

DIN EN ISO/IEC 27043



ICS 35.040

Einsprüche bis 2016-04-26

Entwurf

**Informationstechnik –
IT-Sicherheitsverfahren –
Grundsätze und Prozesse für die Untersuchung von Vorfällen
(ISO/IEC 27043:2015);
Deutsche und Englische Fassung FprEN ISO/IEC 27043:2016**

Information technology –
Security techniques –
Incident investigation principles and processes (ISO/IEC 27043:2015);
German and English version FprEN ISO/IEC 27043:2016

Technologies de l'information –
Techniques de sécurité –
Principes d'investigation numérique et les processus (ISO/IEC 27043:2015);
Version allemande et anglaise FprEN ISO/IEC 27043:2016

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 86 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (FprEN ISO/IEC 27043:2016) 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 27043:2015 im einstufigen Annahmeverfahren (UAP) als FprEN ISO/IEC 27043:2016 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 27043 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 — Grundsätze und Prozesse für die Untersuchung von Vorfällen (ISO/IEC 27043:2015)

Technologies de l'information — Techniques de sécurité — Principes d'investigation numérique et les processus (ISO/IEC 27043:2015)

Information technology — Security techniques — Incident investigation principles and processes (ISO/IEC 27043:2015)

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	11
2 Normative Verweisungen	11
3 Begriffe	11
4 Symbole und Abkürzungen	14
5 Digitale Ermittlungen	14
5.1 Allgemeine Grundsätze	14
5.2 Rechtsgrundsätze	14
6 Digitale Ermittlungsprozesse	15
6.1 Allgemeiner Überblick über die Prozesse	15
6.2 Klassen der digitalen Ermittlungsprozesse	16
7 Bereitstellungsprozesse	18
7.1 Überblick über die Bereitstellungsprozesse	18
7.2 Prozess zur Definition des Szenariums	20
7.3 Prozess zur Identifikation von potentiellen Quellen für digitale Beweismittel	20
7.4 Prozess zur Planung der Sammlung, Speicherung und Bearbeitung von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen	22
7.5 Planung der Analyse von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen	22
7.6 Prozess zur Planung der Vorfallerkennung	22
7.7 Prozess zur Definition der Systemarchitektur	23
7.8 Prozess zur Umsetzung der Systemarchitektur	23
7.9 Prozess zur Umsetzung der Sammlung, Speicherung und Bearbeitung von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen	23
7.10 Prozess zur Umsetzung der Analyse von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen	23
7.11 Prozess zur Umsetzung der Vorfallerkennung	24
7.12 Prozess zur Beurteilung der Umsetzung	24
7.13 Prozess zur Umsetzung der Beurteilungsergebnisse	24
8 Initialisierungsprozesse	25
8.1 Überblick über die Initialisierungsprozesse	25
8.2 Prozess zur Vorfallerkennung	25
8.3 Prozess zur ersten Reaktion	26
8.4 Prozess zur Planung	26
8.5 Prozess zur Vorbereitung	27
9 Erhebungsprozesse	27
9.1 Überblick über die Erhebungsprozesse	27
9.2 Prozess zur Identifikation von potentiellen digitalen Beweismitteln	28
9.3 Prozess zur Sammlung von potentiellen digitalen Beweismitteln	28
9.4 Prozess zur Erhebung von potentiellen digitalen Beweismitteln	29
9.5 Prozess zum Transport von potentiellen digitalen Beweismitteln	29

9.6	Prozess zur Speicherung und Erhaltung von potentiellen digitalen Beweismitteln	29
10	Ermittlungsprozesse	30
10.1	Überblick über die Ermittlungsprozesse	30
10.2	Prozess zur Erhebung von potentiellen digitalen Beweismitteln	31
10.3	Prozess zur Untersuchung und Analyse von potentiellen digitalen Beweismitteln	31
10.4	Prozess zur Interpretation von digitalen Beweismitteln	31
10.5	Prozess zur Berichterstattung	31
10.6	Prozess zur Präsentation	32
10.7	Prozess zum Ermittlungsabschluss	32
11	Parallele Prozesse	33
11.1	Überblick über die parallelen Prozesse	33
11.2	Prozess zum Einholen von Berechtigungen	33
11.3	Prozess zur Dokumentation	33
11.4	Prozess zur Steuerung des Informationsflusses	34
11.5	Prozess zur Erhaltung der Beweismittelkette	34
11.6	Prozess zur Erhaltung der digitalen Beweismittel	34
11.7	Prozess zur Interaktion mit der physischen Ermittlung	34
12	Muster eines digitalen Ermittlungsprozessmodells	35
Anhang A (informativ) Digitale Ermittlungsprozesse: Motivation zur Harmonisierung		37
Literaturhinweise		44

Europäisches Vorwort

Der Text von ISO/IEC 27043:2015 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 27043:2016 übernommen.

Dieses Dokument ist derzeit zum einstufigen Annahmeverfahren vorgelegt.

Anerkennungsnotiz

Der Text von ISO/IEC 27043:2015 wurde vom CEN als FprEN ISO/IEC 27043:2016 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 nicht-staatlich, 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.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Im Besonderen sollten die für die verschiedenen ISO-Dokumentenarten notwendigen Annahmekriterien beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet (siehe www.iso.org/directives).

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. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der empfangenen Patenterklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname wird als Information zum Nutzen der Anwender angegeben und stellt keine Anerkennung dar.

Eine Erläuterung der Bedeutung ISO-spezifischer Benennungen und Ausdrücke, die sich auf Konformitätsbewertung beziehen, sowie Informationen über die Beachtung der WTO-Grundsätze zu technischen Handelshemmnissen (TBT, en: Technical Barriers to Trade) durch ISO enthält der folgende Link: Foreword — Supplementary information.

Einleitung

Über diese Internationale Norm

Diese Internationale Norm liefert Leitlinien, die die Idealmodelle für allgemeine Ermittlungsprozesse in unterschiedlichen Ermittlungsfällen vereinen. Dazu zählen die Prozesse von der Vorbereitung auf einen Vorfall bis hin zur Rückgabe von Beweismitteln zur Speicherung oder Verbreitung, sowie allgemeine Hinweise und Vorbehalte zu Prozessen und die angemessene Identifikation, Sammlung, Erhebung, Erhaltung, Analyse, Interpretation und Präsentation von Beweismitteln. Ein wesentlicher Grundsatz der digitalen Ermittlungen ist die Wiederholbarkeit, bei der ein entsprechend qualifizierter Ermittler in der Lage sein muss, die gleichen Ergebnisse zu erzielen wie ein anderer, ähnlich qualifizierter Ermittler, der unter ähnlichen Bedingungen gearbeitet hat. Dieser Grundsatz ist für jede allgemeine Ermittlung von besonderer Bedeutung. Leitlinien für zahlreiche Ermittlungsprozesse wurden bereitgestellt, um sicherzustellen, dass für jeden einzelnen Prozess beim Erreichen der Ergebnisse Eindeutigkeit und Transparenz herrschen. Im Folgenden sind die Gründe für die Bereitstellung von Leitlinien für die Grundsätze und Prozesse von Vorfallermittlungen angegeben.

Festgelegte Leitlinien, die die Grundsätze und Prozesse von Vorfallermittlungen behandeln, würden die Ermittlungen beschleunigen, da sie eine allgemeine Reihenfolge der Ereignisse, die zu einer Ermittlung gehören, liefern würden. Der Einsatz festgelegter Leitlinien ermöglicht einen reibungslosen Übergang von einem Ereignis während einer Ermittlung zum nächsten. Solche Leitlinien würden außerdem angemessene Schulungen für unerfahrene Ermittler ermöglichen. Ein weiteres Ziel dieser Leitlinien ist es, die Flexibilität bei einer Ermittlung sicherzustellen, weil viele verschiedene Arten von digitalen Ermittlungen möglich sind. Es wurden harmonisierte Grundsätze und Prozesse zur Vorfallermittlung festgelegt und es wird aufgezeigt, wie die Ermittlungsprozesse den unterschiedlichen Ermittlungsszenarien angepasst werden können.

Ein harmonisiertes Modell für den Ermittlungsprozess wird in strafrechtlichen und zivilrechtlichen Anklagefällen benötigt, sowie in anderen Umgebungen, wie Körperschaftsverletzungen der Informationssicherheit und bei der Wiederherstellung von digitalen Informationen von defekten Speichergeräten. Die bereitgestellten Leitlinien enthalten kurze und prägnante Hinweise auf die genauen Prozesse, die während jeder beliebigen digitalen Ermittlung so durchzuführen sind, dass kein Zweifel an der Angemessenheit des Ermittlungsprozesses, der während dieser Ermittlung durchgeführt wird, bestehen sollte.

Jede digitale Ermittlung erfordert ein hohes Maß an Fachwissen. Die an der Ermittlung beteiligten Personen müssen kompetent sein, Erfahrung im Umgang mit den eingesetzten Prozessen haben und validierte Prozesse anwenden (siehe ISO/IEC 27041), die mit den einschlägigen Politiken und/oder Gesetze der jeweiligen Rechtsordnung kompatibel sind.

Besteht die Notwendigkeit, einen Prozess einer Person zuzuweisen, dann erhält diese Person die Verantwortung für den Prozess. Demzufolge wird aus einem engen Zusammenhang zwischen einer Prozessverantwortung und der Eingabe durch eine Person der genaue Ermittlungsprozess bestimmt, der in Übereinstimmung mit den harmonisierten Ermittlungsprozessen, die in dieser Internationalen Norm als Leitlinien angegeben sind, erforderlich ist.

Diese Internationale Norm ist in Anlehnung an einen Top-down-Ansatz strukturiert. Das bedeutet, dass die Ermittlungsgrundsätze und -prozesse zuerst auf einer allgemeinen (abstrakten) Ebene präsentiert werden, bevor sie detaillierter beschrieben werden. Beispielsweise wird zuerst ein allgemeiner Überblick über die Ermittlungsgrundsätze und -prozesse angegeben und in den Bildern als „schwarze Kästen“ dargestellt, und im Anschluss wird jeder allgemeine Prozess in detailliertere (unteilbare) Prozesse unterteilt. Daher wird gegen Ende dieser Internationalen Norm eine weniger allgemeine und detailliertere Sicht auf alle Ermittlungsgrundsätze und -prozesse geboten (siehe Bild 8).

Ziel dieser Internationalen Norm ist es, andere Normen und Dokumente zu ergänzen, die Hinweise zur Ermittlung von und zur Vorbereitung auf Vorfall-Ermittlungen in der Informationssicherheit enthalten. Sie stellt keinen allumfassenden Leitfaden dar, sondern ist eher ein Leitfaden, der eine breite Übersicht über den gesamten Vorfall-Ermittlungsprozess bietet. Dieser Leitfaden legt außerdem bestimmte wesentliche Grundsätze fest, die sicherstellen sollen, dass geeignete Tools, Techniken und Methoden ausgewählt werden können und deren Zweckdienlichkeit bei Bedarf nachgewiesen werden kann.

Zusammenhang mit anderen Normen

Diese Internationale Norm ist dafür vorgesehen, andere Normen und Dokumente, die Leitfäden für die Ermittlung von und für die Vorbereitung von Vorfall-Ermittlungen in der Informationssicherheit enthalten, zu ergänzen. Sie stellt keinen allumfassenden Leitfaden dar, sondern legt bestimmte wesentliche Grundsätze fest, die sicherstellen sollen, dass die richtigen Tools, Techniken und Methoden ausgewählt werden können und dass deren Zweckdienlichkeit bei Bedarf nachgewiesen werden kann.

Zweck dieser Internationalen Norm ist es außerdem, Entscheidungsträger, die die Glaubwürdigkeit der ihnen vorgelegten digitalen Beweismittel feststellen müssen, mit Informationen zu versorgen. Sie gilt für Organisationen, die potentielle digitale Beweismittel schützen, analysieren und vorlegen müssen. Sie ist für richtungsweisende Stellen von Bedeutung, die Verfahren zur digitalen Beweisführung erstellen und auswerten, und die häufig Teil einer größeren Stelle zur Beweisführung sind.

Diese Internationale Norm beschreibt einen Teil eines umfassenden Ermittlungsprozesses, der neben anderen die folgenden Themenbereiche umfasst:

- Handhabung von Vorfällen, einschließlich der Vorbereitung und Planung von Ermittlungen;
- Umgang mit digitalen Beweismitteln;
- Einsatz von Schwärzung und damit verbundene Probleme;
- Angriffspräventions- und -erkennungssysteme, einschließlich Informationen, die aus diesen Systemen erlangt werden können;
- Sicherheit der Speicherung, einschließlich Löschen von Daten auf temporär belegten Speichermedien (en: sanitization);
- Sicherstellen, dass Ermittlungsmethoden zweckdienlich sind;
- Durchführen von Analysen und Interpretationen von digitalen Beweismitteln;
- Verstehen von Grundsätzen und Prozessen bei der Ermittlung von digitalen Beweismitteln;
- Management von Sicherheitsvorfällen, einschließlich der Herleitung von Beweismitteln aus den am Management von Sicherheitsvorfällen beteiligten Systemen;
- Zusammenhang zwischen elektronischen Beweissicherungstechniken und anderen Ermittlungsmethoden, sowie der Einsatz von elektronischen Beweissicherungstechniken in anderen Ermittlungen;
- Steuerung von Ermittlungen, einschließlich forensischer Ermittlungen.

Diese Themenbereiche werden zum Teil von folgenden ISO/IEC-Normen behandelt:

— ISO/IEC 27037

Diese Internationale Norm beschreibt die Mittel, mit denen die Beteiligten der Anfangsphase einer Ermittlung, einschließlich der ersten Reaktion, versichern können, dass ausreichend potentielle digitale Beweismittel gesammelt wurden, um die Ermittlung angemessen durchzuführen.

— ISO/IEC 27038

Manche Dokumente können Informationen enthalten, die einigen Gemeinschaften nicht offen zugänglich gemacht werden dürfen. Modifizierte Dokumente können für diese Gemeinschaften freigegeben werden, nachdem eine angemessene Bearbeitung des Originaldokuments erfolgt ist. Das Entfernen von Informationen, die nicht freigegeben werden dürfen, wird als „Schwärzen“ bezeichnet.

Das digitale Schwärzen von Dokumenten ist ein relativ neuer Bereich des Dokumentenmanagements, der besondere Fragen und potentielle Risiken aufwirft. Wenn digitale Dokumente geschwärzt werden, dürfen die entfernten Informationen nicht wiederherstellbar sein. Demzufolge ist darauf zu achten, dass geschwärzte Informationen dauerhaft aus dem digitalen Dokument entfernt werden (z. B. dürfen sie nicht nur in nicht darstellbaren Teilen des Dokuments ausgeblendet werden).

ISO/IEC 27038 legt Methoden für das digitale Schwärzen von digitalen Dokumenten fest. Darüber hinaus legt sie Anforderungen an die Software fest, die für das Schwärzen verwendet werden kann.

— ISO/IEC 27040

Diese Internationale Norm liefert ausführliche technische Leitlinien darüber, wie Organisationen ein angemessenes Maß an Risikominderung festlegen können, indem sie einen bewährten und konsistenten Ansatz bei der Planung, Gestaltung, Dokumentation und Umsetzung der Datenspeichersicherheit anwenden. Die Speichersicherheit bezieht sich auf den Schutz (Sicherheit) von Informationen an deren Speicherort, und auf die Sicherheit der Informationen bei der Übertragung über die Kommunikationsschnittstellen in Verbindung mit der Speicherung. Die Speichersicherheit umfasst die Sicherheit von Geräten und Medien, die Sicherheit von Managementaktivitäten im Zusammenhang mit Geräten und Medien, die Sicherheit von Anwendungen und Diensten, und die für die Endanwender während der Lebensdauer von Geräten und Medien und nach deren Lebensdauer relevante Sicherheit.

Durch das Einbringen von Verschleierungsfunktionen können Sicherheitsfunktionen, wie Verschlüsselung und das Löschen von Daten auf temporär belegten Speichermedien, die Fähigkeit zur Ermittlung beeinflussen. Sie müssen vor und während der Durchführung einer Ermittlung berücksichtigt werden. Sie können auch wichtig sein bei der Sicherstellung, dass die Speicherung von Beweismitteln während und nach einer Ermittlung angemessen vorgenommen und gesichert wird.

— ISO/IEC 27041

Es ist wichtig, dass die Eignung von Methoden und Prozessen, die während einer Ermittlung zum Einsatz kommen, nachgewiesen werden kann. Diese Internationale Norm liefert Leitlinien darüber, wie die versichert werden kann, dass Methoden und Prozesse die Anforderungen der Ermittlung erfüllen und dass sie entsprechend getestet worden sind.

— ISO/IEC 27042

Diese Internationale Norm beschreibt die Art und Weise, wie die während einer Ermittlung anzuwendenden Methoden und Prozesse ausgelegt und verwirklicht werden können, um eine korrekte Bewertung von potentiellen digitalen Beweismitteln, eine Interpretation von digitalen Beweismitteln und eine effektive Berichterstattung über die Feststellungen zu ermöglichen.

Die folgenden ISO/IEC-Projekte behandeln zum Teil ebenfalls die vorstehend festgelegten Themenbereiche und können als einschlägige Normen zu einem bestimmten Zeitpunkt nach der Veröffentlichung dieser Norm veröffentlicht werden.

— ISO/IEC 27035 (alle Teile)

Diese Normenreihe besteht aus drei Teilen, die einen strukturierten und geplanten Ansatz für Organisationen für das Management von Sicherheitsvorfällen enthalten. Diese Teile sind:

— ISO/IEC 27035-1

— ISO/IEC 27035-2

— ISO/IEC 27035-3

— ISO/IEC 27044

— ISO/IEC 27050 (alle Teile)

— ISO/IEC 30121

Diese Internationale Norm liefert einen Rahmen für Steuerungsgremien von Organisationen (einschließlich der Inhaber, Vorstände, Direktoren, Partner, leitende Angestellte oder ähnliche Personen), um eine Organisation am besten auf digitale Nachforschungen vorzubereiten. Diese Internationale Norm gilt für die Entwicklung von strategischen Prozessen (und Entscheidungen) im Zusammenhang mit der Rückhaltung, Verfügbarkeit, Zugänglichkeit und Wirtschaftlichkeit von digitalen Beweismitteln. Diese Internationale Norm gilt für alle Arten und Größen von Organisationen. Die Internationale Norm behandelt die vorausschauende strategische Vorbereitung von digitalen Ermittlungen durch eine Organisation. Die forensische Bereitschaft versichert, dass eine Organisation geeignete und maßgebliche strategische Vorbereitungen getroffen hat, um potentielle beweiskräftige Ereignisse zu behandeln. Infolge einer unvermeidbaren Verletzung der Datensicherheit, Betrug und Rufschädigung dürfen Maßnahmen eingeleitet werden. In jeder Situation muss die Informationstechnologie (IT) strategisch eingesetzt werden, um die effektive Verfügbarkeit, Zugänglichkeit und Wirtschaftlichkeit der Beweismittel zu maximieren.

Bild 1 zeigt typische Tätigkeiten, die bei einem Vorfall und dessen Ermittlung eine Rolle spielen. Die im Bild dargestellten Zahlen (z. B. 27037) weisen auf eine der vorstehend aufgelisteten Internationalen Normen hin, und schattierte Balken geben an, wo sie jeweils mit hoher Wahrscheinlichkeit direkt angewendet werden können oder Einfluss auf den Ermittlungsprozess besitzen (z. B. durch Festlegen von Regeln oder Beschränkungen). Es wird dennoch empfohlen, alle Dokumente vor und während der Planungs- und Vorbereitungsphasen hinzuzuziehen. Die dargestellten Prozessklassen werden in dieser Norm umfassend definiert und die festgestellten Tätigkeiten stimmen mit den in ISO/IEC 27035-2, ISO/IEC 27037 und ISO/IEC 27042 näher erläuterten Tätigkeiten überein.

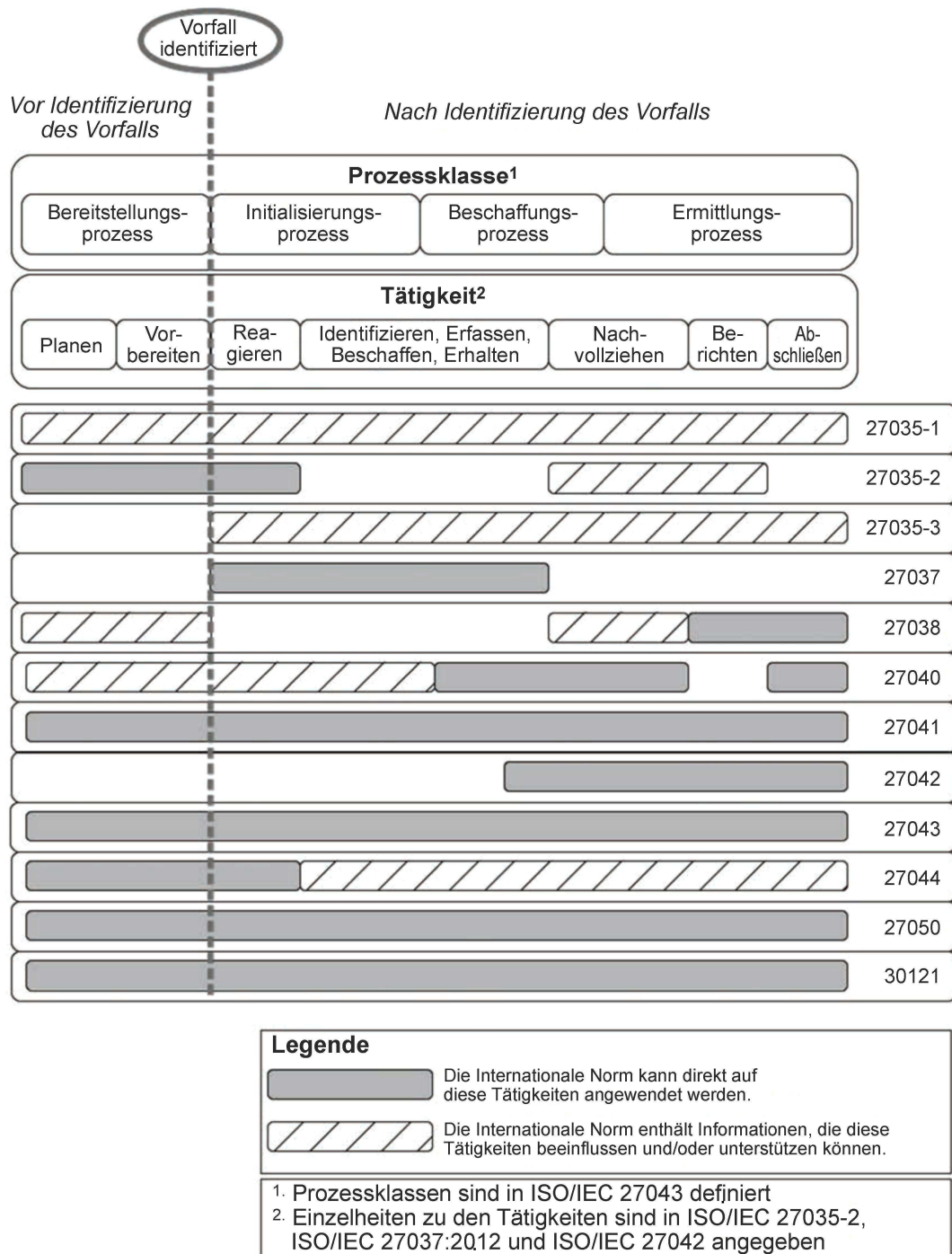


Bild 1 — Anwendbarkeit der Normen auf die Ermittlungsprozessklassen und Ermittlungstätigkeiten

1 Anwendungsbereich

Diese Internationale Norm liefert Leitlinien, die auf Idealmodellen basieren, die für gängige Vorfall-Untersuchungsprozesse in verschiedenen Vorfall-Untersuchungsszenarien gelten, bei denen digitale Beweismittel eine Rolle spielen. Dazu zählen Prozesse von der Vorbereitung auf Vorfälle bis hin zum Ermittlungsabschluss, sowie alle allgemeinen Hinweise und Vorbehalte zu solchen Prozessen. Die Leitlinien beschreiben Prozesse und Grundsätze, die für verschiedene Arten von Ermittlungen anwendbar sind, einschließlich unbefugter Zugriff, Datenbeschädigung, Systemabstürze oder Körperschaftsverletzungen der Informationssicherheit sowie jede andere digitale Ermittlung.

Zusammenfassend liefert diese Internationale Norm einen allgemeinen Überblick über alle Grundsätze und Prozesse von Vorfall-Ermittlungen, ohne dabei bestimmte Details innerhalb aller Grundsätze und Prozesse von Ermittlungen, die in dieser Internationalen Norm behandelt werden, vorzuschreiben. Zahlreiche andere relevante Internationale Normen, die an verschiedenen Stellen dieser Internationalen Norm in Bezug genommen werden, enthalten ausführlichere Inhalte von spezifischen Ermittlungsgrundsätzen und -prozessen.

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, 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/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 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.

[QUELLE: ISO/IEC 27037:2012, 3.1]

3.2

Tätigkeit

Satz aus zusammenhängenden Aufgaben eines Prozesses

[QUELLE: ISO/IEC 12207:2008, 4.3]

3.3

Analyse

Bewertung von potentiellen digitalen Beweismitteln, um deren Relevanz für die Ermittlung zu beurteilen

Anmerkung 1 zum Begriff: Aus potentiellen digitalen Beweismitteln, für die eine Relevanz ermittelt wird, werden digitale Beweismittel.

[QUELLE: ISO/IEC 27042:—, 3.1]

3.4

Sammlung

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

[QUELLE: ISO/IEC 27037:2012, 3.3]

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

[QUELLE: ISO/IEC 27037:2012, 3.5]

3.6

digitale Ermittlung

Einsatz von wissenschaftlich hergeleiteten und bewährten Methoden zur Identifikation, Sammlung, zum Transport, zur Speicherung, Analyse, Interpretation, Präsentation, Weitergabe, Rückgabe und/oder Zerstörung von digitalen Beweismitteln, die aus digitalen Quellen gewonnen wurden, wobei ordnungsgemäße Genehmigungen für alle Tätigkeiten eingeholt werden, alle Tätigkeiten ordnungsgemäß dokumentiert werden, mit der physischen Ermittlung interagiert wird, die digitalen Beweismittel aufrechterhalten werden, und die Beweismittelkette aufrechterhalten wird, um die Wiederherstellung von Ereignissen, die als Vorfall bewertet werden und eine digitale Ermittlung erfordern, zu erleichtern und zu fördern, egal ob er krimineller Art ist oder nicht

3.7

Identifikation

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

[QUELLE: ISO/IEC 27037:2012, 3.12]

3.8

Vorfall

einzelner oder eine Reihe von unerwünschten oder unerwarteten Verstößen gegen die Informationssicherheit oder Informationssicherheitsereignissen, entweder krimineller Art oder nicht, die mit großer Wahrscheinlichkeit die Geschäftsabläufe beeinflussen oder die Informationssicherheit gefährden

3.9

Interpretation

Darstellung einer Begründung, innerhalb vereinbarter Grenzen, für die Sachinformationen über die Beweismittel, die sich aus einer Reihe von Untersuchungen ergeben, und den Analysen, die zusammen die Ermittlung bilden

[QUELLE: ISO/IEC 27042:—, 3.9]

3.10

Ermittlung

Durchführung von Untersuchungen, Analysen und Interpretationen für ein besseres Verständnis des Vorfalls

[QUELLE: ISO/IEC 27042:—, 3.10]

3.11

Methode

Definition eines Arbeitsablaufs, der eingesetzt werden kann, um aus festgelegten Eingaben Daten zu erzeugen oder Informationen herzuleiten, die das Ergebnis darstellen

Anmerkung 1 zum Begriff: Im Idealfall sollte eine Methode unteilbar sein (d. h. sie sollte nicht mehr als eine Funktion umfassen), um den erneuten Einsatz von Methoden und der davon abgeleiteten Prozesse zu ermöglichen und den für die Validierung von Prozessen erforderlichen Arbeitsaufwand zu verringern.

[QUELLE: ISO/IEC 27041:—, 3.11]

3.12

potentielle digitale Beweismittel

Informationen oder Daten, die in binärer Form gespeichert oder übertragen werden und für die noch nicht durch den Untersuchungs- und Analyseprozess bestimmt wurde, ob sie für die Ermittlung relevant sind

[QUELLE: ISO/IEC 27042:—, 3.15, modifiziert — die Definition wurde angepasst, um Bezug auf den abstrakten „Untersuchungs- und Analyseprozess“ anstatt auf nur die Analyse zu nehmen; Anmerkung 1 zum Begriff und Anmerkung 2 zum Begriff wurden gestrichen]

3.13

Erhaltung

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

[QUELLE: ISO/IEC 27037:2012, 3.15, modifiziert — „und digitalen Beweismitteln“ wurde hinzugefügt]

3.14

Prozess

Reihe von Tätigkeiten, die ein gemeinsames Ziel verfolgen und über eine begrenzte Zeit andauern

Anmerkung 1 zum Begriff: Siehe auch ISO/IEC 27000 und ISO 9000 für ähnliche Definitionen eines Prozesses.

Anmerkung 2 zum Begriff: Die Bedeutung eines „Prozesses“ in dieser Internationalen Norm bezieht sich auf einen höheren Abstraktionsgrad als die Definition von „Prozess“ in ISO/IEC 27041.

3.15

Bereitstellung

Prozess der Vorbereitung auf eine digitale Ermittlung, bevor ein Vorfall eingetreten ist

3.16

Validierung

Bestätigung durch die 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, 3.17]

3.17

Verifizierung

Bestätigung durch die Bereitstellung eines objektiven Nachweises, dass festgelegte Anforderungen erfüllt worden sind

Anmerkung 1 zum Begriff: Die Verifizierung versichert ausschließlich, dass ein Produkt seinen Spezifikationen entspricht.

[QUELLE: ISO/IEC 27041:—, 3.20]

3.18

flüchtige Daten

hervorgerufen durch 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.

[QUELLE: ISO/IEC 27037:2012, 3.26, modifiziert — „hervorgerufen durch“ wurde am Anfang der Originaldefinition eingefügt]

4 Symbole und Abkürzungen

DVR	Festplattenrekorder (en: digital video recorder)
IP	Internetprotokoll (en: Internet Protocol)
JPEG	Joint Photographic Experts Group
RAM	Direktzugriffsspeicher (en: Random Access Memory)
PKI	Public-Key-Infrastruktur

5 Digitale Ermittlungen

5.1 Allgemeine Grundsätze

Digitale Ermittlungen werden in der Praxis immer dann durchgeführt, wenn die Notwendigkeit besteht, digitale Beweismittel infolge eines Vorfalls zu ermitteln, egal ob der Vorfall krimineller Art ist oder nicht. Es gibt viele Arten von digitalen Ermittlungen, wie Ermittlungen von Bürorechnern, Laptops, Servern, Datenbeständen, handgehaltenen/mobilen Geräten, Ermittlungen von Echtzeitdaten (z. B. Ermittlungen von Netzwerkdaten und flüchtigen Daten) und Ermittlungen von digitalen Geräten, wie Festplattenrekordern, Spielekonsolen und Steuerungssystemen. Der digitale Ermittlungsprozess ist jedoch so ausgestaltet, dass er für jede Art von digitaler Ermittlung anwendbar ist.

5.2 Rechtsgrundsätze

Es wird ein Überblick über die rechtlichen Anforderungen an digitale Ermittlungen gegeben, besonders über die Zulässigkeit von digitalen Beweismitteln vor Gericht. Es sollte darauf hingewiesen werden, dass rechtliche Anforderungen in verschiedenen Rechtsordnungen in der ganzen Welt sehr unterschiedlich sein können. Die Voraussetzung ist, keine spezifischen Rechtssysteme zu befürworten, sondern eher auf die allgemeinen Anforderungen hinsichtlich Rechtsfragen hinzuweisen, die vom Rechtssystem einer bestimmten Rechtsordnung übernommen werden können. Je nach der Gesetzeslage in einer bestimmten Rechtsordnung sollten spezifische Betrachtungen und Sorgfalt erfolgen, wenn ein Beschuldigter vor Gericht als unschuldig befunden wird. Es sollte beispielsweise Folgendes mit gebührender Sorgfalt und Vorsicht sichergestellt werden:

- sicheres Löschen (siehe ISO/IEC 27040) der Beweismittel und Falldaten am Ende des Gerichtsverfahrens, falls dies gefordert wird;
- nach Möglichkeit, Sicherstellen der Erhaltung von Medien und Geräten, die potentielle digitale Beweismittel enthalten, Sicherstellen der Erhaltung der digitalen Beweismittel selbst und Sicherstellen der Erhaltung von Ermittlungsergebnissen für mögliches späteres Nachlesen; und
- Benachrichtigung der Zielperson über die Ermittlungsergebnisse.

Falls wissenschaftliche, technische oder andere Fachkenntnisse vor Gericht dabei helfen, die Beweismittel zu verstehen oder Tatfragen zu klären, ist es in einigen Rechtsordnungen zulässig, dass ein Zeuge, der aufgrund seiner Erfahrung, seines Wissens, seiner Fähigkeiten, Schulung oder Ausbildung als Experte zugelassen ist, diesbezüglich seine Meinung [2] äußern darf. Um die Zulässigkeit von Expertenmeinungen zu unterstützen, sollten die folgenden Faktoren in Betracht gezogen werden (soweit sie in den jeweiligen Rechtsordnungen anwendbar sind):

- ob die vom wissenschaftlichen Experten angewendeten Theorien und Techniken überprüft worden sind;
- ob sie einer Begutachtung unterzogen und veröffentlicht worden sind;
- falls eine Fehlerquote für die Technik bekannt ist, sollte sie angegeben werden;
- ob sie Normen unterliegen, die deren Anwendung regeln;
- ob die vom Experten angewendeten Theorien und Techniken eine breite Akzeptanz finden.

ANMERKUNG Die Zulässigkeit der Beweismittel selbst und die Zulässigkeit von Expertenmeinungen über die Interpretation der Beweismittel sind zwei verschiedene Aspekte, die zu betrachten sind. Ein Zeuge, der über Fachkenntnisse verfügt, kann beispielsweise in der Lage sein, zu begutachten, wie ein Beweismittel erhoben, erhalten usw. wurde, um sich mit der Eignung solcher Prozesse zu befassen, ohne sich als Experte qualifizieren zu müssen. Mit anderen Worten darf der Experte ebenfalls technische Fakten begutachten. Siehe auch ISO/IEC 27042:—, 8.2.

Anforderungen an die Zulässigkeit können deutlich zwischen den Rechtsordnungen variieren, weshalb es äußerst ratsam ist, kompetente rechtliche Hinweise im Hinblick auf solche spezifischen Anforderungen zu erhalten. Viele Rechtsordnungen nehmen jedoch mindestens Folgendes in ihre Zulässigkeitsanforderungen für die Beweismittel auf:

- **Relevanz** — das Beweismittel sollte eine bestimmte Relevanz für strittigen Angelegenheiten haben;
- **Authentizität** — es sollte dargelegt werden, dass das Beweismittel ist, was es vorgibt zu sein. Falls beispielsweise ein bestimmtes JPEG-Bild, das von der Festplatte eines bestimmten Servers extrahiert wurde, für eine strittige Tatsachenfrage relevant ist, verlangt der Tatsachengutachter nach einer nachweisbaren Zusicherung, dass das Laufwerk tatsächlich aus diesem bestimmten Server stammt, dass es seit der Sammlung in keinsten Weise modifiziert worden ist, dass der eingesetzte Prozess zum Extrahieren des JPEG-Bilds vertrauenswürdig ist usw.

Es ist wichtig, dass Rechtsfragen während des gesamten Ermittlungsprozesses beachtet werden. Bei jedem Teilprozess sollte eine juristische Überprüfung stattfinden, um zu bestimmen, ob die Gesetze und Verordnungen innerhalb einer bestimmten Rechtsordnung eingehalten werden. Bei Unsicherheiten wird empfohlen, rechtlichen Rat innerhalb einer bestimmten Rechtsordnung einzuholen.

6 Digitale Ermittlungsprozesse

6.1 Allgemeiner Überblick über die Prozesse

Die in dieser Internationalen Norm beschriebenen digitalen Ermittlungsprozesse sind absichtlich auf einer abstrakten Ebene ausgelegt, damit sie für unterschiedliche digitale Ermittlungen und verschiedene Arten von digitalen Beweismitteln genutzt werden können. Diese Vorgehensweise ist dafür vorgesehen, die Gestaltung und Entwicklung von allgemeinen Prozessen zu unterstützen, mit der Absicht, sie anschließend in unteilbare Prozesse zu zerlegen (siehe ISO/IEC 27041). Ziel der Prozesse ist es außerdem, umfangreich zu sein, indem sie eine Harmonisierung aller veröffentlichten digitalen Prozesse zum Zeitpunkt der Erstellung dieser Internationalen Norm darstellen. Die Ermittlungsprozesse sind kurz und bündig organisiert und beschreiben, wie diese Prozesse zu befolgen sind.

6.2 Klassen der digitalen Ermittlungsprozesse

Die Liste der digitalen Ermittlungsprozesse ist lang. Um digitale Ermittlungsprozesse auf höherer Ebene zu abstrahieren, können sie in die folgenden Klassen der digitalen Ermittlungsprozesse eingeteilt werden:

- Bereitstellungsprozesse: Prozessklasse, die sich mit Ermittlungsprozessen im Zeitraum vor dem Vorfall beschäftigt. Diese Klasse beschäftigt sich mit der Festlegung von Strategien, die angewendet werden können, um sicherzustellen, dass Systeme eingerichtet sind und dass die am Ermittlungsprozess beteiligten Personen bestens geschult sind, bevor sie sich mit einem eintretenden Vorfall auseinandersetzen. Die Bereitstellungsprozesse sind für den Rest der digitalen Ermittlungsprozesse optional. Der Grund hierfür wird ausführlicher in 7.1 erläutert. Bereitstellungsprozesse umfassen Folgendes:
 - Definition des Szenarios;
 - Identifikation von potentiellen Quellen für digitale Beweismittel;
 - Planung der Sammlung von Informationen aus dem Zeitraum vor dem Vorfall;
 - Speicherung und Bearbeitung von Daten, die potentielle digitale Beweismittel darstellen;
 - Planung der Analyse von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen;
 - Planung der Vorfallerkennung;
 - Definition der Systemarchitektur;
 - Umsetzung der Systemarchitektur;
 - Umsetzung der Sammlung, Speicherung und Bearbeitung von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen;
 - Umsetzung der Analyse von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen;
 - Umsetzung der Vorfallerkennung;
 - Beurteilung der Umsetzung;
 - Umsetzung von Beurteilungsergebnissen.
- Initialisierungsprozesse: Prozessklasse, die sich mit dem Beginn der digitalen Ermittlung beschäftigt. Die Initialisierungsprozesse umfassen Folgendes:
 - Vorfallerkennung;
 - erste Reaktion;
 - Planung;
 - Vorbereitung.

- Erhebungsprozesse: Prozessklasse, die sich mit der physischen Ermittlung eines Falls beschäftigt, bei der potentielle digitale Beweismittel identifiziert und bearbeitet werden. Erhebungsprozesse umfassen Folgendes:
 - Identifikation von potentiellen digitalen Beweismitteln;
 - Erhebung von potentiellen digitalen Beweismitteln;
 - Transport von potentiellen digitalen Beweismitteln;
 - Speicherung von potentiellen digitalen Beweismitteln.
- Ermittlungsprozesse: Prozessklasse, die sich mit dem Aufdecken von potentiellen digitalen Beweismitteln beschäftigt. Ermittlungsprozesse umfassen Folgendes:
 - Untersuchung und Analyse von potentiellen digitalen Beweismitteln;
 - Interpretation von digitalen Beweismitteln;
 - Berichterstattung;
 - Präsentation;
 - Ermittlungsabschluss.
- parallele Prozesse: Prozessklasse, die parallel zu den anderen Prozessen verläuft. Diese Prozessklasse unterscheidet sich von den vorstehend genannten Klassen insoweit, dass sie gleichzeitig mit den anderen Prozessen stattfindet anstatt nach ihnen. Außerdem ist die bestimmte Reihenfolge, in der die parallelen Prozesse ausgeführt werden, im Gegensatz zu den anderen, nicht parallel verlaufenden Prozessen, nicht von Bedeutung. Parallele Prozesse umfassen Folgendes:
 - Einholen von Berechtigungen;
 - Dokumentation;
 - Steuerung des Informationsflusses;
 - Erhaltung der Beweismittelkette;
 - Erhaltung von digitalen Beweismitteln;
 - Interaktion mit der physischen Ermittlung.

Bild 2 zeigt die Zusammenhänge zwischen den verschiedenen Prozessklassen der digitalen Ermittlung.

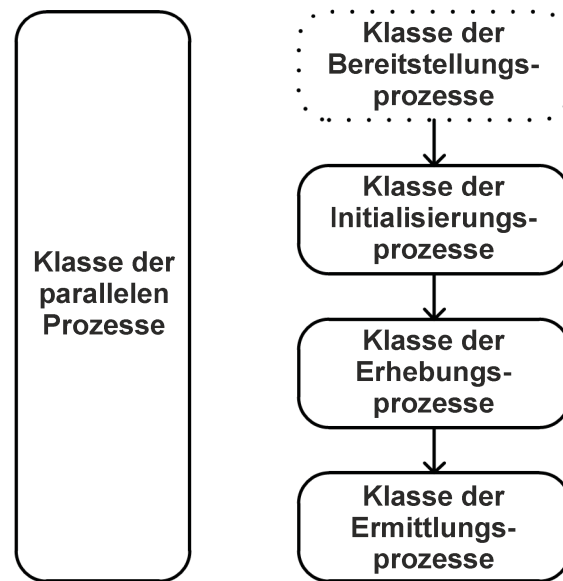


Bild 2 — Die verschiedenen Prozessklassen der digitalen Ermittlung

ANMERKUNG Die gepunkteten Linien um die Prozesse herum geben in allen Bildern an, dass der jeweilige Prozess optional ist.

Das Ziel der sechs parallelen Prozesse ist die Durchführung besagter Prozesse in Form von fortlaufenden Prozessen. Der Grund für die parallelen Prozesse liegt zum einen in der Sicherstellung der Zulässigkeit von digitalen Beweismitteln in einem Rechtssystem, da jede Ermittlung Gefahr laufen kann, dass bei Fehlen solcher Prozesse die zugelassenen potentiellen Beweismittel aufgrund unangemessener Bearbeitung in einem Rechtsstreit ungeeignet sein können, und zum anderen in der Dokumentation von potentiellen digitalen Beweismitteln. Diese parallelen Prozesse basieren daher auf Grundsätzen, die neben den anderen Prozessklassen während einer digitalen Ermittlung zu beachten sind.

Die digitalen Ermittlungsprozesse sind mehrstufige Prozesse, bei denen jeder Prozess aus einer Reihe von Teilprozessen besteht. Teilprozesse können nur für eine bestimmte Art von Vorfall und Ermittlung vollständig definiert werden. Gesetzliche Festlegungen haben möglicherweise ebenfalls großen Einfluss auf die Definition von Teilprozessen. Diese verschiedenen Klassen der digitalen Ermittlungsprozesse werden ausführlicher in den folgenden Abschnitten beschrieben, d. h. in Abschnitt 7 bis Abschnitt 11.

7 Bereitstellungsprozesse

7.1 Überblick über die Bereitstellungsprozesse

Bereitstellungsprozesse betreffen die Prozessklasse, die sich mit der Vorbereitung einer Organisation insoweit beschäftigt, dass in dem Fall, dass eine digitale Ermittlung erforderlich ist, eine solche Organisation über die Möglichkeit verfügt, den Einsatz von digitalen Beweismitteln zu maximieren, während sie Zeit und Kosten einer Ermittlung minimiert. Diese Prozessklasse ist für die digitalen Ermittlungsprozesse optional, da die Organisation das Vorrecht besitzt, diese Prozessklasse selbst umzusetzen, und sie nicht zur Aufgabe des/der Ermittler(s) zu machen.

Bei der Umsetzung von Bereitstellungsprozessen in digitalen Ermittlungen in Organisationen gibt es vier Ziele:

- a) Maximieren der Einsatzmöglichkeit von digitalen Beweismitteln;
- b) Minimieren der Kosten für digitale Ermittlungen, die entweder direkt für das System der Organisation anfallen oder die sich auf die Dienste des Systems beziehen;

- c) Minimieren von Störungen und Unterbrechungen von Geschäftsabläufen der Organisation;
- d) Erhalten oder Verbessern des derzeitigen Zustands der Informationssicherheit von Systemen innerhalb der Organisation.

Bild 3 veranschaulicht die vorstehend beschriebenen Gruppen der Bereitstellungsprozesse, die in die folgenden Prozessgruppen aufgeteilt sind: *Gruppe der Planungsprozesse*, *Gruppe der Umsetzungsprozesse* und *Gruppe der Beurteilungsprozesse*. Die *Gruppe der Planungsprozesse* umfasst die Bereitstellungsprozesse, wie in Bild 4 dargestellt, die sich mit den Planungstätigkeiten beschäftigen, einschließlich:

- Prozess zur Definition des Szenariums;
- Prozess zur Identifikation von Quellen für potentielle digitale Beweismittel;
- Prozess zur Planung der Sammlung von Informationen aus dem Zeitraum vor dem Vorfall;
- Prozess zur Speicherung und Bearbeitung von Daten, die potentielle digitale Beweismittel darstellen;
- Prozess zur Planung der Analyse von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen;
- Prozess zur Planung der Vorfallerkennung; und
- Prozess zur Definition der Systemarchitektur.

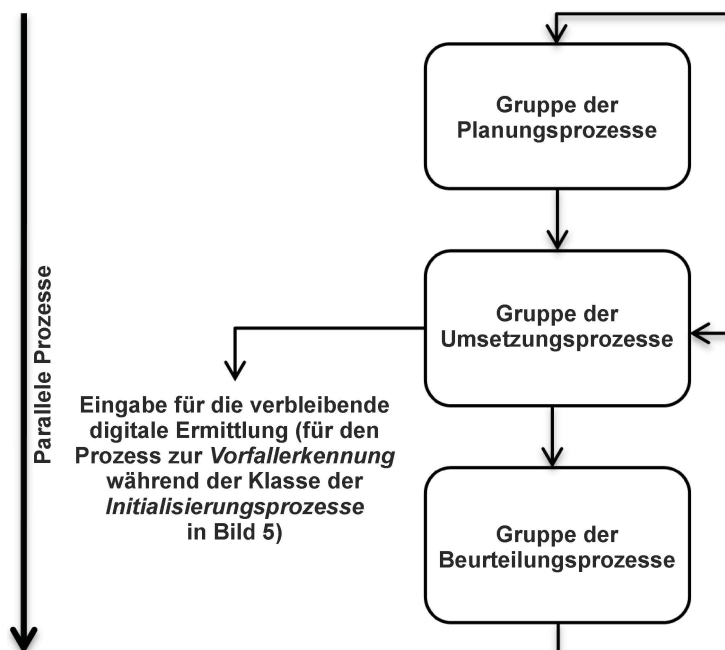


Bild 3 — Gruppen der Bereitstellungsprozesse

Die *Gruppe der Umsetzungsprozesse* umfasst die Bereitstellungsprozesse, wie in Bild 4 dargestellt, die sich mit der Umsetzung der während der Gruppe der Planungsprozesse geplanten Tätigkeiten beschäftigen, einschließlich:

- Prozess zur Umsetzung der Systemarchitektur;
- Prozess zur Umsetzung der Sammlung, Speicherung und Bearbeitung von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen;

- Prozess zur Umsetzung der Analyse von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen; und
- Prozess zur Umsetzung der Vorfallerkennung.

Die *Gruppe der Beurteilungsprozesse* umfasst die Bereitstellungsprozesse, wie in Bild 4 dargestellt, die sich mit der Beurteilung des Umsetzungserfolgs aus der Gruppe der Umsetzungsprozesse beschäftigen, einschließlich:

- Prozess zur Beurteilung der Umsetzung, und
- Prozess zur Umsetzung der Beurteilungsergebnisse.

Es wird darauf hingewiesen, dass der Prozess zur *Umsetzung der Vorfallerkennung* mit dem Prozess zur *Vorfallerkennung* in Bild 8 verknüpft ist, um den Übergang von der Gruppe der Bereitstellungsprozesse zur Gruppe der Initialisierungsprozesse zu schaffen.

Zu den Eingaben für alle Prozesse von Bild 4 zählen alle Informationen über die Systemarchitektur, die Technologie (Hardware und Software), Politiken, Verfahrensweisen und Geschäftsabläufe einer Organisation, soweit zutreffend. Die Eingaben sollten außerdem die vier Ziele der Bereitstellungsprozesse, die bereits zuvor genannt wurden, beachten. Die Eingaben, die sich aus den vier bereits genannten Zielen ergeben, werden im weiteren Verlauf dieser Internationalen Norm als bereits bekannte Systemeingaben bezeichnet.

Die Bereitstellungsprozesse sind iterativ, was bedeutet, dass nach dem letzten Prozess zum vorhergehenden Bereitstellungsprozess zurückgekehrt werden kann, wie in Bild 4 dargestellt. Wenn beispielsweise während des Prozesses zur *Beurteilung der Umsetzung* festgestellt wird, dass eine bestimmte definierte Systemarchitektur nicht ordnungsgemäß umgesetzt worden ist, müsste zum Prozess zur *Umsetzung der Systemarchitektur* zurückgekehrt werden. Ein weiteres Beispiel ist, wenn festgestellt wird, dass die Pläne, die während des Prozesses zur *Planung der Sammlung, Speicherung und Bearbeitung von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen* gemacht wurden, nicht den Zielen der Bereitstellungsprozesse von digitalen Ermittlungen in der jeweiligen Organisation entsprechen und zum Prozess zur *Planung der Sammlung, Speicherung und Bearbeitung von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen* zurückgekehrt werden könnte, um diese Pläne entsprechend zu ändern.

Jeder der Bereitstellungsprozesse wird in den nachstehenden Abschnitten erläutert.

7.2 Prozess zur Definition des Szenariums

In diesem Prozess sollten alle möglichen Szenarien untersucht werden, in denen digitale Beweismittel erforderlich sein können. Das Ergebnis dieses Prozesses sind die definierten Szenarien.

Außerdem wird empfohlen, dass während dieses Prozesses für jedes identifizierte Szenarium eine angemessene Risikobeurteilung durchgeführt wird. Eine Risikobeurteilung würde es ermöglichen, mögliche Bedrohungen, Schwachstellen und damit zusammenhängende Szenarien, die bestimmte Informationsbestände offenlegen würden, besser zu identifizieren. Ausgehend von den behandelten Risiken durch bestimmte Bedrohungen, Schwachstellen oder Szenarien kann in späteren Prozessen besser über erforderliche Maßnahmen entschieden werden, um innerhalb einer Organisation eine Ermittlungsbereitstellung zu erreichen. Das hilft einer Organisation dabei, den Risikograd, Kosten und Vorteile möglicher Maßnahmen mit der Absicht zu berücksichtigen, die identifizierten Risiken zu verringern.

7.3 Prozess zur Identifikation von potentiellen Quellen für digitale Beweismittel

In diesem Prozess sollten potentielle Quellen für digitale Beweismittel in einer Organisation identifiziert werden. Das Ergebnis dieses Prozesses sind definierte potentielle Quellen für digitale Beweismittel.

Einige der identifizierten potentiellen Quellen sind möglicherweise nicht verfügbar. Wenn z. B. Zugangsprotokolle nicht im System hinterlegt sind, bedeutet dies, dass Zugangsprotokolle nicht als Datenquelle für eine digitale Ermittlung verfügbar sind. In diesem Fall sollten Maßnahmen entwickelt werden, um die identifizierte Quelle zur Verfügung zu stellen.

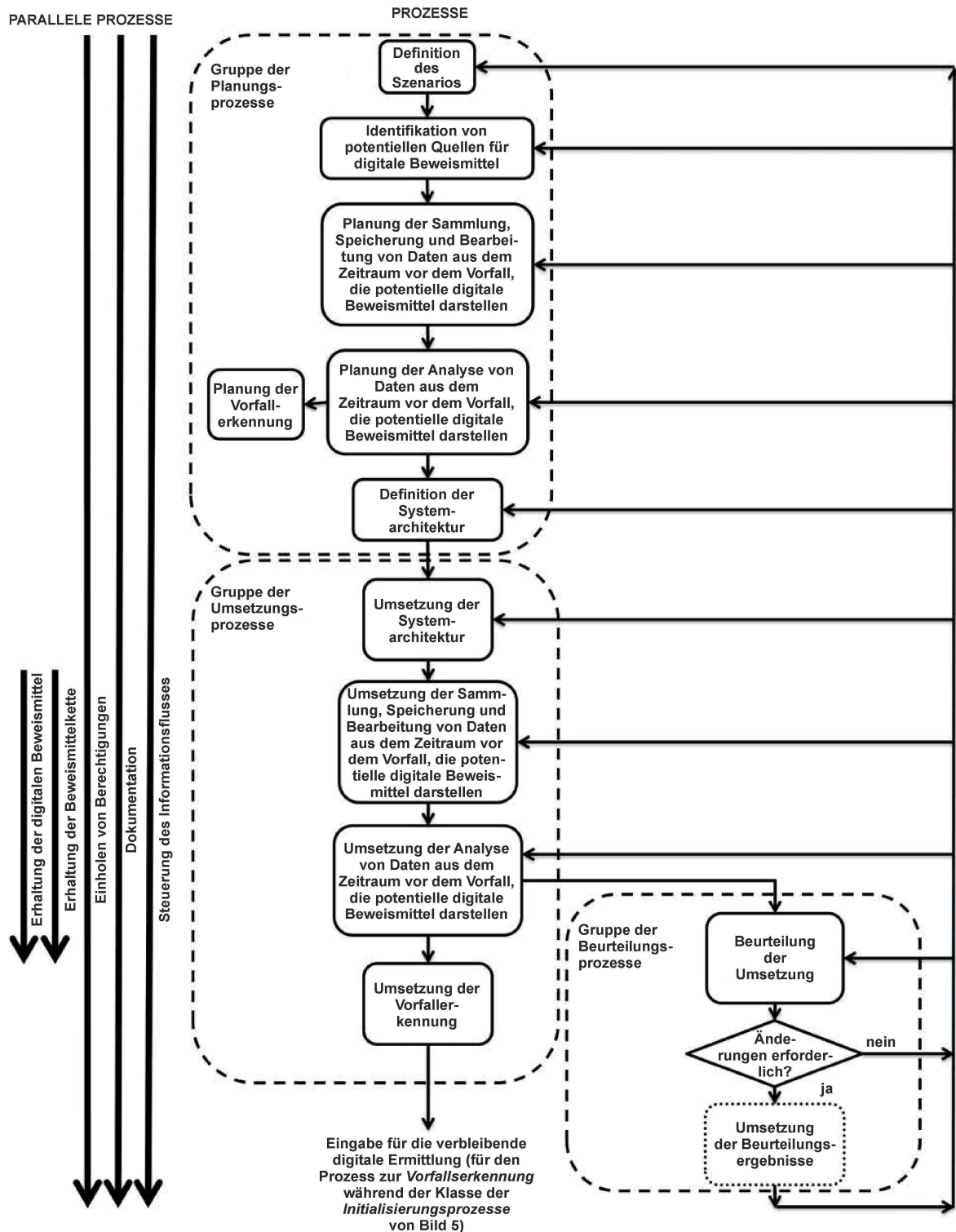


Bild 4 — Bereitstellungsprozesse

7.4 Prozess zur Planung der Sammlung, Speicherung und Bearbeitung von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen

Während dieses Prozesses sollten die Tätigkeiten für die Sammlung, Speicherung und Bearbeitung von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen, festgelegt werden. Das Ergebnis dieses Prozesses sind die festgelegten Tätigkeiten für die Sammlung, Speicherung und Bearbeitung von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen.

Der Sammlungszeitraum für bestimmte Datentypen ist basierend auf einer Risikobeurteilung zu bestimmen. Das Sammeln, Speichern und Bearbeiten von Daten muss außerdem den Grundsätzen der digitalen Ermittlung entsprechen, damit die digitalen Beweismittel vor Gericht zulässig sind. Schließlich ist die Aufbewahrungsfrist für Daten basierend auf den folgenden Faktoren zu bestimmen:

- Risikobeurteilung;
- frühere Erfahrungen in Bezug auf Vorfallerkennung, Datenmengen, Netzwerkkapazität und alle anderen Belange, die einen Einfluss auf die Kosten oder die Effizienz dieses Prozesses haben könnten;
- Gesetze innerhalb der jeweiligen Rechtsordnung;
- Verordnungen;
- geschäftsspezifische Anforderungen.

7.5 Planung der Analyse von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen

Während dieses Prozesses sollten Verfahrensweisen für die Analyse von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen, festgelegt werden.

Die Eingabe für diesen Prozess sind die Szenarien, die während des Prozesses zur Definition des Szenariums festgelegt wurden, sowie die Ausgabe des Prozesses zur Sammlung von Daten aus dem Zeitraum vor dem Vorfall. Die Eingabe sollte außerdem die Ziele der Bereitstellungsprozesse berücksichtigen.

Das Ergebnis dieses Prozesses sind die festgelegten Tätigkeiten für die Analyse von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen. Das Ziel dieser Analyse ist das Erkennen eines Vorfalls. Aus diesem Grund sollten Tätigkeiten, die in diesem Prozess definiert wurden, genaue Informationen darüber enthalten, wie der Vorfall erkannt wird und welches Verhalten einen Vorfall begründet.

Da die Aufgaben der Datenanalyse und Vorfallerkennung oftmals nicht Teil der Funktionen der behandelten Informationssysteme sind, wird empfohlen, dass dieser Prozess eine Schnittstelle zwischen den Bereitstellungsprozessen und einem Überwachungssystem definiert, das Daten analysiert, um Vorfälle zu erkennen. Das Überwachungssystem kann ein beliebiges System sein, das für diesen Zweck geeignet ist. Es kann auch eines der folgenden Systeme sein: Angriffspräventionssysteme, Angriffserkennungssysteme, Systeme zur Änderungsverfolgung, Systeme zur Protokollverarbeitung usw.

7.6 Prozess zur Planung der Vorfallerkennung

Während dieses Prozesses sollten die Maßnahmen festgelegt werden, die durchzuführen sind, wenn ein Vorfall erkannt wurde. Das Ergebnis dieses Prozesses sind definierte Maßnahmen, die durchzuführen sind, sobald ein Vorfall erkannt wurde, besonders die Weitergabe von Informationen an den verbleibenden digitalen Ermittlungsprozess. Informationen sollten auch bereits bekannte Systemeingaben, Ergebnisse aus allen Prozessen der Bereitstellungs-kategorie sowie die Daten, die während der *Gruppe der Umsetzungsprozesse* gesammelt und erstellt wurden, enthalten.

7.7 Prozess zur Definition der Systemarchitektur

Während dieses Prozesses sollte die Systemarchitektur des Informationssystems für die Organisation festgelegt werden, wobei die Ergebnisse aller vorhergehenden Bereitstellungsprozesse berücksichtigt werden. In diesem Kontext bezieht sich die Systemarchitektur des Informationssystems auf die organisatorische Struktur eines Informationssystems, einschließlich notwendiger Anwendungssysteme, Computerausstattungen, einem Kommunikationsnetzwerk und dazugehöriger Software.

Die Eingabe für diesen Prozess ist das Ergebnis aus allen vorhergehenden Bereitstellungsprozessen. Die Eingabe sollte außerdem die Ziele für die Bereitstellungsprozesse berücksichtigen.

Die Ausgabe dieses Prozesses ist die definierte Systemarchitektur für die Organisation. Das Ziel ist es, die Systemarchitektur individuell einzurichten, mit besonderem Augenmerk auf die elektronische Daten- bzw. Informationsspeicherung und den elektronischen Datentransfer bzw. Informationsaustausch innerhalb der Architektur, um dem Erreichen der Ziele der Bereitstellungsprozesse entgegenzukommen. Das Hauptziel dieses Prozesses ist die Identifikation von potentiellen Daten- und/oder Informationsquellen innerhalb der Systemarchitektur.

7.8 Prozess zur Umsetzung der Systemarchitektur

Während dieses Prozesses sollte die Systemarchitektur, wie sie im Prozess zur *Definition der Systemarchitektur* festgelegt ist, umgesetzt werden. Das Ergebnis dieses Prozesses ist die umgesetzte Systemarchitektur.

Beispiele für die *Umsetzung der Systemarchitektur* umfassen die Installation neuer Software, Hardware und/oder Politiken, die es ermöglichen, die verbleibenden Bereitstellungsprozesse im gesamten Informationssystem und in der Organisation zu instanzieren.

7.9 Prozess zur Umsetzung der Sammlung, Speicherung und Bearbeitung von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen

Während dieses Prozesses sollten die Sammlung, Speicherung und Bearbeitung von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen, umgesetzt werden, wie im Prozess zur *Planung der Sammlung, Speicherung und Bearbeitung von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen*, festgelegt. Das Ergebnis dieses Prozesses ist die umgesetzte Sammlung, Speicherung und Bearbeitung von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen.

Beispiele für die *Sammlung, Speicherung und Bearbeitung von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen*, umfassen den Einsatz von Protokollierungssoftware und -hardware mit Zeitstempelung und Funktionen zur digitalen Signatur oder den Einsatz von Individualsoftware zur Sammlung wichtiger Daten (d. h. Daten zur Systemnutzung).

7.10 Prozess zur Umsetzung der Analyse von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen

Während dieses Prozesses sollte die Analyse von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen, umgesetzt werden, wie im Prozess zur *Planung der Analyse von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen*, festgelegt. Das Ergebnis dieses Prozesses ist die Umsetzung der Analyse von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen.

Beispiele für die *Analyse von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen*, umfassen die Ausführung einer Software zur Änderungsverfolgung, z. B. ein Datenintegritätsprüfer, Angriffserkennungs-/präventionssoftware und/oder Anti-Virus-Software. Da das Ergebnis dieses Prozesses in Form von erkannten Vorfällen ausgegeben wird, knüpft es somit an die Eingabe für den Prozess zur Vorfallerkennung der digitalen Ermittlungsprozesse an, wie in Bild 4 dargestellt.

7.11 Prozess zur Umsetzung der Vorfallerkennung

Während dieses Prozesses sollten die Maßnahmen umgesetzt werden, die im Prozess zur *Planung der Vorfallerkennung* festgelegt wurden. Die Umsetzung der Vorfallerkennung hängt außerdem vom Prozess zur *Umsetzung der Analyse von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen*, ab und erhält Eingaben daraus, da die Erkennung basierend auf der durchgeführten Analyse erfolgt.

Während des Prozesses zur *Umsetzung der Vorfallerkennung* erfolgt die Erkennung eines Vorfalls entsprechend den Regeln, die während des Prozesses zur *Planung der Vorfallerkennung* definiert wurden. Während des Prozesses zur *Umsetzung der Vorfallerkennung* sollte außerdem entschieden werden, welche Daten über den Vorfall an den verbleibenden digitalen Ermittlungsprozess weitergegeben werden sollten.

Beispiele für die Vorfallerkennung können sein, wenn eine Software zur Änderungsverfolgung Änderungen in einem bestimmten archivierten Protokoll erkennt oder wenn ein Angriff über das Angriffserkennungssystem erkannt wird.

Die Kriterien, die ein Ereignis als Vorfall deklarieren würden, der eine digitale Ermittlung erfordert, hängen von den Politiken der Organisation ab und können in dieser Internationalen Norm nicht vorgeschrieben werden.

Dieser Prozess ist eine Schnittstelle zum verbleibenden digitalen Ermittlungsprozess. Dieser Prozess ist eine Überschneidung zwischen Bereitstellungsprozessen und einer Ermittlung an sich. Der Grund für die Überschneidung ist, dass die digitale Ermittlung nicht beginnen kann, bevor ein Vorfall erkannt worden ist.

7.12 Prozess zur Beurteilung der Umsetzung

Während des Prozesses zur *Beurteilung der Umsetzung* werden die Ergebnisse aus der *Gruppe der Umsetzungsprozesse* beurteilt und mit den Zielen zur Bereitstellung einer digitalen Ermittlung verglichen. Das Ergebnis dieses Prozesses sind die Ergebnisse der Beurteilung der Umsetzung der Bereitstellung der digitalen Ermittlung für ein Informationssystem. Es wird empfohlen, dass bei diesem Prozess eine juristische Überprüfung aller vorher festgelegten Verfahrensweisen, Maßnahmen und Architekturen durchgeführt wird. Diese Überprüfung sollte unter anderem aufzeigen, ob Konformität mit der rechtlichen Umgebung und den Grundsätzen der digitalen Forensik in der jeweiligen Rechtsordnung besteht, um die Zulässigkeit der potentiellen digitalen Beweismittel vor Gericht zu versichern.

7.13 Prozess zur Umsetzung der Beurteilungsergebnisse

Dieser Prozess beschäftigt sich mit der Umsetzung der Schlussfolgerungen aus dem vorhergehenden Prozess. Da möglicherweise keine Änderungen erforderlich sind, was auf den Prozess zur *Beurteilung der Umsetzung* zurückzuführen ist, ist dieser Prozess optional. Es wird darauf hingewiesen, dass dieser Prozess in Bild 4 als optional angegeben und mithilfe einer gestrichelten Linie um den Prozess herum als solcher gekennzeichnet ist.

Während dieses Prozesses sollte über Änderungsempfehlungen für einen oder mehrere der vorhergehenden Prozesse entschieden werden. Die wichtigste Entscheidung hierbei ist, ob zu einem der Planungsprozesse in der *Gruppe der Planungsprozesse* der *Bereitstellungsklasse* von Prozessen zurückzukehren ist oder ob zu einem der Prozesse in der *Gruppe der Umsetzungsprozesse* zurückzukehren ist, was von den Schlussfolgerungen aus dem Prozess zur *Beurteilung der Umsetzung* abhängt. Es könnte beispielsweise geschlossen werden, dass die Umsetzung einer bestimmten Maßnahme (z. B. dass während der *Umsetzung der Systemarchitektur* die Maßnahmen zur Log-in-Berechtigung nicht ordnungsgemäß umgesetzt wurden, die während des Prozesses zur *Definition der Systemarchitektur* geplant wurden) nicht optimal erfolgte oder es könnte entschieden werden, dass eine neue Umsetzung vorzunehmen ist.