

DIN EN ISO/IEC 27042

ICS 35.040

Einsprüche bis 2016-04-26

Entwurf

**Informationstechnik –
IT-Sicherheitsverfahren –
Leitfaden für die Analyse und Interpretation digitaler Beweismittel
(ISO/IEC 27042:2015);
Deutsche und Englische Fassung FprEN ISO/IEC 27042:2016**

Information technology –
Security techniques –
Guidelines for the analysis and interpretation of digital evidence (ISO/IEC 27042:2015);
German and English version FprEN ISO/IEC 27042:2016

Technologies de l'information –
Techniques de sécurité –
Lignes directrices pour l'analyse et l'interprétation de preuves numériques
(ISO/IEC 27042:2015);
Version allemande et anglaise FprEN ISO/IEC 27042:2016

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 48 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (FprEN ISO/IEC 27042:2016) wurde vom Technischen Komitee ISO/IEC JTC 1/SC 27 „IT Security techniques“ erarbeitet, dessen Sekretariat von DIN (Deutschland) gehalten wird. Auf Grundlage eines CEN/BT Beschlusses wurde ISO/IEC 27042:2015 im einstufigen Annahmeverfahren (UAP) als FprEN ISO/IEC 27041:2016 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 27042 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 27037:2012 siehe DIN EN ISO/IEC 27037¹⁾

ISO/IEC 27041 siehe DIN EN ISO/IEC 27041²⁾

Nationaler Anhang NA (informativ)

Literaturhinweise

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

E DIN EN ISO/IEC 27041, Informationstechnik — IT-Sicherheitsverfahren — Leitfaden zur Sicherung der Tauglichkeit und Eignung von Vorfall-Untersuchungsmethoden (ISO/IEC 27041:2015)

¹⁾ In Bearbeitung.

²⁾ In Bearbeitung.

Informationstechnik — IT-Sicherheitsverfahren — Leitfaden für die Analyse und Interpretation digitaler Beweismittel (ISO/IEC 27042:2015)

Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'analyse et l'interprétation de preuves numériques (ISO/IEC 27042:2015)

Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence (ISO/IEC 27042:2015)

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	12
4 Symbole und Abkürzungen	15
5 Ermittlung	15
5.1 Überblick	15
5.2 Aufrechterhaltung	16
5.3 Wiederholpräzision und Vergleichpräzision	16
5.4 Strukturierter Ansatz	16
5.5 Unsicherheit	17
6 Analyse	18
6.1 Überblick	18
6.2 Allgemeine Grundsätze	18
6.3 Einsatz von Tools	19
6.4 Dokumentation	19
7 Analytische Modelle	19
7.1 Statische Analyse	19
7.2 Echtzeitanalyse	20
7.2.1 Überblick	20
7.2.2 Echtzeitanalyse von Systemen, von denen kein Abbild und keine Kopie erstellt werden kann	20
7.2.3 Echtzeitanalyse von Systemen, von denen ein Abbild oder eine Kopie erstellt werden kann	20
8 Interpretation	21
8.1 Allgemeines	21
8.2 Zulassung von Fakten	21
8.3 Die Interpretation beeinflussende Faktoren	21
9 Berichterstattung	22
9.1 Vorbereitung	22
9.2 Empfohlener Berichtsinhalt	22
10 Kompetenz	23
10.1 Überblick	23
10.2 Kompetenznachweis	23
10.3 Kompetenzerfassung	23
11 Eignung	24
11.1 Überblick	24
11.2 Instrumente für den Eignungsnachweis	24
Anhang A (informativ) Beispiele für die Festlegung von Kompetenz und Eignung	25

A.1	Beispiel für die Festlegung der Kompetenz.....	25
A.2	Beispiel für die Festlegung der Eignung.....	25
	Literaturhinweise.....	26

Europäisches Vorwort

Der Text von ISO/IEC 27042:2015 wurde vom Technischen Komitee ISO/IEC JTC/TC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und auf Grundlage eines CEN/BT Beschlusses als FprEN ISO/IEC 27042:2016 übernommen.

Dieses Dokument ist derzeit zum einstufigen Annahmeverfahren vorgelegt.

Anerkennungsnotiz

Der Text von ISO/IEC 27042:2015 wurde vom CEN als FprEN ISO/IEC 27042:2016 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. Das für dieses Dokument verantwortliche Komitee ist ISO/IEC JTC 1, *Information technology, SC 27, IT Security techniques*.

Einleitung

Allgemeines

Diese Internationale Norm liefert einen Leitfaden für die Durchführung der Analyse und Interpretation von potentiellen digitalen Beweismitteln, um digitale Beweismittel, die als Hilfsmittel für ein besseres Verständnis eines Vorfalls eingesetzt werden können, zu identifizieren und auszuwerten. Die genaue Art der Daten und Informationen, die ein potentielles digitales Beweismittel ausmachen, hängt von der Art des Vorfalls und der Quellen für digitale Beweismittel, die mit dem Vorfall in Zusammenhang stehen, ab.

Bei der Anwendung dieser Internationalen Norm geht der Anwender davon aus, dass der in ISO/IEC 27035-2 und ISO/IEC 27037:2012 enthaltene Leitfaden eingehalten wurde und dass alle eingesetzten Prozesse mit dem Leitfaden nach ISO/IEC 27043:2015 und ISO/IEC 27041¹⁾ kompatibel sind.

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 digitaler Beweismittel;
- Verstehen von Grundsätzen und Prozessen bei der Ermittlung von digitalen Beweismitteln;

1) In Veröffentlichung.

- 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 27040:2015

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, Auslegung, 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 versichert werden kann, dass Methoden und Prozesse die Anforderungen der Ermittlung erfüllen und dass sie entsprechend getestet worden sind.

— ISO/IEC 27043:2015

Diese Internationale Norm legt die üblicherweise wichtigsten Grundsätze und Prozesse fest, die der Ermittlung von Vorfällen zugrunde liegen, und enthält ein Rahmenmodell für alle Stufen der Ermittlung.

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

Dieser Teil enthält die Grundlagen und Phasen des Managements von Informationssicherheitsvorfällen. Er vereint diese Grundlagen mit den Grundsätzen in einem strukturierten Ansatz zur Erkennung von, Berichterstattung von, Beurteilung von, Reaktion auf und Nutzung von Erfahrungen.

— ISO/IEC 27035-2

Dieser Teil enthält die Grundlagen für die Planung und Vorbereitung von Reaktionen auf einen Vorfall. Die Grundlagen, einschließlich Vorfallmanagementpolitik und -plan, Zusammenstellung eines Teams zur Reaktion auf einen Vorfall sowie Unterweisungen und Sensibilisierungen, basieren auf der Planungs- und Vorbereitungsphase des in ISO/IEC 27035-1 dargestellten Modells. Dieser Teil behandelt außerdem die Phase „Gewinnung von Erkenntnissen“ des Modells.

— ISO/IEC 27035-3

Dieser Teil enthält die Verantwortlichkeiten des Personals und praktische Tätigkeiten zur Reaktion auf einen Vorfall innerhalb der Organisation. Ein besonderes Augenmerk wird dabei auf die Tätigkeiten des Teams zur Reaktion auf einen Vorfall gelegt, z. B. Tätigkeiten zur Überwachung, Erkennung, Analyse und Reaktion im Zusammenhang mit den erfassten Daten oder Sicherheitsereignisse.

— ISO/IEC 27044²⁾

Dieses Dokument enthält Leitlinien für Organisationen, die damit beschäftigt sind, den Einsatz von Sicherheitsinformations- und Ereignis-Managementprozessen/-systemen vorzubereiten. Im Einzelnen behandelt es die Auswahl, den Einsatz und die Abläufe von SIEM (Sicherheitsinformations- und Ereignis-Management). Dessen Zweck ist insbesondere, Unterstützung bei der Erfüllung der Anforderungen von ISO/IEC 27001 im Hinblick auf die Umsetzung von Verfahren und anderen Lenkungen zu leisten, die eine sofortige Erkennung von und Reaktion auf Sicherheitsvorfälle ermöglichen können, sowie Überwachungen durchzuführen und Verfahren zu überprüfen, um versuchte und erfolgreiche Sicherheitsverstöße und -vorfälle zu ermitteln.

2) In Veröffentlichung.

— ISO/IEC 27050 (alle Teile)³⁾

Dieses Dokument behandelt Tätigkeiten der elektronischen Beweissicherung, einschließlich unter anderem der Identifizierung, des Erhalts, der Erfassung, der Verarbeitung, der Überprüfung, der Analyse und der Erstellung von elektronisch gespeicherten Informationen (ESI, en: electronically stored information). Außerdem liefert es Leitlinien zu Maßnahmen, die von der ersten Erstellung von ESI bis hin zu deren Verteilung reichen, mit denen eine Organisation ein Risiko mindern und Ausgaben verringern kann, falls die elektronische Beweissicherung relevant werden sollte. Es ist sowohl für technisches Personal als auch für nichttechnisches Personal relevant, das an einigen oder an allen Tätigkeiten der elektronischen Beweissicherung beteiligt ist. Es ist wichtig anzumerken, dass dieser Leitfaden nicht dafür vorgesehen ist, lokalen Gesetzen und Verordnungen zu widersprechen oder sie zu ersetzen.

Die elektronische Beweissicherung dient häufig als Einflussfaktor für Ermittlungen, sowie auch für Beweissuch- und Beweisaufnahmetätigkeiten. Des Weiteren müssen die Empfindlichkeit und die Kritikalität der Daten manchmal besonders geschützt werden, wie z. B. durch die Speichersicherheit zum Schutz vor Verletzungen der Datensicherheit.

— ISO/IEC 30121:2015

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 können 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 und ISO/IEC 27037 näher erläuterten Tätigkeiten überein.

3) In Veröffentlichung.

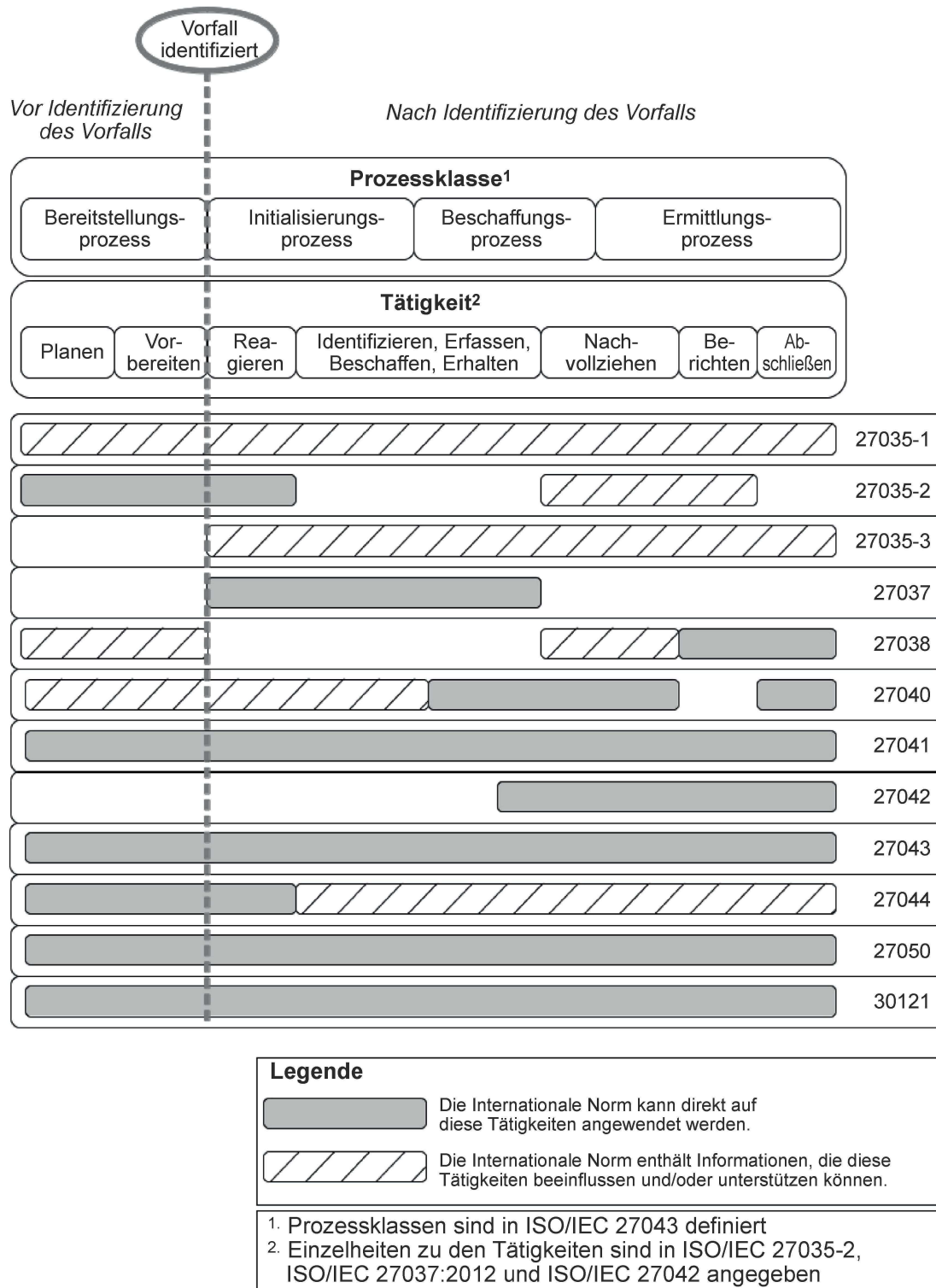


Bild 1 — Anwendbarkeit der Normen auf die Ermittlungsprozessklassen und Ermittlungstätigkeiten

1 Anwendungsbereich

Diese Internationale Norm liefert Leitlinien für die Analyse und Interpretation von digitalen Beweismitteln, wobei auf die Fragen der Aufrechterhaltung, Gültigkeit, Vergleichspräzision und Wiederholpräzision eingegangen wird. Sie beschreibt bewährte Verfahrensweisen (Best Practice) für die Auswahl, Auslegung und Umsetzung von Analyseprozessen sowie die Aufzeichnung von ausreichend Informationen, um solche Prozesse, sofern erforderlich, unabhängigen Überprüfungen zu unterziehen. Sie liefert Hinweise zu geeigneten Instrumenten für den Nachweis der Eignung und Kompetenz der Ermittlungsgruppe.

Die Analyse und Interpretation von digitalen Beweismitteln kann ein komplexer Prozess sein. Unter Umständen kann es mehrere Methoden geben, die angewendet werden könnten, und die Mitglieder der Ermittlungsgruppe müssen ihre Entscheidung für einen bestimmten Prozess begründen und zeigen, inwieweit er mit anderen Prozessen, die von anderen Ermittlern angewendet werden, übereinstimmt. Unter anderen Umständen dürfen Ermittler neue Methoden zur Untersuchung digitaler Beweismittel entwickeln, die zuvor nicht berücksichtigt wurden, und aufzeigen sollten, dass die entwickelte Methode „zweckdienlich“ ist.

Durch die Anwendung einer bestimmten Methode kann die Interpretation von digitalen Beweismitteln, die mit dieser Methode verarbeitet worden sind, beeinflusst werden. Die verfügbaren digitalen Beweismittel können die Auswahl der Methoden für weitere Analysen der digitalen Beweismittel, die bereits gewonnen wurden, beeinflussen.

Diese Internationale Norm liefert einen gemeinsamen Rahmen für die Analyse- und Interpretationselemente für den Umgang mit Sicherheitsvorfällen in Informationssystemen, der zur Unterstützung bei der Umsetzung neuer Methoden eingesetzt werden kann und einen gemeinsamen Mindeststandard für digitale Beweismittel, die aus solchen Aktivitäten hervorgehen, liefern kann.

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 27000:2013, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

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

ISO/IEC 27041⁴⁾, *Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method*

4) In Veröffentlichung.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 27000:2013 und die folgenden Begriffe.

3.1 Analyse
Bewertung von *potentiellen digitalen Beweismitteln* (3.15), um deren Relevanz für die Ermittlung zu beurteilen

Anmerkung 1 zum Begriff: Aus *potentiellen digitalen Beweismitteln* (3.15), für die eine Relevanz ermittelt wird, werden *digitale Beweismittel* (3.5).

Anmerkung 2 zum Begriff: Siehe auch Bild 2.

3.2 Auftraggeber
natürliche oder juristische Person, in deren Namen die Ermittlung durchgeführt werden soll

3.3 Kompetenz
Eignung, Wissen und Fertigkeiten anzuwenden, um beabsichtigte Ergebnisse zu erzielen

[QUELLE: ISO/IEC 17021:2011, 3.7]

3.4 zeitgleiche Notizen
zeitgleiche Aufzeichnungen
schriftliche Aufzeichnungen über durchgeführte Tätigkeiten und getroffene Entscheidungen, die erstellt werden, während die Tätigkeiten durchgeführt und die Entscheidungen getroffen werden, oder im Anschluss daran, sobald dies praktisch möglich ist

Anmerkung 1 zum Begriff: In vielen Zuständigkeitsbereichen wird gefordert, dass zeitgleiche Notizen handschriftlich mit nicht löschbarer Tinte in einem manipulationssicheren Notizbuch angefertigt werden, um in Fragen der Nichtabstreitbarkeit und Zulässigkeit Hilfestellung zu leisten.

3.5 digitale Beweismittel
Informationen oder Daten, die in binärer Form gespeichert oder übertragen werden und die durch eine Analyse als relevant für die Ermittlung befunden wurden

Anmerkung 1 zum Begriff: Digitale Beweismittel sollten nicht mit *rechtskräftigen digitalen Beweismitteln* (3.14) oder *potentiellen digitalen Beweismitteln* (3.15) verwechselt werden.

Anmerkung 2 zum Begriff: Siehe auch Bild 2.

[QUELLE: ISO/IEC 27037:2012, 3.5, modifiziert — Anmerkung 1 und Anmerkung 2 zum Begriff wurden hinzugefügt; die Definition wurde angepasst, um zwischen Beweismitteln für den Vorfall, der Gegenstand der Ermittlung ist, und anderen nicht relevanten Informationen oder Daten zu unterscheiden.]

3.6 Nachbilden
Emulieren
genaues Nachahmen einer anderen Anwendung oder Umgebung oder das Durchführen auf die gleiche Weise

3.7

Untersuchung

Reihe von Prozessen, die durchgeführt werden, um relevante potentielle digitale Beweismittel aus einer oder mehreren Quellen zu identifizieren und wiederherzustellen

3.8

Verschleierung von Beweismitteln

Folge einer Handlung, die an potentiellen digitalen Beweismitteln durchgeführt wurde und dazu führt, dass die digitalen Beweismittel auf irgendeine Weise verborgen oder verschleiert werden

Anmerkung 1 zum Begriff: Die Verschleierung kann das Ergebnis einer gewollten oder einer ungewollten Handlung sein und kann bzw. kann nicht zur Vereitelung der digitalen Beweismittel führen.

3.9

Interpretation

Zusammenwirken 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

3.10

Ermittlung

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

3.11

Leiter der Ermittlungsgruppe

Person, die die Ermittlungen auf strategischer Ebene anführt

3.12

Ermittlungsgruppe

alle Personen, die direkt an der Durchführung der Ermittlung beteiligt sind

3.13

Ermittler

Mitglied der Ermittlungsgruppe, einschließlich des *Leiters der Ermittlungsgruppe* (3.11)

3.14

rechtskräftige digitale Beweismittel

digitale Beweismittel (3.5), die vor Gericht zugelassen sind

Anmerkung 1 zum Begriff: Siehe auch Bild 2.

3.15

potentielle digitale Beweismittel

Informationen oder Daten, die in binärer Form gespeichert oder übertragen werden und für die noch nicht durch eine Analyse bestimmt wurde, ob sie für die Ermittlung relevant sind

Anmerkung 1 zum Begriff: Durch die Analyse wird bestimmt, welche der *potentiellen digitalen Beweismittel* auch tatsächlich *digitale Beweismittel* (3.5) sind.

Anmerkung 2 zum Begriff: Siehe auch Bild 2.