

DIN EN ISO/IEC 27043

ICS 35.030

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

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

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

Gesamtumfang 48 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (EN ISO/IEC 27043:2016) 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 27043:2015 im einstufigen Annahmeverfahren (UAP), als EN 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).

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

ISO/IEC 27000 siehe DIN ISO/IEC 27000*)

Nationaler Anhang NA (informativ)

Literaturhinweise

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

*) In Bearbeitung.

Deutsche Fassung

Informationstechnik —
IT-Sicherheitsverfahren —
Grundsätze und Prozesse für die Untersuchung von Vorfällen
(ISO/IEC 27043:2015)

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

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

Diese Europäische Norm wurde vom CEN am 19. Juni 2016 angenommen.

Die CEN und CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Management-Zentrum des CEN-CENELEC oder bei jedem CEN und CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN- und CENELEC-Mitglieder sind die nationalen Normungsinstitute und elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION

CEN-CENELEC Management-Zentrum: Avenue Marnix 17, B-1000 Brüssel

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 Untersuchungen	14
5.1 Allgemeine Grundsätze	14
5.2 Rechtsgrundsätze	14
6 Digitale Untersuchungsprozesse	16
6.1 Allgemeiner Überblick über die Prozesse	16
6.2 Klassen der digitalen Untersuchungsprozesse	16
7 Bereitschaftsprozesse	18
7.1 Überblick über die Bereitschaftsprozesse	18
7.2 Prozess zur Definition des Szenarios	20
7.3 Prozess zur Identifikation von potentiellen Quellen für digitale Beweismittel	21
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	26
8.3 Prozess zur ersten Reaktion	26
8.4 Prozess zur Planung	27
8.5 Prozess zur Vorbereitung	27
9 Sicherungsprozesse	27
9.1 Überblick über die Sicherungsprozesse	27
9.2 Prozess zur Identifikation von potentiellen digitalen Beweismitteln	28
9.3 Prozess zur Mitnahme von potentiellen digitalen Beweismitteln	28
9.4 Prozess zur Sicherung 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 Untersuchungsprozesse	30

10.1	Überblick über die Untersuchungsprozesse	30
10.2	Prozess zur Sicherung von potentiellen digitalen Beweismitteln.....	31
10.3	Prozess zur Prüfung 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 Untersuchungsabschluss.....	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 Obhutskette.....	34
11.6	Prozess zur Erhaltung der digitalen Beweismittel.....	34
11.7	Prozess zur Interaktion mit den physischen Untersuchungen	34
12	Musterschema eines digitalen Untersuchungsprozesses.....	34
Anhang A (informativ) Digitale Untersuchungsprozesse: Gründe für die Harmonisierung		37
Literaturhinweise.....		44

Bilder

Bild 1 —	Anwendbarkeit der Normen auf die Untersuchungsprozessklassen und Untersuchungstätigkeiten.....	10
Bild 2 —	Die verschiedenen Prozessklassen von digitalen Untersuchungen	18
Bild 3 —	Gruppen der Bereitschaftsprozesse	19
Bild 4 —	Bereitschaftsprozesse.....	21
Bild 5 —	Initialisierungsprozesse	25
Bild 6 —	Sicherungsprozesse.....	28
Bild 7 —	Untersuchungsprozesse.....	30
Bild 8 —	Harmonisiertes Schema eines digitalen Untersuchungsprozesses	36

Tabellen

Tabelle 1 —	Vergleich von bestehenden Modellen mit dem harmonisierten Modell.....	39
-------------	---	----

Europäisches Vorwort

Der Text von ISO/IEC 27043:2015 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und als EN ISO/IEC 27043:2016 übernommen.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Februar 2017, und etwaige entgegenstehende nationale Normen müssen bis Februar 2017 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN [und/oder CENELEC] sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die ehemalige jugoslawische Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO/IEC 27043:2015 wurde vom CEN als EN 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 und IEC sind 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 Begriffen und Aussagen, 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:
<http://www.iso.org/iso/foreword.html>.

Für dieses Dokument ist das Komitee ISO/IEC JTC 1 *Information technology*, Unterkomitee SC 27 *Security techniques* verantwortlich.

Einleitung

Über diese Internationale Norm

Diese Internationale Norm liefert Leitlinien, die die Idealmodelle für allgemeine Untersuchungsprozesse in unterschiedlichen Szenarien von Untersuchungen umfassen. Dazu zählen die Prozesse von der Vorbereitung auf einen Vorfall bis hin zur Rückgabe von Beweismitteln zur Speicherung oder Verteilung sowie allgemeine Hinweise und Vorbehalte zu Prozessen und die angemessene Identifikation, Mitnahme, Sicherung, Erhaltung, Analyse, Interpretation und Präsentation von Beweismitteln. Ein wesentlicher Grundsatz der digitalen Untersuchung ist die Wiederholbarkeit, bei der ein entsprechend qualifizierter Untersucher in der Lage sein muss, die gleichen Ergebnisse zu erzielen wie ein anderer, ähnlich qualifizierter Untersucher, der unter ähnlichen Bedingungen gearbeitet hat. Dieser Grundsatz ist für jede allgemeine Untersuchung von besonderer Bedeutung. Leitlinien für zahlreiche Untersuchungsprozesse wurden bereitgestellt, um für jeden einzelnen Prozess beim Erzielen der Ergebnisse Eindeutigkeit und Transparenz sicherzustellen. Im Folgenden sind die Gründe für die Bereitstellung von Leitlinien für die Grundsätze und Prozesse von Untersuchungen von Vorfällen angegeben.

Festgelegte Leitlinien, die die Grundsätze und Prozesse von Vorfalluntersuchungen behandeln, würden die Untersuchungen beschleunigen, da sie eine allgemeine Reihenfolge der Ereignisse, die zu einer Untersuchung gehören, liefern würden. Der Einsatz festgelegter Leitlinien ermöglicht während einer Untersuchung einen reibungslosen Übergang von einem Ereignis zum nächsten. Solche Leitlinien würden außerdem angemessene Schulungen für unerfahrene Untersucher ermöglichen. Ein weiteres Ziel dieser Leitlinien ist es, die Flexibilität bei einer Untersuchung sicherzustellen, weil viele verschiedene Arten von Untersuchungen im IT-Bereich möglich sind. Es wurden harmonisierte Grundsätze und Prozesse zur Vorfalluntersuchung festgelegt, und es wird aufgezeigt, wie die Untersuchungsprozesse den unterschiedlichen Untersuchungsszenarien angepasst werden können.

Ein harmonisiertes Modell für den Untersuchungsprozess wird in der strafrechtlichen und zivilrechtlichen Strafverfolgung benötigt sowie in anderen Umgebungen, wie bei Informationssicherheitslücken bei Unternehmen 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 Untersuchung im IT-Bereich so durchzuführen sind, dass kein Zweifel an der Angemessenheit des Untersuchungsprozesses, der während dieser Untersuchung durchgeführt wird, bestehen sollte.

Jede Untersuchung im IT-Bereich erfordert ein hohes Maß an Fachwissen. Die an der Untersuchung 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 Richtlinien und/oder Gesetzen der jeweiligen Rechtsordnung kompatibel sind.

Besteht die Notwendigkeit, einen Prozess einer Person zuzuweisen, dann erhält diese Person die Verantwortung für den Prozess. Demzufolge besteht ein enger Zusammenhang zwischen einer Prozessverantwortung und den Aktionen der Person, die den genauen Untersuchungsablauf bestimmt, der in Übereinstimmung mit den harmonisierten Untersuchungsprozessen, 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 Untersuchungsgrundsätze und -prozesse zuerst auf einer allgemeinen (abstrakten) Ebene präsentiert werden, bevor sie detaillierter beschrieben werden. Beispielsweise wird zuerst ein allgemeiner Überblick über die Untersuchungsgrundsätze und -prozesse angegeben und in den Bildern als „Black Boxes“ dargestellt, und im Anschluss wird jeder allgemeine Prozess in detailliertere (unteilbare) Prozesse unterteilt. Daher wird gegen Ende dieser Internationalen Norm eine weniger abstrakte und detailliertere Sicht auf alle Untersuchungsgrundsätze und -prozesse geboten (siehe Bild 8).

Ziel dieser Internationalen Norm ist es, andere Normen und Dokumente zu ergänzen, die Leitlinien zur Untersuchung von und zur Vorbereitung auf Vorfall-Untersuchungen in der Informationssicherheit enthalten. Sie stellt keinen allumfassenden Leitfaden dar, sondern ist eher ein Leitfaden, der eine breite Übersicht über den gesamten Vorfall-Untersuchungsprozess bietet. Dieser Leitfaden legt außerdem bestimmte wesentliche Grundsätze fest, die sicherstellen sollen, dass geeignete Werkzeuge, Techniken und Methoden ausgewählt werden können und dass 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 Untersuchung von Vorfällen und für die Vorbereitung von Vorfall-Untersuchungen in der Informationssicherheit enthalten, zu ergänzen. Sie stellt keinen allumfassenden Leitfaden dar, sondern legt bestimmte wesentliche Grundsätze fest, die sicherstellen sollen, dass die richtigen Werkzeuge, 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 ist geeignet für Organisationen, die potentielle digitale Beweismittel schützen, analysieren und vorlegen müssen. Sie ist für Entscheidungsgremien von Bedeutung, die Verfahrensweisen bezogen auf digitale Beweismittel erstellen und bewerten, welche häufig Teil einer größeren Beweismenge 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 Untersuchungen;
- Umgang mit digitalen Beweismitteln;
- Einsatz von Schwärzung (en: redaction) und damit verbundene Probleme;
- Angriffspräventions- und -erkennungssysteme, einschließlich der Informationen, die aus diesen Systemen erlangt werden können;
- Sicherheit der Speicherung, einschließlich des Löschens von Datenträgern (en: sanitization);
- Sicherstellen, dass Untersuchungsmethoden zweckdienlich sind;
- Durchführen von Analysen und Interpretationen von digitalen Beweismitteln;
- Verstehen von Grundsätzen und Prozessen bei der Untersuchung von digitalen Beweismitteln;
- Management von Sicherheitsvorfällen, einschließlich der Herleitung von Beweismitteln aus den am Management von Sicherheitsvorfällen beteiligten Systemen;
- Zusammenhang zwischen E-Discovery (en: electronic discovery) und anderen Untersuchungsmethoden, sowie der Einsatz von E-Discovery-Verfahren in anderen Untersuchungen;
- Steuerung von Untersuchungen, einschließlich forensischer Untersuchungen.

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 Untersuchung, einschließlich des ersten Einschreitens (en: initial response), versichern können, dass ausreichend potentielle digitale Beweismittel gesammelt wurden, um die Untersuchung angemessen durchzuführen.

— ISO/IEC 27038

Manche Dokumente können Informationen enthalten, die einigen Personengruppen nicht offen zugänglich gemacht werden dürfen. Modifizierte Dokumente können für diese Personengruppen freigegeben werden, nachdem eine angemessene Bearbeitung des Originaldokuments erfolgt ist. Das Entfernen von Informationen, die nicht freigegeben werden dürfen, wird als „Schwärzen“ (en: redaction) 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 ausgeblendeten Teilen des Dokuments versteckt 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 Datenträgern, die Sicherheit von Managementaktivitäten im Zusammenhang mit Geräten und Datenträgern, die Sicherheit von Anwendungen und Diensten, und die für die Endanwender während der Lebensdauer und nach dem Gebrauch von Geräten und Datenträgern relevante Sicherheit.

Durch die sie begleitenden Verschleierungsmechanismen (en: obfuscation mechanisms) können Sicherheitsfunktionen, wie Verschlüsselung und das Löschen von Daten, die Untersuchungsmöglichkeiten beeinflussen. Sie müssen vor und während der Durchführung einer Untersuchung berücksichtigt werden. Sie können auch wichtig sein bei der Sicherstellung, dass die Speicherung von Beweismitteln während und nach einer Untersuchung angemessen vorbereitet und abgesichert wird.

— ISO/IEC 27041

Es ist wichtig, dass die Eignung von Methoden und Prozessen, die während einer Untersuchung zum Einsatz kommen, nachgewiesen werden kann. Dieses Dokument liefert Leitlinien darüber, wie sichergestellt werden kann, dass Methoden und Prozesse die Anforderungen der Untersuchung erfüllen und dass sie entsprechend getestet worden sind.

— ISO/IEC 27042

Diese Internationale Norm beschreibt die Art und Weise, wie die während einer Untersuchung anzuwendenden Methoden und Prozesse konzipiert und umgesetzt 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 Normenreihe umfasst:

— 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 Leitungsebenen von Organisationen (einschließlich Inhaber, Vorstände, Direktoren, Partner, leitende Angestellte oder ähnliche Personen), um eine Organisation optimal auf digitale Untersuchungen vorzubereiten, bevor diese durchgeführt werden. Diese Internationale Norm gilt für die Entwicklung von strategischen Prozessen (und Entscheidungen) im Zusammenhang mit der Rückhaltung, Verfügbarkeit, Zugänglichkeit und Wirtschaftlichkeit bei der Offenlegung von digitalen Beweismitteln. Diese Internationale Norm gilt für alle Arten und Größen von Organisationen. Die Internationale Norm behandelt die vorausschauende strategische Vorbereitung von digitalen Untersuchungen durch eine Organisation. Die forensische Bereitschaft (en: forensic readiness) stellt sicher, dass eine Organisation geeignete und maßgebliche strategische Vorbereitungen getroffen hat, um potentielle beweiskräftige Ereignisse zu behandeln. Infolge von unvermeidbaren Sicherheitsverstößen, 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 Untersuchung eine Rolle spielen. Die im Bild dargestellten Zahlen (z. B. 27037) weisen auf eine der oben aufgelisteten Internationalen Normen hin, und schattierte Balken geben an, wo sie jeweils mit hoher Wahrscheinlichkeit direkt angewendet werden können oder Einfluss auf den Untersuchungsprozess besitzen (z. B. durch Festlegen von Regeln oder Beschränkungen). Es wird dennoch empfohlen, dass alle Dokumente vor und während der Planungs- und Vorbereitungsphasen hinzugezogen werden. 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.

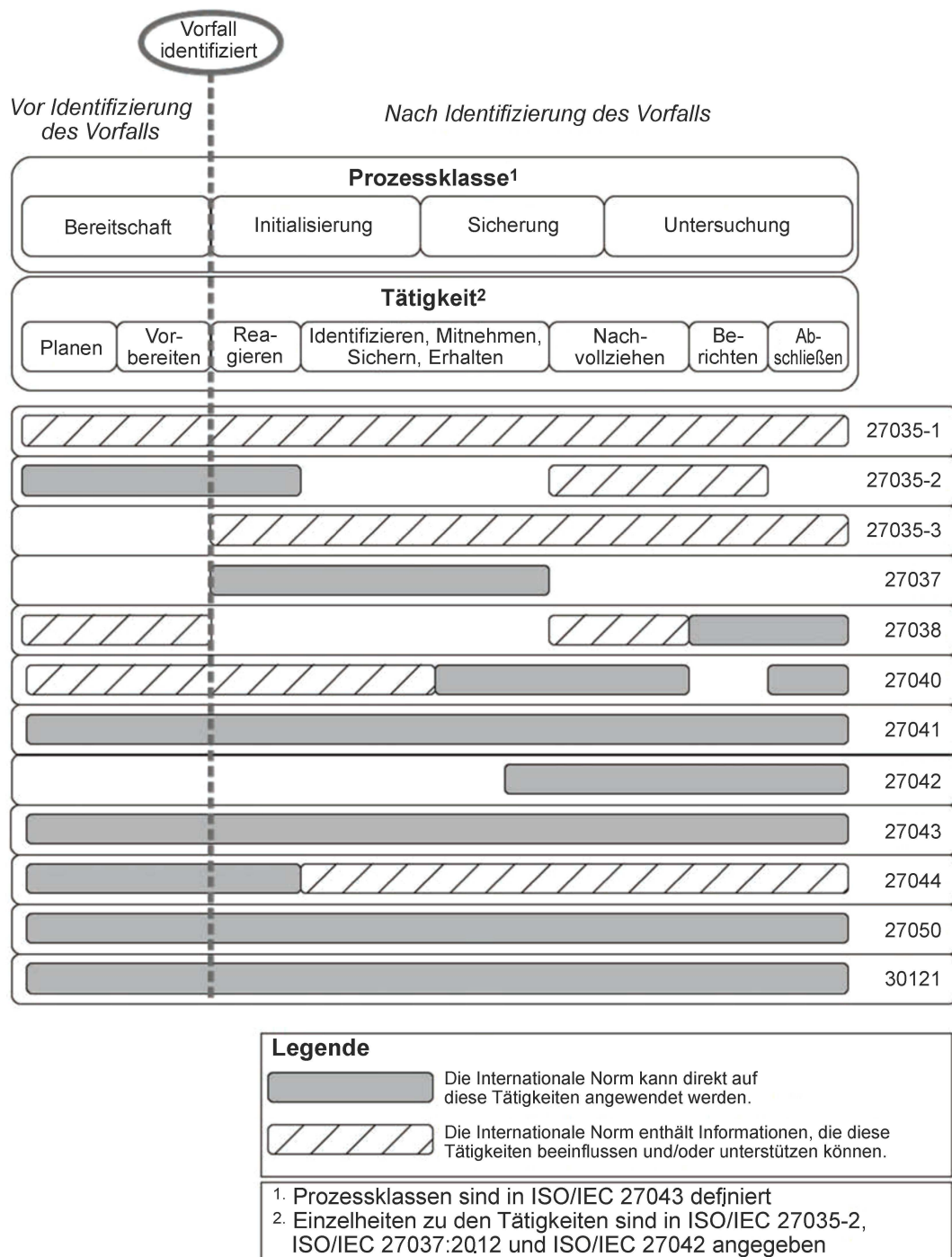


Bild 1 — Anwendbarkeit der Normen auf die Untersuchungsprozessklassen und Untersuchungstätigkeiten

Informationstechnik — IT-Sicherheitsverfahren — Grundsätze und Prozesse für die Untersuchung von Vorfällen

1 Anwendungsbereich

Diese Internationale Norm liefert Leitlinien, die auf Idealmodellen basieren, die für gängige Untersuchungsprozesse von Vorfällen in verschiedenen Vorfall-Untersuchungsszenarien gelten, bei denen digitale Beweismittel eine Rolle spielen. Dazu zählen Prozesse von der Vorbereitung auf Vorfälle bis hin zum Abschluss der Untersuchung sowie alle allgemeinen Hinweise und Vorbehalte zu solchen Prozessen. Die Leitlinien beschreiben Prozesse und Grundsätze, die für verschiedene Arten von Untersuchungen anwendbar sind, wie unter anderem unbefugter Zugriff, Datenbeschädigung, Systemabstürze oder Informationssicherheitslücken bei Unternehmen sowie jede andere Untersuchung im IT-Bereich.

Zusammenfassend liefert diese Internationale Norm einen allgemeinen Überblick über alle Grundsätze und Prozesse von Vorfall-Untersuchungen, ohne dabei bestimmte Details innerhalb aller Grundsätze und Prozesse von Untersuchungen, 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 Untersuchungsgrundsätzen 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

Sicherung

(en: acquisition)

Prozess zur Erstellung einer Kopie von Daten innerhalb eines festgelegten Bereiches

Anmerkung 1 zum Begriff: Das Ergebnis der Sicherung 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 Untersuchung 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

Mitnahme

(en : collection)

Prozess zur Sammlung 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 eines Beweismittels als relevant befunden wurden

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

3.6

digitale Untersuchung

Einsatz von wissenschaftlich hergeleiteten und bewährten Methoden zur Identifikation, Mitnahme, 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, die mit der physischen Untersuchung in Zusammenhang stehen, wie das Erhalten der digitalen Beweismittel, und die Aufrechterhaltung der Obhutskette (en: chain of custody), um die Rekonstruktion von Ereignissen, die als Vorfall bewertet werden und eine digitale Untersuchung erfordern, zu ermöglichen und zu fördern, egal ob sie krimineller Art sind oder nicht

3.7

Identifikation

Prozess, der die Suche 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 Ereignisse, entweder krimineller Art oder nicht, die mit großer Wahrscheinlichkeit die Geschäftsabläufe beeinflussen oder die Informationssicherheit gefährden

3.9

Interpretation

Erstellen einer Erklärung, innerhalb vereinbarter Grenzen, für die Sachinformationen aus den Beweismitteln, die sich aus einer Reihe von Prüfungen und Analysen ergeben, welche zusammen die Untersuchung bilden

[QUELLE: ISO/IEC 27042:—, 3.9]

3.10

Untersuchung

Durchführung von Prüfungen, 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 Prüfungs- und Analyseprozess festgestellt wurde, ob sie für die Untersuchung relevant sind

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

Bereitschaft

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

3.16

Validierung

Bestätigung durch die Bereitstellung eines objektiven Nachweises, dass die Anforderungen für eine(n) spezifische(n) beabsichtigte(n) Gebrauch oder Anwendung erfüllt worden sind

[QUELLE: ISO/IEC 27004:2009, 3.17]