DIN EN ISO/IEC 27042:2016-12 (D)

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

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