

DIN EN ISO/IEC 27041

ICS 35.030

**Informationstechnik –
IT-Sicherheitsverfahren –
Leitfaden zur Sicherung der Eignung und Angemessenheit von
Vorfall-Untersuchungsmethoden (ISO/IEC 27041:2015);
Deutsche Fassung EN ISO/IEC 27041:2016**

Information technology –
Security techniques –
Guidance on assuring suitability and adequacy of incident investigative method
(ISO/IEC 27041:2015);
German version EN ISO/IEC 27041:2016

Technologies de l'information –
Techniques de sécurité –
Directives sur la façon d'assurer l'aptitude à l'emploi et l'adéquation d'une méthode
d'investigation d'incident (ISO/IEC 27041:2015);
Version allemande EN ISO/IEC 27041:2016

Gesamtumfang 32 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (EN ISO/IEC 27041:2016) 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 27041:2015 im einstufigen Annahmeverfahren (UAP) als EN 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).

Deutsche Fassung

Informationstechnik —
IT-Sicherheitsverfahren —
Leitfaden zur Sicherung der Eignung und Angemessenheit
von Vorfall-Untersuchungsmethoden
(ISO/IEC 27041:2015)

Information technology —
Security techniques —
Guidance on assuring suitability and adequacy
of incident investigative method
(ISO/IEC 27041:2015)

Technologies de l'information —
Techniques de sécurité —
Directives sur la façon d'assurer l'aptitude à l'emploi et
l'adéquation d'une méthode d'investigation d'incident
(ISO/IEC 27041:2015)

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	15
5 Entwicklung von Methoden und deren Sicherung	15
5.1 Überblick	15
5.2 Allgemeine Grundsätze	15
5.3 Allgemeines Entwicklungs- und Einsatzmodell	15
5.4 Sicherungsstufen	16
5.5 Erfassung und Analyse von Anforderungen	17
5.5.1 Allgemeine Grundsätze der Anforderungen	17
5.5.2 Funktionale Anforderungen	18
5.5.3 Verifizierung von Anforderungen	18
5.6 Prozessgestaltung	18
5.6.1 Überblick	18
5.6.2 Auswahl des Tools	18
5.6.3 Unsicherheit und Risikobewertung	19
5.7 Prozessimplementierung	19
5.7.1 Überblick	19
5.7.2 Auswahl des Tools — Hinweise für den Einsatz	20
5.8 Prozessverifizierung	20
5.8.1 Allgemeine Grundsätze der Verifizierung	20
5.8.2 Verifizierung von Prozessen	20
5.8.3 Verifizierung von Tools	20
5.9 Prozessvalidierung	21
5.9.1 Allgemeine Grundsätze der Validierung	21
5.9.2 Umfassende Validierung	21
5.9.3 Ausreichende Validierung	21
5.9.4 Vollständig validierte Prozesse	22
5.9.5 Nicht bestandene Validierung	22
5.10 Bestätigung	22
5.11 Einsatz	22
5.11.1 Auswahl der Tools	22
5.12 Überprüfung und Aufrechterhaltung	22
6 Sicherungsmodelle	23
6.1 Überblick	23
6.2 Interne Sicherung	23
6.3 Externe Sicherung	23
6.4 Kombinierte Sicherung	23
7 Erstellung von Sicherungsnachweisen	24
7.1 Überblick	24

7.2	Vorbereitung der Validierung	24
7.3	Erstellen von Validierungsnachweisen	24
7.4	Aufrechterhaltung der Validierung	24
7.5	Validierung von Prüfungen.....	25
7.6	Validierung von Untersuchungen.....	25
Anhang A (informativ) Beispiele		26
A.1	Arbeitsanweisung.....	26
A.2	Validierungsplan	27
A.3	Validierungsnachweis	28
A.4	Aussage zur Bestätigung	29
Literaturhinweise.....		30

Europäisches Vorwort

Der Text von ISO/IEC 27041:2015 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 als EN ISO/IEC 27041:2016 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 27041:2015 wurde vom CEN als EN ISO/IEC 27041:2016 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: <http://www.iso.org/iso/foreword.html>.

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

Einleitung

Über diese Internationale Norm

Diese Internationale Norm befasst sich damit, sicherzustellen, dass das verwendete Untersuchungsverfahren für den zu untersuchenden Vorfall und die geforderten Ergebnisse geeignet ist. Sie beschreibt außerdem auf abstrakter Ebene das Konzept des Aufspaltens eines scheinbar komplexen Prozesses in eine Reihe kleinerer, unteilbarer Teilprozesse, was bei der Entwicklung von einfachen aber dennoch soliden Untersuchungsmethoden behilflich sein sollte. Sie sollte von jeder Person berücksichtigt werden, die eine Untersuchung genehmigt, anleitet, lenkt oder durchführt. Sie sollte vor jeder Untersuchung bezüglich der Grundsätze und Prozesse (definiert in ISO/IEC 27043:2015) und der ordnungsgemäßen Vorbereitung und Planung (definiert in ISO/IEC 27035-2¹⁾) angewendet werden, um sicherzustellen, dass die Methoden zur Einbindung in die Untersuchungsprozesse nach ISO/IEC 27037:2012 und ISO/IEC 27042:2015 geeignet sind.

Zusammenhang mit anderen Normen

Diese Internationale Norm ist dafür vorgesehen, andere Normen und Dokumente, die Leitfäden für die Untersuchung von Vorfällen und für die Vorbereitungen von Untersuchungen von Vorfällen 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 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 Untersuchungsprozesses, 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 Interpretation digitaler Beweismittel;
- Verstehen von Grundsätzen und Prozessen bei der Untersuchung von digitalen Beweismitteln;

1) In Veröffentlichung.

- 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 27037:2012

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

- ISO/IEC 27038:2014

Manche Dokumente können Informationen enthalten, die einigen Personengruppen nicht offen zugänglich gemacht werden dürfen. Modifizierte Dokumente können für diese Gruppen 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 27038:2014 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, 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 von Geräten und Datenträgern und nach deren Lebensdauer 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 27042:2015

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

— ISO/IEC 27043:2015

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

Die folgenden ISO/IEC-Projekte behandeln zum Teil ebenfalls die vorstehend festgelegten Themenbereiche und können zur Veröffentlichung von relevanten Normen zu einem bestimmten Zeitpunkt nach der Veröffentlichung dieser Internationalen Norm führen.

— ISO/IEC 27035 (alle Teile)²⁾

Diese dreiteilige Normenreihe ermöglicht Organisationen einen strukturierten und geplanten Ansatz für das Management von Sicherheitsvorfällen. Sie besteht aus:

— ISO/IEC 27035-1³⁾

Dieser Teil enthält die Grundkonzepte und Phasen des Managements von Informationssicherheitsvorfällen. Er vereint diese Konzepte mit den Grundsätzen in einem strukturierten Ansatz zum Erkennen, Berichterstellen, Beurteilen, Reagieren und Nutzen von gewonnenen Erkenntnissen.

— ISO/IEC 27035-2⁴⁾

Dieser Teil enthält die Konzepte für die Planung und Vorbereitung von Reaktionen auf einen Vorfall. Die Konzepte, einschließlich Vorfallmanagementpolitik und -plan, Zusammenstellung eines Teams zur Reaktion auf einen Vorfall (en: incident response team) sowie Sensibilisierungen und Unterweisungen, basieren auf der Planungs- und Vorbereitungsphase des in ISO/IEC 27035-1⁵⁾ dargestellten Modells. Dieser Teil behandelt außerdem die Phase „Gewinnung von Erkenntnissen“ (en: „Lessons Learned“) des Modells.

— ISO/IEC 27035-3⁶⁾

Dieser Teil enthält die Verantwortlichkeiten des Personals und die technischen Maßnahmen in 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 in Zusammenhang mit den erfassten Daten oder Sicherheitsereignissen.

2) In Veröffentlichung.

3) In Veröffentlichung.

4) In Veröffentlichung.

5) In Veröffentlichung.

6) In Veröffentlichung.