nicht vom Untersuchungsgegenstand erfasster Daten birgt die Gefahr von Zufallsfunden durch die Behörden.
Umgang mit sensitiven/ für den Untersuchungsgegenstand irrelevanten Informationen Im Zeugenstatus möglicherweise (und in Abstimmung mit Rechtsbeistand und Behörden) Identifikation/ Schwärzung von Informationen, die zwar in den Untersuchungszeitraum fallen, für den Untersuchungsgenstand jedoch nicht relevant sind.	**Missachtung datenschutzrechtlicher Bestimmungen** Missachtung rechtlicher Vorgaben/ Limitierungen (beispielsweise durch grenzüberschreitende Gesetze wie das Chinese State Secrets Law) oder gar planloses Sichern von Daten.
Chain of custody Sicherstellung der „chain of custody", um lückenlosen Nachweis von der Datenquelle bis zur Übergabe an Behörde(n) zu gewährleisten, inklusive technischer Maßnahmen zur Prüfung der Integrität der Daten (Prüfsummen).	

VI. Ausblick: „Neue“ Applikationen (z.B. Messenger-Dienste)

„Neue“ Applikationen wie Messenger-Dienste (z.B. WhatsApp, Skype) sind zu Alltagswerkzeugen im geschäftlichen Umfeld geworden. Bei Ermittlungen sind bestimmte Aspekte beziehungsweise Risiken in diesem Zusammenhang zu beachten. Einige Risikofaktoren werden im Folgenden exemplarisch und kurz skizziert.

1. Welche Daten könnten mit dem Kommunikationsmittel versendet werden?

Neben reinen Textnachrichten, die natürlich auch vertrauliche Informationen (Geschäftsgeheimnisse) enthalten können, birgt vor allem die Möglichkeit, verschiedene Datenformate (zum Beispiel MS-Office, PDFs, Bilddateien) zu versenden, ein erhöhtes Risiko eines unerwünschten Datenverlustes (zum Beispiel schützenswertes Know-how des Unternehmens oder von Geschäftspartnern, vertrauliche Unterlagen). Daher ist bei Nutzung dieser Applikationen stets sicherzustellen, dass interne Regeln zum Schutz vertraulicher Informationen eingehalten und keine Vertraulichkeitsvereinbarungen, die mit externen Bezugsgruppen abgeschlossen wurden, verletzt werden.

2. Verarbeitung der Daten und potenzielles Ausspähris iko

Die Server der genutzten Kommunikationsmittel befinden sich häufig in Ländern außerhalb der EU, die im Sinne der EU-Datenschutzgrundverordnung datenschutzrechtlich als „unsichere Drittländer“ (so zum Beispiel auch die USA) gelten. Das kann einerseits zu einem erhöhten Risiko hinsichtlich Ausspähens der Daten führen, wenn beispielsweise US-Behörden grundsätzlich Zugriff darauf haben. Andererseits ist bei Verstößen eine Rechtsverfolgung bei den örtlichen Stellen/ Gerichten entweder gar nicht oder nur sehr schwer möglich ist. Außerdem ist das sogenannte „US-EU Privacy Shield“, das bis vor kurzem eine „sichere“ Übertragung personenbezogener Daten an zertifizierte US-Unternehmen ermöglicht hat, vom Europäischen Gerichtshof für ungültig erklärt worden. Daher herrscht gegenwärtig Unsicherheit, auf welchem Wege (zum Beispiel über EU-Standardvertragsklauseln) eine rechtlich sichere Alternative erreicht werden kann.

3. Protokollierung der Nutzung

Im Vergleich zu den „klassischen“ Kommunikationsmitteln und -systemen wie E-Mail (zum Beispiel Lotus Notes oder Microsoft Outlook) gestaltet sich die Protokollierung der Datentransfers bei „neuen“ Applikationen und Messenger-Diensten oftmals anders, etwa hinsichtlich Detaillierung der Protokollierung und deren Verfügbarkeitsdauer. Das erschwert unter Umständen auch die nachträgliche Auswertung erheblich, etwa im Rahmen interner Ermittlungen. E-Mail-Daten werden beispielsweise direkt in den E-Mail-Accounts abgelegt und archiviert. Eine vergleichbare Methode ist bei Messenger-Diensten nicht zwingend vorhanden. Die konkrete Ausgestaltung sollte daher mit den betroffenen IT-Dienstleistern festgelegt werden. Auf diese Weise kann geklärt werden, wie Daten in einem ausreichenden Umfang gespeichert und für interne Ermittlungen schnell verfügbar gemacht werden können. Diesem Ziel könnten zum Beispiel schwer zugängliche Daten auf Cloud-Servern im Ausland entgegenstehen.

4. Beschränkung der Nutzung auf Firmengeräte

Es empfiehlt sich zu klären, ob die Nutzung „neuer“ Applikationen und Kommunikationsmittel ausschließlich auf firmeneigenen Geräten gestattet werden soll, um dadurch Sicherheitsstandards vorgeben zu können. Ebenso kann die Nutzung unter Umständen für bestimmte Abteilungen, die tatsächlich einen berechtigten Bedarf wie für den Vertrieb in bestimmten Regionen daran haben, beschränkt werden kann. Außerdem sollte die berufliche Nutzung auf freiwilliger Basis erfolgen und von Nutzern eine spezielle Nutzungs- und Vertraulichkeitserklärung eingeholt werden, die auch datenschutzrechtliche Aspekte abdecken kann.

5. Risiken bei gestatteter Privatnutzung der betrieblichen IT-Systeme

Abschließend sei wiederholt darauf hingewiesen, dass es eine erhebliche Rolle für Auswertungen im Rahmen interner Ermittlungen spielt, ob eine Privatnutzung der betrieblich zur Verfügung gestellten IT-Systeme generell gestattet ist oder nicht. Bei nicht erlaubter Privatnutzung wird angenommen, dass sämtliche Daten in allen Programmen firmenbezogen sind. Eine klare formale Regelung unter Berücksichtigung relevanter datenschutzrechtlicher und betriebsverfassungsrechtlicher Anforderungen wie dem Mitbestimmungsrecht des Betriebsrats kann potenzielle Datenauswertungen bei internen Ermittlungen erheblich vereinfachen. Zu beachten ist in diesem Zusammenhang, dass die Privatnutzung nicht nur ausdrücklich untersagt sein muss (zum Beispiel in einer Betriebsvereinbarung), sondern dass diese auch vom Unternehmen unter Ahndung von Verstößen kontrolliert werden muss. Andernfalls kann eine sogenannte „betriebliche Übung“ entstehen. Das Unternehmen kann sich im Zweifel, also etwa bei Einsprüchen betroffener Mitarbeiter gegen Einsichtnahme in ihr Nutzerkonto, nicht mehr auf das Verbot der Privatnutzung berufen, da das Unternehmen die Privatnutzung stillschweigend toleriert hat.

6. Praxistipp

Als Konsequenzen sollten hinsichtlich möglicher Risiken und einer effektiven Durchführbarkeit von internen Ermittlungen beim Einsatz „neuer“ Applikationen mehrere Aspekte berücksichtigt werden. Die Entscheidung über eine Nutzung sollte sich einerseits an der Sensibilität der verarbeiteten Unternehmensdaten orientieren: Könnten potenzielle Geschäftsgeheimnisse gefährdet sein? Andererseits können interne Ermittlungen durch den Einsatz unnötig erschwert werden. Dies könnte etwa bei einer gestatteten Privatnutzung betrieblicher IT-Infrastruktur der Fall sein, da dann in der Regel „private“ Daten enthalten sind, die nicht ohne weiteres ausgewertet werden dürfen. Auch deshalb sollten grundsätzlich Datenschutz und Betriebsrat einbezogen werden. Schließlich empfiehlt sich die Festlegung von klaren und auch an die Belegschaft kommunizierten „Spielregeln“. Dies passiert am besten in Form von Nutzungsleitfäden (inklusive „Dos and Don‘ts“) und der deutlichen Darstellung möglicher Konsequenzen bei Verstößen.

VII. Anhang: Vorlage/ Formular „eDiscovery“

Allgemeine Informationen			
Projektname		Wesentlicher Stakeholder	
Kontaktpunkt/ Stakeholder	Projekt-Manager, IT, Forensic Technology, DPO, Betriebsrat		
Projektbeschreibung			
Projektbudget		Blatt-Nummer	

Fristen			
1. Datenakquise		3. Abschlussbericht	
2. Review Start		4. Sonstiges	

Umfang												
Namen der Custodians (nach Priorität geordnet)	Datenquellen (E-Mails, Laptop/Desktop, Telefon, Homeshare, Server, etc.)								Anzahl/ Größe der Einheiten	Datenschutz-berücksichtigung		
										☐	erledigt	
										☐	erledigt	
										☐	erledigt	
										☐	erledigt	
										☐	erledigt	
										☐	erledigt	
Untersuchter Zeitraum	Start:				Ende:							
	☐	Zeitplananalyse	☐	Daten-Zeitanalyse					☐	Bericht über gelöschte Dateien		
	☐	E-Mails	☐	Internet Messaging		☐	Sonstiges:					

Verarbeitung – Ausnahmen zu Kommentaren hinzufügen													
Deduplizierung	☐	global	☐	nach Custodian	☐	länderübergreifend	☐	Keine	☐	Sonstiges:			
	Ausschluss privater Daten		Beschreibung:										
	Sensible militärische Daten		Beschreibung:										
Gelöschte Dateien wiederherstellen	☐	Level 1 – Gelöschte Dateien wiederherstellen (restore)	☐	Level 2 – Gelöschte Dateien wiederherstellen (carving)	☐	Keine							

Strategie der Dokumentensichtung													
Sichtungs-ebenen	☐	1st Level	☐	2nd Level	☐	vertraulich	☐	Fremdsprache	☐	Qualitätskontrolle			
	☐	Sonstiges:											
Familienkonsistenz	☐	Ja, inkl. Familienüberprüfung					☐	Nein, nur Suchtreffer					
Sichtung	☐	Suchbegriffsbasierend	☐	Adhoc-Suchen	☐	TAR	☐	Sonstiges:					
Antwortmöglichkeiten	☐	hoch relevant	☐	relevant	☐	Nicht relevant	☐	unsicher	☐	Fremdsprache			
	☐	nicht einsehbar	☐	privat oder geschützt			☐	Sonstiges:					
Kommentare	☐	Ja	☐	Nein	Überprüfungsebene überschreiben		☐	Ja	☐	Nein			
Themen					Sonstiges								

Analytik	☐ E-Mail-Threading	☐ Deduplizierung ähnlicher Texte	Ähnlichkeitswert (in %)
	☐ Sprachidentifikation	☐ Gruppierung	☐ Sonstiges:

Berechtigungen													
1st Level	☐	Ausdruck	☐	Schwärzung	☐	Lokaler Zugriff	☐	Gespeicherte Suchabfragen	☐	Treffer Hervor-hebung	☐	Sonstiges:	
2nd Level	☐	Ausdruck	☐	Schwärzung	☐	Lokaler Zugriff	☐	Gespeicherte Suchabfragen	☐	Treffer Hervor-hebung	☐	Sonstiges:	
Vertraulich	☐	Ausdruck	☐	Schwärzung	☐	Lokaler Zugriff	☐	Gespeicherte Suchabfragen	☐	Treffer Hervor-hebung	☐	Sonstiges:	
Fremdsprache	☐	Ausdruck	☐	Schwärzung	☐	Lokaler Zugriff	☐	Gespeicherte Suchabfragen	☐	Treffer Hervor-hebung	☐	Sonstiges:	
Qualitäts-prüfung	☐	Ausdruck	☐	Schwärzung	☐	Lokaler Zugriff	☐	Gespeicherte Suchabfragen	☐	Treffer Hervor-hebung	☐	Sonstiges:	
Sonstiges:	☐	Ausdruck	☐	Schwärzung	☐	Lokaler Zugriff	☐	Gespeicherte Suchabfragen	☐	Treffer Hervor-hebung	☐	Sonstiges:	
Sonstiges:	☐	Ausdruck	☐	Schwärzung	☐	Lokaler Zugriff	☐	Gespeicherte Suchabfragen	☐	Treffer Hervor-hebung	☐	Sonstiges:	

Tools			
Name	Aufgaben (Datenerfassung, Verarbeitung, Review, Analytik, Produktion)	Lizenzierung/ Kosten	Datenschutz-berücksichtigung

Kommunikation															
Typ/ Aufgabe			Kanal (E-Mail, Cloud, etc.)			Frequenz (täglich, wöchentlich, monatlich)				Zeitplan		Kommentar			
Fortschritt Datenverarbeitung															
Überprüfungsfortschritt															
Suchbegriffsberichte															
Analyse sozialer Netzwerke															
Kommunikationsanalyse															
Zeitplananalyse															
Wasserfall-Bericht	☐	Ja	☐	Nein	OCR	☐	Ja	☐	Nein	Sonstiges:					

Begleitende Notizen	
Datum/ Uhrzeit	Notiz

Formular aus-gefüllt von		Datum (tt/mm/jj)		Ort		Unterschrift	