

DIN EN ISO/IEC 27037



ICS 35.040

Einsprüche bis 2016-04-26

Entwurf

**Informationstechnik –
IT-Sicherheitsverfahren –
Leitfaden für die Identifikation, Sammlung, Erhebung und Erhaltung der
digitalen Beweissicherung (ISO/IEC 27037:2012);
Deutsche und Englische Fassung FprEN ISO/IEC 27037:2016**

Information technology –
Security techniques –
Guidelines for identification, collection, acquisition and preservation of digital evidence
(ISO/IEC 27037:2012);
German and English version FprEN ISO/IEC 27037:2016

Technologies de l'information –
Techniques de sécurité –
Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves
numériques (ISO/IEC 27037:2012);
Version allemande et anglaise FprEN ISO/IEC 27037:2016

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2016-02-26 wird der Öffentlichkeit zur Prüfung und
Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes
besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de bzw. für Norm-Entwürfe
der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort
wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im
Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter
www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA),
10772 Berlin (Hausanschrift: Burggrafenstr. 6, 10787 Berlin).

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten
Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 98 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (FprEN ISO/IEC 27037:2016) wurde vom Technischen Komitee ISO/IEC JTC 1/SC 27 „IT Security techniques“ erarbeitet, dessen Sekretariat vom DIN (Deutschland) gehalten wird. Auf Grundlage eines CEN/BT Beschlusses wurde ISO/IEC 27037:2012 im einstufigen Annahmeverfahren (UAP) als FprEN ISO/IEC 27037:2016 ohne Abänderung übernommen.

Das zuständige deutsche Spiegelgremium ist der Arbeitskreis NA 043-01-27-04 AK „IT-Sicherheitsmaßnahmen und Dienste“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung der FprEN ISO/IEC 27037 beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

Für die in diesem Dokument zitierten Internationalen Normen wird im Folgenden auf die entsprechenden Deutschen Normen hingewiesen:

ISO/IEC 27000 siehe DIN ISO/IEC 27000¹⁾

Nationaler Anhang NA (informativ)

Literaturhinweise

E DIN ISO/IEC 27000, *Informationstechnik — IT-Sicherheitsverfahren — Informationssicherheits-
Managementsysteme — Überblick und Terminologie (ISO/IEC DIS 27000:2015)*

¹⁾ In Bearbeitung.

Informationstechnik — IT-Sicherheitsverfahren — Leitfaden für die Identifikation, Sammlung, Erhebung und Erhaltung der digitalen Beweissicherung (ISO/IEC 27037:2012)

Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques (ISO/IEC 27037:2012)

Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence (ISO/IEC 27037:2012)

ICS:

Deskriptoren

Dokument-Typ: Europäische Norm
Dokument-Untertyp:
Dokument-Stage: Einstufiges Annahmeverfahren
Dokument-Sprache: D

STD Version 2.7g

Inhalt

	Seite
Europäisches Vorwort	4
Vorwort	5
Einleitung	6
1 Anwendungsbereich	8
2 Normative Verweisungen	8
3 Begriffe	9
4 Abkürzungen	12
5 Überblick	13
5.1 Kontext für die Sammlung von digitalen Beweismitteln	13
5.2 Grundsätze der digitalen Beweisführung	13
5.3 Anforderungen an die Bearbeitung von digitalen Beweismitteln	14
5.3.1 Allgemeines	14
5.3.2 Auditierbarkeit	14
5.3.3 Wiederholbarkeit	14
5.3.4 Vergleichbarkeit	15
5.3.5 Begründbarkeit	15
5.4 Prozesse zur Bearbeitung von digitalen Beweismitteln	15
5.4.1 Überblick	15
5.4.2 Identifikation	16
5.4.3 Sammlung	16
5.4.4 Erhebung	17
5.4.5 Erhaltung	18
6 Schlüsselkomponenten bei der Identifikation, Sammlung, Erhebung und Erhaltung von digitalen Beweismitteln	18
6.1 Beweismittelkette	18
6.2 Vorkehrungen am Vorfallort	19
6.2.1 Allgemeines	19
6.2.2 Personal	20
6.2.3 Potentielle digitale Beweismittel	20
6.3 Rollen und Verantwortlichkeiten	21
6.4 Kompetenz	21
6.5 Anwendung angemessener Sorgfalt	22
6.6 Dokumentation	22
6.7 Einsatzbesprechung (Briefing)	23
6.7.1 Allgemeines	23
6.7.2 Spezifische Einsatzbesprechung für digitale Beweismittel	23
6.7.3 Personalbezogene Einsatzbesprechung	24
6.7.4 Echtzeit-Vorfälle	24
6.7.5 Sonstige Informationen aus der Besprechung	24
6.8 Priorisierung der Sammlung und Erhebung	25
6.9 Erhaltung von potentiellen digitalen Beweismitteln	26
6.9.1 Überblick	26
6.9.2 Erhalten von potentiellen digitalen Beweismitteln	26
6.9.3 Verpacken von digitalen Geräten und potentiellen digitalen Beweismitteln	26

6.9.4	Transport von potentiellen digitalen Beweismitteln	28
7	Phasen der Identifikation, Sammlung, Erhebung und Erhaltung	28
7.1	Computer, Peripheriegeräte und digitale Speichermedien.....	28
7.1.1	Identifikation	28
7.1.2	Sammlung.....	31
7.1.3	Erhebung	35
7.1.4	Erhaltung.....	40
7.2	Netzwerkgeräte.....	40
7.2.1	Identifikation	40
7.2.2	Sammlung, Erhebung und Erhaltung	42
7.3	Sammlung, Erhebung und Erhaltung von Daten aus CCTV-Systemen.....	44
Anhang A (informativ) Beschreibung von Schlüsselqualifikationen und Kompetenzen des DEFR.....		47
Anhang B (informativ) Mindestanforderungen an die Dokumentation für den Transfer von Beweismitteln.....		50
Literaturhinweise.....		51

Europäisches Vorwort

Der Text von ISO/IEC 27037:2012 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“, Unterkomitee SC 27 „IT security techniques“ der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und auf Grundlage eines CEN/BT Beschlusses als FprEN ISO/IEC 27037:2016 übernommen. Dieses Dokument ist derzeit zum einstufigen Annahmeverfahren vorgelegt.

Anerkennungsnotiz

Der Text von ISO/IEC 27037:2012 wurde vom CEN als FprEN ISO/IEC 27037:2016 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Internationale Organisationen, staatlich und nichtstaatlich, in Liaison mit ISO und IEC, nehmen ebenfalls an der Arbeit teil. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames technisches Komitee (JTC, en: joint technical committee), ISO/IEC JTC 1, eingerichtet. Internationale Normen werden in Übereinstimmung mit den Regeln nach ISO/IEC Direktive, Teil 2 erarbeitet.

Die Hauptaufgabe von Technischen Komitees ist es Internationale Normen zu erarbeiten. Internationale Norm-Entwürfe, die von Technischen Komitees verabschiedet wurden, werden den Mitgliedsorganisationen zur Abstimmung zur Verfügung gestellt. Für die Veröffentlichung als Internationale Norm werden mindestens 75 % Zustimmung der Mitgliedsorganisationen benötigt.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

ISO/IEC 27037:2012 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“, Unterkomitee SC 27 „IT security techniques“, erarbeitet.

Einleitung

Diese Internationale Norm liefert einen Leitfaden für spezifische Tätigkeiten bei der Bearbeitung von potentiellen digitalen Beweismitteln; diese Prozesse sind: Identifikation, Sammlung, Erhebung und Erhaltung von potentiellen digitalen Beweismitteln. Diese Prozesse sind bei einer Ermittlung erforderlich, die ausgelegt ist, die Integrität der digitalen Beweismittel aufrechtzuerhalten — eine akzeptable Vorgehensweise bei der Erhebung von digitalen Beweismitteln, die deren Zulässigkeit vor Gericht und in Disziplinarverfahren sowie in anderen Instanzen unterstützt. Diese Internationale Norm bietet außerdem einen allgemeinen Leitfaden für die Sammlung von nicht digitalen Beweismitteln, die bei der Analyse von potentiellen digitalen Beweismitteln behilflich sein können.

Ziel dieser Internationalen Norm ist es, einen Leitfaden für diejenigen Personen bereitzustellen, die für die Identifikation, Sammlung, Erhebung und Erhaltung von potentiellen digitalen Beweismitteln verantwortlich sind. Zu diesen Personen zählen Experten für digitale Spurensicherung (DEFR, en: Digital Evidence First Responder), Spezialisten für digitale Beweismittel (DES, en: Digital Evidence Specialist), Spezialisten für die Reaktion auf einen Vorfall und Leiter von kriminaltechnischen Laboratorien. Diese Internationale Norm stellt sicher, dass die verantwortlichen Personen die potentiellen digitalen Beweismittel auf praktische, weltweit anerkannte Art und Weise handhaben, während ihre Integrität und Authentizität erhalten bleiben, mit dem Ziel, die Ermittlung im Zusammenhang mit digitalen Geräten und digitalen Beweismitteln auf systematische und objektive Weise zu erleichtern.

Ziel dieser Internationalen Norm ist es außerdem, Informationen für diejenigen Entscheidungsträger zu liefern, die dafür zuständig sind, die Verlässlichkeit der ihnen vorgelegten digitalen Beweismittel zu bestimmen. Sie gilt für Organisationen, deren Aufgabe es ist, potentielle digitale Beweismittel zu schützen, zu analysieren und zu präsentieren. Sie ist für Stellen zur politischen Entscheidungsfindung relevant, die Verfahrensweisen in Bezug auf die digitalen Beweismittel erstellen und bewerten, und die oftmals Teil einer größeren beweisführenden Stelle sind.

Die in dieser Internationalen Norm in Bezug genommenen potentiellen digitalen Beweismittel können aus verschiedenen Arten von digitalen Geräten, Netzwerken, Datenbanken usw. bezogen werden. Diese Internationale Norm bezieht sich auf Daten, die bereits in einem digitalen Format vorliegen. Es ist nicht das Ziel dieser Internationalen Norm, die Umwandlung von analogen Daten in ein digitales Format zu behandeln.

Wegen der Fragilität von digitalen Beweismitteln ist es notwendig, eine zulässige Vorgehensweise umzusetzen, um die Integrität und Authentizität der potentiellen digitalen Beweismittel sicherzustellen. Diese Internationale Norm fordert nicht den Einsatz bestimmter Tools oder Methoden. Schlüsselkomponenten, die der Ermittlung Glaubwürdigkeit verleihen, sind die umgesetzte Vorgehensweise während des Prozesses sowie die Personen, die für die Durchführung der in der Vorgehensweise festgelegten Aufgaben qualifiziert sind. Diese Internationale Norm behandelt nicht die Vorgehensweise bei Gerichtsverfahren, Disziplinarverfahren und anderen damit zusammenhängenden Maßnahmen zur Handhabung von potentiellen digitalen Beweismitteln, die nicht unter die Identifikation, Sammlung, Erhebung und Erhaltung fallen.

Die Anwendung dieser Internationalen Norm erfordert die Einhaltung nationaler Gesetze, Regeln und Verordnungen. Sie sollte keine spezifischen rechtlichen Anforderungen einer Rechtsordnung ersetzen. Stattdessen kann sie als praktischer Leitfaden für jeden DEFR oder DES bei der Ermittlung im Zusammenhang mit potentiellen digitalen Beweismitteln dienen. Sie betrifft nicht die Analyse von digitalen Beweismitteln und ersetzt keine spezifischen Anforderungen einer Rechtsordnung, die Angelegenheiten wie Zulässigkeit, Beweiskraft, Relevanz und andere rechtlich geregelten Einsatzgrenzen von potentiellen digitalen Beweismitteln vor Gericht betreffen. Diese Internationale Norm kann den Austausch von potentiellen digitalen Beweismitteln zwischen verschiedenen Rechtsordnungen fördern. Um die Integrität der digitalen Beweismittel aufrechtzuerhalten, wird von den Anwendern dieser Internationalen Norm gefordert, dass sie die in dieser Internationalen Norm beschriebenen Verfahrensweisen übernehmen und in Übereinstimmung mit den spezifischen rechtlichen Anforderungen an Beweismittel der jeweiligen Rechtsordnung ergänzen.

Auch wenn diese Internationale Norm keine kriminaltechnische Bereitstellung behandelt, kann eine angemessene kriminaltechnische Bereitstellung die Identifikations-, Sammlungs-, Erhebungs- und Erhaltungsprozesse von digitalen Beweismitteln deutlich unterstützen. Die kriminaltechnische Bereitstellung ist das Erreichen einer angemessenen Fähigkeit der Organisation, mit der sie digitale Beweismittel identifizieren, sammeln, erheben, erhalten, schützen und analysieren kann. Während die in dieser Internationalen Norm beschriebenen Prozesse und Aktivitäten grundlegend reaktive Maßnahmen sind, die für die Ermittlung eines Vorfalls nach dessen Eintreten eingesetzt werden, ist die kriminaltechnische Bereitstellung ein proaktiver Prozess, bei dem versucht wird, solche Ereignisse vorherzusagen.

Diese Internationale Norm ergänzt ISO/IEC 27001 und ISO/IEC 27002, insbesondere die Anforderungen an die erforderlichen Maßnahmen bei der Erhebung von potentiellen digitalen Beweismitteln durch Bereitstellung zusätzlicher Umsetzungsregeln. Des Weiteren findet diese Internationale Norm Anwendung in Kontexten, die nicht im Zusammenhang mit ISO/IEC 27001 und ISO/IEC 27002 stehen. Diese Internationale Norm sollte in Verbindung mit anderen Normen zu digitalen Beweismitteln und zur Ermittlung von Informationssicherheits-Vorfällen gelesen werden.

1 Anwendungsbereich

Diese Internationale Norm bietet einen Leitfaden für spezifische Tätigkeiten bei der Bearbeitung von digitalen Beweismitteln, wozu die Identifikation, Sammlung, Erhebung und Aufrechterhaltung von beweiskräftigen digitalen Beweismitteln zählt. Diese Internationale Norm liefert einen Leitfaden für Personen im Hinblick auf übliche Situationen, die während des Bearbeitungsprozesses von digitalen Beweismitteln eintreten, und unterstützt Organisationen bei deren Disziplinarverfahren und bei der Erleichterung des Austauschs von digitalen Beweismitteln zwischen Rechtsordnungen.

Diese Internationale Norm enthält Hinweise für folgende Geräte und/oder Funktionen, die unter verschiedenen Umständen zum Einsatz kommen:

- digitale Speichermedien, die in handelsüblichen Computern verbaut sind, wie Festplatten, Floppy Disks, optische Datenspeicher und magneto-optische Disketten, Datenträger mit vergleichbaren Funktionen;
- Mobiltelefone, persönliche digitale Assistenten (PDA), persönliche elektronische Geräte (PED), Speicherkarten;
- mobile Navigationssysteme;
- digitale Photo- und Videokameras (einschließlich CCTV);
- handelsübliche Computer mit Netzwerkanschlüssen;
- auf TCP/IP basierende und auf anderen Protokollen basierende Netzwerke; und
- Geräte mit vergleichbaren Funktionen, wie vorstehend genannt.

ANMERKUNG 1 Die vorstehende Auflistung der Geräte ist eine exemplarische Liste und erhebt keinen Anspruch auf Vollständigkeit.

ANMERKUNG 2 Die Umstände umfassen die vorstehend genannten Geräte, die in unterschiedlichen Varianten vorliegen können. Beispielsweise kann ein Automobilsystem ein mobiles Navigationssystem enthalten, einen Datenspeicher und ein sensorisches System.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/TR 15801, *Document management — Information stored electronically — Recommendations for trustworthiness and reliability*

ISO/IEC 17020, *Conformity assessment — Requirements for the operation of various types of bodies performing inspection*

ISO/IEC 17025:2005, *General requirements for the competence of testing and calibration laboratories*

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 27000, ISO/IEC 17020, ISO/IEC 17025, ISO/TR 15801 und die folgenden Begriffe.

3.1

Erhebung

Prozess zur Erstellung einer Kopie von Daten innerhalb eines festgelegten Datensatzes

Anmerkung 1 zum Begriff: Das Ergebnis der Erhebung ist eine Kopie von potentiellen digitalen Beweismitteln.

3.2

vorgesehener Speicherplatz

Bereich auf einem digitalen Speichermedium, einschließlich des Primärspeichers, der zur Speicherung von Daten, einschließlich Metadaten, genutzt wird

3.3

Sammlung

Prozess zur Aufnahme von physischen Elementen, die potentielle digitale Beweismittel enthalten

3.4

digitales Gerät

elektronische Vorrichtung zur Verarbeitung oder Speicherung von digitalen Daten

3.5

digitale Beweismittel

Informationen oder Daten, die in binärer Form gespeichert oder übertragen werden, und die im Sinne von Beweismitteln als relevant befunden wurden

3.6

digitale Beweismittelkopie

Kopie des digitalen Beweismittels, die erstellt wurde, um die Verlässlichkeit des Beweismittels aufrechtzuerhalten, indem sowohl das digitale Beweismittel als auch die Verifizierungsmaßnahmen eingeschlossen sind, wobei die Verifizierungsmethode entweder in die zur Verifizierung verwendeten Tools eingebettet sein oder eigenständig vorliegen kann

3.7

Experte für digitale Spurensicherung

DEFR

(en: Digital Evidence First Responder)

Person, die dazu befugt, ausgebildet und qualifiziert ist, um als erste am Vorfallort tätig zu werden und die Sammlung und Erhebung von digitalen Beweismitteln vorzunehmen und dabei die Verantwortung für die Bearbeitung dieser Beweismittel trägt

Anmerkung 1 zum Begriff: Befugnis, Ausbildung und Qualifikation sind die vorausgesetzten Anforderungen, die notwendig sind, um verlässliche digitale Beweismittel zu erbringen, wobei jedoch individuelle Gegebenheiten dazu führen können, dass eine Person nicht alle drei Anforderungen erfüllt. In diesem Fall sollten die vor Ort geltenden Gesetze, Organisationspolitiken und die individuellen Gegebenheiten berücksichtigt werden.

3.8

Spezialist für digitale Beweismittel

DES

(en: Digital Evidence Specialist)

Person, die die Aufgaben eines DEFR übernehmen kann und über besondere Fachkenntnisse, Fähigkeiten und Fertigkeiten verfügt, um eine Vielzahl an technischen Fragen zu beantworten

Anmerkung 1 zum Begriff: Ein DES kann spezielle Kompetenzen besitzen, wie der Zugang zu Netzwerken, RAM-Zugriff, Ausführen von Systemsoftware oder Kenntnisse über Großrechner (Mainframes).

3.9

digitales Speichermedium

Gerät, auf dem digitale Daten aufgezeichnet werden können

[übernommen aus ISO/IEC 10027:1990]

3.10

Beweissicherungseinrichtung

sichere Umgebung oder ein Ort, in der bzw. an dem die gesammelten oder erhobenen Beweismittel gespeichert werden

Anmerkung 1 zum Begriff: Eine Beweissicherungseinrichtung sollte frei von Magnetfeldern, Staub, Schwingungen, Feuchtigkeit oder anderen Umweltelementen (wie extreme Temperaturen oder Luftfeuchte), die die potentiellen digitalen Beweismittel in der Einrichtung schädigen können, sein.

3.11

Hash-Wert

Bit-Kette als Ergebnis einer Hash-Funktion

[ISO/IEC 10118-1:2000]

3.12

Identifikation

Prozess, der die Such nach, das Erkennen von und die Dokumentation von potentiellen digitalen Beweismitteln umfasst

3.13

Imaging

Prozess zur Erstellung einer bitweisen Kopie eines digitalen Speichermediums

Anmerkung 1 zum Begriff: Die bitweise Kopie wird auch als physische Kopie bezeichnet.

BEISPIEL Beim Imaging-Prozess einer Festplatte würde der DEFR auch die Daten kopieren, die zuvor gelöscht worden sind.

3.14

Peripheriegerät

Gerät, das an ein digitales Gerät angeschlossen ist, um dessen Funktionalität zu erweitern

3.15

Erhaltung

Prozess zur Aufrechterhaltung und Sicherung der Integrität und/oder des Originalzustands von potentiellen digitalen Beweismitteln

3.16

Verlässlichkeit

Eigenschaft der Übereinstimmung zwischen beabsichtigtem Verhalten und den Ergebnissen

[ISO/IEC 27000:2009]

3.17

Wiederholpräzision

Wiederholbarkeit

Eigenschaft eines durchgeführten Prozesses, die gleichen Prüfergebnisse in derselben Prüfumgebung zu erhalten (derselbe Rechner, dieselbe Festplatte, dieselbe Verfahrensweise usw.)

3.18

Vergleichpräzision

Vergleichbarkeit

Eigenschaft eines Prozesses, die gleichen Prüfergebnisse in einer anderen Prüfumgebung zu erhalten (anderer Rechner, andere Festplatte, anderer Bearbeiter usw.)

3.19

Beweisvereitelung

durchführen oder zulassen von Änderungen an potentiellen digitalen Beweismitteln, wodurch deren Beweiswert verringert wird

3.20

Systemzeit

Zeit, die von der Systemuhr generiert und vom Betriebssystem verwendet wird, und nicht die Zeit, die vom Betriebssystem errechnet wurde

3.21

Verfälschen

Vorgang der vorsätzlichen Durchführung oder Genehmigung von Änderungen an den digitalen Beweismitteln (d. h. absichtliche oder zielgerichtete Beweisvereitelung)

3.22

Zeitstempel

zeitabhängiger Parameter, der einen Zeitpunkt im Hinblick auf einen gemeinsamen Zeitbezug bezeichnet

[ISO/IEC 11770-1:1996]

3.23

nicht vorgesehener Speicherplatz

Bereich auf einem digitalen Speichermedium, einschließlich des Primärspeichers, der nicht vom Betriebssystem vorgesehen ist und der für die Speicherung von Daten, einschließlich Metadaten, zur Verfügung steht

3.24

Validierung

Bestätigung durch Bereitstellung eines objektiven Nachweises, dass die Anforderungen für einen spezifischen beabsichtigten Gebrauch oder eine spezifische beabsichtigte Anwendung erfüllt worden sind

[QUELLE: ISO/IEC 27004:2009]

3.25

Verifizierungsfunktion

Funktion, die verwendet wird, um zu verifizieren, dass zwei Datensätze identisch sind

Anmerkung 1 zum Begriff: Zwei verschiedene Datensätze sollten mithilfe der Verifizierungsfunktion keine Übereinstimmung ergeben.

Anmerkung 2 zum Begriff: Verifizierungsfunktionen werden in der Regel mit Hash-Funktionen, wie MD5, SHA1 usw. umgesetzt, wobei jedoch andere Methoden ebenfalls angewendet werden dürfen.

3.26

flüchtige Daten

Daten, die besonders anfällig für Änderungen sind und leicht modifiziert werden können

Anmerkung 1 zum Begriff: Eine Änderung kann das Abschalten der Stromversorgung oder das Passieren durch ein Magnetfeld hindurch sein. Zu den flüchtigen Daten zählen ebenfalls Daten, die sich ändern, wenn sich der Systemstatus ändert. Beispiele sind im RAM gespeicherte Daten und dynamische IP-Adressen.

4 Abkürzungen

AVI	Audio Video Interleave
CCTV	Videouberwachungsanlage (en: Closed Circuit Television)
CD	Compact Disk
DNS	Desoxyribonukleinsäure
DEFR	Experte für digitale Spurensicherung (en: Digital Evidence First Responder)
DES	Spezialist für digitale Beweismittel (en: Digital Evidence Specialist)
DVD	Digital Video/Versatile Disk
ESN	elektronische Seriennummer (en: Electronic Serial Number)
GPS	globales Positionsbestimmungssystem (en: Global Positioning System)
GSM	globales System für mobile Funkkommunikation (en: Global System for Mobile Communication)
IMEI	International Mobile Equipment Identity
IP	Internetprotokoll (en: Internet Protocol)
ISIRT	Informationssicherheitsnotfallteam (en: Information Security Incident Response Team)
LAN	lokales Netzwerk (en: Local Area Network)
MD5	Message-Digest Algorithm 5
MP3	MPEG Audio Layer 3
MPEG	Expertengruppe für bewegte Bilder (en: Moving Picture Experts Group)
NAS	netzgebundener Speicher (en: Network Attached Storage)
PDA	persönlicher digitaler Assistent (en: Personal Digital Assistant)
PED	persönliches elektronisches Gerät (en: Personal Electronic Device)
PIN	persönliche Identifikationsnummer (en: Personal Identification Number)
PUK	PIN-Entsperrschlüssel (en: PIN Unlock Key)
RAID	redundante Anordnung unabhängiger Festplatten (en: Redundant Array of Independent Disks)
RAM	Direktzugriffsspeicher (en: Random Access Memory)
RFID	Identifizierung mithilfe elektromagnetischer Wellen (en: Radio Frequency Identification)
SAN	Speichernetzwerk (en: Storage Area Network)
SHA	sicherer Hash-Algorithmus (en: Secure Hash Algorithm)

SIM	Teilnehmer-Identitätsmodul (en: Subscriber Identity Module)
USB	universeller serieller Bus (en: Universal Serial Bus)
UPS	unterbrechungsfreie Stromversorgung (en: Uninterruptible Power Supply)
USIM	universelles Teilnehmer-Identitätsmodul (en: Universal Subscriber Identity Module)
UV	Ultraviolett
Wi-Fi	kabellose Netzwerkverbindung (en: Wireless Fidelity)

5 Überblick

5.1 Kontext für die Sammlung von digitalen Beweismitteln

Digitale Beweismittel können für den Einsatz in vielen verschiedenen Szenarien erforderlich sein, bei denen ein jeweils unterschiedliches Gleichgewicht der Einflussfaktoren Beweiskraft, Aktualität der Analyse, Wiederherstellung von Systemen und Kosten für die Sammlung der digitalen Beweismittel vorliegt. Aus diesem Grund wird von Organisationen gefordert, einen Priorisierungsprozess durchzuführen, der die Bedürfnisse ermittelt und ein Gleichgewicht zwischen Beweiskraft, Aktualität und Systemwiederherstellung schafft, bevor der DEFR beauftragt wird. Ein Priorisierungsprozess umfasst die Durchführung einer Bewertung des verfügbaren Materials, um den möglichen Beweiswert sowie die Reihenfolge, in der die potentiellen digitalen Beweismittel gesammelt, erhoben oder erhalten werden sollten, zu bestimmen. Die Priorisierung wird durchgeführt, um das Risiko, dass potentielle digitale Beweismittel vereitelt werden, auf ein Mindestmaß zu verringern, und um die Beweiskraft der gesammelten potentiellen digitalen Beweismittel auf ein Höchstmaß zu steigern.

5.2 Grundsätze der digitalen Beweisführung

In den meisten Rechtsordnungen und Organisationen wird die digitale Beweisführung von drei wesentlichen Grundsätzen gesteuert: Relevanz, Verlässlichkeit und Vollständigkeit. Diese drei Grundsätze sind für alle Ermittlungen wichtig, nicht nur für die Ermittlung von digitalen Beweismitteln, die in Gerichtsverfahren zulässig sind. Digitale Beweismittel sind relevant, wenn ein Element eines spezifischen Falls, der ermittelt wird, zu belegen oder zu widerlegen ist. Auch wenn die ausführliche Definition von „Verlässlichkeit“ in den verschiedenen Rechtsordnungen unterschiedlich ausgelegt wird, ist die allgemeine Bedeutung dieses Grundsatzes, „sicherzustellen, dass das digitale Beweismittel ist, was es vorgibt zu sein“, weit verbreitet. Nicht immer ist es notwendig, dass der DEFR alle Daten sammeln muss oder eine vollständige Kopie des digitalen Originalbeweismittels anfertigen muss. Vielmehr bedeutet das Konzept der Vollständigkeit in vielen Rechtsordnungen, dass der DEFR ausreichend potentielle digitale Beweismittel sammeln muss, um deren Elemente angemessen untersuchen oder ermitteln zu können. Dieses Konzept zu verstehen ist für den DEFR von großer Bedeutung, um den Aufwand ordnungsgemäß priorisieren zu können, wenn Zeit und Kosten zu berücksichtigen sind.

ANMERKUNG Der DEFR sollte sicherstellen, dass die Sammlung von potentiellen digitalen Beweismitteln in Übereinstimmung mit den Gesetzen und Verordnungen der örtlichen Rechtsordnung erfolgt, die durch diese spezifischen Gegebenheiten verlangt werden.

Alle vom DEFR und DES zu verwendenden Prozesse sollten vor ihrem Einsatz validiert worden sein. Falls die Validierung extern erfolgt, sollte der DEFR oder der DES verifizieren, dass die Validierung für den spezifischen Einsatz der Prozesse und für die Umgebung und die Gegebenheiten, unter denen die Prozesse durchgeführt werden, angemessen ist. Der DEFR oder DES sollte außerdem:

- a) alle Maßnahmen dokumentieren;
- b) eine Methode bestimmen und anwenden, mit der die Genauigkeit und Verlässlichkeit der Kopie der potentiellen digitalen Beweismittel im Vergleich zur Originalquelle festgestellt werden kann; und
- c) erkennen, dass der Vorgang der Erhaltung von potentiellen digitalen Beweismitteln nicht immer eingriffsfrei erfolgen kann.

5.3 Anforderungen an die Bearbeitung von digitalen Beweismitteln

5.3.1 Allgemeines

Die in 5.2 dargelegten Grundsätze können wie folgt eingehalten werden:

- Relevanz: Es sollte die Möglichkeit bestehen, aufzuzeigen, dass das erworbene Beweismaterial für die Ermittlung relevant ist — d. h. dass es wertvolle Informationen zur Unterstützung der Ermittlung des jeweiligen Vorfalls enthält und dass es gute Gründe für deren Erhebung gab. Durch Audits und Begründungen sollte der DEFR in der Lage sein, die umgesetzten Verfahren zu beschreiben und zu erläutern, wie die Entscheidung für jedes erhobene Element getroffen wurde.
- Verlässlichkeit: Alle Prozesse, die bei der Bearbeitung von potentiellen digitalen Beweismitteln eingesetzt werden, sollten auditierbar und wiederholbar sein. Die Ergebnisse aus der Anwendung solcher Prozesse sollten vergleichbar sein.
- Vollständigkeit: Der DEFR sollte darauf achten, dass ausreichend Beweismaterial erfasst worden ist, um eine ordentliche Ermittlung durchführen zu können. Der DEFR sollte in der Lage sein, durch Audits und Begründungen eine Angabe darüber zu machen, wie viel Beweismaterial insgesamt betrachtet worden ist und welche Verfahren angewendet wurden, um zu entscheiden, wie viel und welches Beweismaterial zu erheben ist.

ANMERKUNG Das Beweismaterial darf durch Erhebungs- und/oder Sammeltätigkeiten erfasst werden.

Es gibt vier grundlegende Aspekte bei der Bearbeitung von digitalen Beweismitteln: Auditierbarkeit, Begründbarkeit und entweder Wiederholbarkeit oder Vergleichbarkeit, je nach den jeweiligen Gegebenheiten.

5.3.2 Auditierbarkeit

Für einen unabhängigen Gutachter oder andere befugte interessierte Parteien sollte die Möglichkeit bestehen, die Tätigkeiten zu bewerten, die vom DEFR und DES ausgeübt werden. Dies wird durch eine angemessene Dokumentation aller umgesetzten Maßnahmen ermöglicht. Der DEFR und der DES sollten in der Lage sein, den Entscheidungsfindungsprozess bei der Auswahl einer bestimmten Vorgehensweise zu begründen. Vom DEFR und DES durchgeführte Prozesse sollten für ein unabhängiges Gutachten zur Verfügung stehen, um zu bestimmen, ob eine geeignete wissenschaftliche Methode, Technik oder ein geeignetes wissenschaftliches Verfahren eingehalten wurde.

5.3.3 Wiederholbarkeit

Die Wiederholbarkeit gilt als erreicht, wenn unter den folgenden Bedingungen die gleichen Prüfergebnisse erzielt werden:

- durch Einsatz derselben Messverfahren und Messmethoden;
- durch Einsatz derselben Messgeräte und unter denselben Messbedingungen; und
- durch die Möglichkeit der Wiederholung der Prüfung jederzeit nach der ursprünglichen Prüfung.

Ein DEFR mit geeigneten Fähigkeiten und Erfahrungen sollte in der Lage sein, alle in der Dokumentation beschriebenen Prozesse durchzuführen und dabei ohne jede Hilfe oder Interpretation die gleichen Ergebnisse zu erzielen. Der DEFR sollte darüber Bescheid wissen, dass es zu Situationen kommen kann, in denen es nicht möglich sein könnte, den Test zu wiederholen, z. B. wenn eine Original-Festplatte kopiert und wieder in Gebrauch genommen wurde oder wenn ein Element einen flüchtigen Speicher umfasst. In diesem Fall sollte der DEFR versichern, dass der Erhebungsprozess verlässlich ist. Um die Wiederholbarkeit herzustellen, sollten eine Qualitätskontrolle und eine Dokumentation des Prozesses erfolgen.

5.3.4 Vergleichbarkeit

Die Vergleichbarkeit gilt als erreicht, wenn unter den folgenden Bedingungen die gleichen Prüfergebnisse erzielt werden:

- durch Einsatz derselben Messmethoden;
- durch Einsatz unterschiedlicher Messgeräte und unter anderen Messbedingungen; und
- durch die Möglichkeit des Reproduzierens der Prüfung jederzeit nach der ursprünglichen Prüfung.

Das Verlangen nach einem Vergleich der Ergebnisse variiert in Abhängigkeit von der Rechtsordnung und den Gegebenheiten, so dass der DEFR oder die Person, die den Vergleich durchführt, über die geltenden Bedingungen informiert sein muss.

5.3.5 Begründbarkeit

Der DEFR sollte in der Lage sein, den Einsatz aller Maßnahmen und Methoden bei der Bearbeitung von potentiellen digitalen Beweismitteln zu begründen. Diese Begründung kann erfolgen, indem aufgezeigt wird, dass die Entscheidung die beste gewesen ist, mit der alle potentiellen digitalen Beweismittel abgedeckt wurden. Ein anderer DEFR oder DES könnte dies ebenfalls aufzeigen, indem er erfolgreich die eingesetzten Maßnahmen und Methoden vergleicht oder validiert.

Es liegt im besten Interesse einer einzelnen Organisation, einen DEFR oder DES einzustellen, der über die Schlüsselqualifikationen und Kompetenzen nach Anhang A dieser Internationalen Norm verfügt. Dadurch wird sichergestellt, dass bei der Bearbeitung von potentiellen digitalen Beweismitteln die richtigen Prozesse und Verfahren befolgt werden, um die spätere Erhaltung der möglicherweise beweiskräftigen digitalen Beweismittel sicherzustellen. Außerdem stellt dies sicher, dass die Organisationen in der Lage sind, die potentiellen digitalen Beweismittel einzusetzen, z. B. in deren Disziplinarverfahren oder zur Erleichterung des Austauschs von potentiellen digitalen Beweismitteln zwischen Rechtsordnungen.

ANMERKUNG Die in Anhang A beschriebene Kompetenz beschränkt sich auf die Funktion des DEFR, die sich an der Rolle des DES nach 3.8 orientiert.

5.4 Prozesse zur Bearbeitung von digitalen Beweismitteln

5.4.1 Überblick

Obwohl der komplette Prozess zur Bearbeitung von digitalen Beweismitteln weitere Tätigkeiten umfasst (d. h. Präsentation, Entsorgung usw.), bezieht sich der Anwendungsbereich dieser Internationalen Norm ausschließlich auf den Erstbearbeitungsprozess, der sich aus der Identifikation, Sammlung, Erhebung und Erhaltung von potentiellen digitalen Beweismitteln zusammensetzt.

Digitale Beweismittel können aufgrund ihrer Art fragil sein. Sie können durch unangemessene Bearbeitung oder Untersuchung verändert, verfälscht oder zerstört werden. Bearbeiter von digitalen Beweismitteln sollten über die nötige Kompetenz verfügen, um die Risiken und Konsequenzen von möglichen Vorgehensweisen bei der Bearbeitung von digitalen Beweismitteln zu identifizieren und zu lenken. Fehler bei der ordnungsgemäßen Handhabung von digitalen Geräten können die potentiellen digitalen Beweismittel auf diesen digitalen Geräten unbrauchbar machen.

Der DEFR und der DES sollten dokumentierte Verfahren einhalten, um sicherzustellen, dass die Integrität und Verlässlichkeit der potentiellen digitalen Beweismittel aufrechterhalten werden. Die Verfahren sollten die Bearbeitungsrichtlinien für die Quellen von potentiellen digitalen Beweismitteln enthalten und sollten die folgenden wesentlichen Grundsätze aufweisen:

- Verringerung der Bearbeitung des originalen digitalen Datenträgers oder der potentiellen digitalen Beweismittel auf ein Mindestmaß;
- Berücksichtigung jeglicher Änderungen und Dokumentation von ergriffenen Maßnahmen (in einem solchen Umfang, dass ein Experte in der Lage ist, sich eine Meinung über die Verlässlichkeit zu bilden);

- Einhaltung lokaler Regeln der Beweisführung; und
- der DEFR und der DES sollten keine Maßnahmen über ihren Kompetenzbereich hinaus ergreifen.

Durch Einhaltung der wesentlichen Grundsätze und Anforderungen bei der Bearbeitung von potentiellen digitalen Beweismitteln sollte das Beweismittel erhalten bleiben. Insbesondere in dem Fall, dass unvermeidbare Änderungen vorzunehmen sind, müssen alle Maßnahmen und Begründungen dokumentiert werden. Jeder Prozess bei der Bearbeitung von digitalen Beweismitteln, d. h. Identifikation, Sammlung, Erhebung und Erhaltung, wird ausführlicher in den nachstehenden Abschnitten erläutert.

5.4.2 Identifikation

Digitale Beweismittel liegen in physischer und in logischer Form vor. Die physische Form umfasst das Vorhandensein von Daten in einem konkreten Gerät. Die logische Form der potentiellen digitalen Beweismittel bezieht sich auf die virtuelle Darstellung von Daten in einem Gerät.

Der Identifikationsprozess umfasst die Suche nach potentiellen digitalen Beweismitteln sowie deren Erkennung und deren Dokumentation. Der Identifikationsprozess sollte digitale Speichermedien und verarbeitende Geräte identifizieren, die vorfallrelevante potentielle digitale Beweismittel enthalten können. Dieser Prozess umfasst außerdem eine Tätigkeit zur Priorisierung der Beweismittelsammlung basierend auf deren Flüchtigkeit. Die Flüchtigkeit von Daten sollte bestimmt werden, um die richtige Reihenfolge der Sammlungs- und Erhebungsprozesse sicherzustellen, damit eine Beschädigung der potentiellen digitalen Beweismittel auf ein Mindestmaß verringert wird und das bestmögliche Beweismittel erhalten wird. Des Weiteren sollte der Prozess möglicherweise versteckte potentielle digitale Beweismittel identifizieren. Dem DEFR und DES sollte bewusst sein, dass nicht alle Arten von digitalen Speichermedien leicht identifiziert und lokalisiert werden können, z. B. Cloud-Computing, NAS und SAN — sie alle ergänzen den Identifikationsprozess um eine weitere virtuelle Komponente.

Der DEFR sollte systematisch eine gründliche Suche nach Elementen durchführen, die möglicherweise potentielle digitale Beweismittel enthalten können. Diverse digitale Gerätetypen, die potentielle digitale Beweismittel enthalten könnten, können leicht übersehen werden (z. B. aufgrund ihrer geringen Größe), verborgen liegen oder mit anderem nicht relevanten Material vermischt sein.

In 6.1 und 6.6 sind weitere Informationen über die Beweismittelkette, die Verpackungs- und die Kennzeichnungsaspekte für die Identifikation von digitalen Beweismitteln enthalten. Abschnitt 7 legt Leitlinien fest, die für bestimmte Phasen der Identifikation, Sammlung, Erhebung und Erhaltung von digitalen Beweismitteln von Bedeutung sind.

5.4.3 Sammlung

Nachdem die digitalen Geräte, die potentielle digitale Beweismittel enthalten können, identifiziert worden sind, sollten der DEFR und der DES darüber entscheiden, ob im nächsten Prozess die Sammlung oder die Erhebung erfolgen soll. Für diese Entscheidung gibt es mehrere Einflussfaktoren, die ausführlicher in Abschnitt 7 beschrieben sind. Die Entscheidung sollte auf den jeweiligen Gegebenheiten basieren.

Die Sammlung ist ein Prozess während der Bearbeitung von digitalen Beweismitteln, bei dem die Geräte, die potentielle digitale Beweismittel enthalten können, von ihrem Ursprungsort entfernt und in ein Labor oder eine andere kontrollierte Umgebung gebracht werden, um anschließend die Erhebung und Analyse durchzuführen. Geräte, die potentielle digitale Beweismittel enthalten, können sich in einem der beiden folgenden Zustände befinden: wenn das System eingeschaltet ist oder wenn das System ausgeschaltet ist. Je nach Zustand des Geräts sind unterschiedliche Ansätze und Tools erforderlich. Für die im Sammlungsprozess verwendeten Ansätze und Tools können lokale Leitlinien gelten.

Dieser Prozess umfasst die Dokumentation des gesamten Ansatzes sowie die Verpackung dieser Geräte vor dem Transport. Für den DEFR und den DES ist es wichtig, jegliches Material zu sammeln, das möglicherweise mit den potentiellen digitalen Informationen in Zusammenhang stehen kann (z. B. ein Blatt Papier mit notierten Passwörtern, Ladestationen und Netzgerätestecker für integrierte Systemeinheiten). Potentielle digitale Beweismittel können verloren gehen oder beschädigt werden, falls nicht sorgfältig genug mit ihnen umgegangen wird. Der DEFR und der DES sollten ausgehend von der Situation, dem Kosten- und dem Zeitfaktor die bestmögliche Sammlungsmethode anwenden und die Entscheidung für den Einsatz einer bestimmten Methode dokumentieren.

ANMERKUNG 1 Das Entfernen von digitalen Speichermedien ist nicht immer empfehlenswert und der DEFR sollte sich sicher sein, dass er über die ausreichende Kompetenz verfügt, um Speichermedien zu entfernen, und sollte erkennen, wenn dies angemessen und erlaubt ist.

ANMERKUNG 2 Einzelheiten zu nicht gesammelten digitalen Geräten sollten mit einer Begründung für deren Ausschluss in Übereinstimmung mit den Anforderungen der jeweiligen Rechtsordnung dokumentiert werden.

5.4.4 Erhebung

Der Erhebungsprozess umfasst das Erstellen einer digitalen Beweismittelkopie der (z. B. einer Kopie der kompletten Festplatte, der Partition, ausgewählter Dateien) und die Dokumentation der eingesetzten Methoden und durchgeführten Tätigkeiten. Der DEFR sollte ausgehend von der Situation, dem Kosten- und dem Zeitfaktor eine geeignete Erhebungsmethode anwenden und die Entscheidung für den Einsatz einer bestimmten Methode oder eines bestimmten Tools dokumentieren.

Die Methoden, die angewendet werden, um potentielle digitale Beweismittel zu erheben, sollten deutlich und ausführlich dokumentiert werden, und sollten möglichst durch einen kompetenten DEFR reproduzierbar oder verifizierbar sein. Ein DEFR oder ein DES sollte die potentiellen digitalen Beweismittel auf die am wenigsten invasive Weise erheben, um Änderungen möglichst zu vermeiden. Bei der Ausführung dieses Prozesses sollte der DEFR die am besten geeignete Methode in Betracht ziehen. Falls der Prozess zu unvermeidbaren Änderungen an den digitalen Daten führt, sollten die durchgeführten Tätigkeiten dokumentiert werden, um die Änderungen an den Daten zu erklären.

Die angewendete Erhebungsmethode sollte eine digitale Beweismittelkopie der potentiellen digitalen Beweismittel oder der digitalen Geräte, die potentielle digitale Beweismittel enthalten können, hervorbringen. Sowohl die Originalquelle als auch die digitale Beweismittelkopie sollte mit einer bewährten Verifizierungsfunktion (zu diesem Zeitpunkt als bewährt geltend) verifiziert werden, die für die Person annehmbar ist, die das Beweismittel weiterverwendet. Die Originalquelle und jede digitale Beweismittelkopie sollten zu den gleichen Ergebnissen der Verifizierungsfunktion führen.

In Situationen, in denen der Verifizierungsprozess nicht durchgeführt werden kann, wenn z. B. Erhebungen eines laufenden Systems vorgenommen werden, enthält die Kopie Fehlersektoren oder der Erhebungszeitraum ist begrenzt. Unter solchen Umständen sollte der DEFR die beste verfügbare Methode anwenden und in der Lage sein, die Auswahl dieser Methode zu begründen und zu rechtfertigen. Falls der Imaging-Prozess nicht verifiziert werden kann, muss diese Tatsache dokumentiert und begründet werden. Falls notwendig, sollte die angewendete Erhebungsmethode den vorgesehenen Speicherplatz und den nicht vorgesehenen Speicherplatz erfassen.

ANMERKUNG 1 Wenn der Verifizierungsprozess aufgrund von Fehlern in der Quelle nicht für die komplette Quelle durchgeführt werden kann, dann darf eine Verifizierung derjenigen Bereiche der Quelle durchgeführt werden, die zuverlässig gelesen werden können.

Es kann Phasen geben, in denen es nicht möglich oder erlaubt ist, eine digitale Beweismittelkopie einer beweiskräftigen Quelle anzufertigen, z. B. weil die Quelle zu umfangreich ist. Unter diesen Umständen darf ein DEFR eine logische Erhebung vornehmen, die sich ausschließlich auf bestimmte Datentypen, Verzeichnisse oder Speicherorte konzentriert. Dies findet in der Regel auf einer Datei- und Partitionsebene statt. Während der logischen Erhebung dürfen aktive Dateien und nicht dateibasierte vorgesehene Speicherplätze auf dem digitalen Speichermedium kopiert werden; gelöschte Dateien und nicht vorgesehene Speicherplätze

dürfen in Abhängigkeit von der angewendeten Methode nicht kopiert werden. Andere Phasen, in denen diese Methode hilfreich sein kann, sind Phasen, an denen auftragsentscheidende Systeme beteiligt sind, die nicht abgeschaltet werden können.

ANMERKUNG 2 Einige Rechtsordnungen können einen besonderen Umgang mit Daten fordern; z. B. Versiegeln von Daten in Anwesenheit des Eigentümers der Daten. Das Versiegeln sollte in Übereinstimmung mit den vor Ort geltenden (gesetzlichen und verfahrensrechtlichen) Anforderungen erfolgen.

5.4.5 Erhaltung

Potentielle digitale Beweismittel sollten erhalten bleiben, um deren Nützlichkeit bei der Ermittlung sicherzustellen. Es ist wichtig, die Integrität der Beweismittel zu schützen. Der Erhaltungsprozess umfasst den Schutz vor Verfälschung oder Vereitelung von potentiellen digitalen Beweismitteln und von digitalen Geräten, die potentielle digitale Beweismittel enthalten können. Der Erhaltungsprozess sollte in allen Bearbeitungsprozessen von digitalen Beweismitteln ausgeführt und beibehalten werden, beginnend bei der Identifikation der digitalen Geräte, die potentielle digitale Beweismittel enthalten.

Im Optimalfall sollte keine Beweismittelvereitelung der Daten selbst oder von dazugehörigen Metadaten (z. B. Datums- und Zeitstempel) auftreten. Der DEFR sollte aufzeigen können, dass die Beweismittel seit ihrer Sammlung oder Erhebung nicht modifiziert wurden, oder sollte eine Begründung und dokumentierte Maßnahmen angeben, falls unvermeidbare Änderungen vorgenommen wurden.

ANMERKUNG In einigen Fällen stellt die Vertraulichkeit von potentiellen digitalen Beweismitteln eine Anforderung dar, entweder eine geschäftliche Anforderung oder eine rechtliche Anforderung (z. B. Datenschutz). Bei der Erhaltung von potentiellen digitalen Beweismitteln sollte sichergestellt sein, dass die Vertraulichkeit der Daten gewahrt ist.

6 Schlüsselkomponenten bei der Identifikation, Sammlung, Erhebung und Erhaltung von digitalen Beweismitteln

6.1 Beweismittelkette

Bei jeder Ermittlung sollte der DEFR in der Lage sein, die Verantwortung für alle erhobenen Daten und entgegengenommenen Geräte über den Zeitraum, in dem sie sich in seinem Gewahrsam befinden, zu tragen. Das Protokoll der Beweismittelkette ist ein Dokument, in dem die Chronologie der Weitergabe und Bearbeitung von potentiellen digitalen Beweismitteln festgehalten wird. Es sollte während des Sammlungs- oder Erhebungsprozesses erstellt werden. Dies erfolgt üblicherweise durch die zeitliche Rückverfolgung des Elements vom Zeitpunkt, an dem es von der Ermittlungsgruppe identifiziert, gesammelt oder erhoben worden ist, bis hin zum derzeitigen Status und (Speicher-)Ort.

Das Protokoll der Beweismittelkette ist ein Dokument oder eine Reihe von zusammenhängenden Dokumenten, entweder in digitaler Form oder in einem anderen Format (z. B. in Papierform), in dem/denen die Beweismittelkette ausführlich beschrieben ist und in dem/denen aufgezeichnet ist, wer für die Bearbeitung der potentiellen digitalen Beweismittel verantwortlich war. Das Ziel der Erstellung eines Protokolls der Beweismittelkette ist es, die Identifikation von Zugriff auf und Weitergaben von potentiellen digitalen Beweismitteln zu jedem beliebigen Zeitpunkt zu ermöglichen. Das Protokoll der Beweismittelkette selbst kann aus mehr als einem Dokument bestehen, z. B. sollte für potentielle digitale Beweismittel ein zeitgleiches Dokument vorliegen, in dem die Erhebung von digitalen Daten eines bestimmten Gerätes und die Weitergabe dieses Geräts aufgezeichnet werden, und eine Dokumentation, in der nachträgliche Extraktionen oder Kopien von potentiellen digitalen Beweismitteln für die Analyse oder sonstige Zwecke aufgezeichnet werden. Das Protokoll der Beweismittelkette sollte mindestens die folgenden Informationen enthalten:

- eine eindeutige Beweismittelkennzeichnung;
- die Person, die Zugriff auf das Beweismittel hatte, sowie Ort und Zeit des Zugriffs;
- die Person, die das Beweismittel in der Beweissicherungseinrichtung eingereicht hat und die sich das Beweismittel dort herausgeben lassen hat, sowie der Zeitpunkt für das Einreichen und für die Herausgabe;

- der Grund für die Herausgabe des Beweismittels (der Ermittlungsfall und der Zweck) und die zuständige Behörde, sofern zutreffend;
- alle unvermeidbaren Änderungen an den potentiellen digitalen Beweismitteln, sowie der Name der dafür verantwortlichen Person und die Begründung für die Durchführung der Änderung.

Die Beweismittelkette sollte während der gesamten Lebensdauer des Beweismittels aufrechterhalten werden und für einen bestimmten Zeitraum nach dem Lebensdauerende des Beweismittels aufbewahrt werden — dieser Zeitraum kann durch örtliche Rechtsordnungen für die Sammlung und Verwendung von Beweismitteln festgelegt werden. Sie sollte mit der Erhebung digitaler Geräte und/oder potentieller digitaler Beweismittel erstellt und nicht beeinträchtigt werden.

ANMERKUNG Einige Rechtsordnungen können besondere Anforderungen an die Beweismittelkette stellen. Der DEFR sollte diese Anforderungen einhalten.

6.2 Vorkehrungen am Vorfallort

6.2.1 Allgemeines

Nach dem Eintreffen des DEFR am Vorfallort sollte er Tätigkeiten zur Sicherung und zum Schutz des Speicherorts der potentiellen digitalen Beweismittel ausführen. Die Tätigkeiten sollten Folgendes entsprechend der lokalen Gesetzgebung unterstützen:

- sichern und kontrollieren des Bereichs, in dem sich die Geräte befinden;
- bestimmen der Person, die für den Ort die Verantwortung trägt;
- sicherstellen, dass Personen von den Geräten und von der Stromversorgung ferngehalten werden;
- dokumentieren aller Personen, die Zugang zum Ort haben, und jeder Person, für die ein Motiv für eine Beteiligung am Vorfallort vorliegt;
- ist das Gerät eingeschaltet, darf das Gerät nicht ausgeschaltet werden und falls das Gerät ausgeschaltet ist, darf es nicht eingeschaltet werden;
- falls möglich, Dokumentieren (z. B. Erstellen von Skizzen, Photo- oder Videoaufnahmen) des Vorfallorts, mit allen Komponenten und Kabeln in ihrer ursprünglichen Position. Falls keine Kamera und/oder Videokamera verfügbar ist, wird eine Skizze des Systems angefertigt und die Anschlüsse und Kabel werden gekennzeichnet, damit das System zu einem späteren Zeitpunkt validiert und rekonstruiert werden kann; und
- falls zulässig, werden die Bereiche nach Elementen, wie Haftnotizen, Terminkalendern, Akten, Laptops oder Handbüchern für Hardware und Software mit entscheidenden Hinweisen über die Geräte, wie Passwörter und PINs, durchsucht.

ANMERKUNG 1 In einigen Rechtsordnungen können besondere Anforderungen an die Zulässigkeit von Photo- und Videoaufnahmen als Beweismittel gelten. Der DEFR sollte diese Anforderungen einhalten.

ANMERKUNG 2 Dem DEFR muss bewusst sein, dass potentielle digitale Beweismittel nicht immer an offensichtlichen Stellen auffindbar sind, sondern verstreut oder virtuell gespeichert sind.

Der DEFR sollte zunächst alle Risiken in Verbindung mit der Durchführung aller Prozesse während der Ermittlung kennen. Der Schutz des Personals und der potentiellen digitalen Beweismittel am Vorfallort sollte berücksichtigt werden.

6.2.2 Personal

Es ist wichtig, vor Beginn des Prozesses eine Risikobeurteilung im Hinblick auf die Sicherheit des Personals durchzuführen, da die Sicherheit des am Prozess beteiligten Personals unbedingt notwendig ist. Die Beurteilung von Risiken für das Personal betrifft, unter anderem, folgende Aspekte:

- Ist/Sind die Person(en), gegen die ermittelt wird, anwesend? Falls ja, ist/sind sie gewaltbereit?
- Zu welcher Tageszeit erfolgt der Einsatz?
- Kann der Vorfalldort vor Unbeteiligten abgesichert werden?
- Befinden sich Waffen in diesem Bereich?
- Bestehen objektive Risiken für Personen?
- Könnte irgendetwas in der Nähe, einschließlich des Gerätes, so konfiguriert worden sein, dass es zu Körperverletzungen führen kann, falls es auf unangemessene Weise bearbeitet wird, z. B. versteckte Falle?
- Ist es wahrscheinlich, dass das zu sammelnde Beweismaterial psychische Schäden oder eine anstößige Wirkung hervorruft?
- Kann der Vorfalldort als unsicher betrachtet werden?
- Hat der umliegende Bereich einen Einfluss auf das Risikopotential?

6.2.3 Potentielle digitale Beweismittel

Der DEFR sollte behutsam vorgehen, wenn er ein bestimmtes Tool verwendet, um potentielle digitale Beweismittel zu sammeln oder zu erheben. Werden die Risiken nicht berücksichtigt, bevor er tätig wird, kann dies aufgrund der Technik, die während der Sammlung oder Erhebung zum Einsatz kommt, zum Verlust einiger oder aller potentiellen digitalen Beweismittel führen. Die Risiken sollten beurteilt werden, um das Auftreten von Schadensersatzansprüchen zu verringern.

Die Risikobeurteilung umfasst die systematische Bewertung von Risiken und deren potentiellen Auswirkungen auf die Ermittlung der digitalen Beweismittel. Die während der Risikobeurteilung für potentielle digitale Beweismittel zu berücksichtigenden Gesichtspunkte sind unter anderem folgende:

- Welche Art von Sammlungs-/Erhebungsmethode wird angewendet?
- Welche Ausrüstung wird möglicherweise vor Ort benötigt?
- Inwieweit sind die Daten und Informationen im Hinblick auf die potentiellen digitalen Beweismittel flüchtig?
- Ist ein Fernzugriff auf irgendein digitales Gerät möglich und stellt er eine Bedrohung für die Beweismittelintegrität dar?
- Was passiert, wenn der Datenbestand beschädigt wurde?
- Könnte der Datenbestand beschädigt/beeinträchtigt worden sein?
- Könnte das digitale Gerät so konfiguriert worden sein, dass Daten zerstört (z. B. Logikbombe), vereitelt oder verschleiert werden, wenn das Gerät ausgeschaltet wird oder ein unkontrolliert Zugriff erfolgt?

6.3 Rollen und Verantwortlichkeiten

Die Rolle des DEFR umfasst die Identifikation, Sammlung, Erhebung und Erhaltung von potentiellen digitalen Beweismitteln am Vorfallort. Dazu zählt das Erstellen eines Sammlungs- und Erhebungsberichts, aber nicht unbedingt das Erstellen des Analyseberichts. Die Rolle des DEFR umfasst außerdem das Sicherstellen der Integrität und Authentizität von potentiellen digitalen Beweismitteln. Um seiner Rolle gerecht zu werden, sollte der DEFR ausreichend Erfahrung, Fähigkeiten und Wissen in Bezug auf die Bearbeitung von potentiellen digitalen Beweismitteln mit sich bringen. Dies ist von grundlegender Bedeutung, da potentielle digitale Beweismittel leicht vereitelt werden können.

Der DEFR kann außerdem Unterstützung vom Personal des technischen Supports im zutreffenden Bereich fordern. Die Rolle eines DES umfasst die Bereitstellung des technischen Supports für den DEFR bei der Identifikation, Sammlung, Erhebung und Erhaltung der potentiellen digitalen Beweismittel am Vorfallort. Der DES versorgt den DEFR mit spezialisiertem Fachwissen. Die Kompetenzmatrix für den DEFR (siehe Anhang A) dient als Leitfaden zur Identifizierung seiner relevanten Kompetenzstufen.

ANMERKUNG Im Zusammenhang mit der Bearbeitung von Vorfällen, an der ein ISIRT (Informationssicherheitsnotfallteam) beteiligt ist, werden die Rollen eines DEFR und/oder DES als Mitglied des ISIRT in ISO/IEC 27035:2011 behandelt.

6.4 Kompetenz

Der DEFR und/oder DES sollte über die einschlägigen technischen und juristischen Kompetenzen (z. B. die in Anhang A aufgeführten Kompetenzen) verfügen und sollte nachweisen können, dass er angemessen ausgebildet ist und über ein ausreichendes technisches und juristisches Verständnis verfügt, um potentielle digitale Beweismittel auf geeignete Weise zu bearbeiten. Dazu zählt ein Verständnis der Prozesse und der Methoden, die für die Bearbeitung von potentiellen Quellen der digitalen Beweismittel geeignet sind. Eine angemessene Ausbildung ermöglicht dem DEFR, solche digitalen Geräte, die potentielle digitale Beweismittel enthalten, zu bearbeiten. Der beste Tool-Satz liefert keine Garantie für die Qualität der digitalen Beweismittel, solange der DEFR nicht über die nötige Kompetenz für die Durchführung der Aufgaben verfügt.

In einigen Rechtsordnungen ist vorgeschrieben, wie der DEFR seine Qualifikationen erlangen sollte. Es liegt in der Verantwortung des DEFR sich ordnungsgemäß darüber zu informieren, wie dies in der jeweiligen Rechtsordnung zu tun ist. Sofern erforderlich, sollte der DEFR und/oder DES darlegen können, dass er über die Kompetenz zur Bearbeitung von potentiellen digitalen Beweismitteln mithilfe von Tools und Methoden, die zur Durchführung der Aufgaben ausgewählt wurden, verfügt. Außerdem ist es erforderlich, dass der DEFR fortlaufend seine Kompetenz nachweisen kann.

Einige Voraussetzungen für den DEFR sind:

- er sollte ordnungsgemäß und angemessen ausgebildet worden sein, um digitale Geräte im Zuge der Ermittlungstätigkeiten zu bearbeiten;
- er sollte seine Fähigkeiten und Kompetenzen auf dem jeweiligen Gebiet zur Bearbeitung von potentiellen digitalen Beweismitteln gegenüber den entsprechenden Behörden nachweisen und aufrechterhalten;
- es liegt in der Verantwortung jedes einzelnen DEFR und des Arbeitgebers, sicherzustellen, dass der DEFR angemessen ausgebildet ist und seine Fähigkeiten und Kompetenz aufrechterhält.

ANMERKUNG Die Kompetenz eines DEFR kann in verschiedenen Rechtsordnungen variieren.

6.5 Anwendung angemessener Sorgfalt

Alle Vorgänge, die durch beabsichtigte oder unbeabsichtigte Handlungen zur Vereitelung von potentiellen digitalen Beweismitteln, die auf digitalen Geräten gespeichert sind, führen könnten, sind zu vermeiden. Die Beanspruchung mit einem Magnetfeld kann beispielsweise potentielle digitale Beweismittel, die sich auf einem Magnetspeichermedium befinden, vereiteln. Der DEFR sollte nicht auf digitale Geräte zugreifen, z. B. das Erstellen eines Speicherauszugs von einem digitalen Echtzeit-Medium, solange er nicht über die erforderliche Kompetenz verfügt und keine verlässlichen und validierten Prozesse anwendet.

Es gibt Situationen, in denen es praktisch nicht möglich ist, potentielle digitale Beweismittel zu sammeln oder zu erheben. Der DEFR sollte die folgenden Situationen in Betracht ziehen, ohne sich auf sie zu beschränken:

- wenn kein Rechtsanspruch oder keine Berechtigung vorliegt, das digitale Gerät an sich zu nehmen;
- wenn eine Verbindlichkeit besteht, andere Methoden anzuwenden (z. B. um eine Unterbrechung von Geschäftsabläufen zu vermeiden);
- wenn der DEFR die Vorgehensweise eines Verdächtigen während des Missbrauchs eines Systems feststellen möchte;
- wenn die Sammlung oder Erhebung verdeckt erfolgen sollte, falls dies von der Rechtsordnung als gesetzlich vertretbar betrachtet wird;
- wenn es sich um ein auftragsentscheidendes digitales Gerät handelt, das keine Ausfallzeit zulässt;
- wenn die physische Größe des digitalen Geräts zu umfangreich ist, z. B. ein Server eines Rechenzentrums oder ein RAID-System;
- wenn es sich um ein sicherheitskritisches digitales Gerät handelt, das bei Abschaltung eine Lebensgefahr darstellen würde; und
- wenn es sich um ein digitales Gerät handelt, das auch von unschuldigen Parteien genutzt wird.

6.6 Dokumentation

Für die Bearbeitung von digitalen Geräten, die potentielle digitale Beweismittel enthalten können, ist eine Dokumentation von grundlegender Bedeutung. Der DEFR sollte die folgenden Punkte bei der Dokumentation einhalten:

- Jede durchgeführte Tätigkeit sollte dokumentiert werden. Damit soll sichergestellt werden, dass keine Details während der Identifikations-, Sammlungs-, Erhebungs- und Erhaltungsprozesse ausgelassen werden. Dies kann auch bei einer grenzüberschreitenden Ermittlung hilfreich sein, bei der die potentiellen digitalen Beweismittel, die in einem anderen Teil der Welt erfasst wurden, entsprechend zurückverfolgt werden können.
- Der DEFR sollte auf die Zeit- und Datumseinstellungen achten, falls die digitalen Geräte eingeschaltet sind. Die Zeiteinstellungen werden mit verlässlichen Zeitquellen verglichen, z. B. mit einer Zeitangabe, die mit einer verlässlichen und nachvollziehbaren Zeitquelle synchronisiert wird. Diese Zeiteinstellungen sollten dokumentiert werden und es sollte auf mögliche erkennbare Unterschiede hingewiesen werden. Einige Systeme erfordern eine enorme Interaktion mit dem Anwender, um die Zeit- und Datumseinstellungen einzusehen. Der DEFR sollte darauf achten, das System nicht zu modifizieren. Nur ordnungsgemäß ausgebildetes Personal sollte diese Einstellungen abfragen.
- Der DEFR sollte alles, was auf dem Bildschirm des digitalen Geräts sichtbar ist, dokumentieren: aktive Programme und Prozesse sowie die Dateinamen von geöffneten Dokumenten. Diese Dokumentation sollte eine Beschreibung von allem, was sichtbar ist, umfassen, wobei sich einige Schadsoftware als bekannte Software ausgeben kann.

- Jede Weitergabe der digitalen Geräte sollte in Übereinstimmung mit den vor Ort geltenden Anforderungen dokumentiert werden.
- Alle eindeutigen Erkennungszeichen der digitalen Geräte und Zubehörteile, wie Seriennummern und eindeutige Kennzeichen, sind zu dokumentieren.

Beispiele für den Mindestumfang der Dokumentation für den Austausch von potentiellen digitalen Beweismitteln zwischen Rechtsordnungen sind in Anhang B dargestellt.

ANMERKUNG Weitere Informationen zur Dokumentation sind in den Abschnitten zur Lenkung der Dokumente und zur Lenkung von Aufzeichnungen (Schriftgutverwaltung) in ISO/IEC 17025:2005 enthalten.

6.7 Einsatzbesprechung (Briefing)

6.7.1 Allgemeines

Es ist von grundlegender Bedeutung, dass der DEFR und der DES von der entsprechenden Behörde angemessen eingewiesen worden sind, bevor sie ihre Aufgaben beginnen durchzuführen, wobei sämtliche Gesetze zum Schutz der Privatsphäre und der Verschwiegenheitspflicht (d. h. Need-to-know-Prinzip) befolgt werden. Es ist wichtig, offizielle Einsatzbesprechungen durchzuführen, um den Vorfall zu verstehen, um zu verstehen, was während der Ermittlung zu erwarten ist bzw. nicht zu erwarten ist, und zur Ermahnung, Beweismittel weder zu verfälschen noch zu vereiteln. Die Einsatzbesprechung sollte umfangreich genug sein, damit die Teilnehmer gut vorbereitet ihre Rollen und Verantwortlichkeiten einnehmen können; dadurch wird die Extraktion aller relevanten potentiellen digitalen Beweismittel sichergestellt.

6.7.2 Spezifische Einsatzbesprechung für digitale Beweismittel

Es ist eine Einsatzbesprechung notwendig, die sich ausschließlich auf die Hinweise konzentriert, die speziell für digitale Beweismittel gelten, um die DEFR über bestimmte Ermittlungsdetails zu informieren. Während der Einsatzbesprechung sollten der DEFR und der DER mit den einschlägigen Informationen und detaillierten Anweisungen über zu sammelnde oder zu erhebende potentielle digitale Beweismittel versorgt werden. Dazu kann Folgendes zählen:

- Art des Vorfalls (sofern bekannt);
- Datum und Uhrzeit des Vorfalls (sofern bekannt);
- Ermittlungsplan (Sammlung und/oder Erhebung, bekannte Netzwerkaktivitäten, Anforderungen an bekannte flüchtige Daten usw.);
- es wird erörtert, wo und wie die potentiellen digitalen Beweismittel nach der Sammlung oder Erhebung gespeichert/transportiert werden;
- spezielle Tools, die benötigt werden, um die potentiellen digitalen Beweismittel zu erheben;
- potentielle digitale Beweismittel, die eine bestimmte Art der Ermittlung erfordern;
- Ausrüstungen und Handbücher für die digitalen Geräte;
- Erinnerung der Gruppen, sämtliche Bluetooth- oder Wi-Fi-Einstellungen an ihren Telefonen/Computern auszuschalten, damit sie nicht versehentlich mit den digitalen Geräten interagieren, außer bei Telefonen/Computern, die zum Erkennen solcher Verbindungen genutzt werden;
- die Bedeutung der Dokumentation während der Ermittlung; und
- geltende rechtliche oder sonstige Faktoren, die möglicherweise das Einsammeln von Geräten oder das Sammeln der auf diesen Geräten enthaltenen potentiellen digitalen Beweismittel verbieten.

Diese spezifische Einsatzbesprechung darf einen Teil der allgemeinen Einsatzbesprechung nach 6.7.1 ausmachen.

6.7.3 Personalbezogene Einsatzbesprechung

Es ist eine Einsatzbesprechung notwendig, die sich ausschließlich auf personalbezogene Hinweise konzentriert, um die DEFR über Einzelheiten zu den an der Ermittlung beteiligten Parteien zu informieren. Während der Einsatzbesprechung wird die Ermittlungsgruppe mit personalbezogenen Anweisungen versorgt. Dazu kann Folgendes zählen:

- Zuweisungen, Rollen und Verantwortlichkeiten der Mitglieder der Ermittlungsgruppe am Vorfallort;
- ob voraussichtlich weitere Behörden (medizinisches Personal, Ermittler der biologischen Forensik) an der Ermittlung teilnehmen;
- Ermahnung der Mitglieder der Ermittlungsgruppe keine technische Unterstützung von Unbefugten anzunehmen; und
- Ermahnung der Mitglieder der Ermittlungsgruppe die Verfahren zur Minimierung des Risikos der Vereitelung von potentiellen digitalen Beweismitteln strikt zu befolgen, z. B. das Vermeiden der Verwendung von Tools oder Materialien, die statische Elektrizität oder ein Magnetfeld erzeugen oder aussenden könnten, da dies die potentiellen digitalen Beweismittel beschädigen oder zerstören könnte.

Diese spezifische Einsatzbesprechung darf einen Teil der allgemeinen Einsatzbesprechung nach 6.7.1 ausmachen.

6.7.4 Echtzeit-Vorfälle

Es ist äußerst erstrebenswert, dass die Ermittlung eines Vorfalls im Voraus geplant werden sollte, wobei es jedoch Situationen geben kann (z. B. wenn ein Vorfall entsteht und auch in Echtzeit auf ihn reagiert wird), in denen eine vollständige Planung nicht möglich ist. In diesen Situationen sollte die Ermittlungsgruppe zu Erststrategien und Taktiken der Ermittlung unterwiesen und ihr die Möglichkeit geboten werden, neue Strategien und Taktiken zur Reaktion auf die vorherrschenden Bedingungen zu entwickeln. Informationen über den Vorfall zum Zeitpunkt seines Entstehens sollten innerhalb der Ermittlungsgruppe schnellstmöglich geteilt werden, um sicherzustellen, dass die Entscheidungen über zu ergreifende Maßnahmen effektiv und unter Beachtung der nötigen Begründung getroffen werden können.

6.7.5 Sonstige Informationen aus der Besprechung

Neben den Informationen zu digitalen Beweismitteln und zum Personal zählen zu den wichtigen Informationen, die den Ermittlungsgruppen in den Besprechungen mitzuteilen sind, folgende:

- Bezeichnung des Bereichs der Ermittlung, einschließlich des Namens der Organisation, deren Anschrift und eines Lageplans (falls verfügbar);
- Ermittlungsauftrag;
- Einzelheiten zum Durchsuchungsbefehl und zu anderen Befugnissen, die für die Ermittlung gelten, einschließlich der Grenzen der Suche und der Beschlagnahmung;
- rechtliche Aspekte und Konsequenzen;
- zeitlicher Ermittlungsrahmen;
- benötigte Ausrüstung, die für die Ermittlung an den Vorfallort mitzubringen ist;
- Logistikinformationen; und
- mögliche Interessenkonflikte.

Der DEFR sollte Situationen meiden, in denen voreingenommene Beschuldigungen gemacht werden können. Ein Beispiel einer voreingenommenen Beschuldigung ist, wenn ein DEFR aufgrund der in der Besprechung gebildeten Auffassung ein Duplikat eines Computers aber keines anderen Computers (von dem sich später herausstellt, dass er entlastendes Beweismaterial enthält) erstellt.

6.8 Priorisierung der Sammlung und Erhebung

Bei der Priorisierung der Sammlung oder der Erhebung von potentiellen digitalen Beweismitteln ist es für den DEFR unerlässlich, den Grund für die Sammlung oder Erhebung der potentiellen digitalen Beweismittel zu verstehen. Ein allgemeingültiger Grundsatz ist, dass der DEFR versuchen sollte, die durch die Sammlungs- und Erhebungstätigkeiten erfasste Datenmenge zu maximieren. Es kann jedoch notwendig sein, Elemente anhand ihrer Flüchtigkeit und/oder ihrer Relevanz/ihres potentiellen Beweiswerts zu priorisieren. Elemente von hoher Relevanz/hohem potentielltem Beweiswert sind diejenigen, die mit der größten Wahrscheinlichkeit Daten mit direktem Bezug auf den zu ermittelnden Vorfall enthalten.

Eine Priorisierung anhand der Flüchtigkeit ist nur dann möglich, wenn die besonderen Umstände des Ermittlungsfalls dies erfordern. Potentielle digitale Beweismittel können in zwei Kategorien unterteilt werden: flüchtige Daten und nicht-flüchtige Daten. Flüchtige Daten können leicht zerstört werden oder für immer verloren gehen, falls sie nicht sorgfältig geschützt werden. Beispielsweise kann das Trennen der Stromzufuhr eines digitalen Geräts zum Verlust flüchtiger Daten führen. Nicht-flüchtige Daten verbleiben hingegen auf dem Speichermedium, selbst wenn die Stromzufuhr unterbrochen wird. Da einige Arten von digitalen Beweismitteln eine kurze Lebensdauer besitzen, können potentielle digitale Beweismittel leicht verfälscht oder vereitelt werden. Wenn nicht eindeutig ist, ob digitale Geräte etwaige potentielle digitale Beweismittel enthalten, oder welche der Elemente eine höhere Relevanz besitzen als andere, kann es notwendig sein, sie vor der Sammlung mithilfe eines Prozesses zur Bestimmung der Priorität zu untersuchen. Zu den digitalen Geräten, die bei der Sammlung zu berücksichtigen sind, zählen unter anderem: Computerausrüstung und digitale Speichermedien, CCTV-Systeme, PEDs, Automobilsysteme, Steuerungssysteme und Hilfelektronik. Die potentiellen digitalen Beweismittel mit der stärksten Flüchtigkeit werden zuerst erhoben, wie RAM, Auslagerungsspeicher, ausgeführte Prozesse usw. Der DEFR sollte fundiertes Wissen besitzen, um die Priorisierung anhand der Flüchtigkeit vorzunehmen.

Bei der Identifikation sollte der DEFR:

- potentielle digitale Beweismittel priorisieren, die für immer verloren gehen würden, falls die Stromversorgung unterbrochen wird; und
- schnelle Maßnahmen einleiten, um diese Daten mit validierten Methoden zu sammeln und zu erheben.

ANMERKUNG 1 Einige flüchtige Daten können sich durch bestimmte Einflussfaktoren, wie z. B. dem Ort, der Zeit und Änderungen an umliegenden digitalen Geräten, verändern — es wird sichergestellt, dass solche Daten vor der Weitergabe des Geräts erfasst worden sind.

ANMERKUNG 2 Digitale Geräte, die potentielle digitale Beweismittel enthalten, können eine Quelle für Sachbeweise darstellen (z. B. Fingerabdrücke, DNS usw.). Die DEFR müssen darauf achten, solche Beweise nicht zu vereiteln und sich mit den jeweiligen Beweissammlern abstimmen, bevor sie mit den nächsten Tätigkeiten fortfahren.

ANMERKUNG 3 Wenn eine Verschlüsselung oder Schadsoftware vermutet wird, ist es erstrebenswert, die flüchtigen Daten zu untersuchen.

Unter diesen Umständen kann die Zeit einen begrenzenden Faktor für die Ermittlung darstellen. In diesen Fällen sollten potentielle digitale Beweismittel, die für den spezifischen Vorfall als relevant identifiziert wurden, bevorzugt behandelt werden.

6.9 Erhaltung von potentiellen digitalen Beweismitteln

6.9.1 Überblick

Zur Erhaltung von erhobenen potentiellen digitalen Beweismitteln und gesammelten digitalen Geräten während des Verpackens ist es wichtig, diese Elemente so zu sichern, dass eine Vereitelung oder Verfälschung ausgeschlossen ist. Die Beweismittelvereitelung kann durch magnetische Beeinflussung, elektrische Beeinflussung, Wärme, hohe oder niedrige Luftfeuchte sowie Stoß und Schwingung entstehen. Die Verfälschung kann durch vorsätzliches Ändern oder durch Zulassen von Änderungen der potentiellen digitalen Beweismittel entstehen. Aus diesem Grund ist es von wesentlicher Bedeutung, die potentiellen digitalen Beweismittel bestmöglich zu schützen und so selten wie möglich die Originaldaten zu verwenden. Es ist wichtig, dass der DEFR mit den spezifischen Verpackungsanforderungen der jeweiligen Rechtsordnung vertraut ist.

6.9.2 Erhalten von potentiellen digitalen Beweismitteln

Alle gesammelten digitalen Geräte und erhobenen potentiellen digitalen Beweismittel sollten weitestgehend vor Verlust, Verfälschung oder Vereitelung geschützt werden. Der wichtigste Aspekt im Erhaltungsprozess ist die Aufrechterhaltung der Integrität und Authentizität der potentiellen digitalen Beweismittel und deren Beweismittelkette.

Die gesammelten digitalen Geräte und erhobenen potentiellen digitalen Beweismittel sollten in einer Beweissicherungseinrichtung, in der physische Sicherheitskontrollen, wie Zugangskontrollsysteme, Überwachungssysteme oder Angriffserkennungssysteme eingesetzt werden, oder in einer anderen kontrollierten Umgebungen für den Erhalt der digitalen Beweismittel gespeichert werden. Das Hauptziel der physischen Sicherheit ist der Schutz vor und das Vermeiden von Verlust, Beschädigung und Verfälschung sowie das Ermöglichen der Auditierbarkeit.

Die gesammelten digitalen Geräte sollten eingepackt oder in eine geeignete Verpackung gelegt werden, die für die Art der Geräte geeignet ist, um Verunreinigungen der digitalen Geräte vor dem Transport an (einen) andere(n) Ort(e) zu vermeiden. Stoßresistente Verpackungen können verwendet werden, um physische Schäden an Gerätekomponenten zu vermeiden.

- Der DEFR sollte die Empfindlichkeit des digitalen Geräts gegenüber statischer Elektrizität berücksichtigen. Falls sie von Belang ist, sollte das Gerät in einem antistatischen Beutel verstaut werden.
- Hauptsystemeinheiten und Laptops müssen in einem geeigneten Behälter verstaut werden, um Verfälschungen oder eine Beweisvereitelung der potentiellen digitalen Beweismittel, die möglicherweise dort gespeichert sind, zu vermeiden.

ANMERKUNG Die Verwendung eines Faradayschen Beutels oder anderer Verpackungen mit Hochfrequenzabschirmung können den Akkuverbrauch von Mobiltelefonen erhöhen. Daher kann die Bereitstellung einer Notstromversorgung für das Gerät erforderlich werden, während es sich in dem Beutel befindet, falls die Ressourcen es zulassen.

6.9.3 Verpacken von digitalen Geräten und potentiellen digitalen Beweismitteln

6.9.3.1 Grundlagen: Verpacken von potentiellen digitalen Beweismitteln

Die Grundlagen sollten eingehalten werden, sofern es keine guten Gründe gibt, die gegen sie sprechen. Sie können auch als die mindestens zu ergreifenden Maßnahmen bezeichnet werden. Während der Verpackung sollte der DEFR folgende Grundlagen beachten und einhalten:

- Das Magnetband nicht berühren, sondern besser die Bänder an ihren Schutzhüllen oder an den Bereichen anfassen, von denen bekannt ist, dass sie keine Daten enthalten (z. B. die Ränder von optischen Speicherplatten). Der DEFR sollte dies nur mit fusselfreien Handschuhen tun.

ANMERKUNG Die spezifischen Bereiche der Speichermedien, von denen bekannt ist, dass sie keine Daten enthalten, hängen vom Medientyp ab. Es liegt in der Verantwortung des DEFR, den derzeitigen Stand der Technik zu kennen und mit der Handhabung von Speichermedien vertraut zu sein.

- Um eine korrekte Identifikation sicherzustellen, sollte der DEFR alle potentiellen digitalen Beweismittel kennzeichnen. In einigen Rechtsordnungen gelten spezielle Anforderungen hinsichtlich des Formats zur Kennzeichnung von Beweismaterial. Der DEFR sollte mit den geltenden Kennzeichnungsanforderungen vertraut sein und sie einhalten. Der DEFR sollte alle potentiellen digitalen Beweismittel, alle gesammelten digitalen Geräte und sämtliche Hardwarekomponenten, die zu den Geräten gehören, mit Originalitätssiegeln versehen. Die Siegel sollten nicht direkt auf den mechanischen Teilen des digitalen Geräts angebracht werden und sollten keine wichtigen Angaben verdecken oder verbergen. Alle potentiellen digitalen Beweismittel in gesammelten digitalen Geräten sollten erhoben und so gespeichert werden, dass die Integrität der Beweismittel sichergestellt ist.
- Nach Möglichkeit sollten digitale Geräte mit Öffnungen und beweglichen Komponenten mit Originalitätssiegeln versiegelt werden, die für das Gerät geeignet sind, und der DEFR sollte auf dem Siegel unterschreiben.
- Akkubetriebene Geräte, die flüchtige Daten enthalten, sollten regelmäßig überprüft werden, um sicherzustellen, dass sie stets über eine ausreichende Stromversorgung verfügen.
- Digitale Geräte werden identifiziert und in Behältern, die für die Art der Geräte geeignet sind und vor möglichen Bedrohungen schützen, sichergestellt.
- Computer und digitale Geräte sollten so verpackt werden, dass sie vor Beschädigungen durch Stoß, Schwingung, große Höhen, Wärme und Hochfrequenzbeanspruchung während des Transports geschützt sind.
- Magnetspeichermedien sollten in einer Verpackung gelagert werden, die magnetisch träge, antistatisch und frei von Partikeln ist.
- Digitale Geräte können auch verborgene Beweise, Spuren von Beweisen oder biologisches Beweismaterial enthalten. In diesem Fall müssen entsprechende Tätigkeiten durchgeführt werden, um die potentiellen digitalen Beweismittel zu erhalten. Ein Image der digitalen Beweismittel sollte erstellt werden, nachdem die Sammlungsprozesse für verborgene Beweise, Spuren von Beweisen oder biologisches Beweismaterial am Gerät durchgeführt worden sind. Die Entscheidung über die Priorisierung der Sammlung von Beweismitteln sollte dennoch gründlich bewertet werden, um die Beweismittel zu erhalten.

6.9.3.2 Zusätzliche Maßnahmen: Verpacken von potentiellen digitalen Beweismitteln

Mit zusätzlichen Maßnahmen sind Maßnahmen gemeint, deren Umsetzung dringend empfohlen wird. Während der Verpackung sollte der DEFR die folgenden zusätzlichen Maßnahmen, soweit zutreffend, beachten und umsetzen:

- Tragen von fusselfreien Handschuhen und Sicherstellen, dass die Hände sauber und trocken sind;
- Schützen der digitalen Geräte vor dem Einfluss elektromagnetischer Quellen (z. B. Polizeifunkgeräte, Lautsprecher, Röntgengeräte). Die Verpackungsumgebung sollte frei von statischer Elektrizität sein;
- die Verpackungsumgebung sollte staubfrei, fettfrei und frei von chemischen Schadstoffen sein, die die oxidationsbedingte Zerstörung und den Feuchtigkeitsniederschlag auf der Magnetschicht fördern;
- Minimieren der Möglichkeit des Durchdruckens (die Übertragung eines Signals von einer Schleife des Bands auf die nächste Schleife), das eintreten kann, wenn Bänder über einen längeren Zeitraum ohne aktive Nutzung gelagert werden, was zu einer schlechten Signalqualität führt;
- soweit notwendig, sollten die Verpackungsbereiche frei von UV-Licht sein. UV-Licht kann eine Schädigung der DNA oder Schäden an einigen Medientypen hervorrufen. Der DEFR sollte überlegen, ob UV-Licht ein Risiko für potentielle digitale Beweismittel darstellt, bevor er einen Verpackungsbereich auswählt;
- digitale Medien sollten dringend vor Temperaturwechseln geschützt werden.

6.9.4 Transport von potentiellen digitalen Beweismitteln

Während des Transports sollte der DEFR die gesammelten digitalen Geräte und die erhobenen potentiellen digitalen Beweismittel erhalten. Potentielle digitale Beweismittel sollten während des Transports nicht unbeaufsichtigt bleiben. Der DEFR sollte die Beweismittelkette während des Transports aufrechterhalten, um mögliche Verfälschungen oder Vereitelungen zu verhindern, und er sollte die Integrität und Authentizität der digitalen Geräte und potentiellen digitalen Beweismittel aufrechterhalten. Falls die potentiellen digitalen Beweismittel nicht vom DEFR oder DES transportiert werden, wird empfohlen, sie zu verschlüsseln.

ANMERKUNG Der DEFR sollte sicherstellen, dass die Sammlung von vertraulichen oder persönlichen Informationen in Übereinstimmung mit den örtlichen Gesetzen und Verordnungen des Datenschutzes der jeweiligen Rechtsordnung erfolgt.

Während des Verpackens und des Transports muss der DEFR sich bewusst sein, dass möglicherweise elektrostatische Entladungen auftreten können, die den Beweiswert der potentiellen digitalen Beweismittel schädigen können. Der DEFR sollte sicherstellen, dass Computer und digitale Geräte für den Transport sicher verpackt sind, um Schäden durch Stoß und Schwingungen zu verhindern.

Für den Transportprozess sollte eine leitfähige und kontrollierte Umgebung vorgesehen werden. Der Feuchtigkeitsgehalt, die Luftfeuchte und die Temperatur sollten für die digitalen Geräte geeignet sein. Es wird vermieden, die potentiellen digitalen Beweismittel und digitalen Geräte für längere Zeit im Transportfahrzeug zu lagern sowie sie UV-Licht auszusetzen.

In einigen Rechtsordnungen kann der DEFR unter Umständen die Beweismittel nicht begleiten. In solchen Fällen können angemessene und autorisierte Versandarten eingesetzt werden, um die ordnungsgemäße Sicherheit der Beweismittel während des Transports sicherzustellen. Die Transportpapiere und eine Verifizierung der Verpackungsintegrität sollten Teil der Beweismittelkette sein.

7 Phasen der Identifikation, Sammlung, Erhebung und Erhaltung

7.1 Computer, Peripheriegeräte und digitale Speichermedien

7.1.1 Identifikation

7.1.1.1 Physische Durchsuchung des Vorfalles und Dokumentation

Für die Anwendung dieses Abschnitts gelten Computer als eigenständige digitale Geräte, die Daten empfangen, verarbeiten und speichern, und Ergebnisse hervorbringen. Diese Computergeräte werden nicht mit einem Netzwerk verbunden, dürfen aber mit Peripheriegeräten, wie Druckern, Scannern, Webcams, MP3-Playern, GPS-Systemen, RFID-Geräten usw., verbunden werden. Ein digitales Gerät, das über eine Netzwerkschnittstelle verfügt, zum Zeitpunkt der Sammlung oder Erhebung jedoch nicht mit einem Netzwerk verbunden ist, sollte (für die Anwendung dieser Internationalen Norm) als Einzelplatz-Computer angesehen werden. Wird ein Computer mit einer Netzwerkschnittstelle, aber ohne offensichtliche bestehende Verbindung aufgefunden, sollten Maßnahmen ergriffen werden, um Geräte zu identifizieren, die möglicherweise in jüngster Vergangenheit mit ihm verbunden waren.

In der Regel werden an den Vorfällen verschiedene Arten von digitalen Speichermedien vorgefunden. Digitale Speichermedien, deren Speicherkapazitäten variieren können, werden verwendet, um Daten von digitalen Geräten zu speichern. Beispiele für digitale Speichermedien sind unter anderem externe tragbare Festplatten, Flash-Speicher, CDs, DVDs, Blu-ray Discs, Floppy Disks, Magnetbänder und Speicherkarten.