

DIN EN ISO/IEC 27042

ICS 35.030

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

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

Gesamtumfang 29 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (EN 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 EN ISO/IEC 27042:2016 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 einige relevante Fachbegriffe existieren nur unpräzise deutsche Übersetzungen. Um Missverständnisse zu vermeiden, wird bei derartigen Begriffen das englische Originalwort in Klammern mit aufgeführt. Die folgenden englischen Begriffe bedürfen darüber hinaus der näheren Erläuterung:

Electronic Discovery, e-discovery

Der Begriff „electronic discovery“ (in unterschiedlichen Schreibweisen) bezieht sich – in seiner ursprünglichen Bedeutung – auf den elektronischen Informationsaustausch im Rahmen von Gerichtsverfahren und ist ein wichtiger Bestandteil anglo-amerikanischer Rechtssysteme. Mittlerweile existiert jedoch eine Vielzahl unterschiedlicher Interpretationen bzw. Abwandlungen dieses Begriffs und entsprechender Übersetzungen (z.B. „elektronische Beweissicherung“, „elektronische Recherche“ etc.). Es wurde daher entschieden, in der deutschen Übersetzung dieser Norm den Begriff „E-Discovery“ beizubehalten.

Investigation

Dieser Begriff wurde grundsätzlich mit „Untersuchung“ übersetzt. Die Bezeichnung „Ermittlung“ ist in den meisten Fällen missverständlich, da eine „Ermittlung“ im Sinne der Strafverfolgung eine Vielzahl weiterer Tätigkeiten umfasst. Die Übersetzung „Ermittlung“ kommt hier nur zur Anwendung, wenn tatsächlich die übergeordneten Ermittlungshandlungen gemeint sind.

Proficiency

Dieser englische Begriff (auf Deutsch in etwa: „Leistungsfähigkeit“ oder „Können“) wird in der Begriffsdefinition unter 3.16 und unter 11.1 mit der Fähigkeit eines Untersuchungsteams erklärt, Ergebnisse zu liefern, die gleichwertig zu den Ergebnissen eines anderen Untersuchungsteams sind, welches dieselben potentiellen digitalen Beweisquellen zur Verfügung hatte. Diese Definition wird als unzureichend erachtet, um den deutschen Begriff der „Leistungsfähigkeit“ hinreichend zu erklären.

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 27037

ISO/IEC 27041:2015 siehe DIN EN ISO/IEC 27041

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO/IEC 27037, Informationstechnik — IT-Sicherheitsverfahren — Leitfaden für die Identifikation, Mitnahme, Sicherung und Erhaltung digitaler Beweismittel (ISO/IEC 27037:2012)

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

— Leerseite —

Deutsche Fassung

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

Information technology —
Security techniques —
Guidelines for the analysis and
interpretation of digital evidence
(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)

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	3
Vorwort	4
Einleitung	5
1 Anwendungsbereich	10
2 Normative Verweisungen	10
3 Begriffe	11
4 Symbole und Abkürzungen	14
5 Untersuchung	15
5.1 Überblick	15
5.2 Kontinuität	15
5.3 Wiederholbarkeit und Reproduzierbarkeit	15
5.4 Strukturierte Vorgehensweise	15
5.5 Unsicherheiten	16
6 Analyse	17
6.1 Überblick	17
6.2 Allgemeine Grundsätze	17
6.3 Einsatz von Tools	18
6.4 Führung von Aufzeichnungen	18
7 Analytische Modelle	18
7.1 Statische Analyse	18
7.2 Live-Analyse	19
7.2.1 Überblick	19
7.2.2 Live-Analyse von Systemen, die nicht gesichert oder kopiert werden können	19
7.2.3 Live-Analyse von Systemen, die gesichert oder kopiert werden können	19
8 Interpretation	20
8.1 Allgemeines	20
8.2 Hervorhebung von Fakten	20
8.3 Die Interpretation beeinflussende Faktoren	20
9 Berichterstattung	21
9.1 Vorbereitung	21
9.2 Empfohlener Berichtsinhalt	21
10 Kompetenz	22
10.1 Überblick	22
10.2 Kompetenznachweis	22
10.3 Kompetenzerfassung	22
11 Leistungsfähigkeit (en: proficiency)	23
11.1 Überblick	23
11.2 Instrumente für den Nachweis der Leistungsfähigkeit	23
Anhang A (informativ) Beispiele für die Spezifikation von Kompetenz und Leistungsfähigkeit	24
A.1 Beispiel für die Spezifikation der Kompetenz	24
A.2 Beispiel für die Spezifikation der Leistungsfähigkeit	24
Literaturhinweise	25

Europäisches Vorwort

Der Text von ISO/IEC 27042:2015 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 27042:2016 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 27042:2015 wurde vom CEN als EN 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 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 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 (www.iso.org/iso/foreword.html).

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 zum Nachvollziehen 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 ab, die mit dem Vorfall in Zusammenhang stehen.

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

1) Wird in Kürze veröffentlicht.