E DIN EN ISO/IEC 27037:2016-03 (D/E)

Erscheinungsdatum: 2016-02-26

Informationstechnik - IT-Sicherheitsverfahren - Leitfaden für die Identifikation, Sammlung, Erhebung und Erhaltung der digitalen Beweissicherung (ISO/IEC 27037:2012); Deutsche und Englische Fassung FprEN ISO/IEC 27037:2016

Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence (ISO/IEC 27037:2012); German and English version FprEN ISO/IEC 27037:2016

Inhalt

Seite

Europäisches Vorwort 4

Vorwort 5

Einleitung 6

1 Anwendungsbereich 8

2 Normative Verweisungen 8

3 Begriffe 9

4 Abkürzungen 12

5 Überblick 13
5.1 Kontext für die Sammlung von digitalen Beweismitteln 13
5.2 Grundsätze der digitalen Beweisführung 13
5.3 Anforderungen an die Bearbeitung von digitalen Beweismitteln 14
5.3.1 Allgemeines 14
5.3.2 Auditierbarkeit 14
5.3.3 Wiederholbarkeit 14
5.3.4 Vergleichbarkeit 15
5.3.5 Begründbarkeit 15
5.4 Prozesse zur Bearbeitung von digitalen Beweismitteln 15
5.4.1 Überblick 15
5.4.2 Identifikation 16
5.4.3 Sammlung 16
5.4.4 Erhebung 17
5.4.5 Erhaltung 18

6 Schlüsselkomponenten bei der Identifikation, Sammlung, Erhebung und Erhaltung von digitalen Beweismitteln 18
6.1 Beweismittelkette 18
6.2 Vorkehrungen am Vorfallort 19
6.2.1 Allgemeines 19
6.2.2 Personal 20
6.2.3 Potentielle digitale Beweismittel 20
6.3 Rollen und Verantwortlichkeiten 21
6.4 Kompetenz 21
6.5 Anwendung angemessener Sorgfalt 22
6.6 Dokumentation 22
6.7 Einsatzbesprechung (Briefing) 23
6.7.1 Allgemeines 23
6.7.2 Spezifische Einsatzbesprechung für digitale Beweismittel 23
6.7.3 Personalbezogene Einsatzbesprechung 24
6.7.4 Echtzeit-Vorfälle 24

6.7.5 Sonstige Informationen aus der Besprechung 24
6.8 Priorisierung der Sammlung und Erhebung 25
6.9 Erhaltung von potentiellen digitalen Beweismitteln 26
6.9.1 Überblick 26
6.9.2 Erhalten von potentiellen digitalen Beweismitteln 26
6.9.3 Verpacken von digitalen Geräten und potentiellen digitalen Beweismitteln 26
6.9.4 Transport von potentiellen digitalen Beweismitteln 28

7 Phasen der Identifikation, Sammlung, Erhebung und Erhaltung 28
7.1 Computer, Peripheriegeräte und digitale Speichermedien 28
7.1.1 Identifikation 28
7.1.2 Sammlung 31
7.1.3 Erhebung 35
7.1.4 Erhaltung 40
7.2 Netzwerkgeräte 40
7.2.1 Identifikation 40
7.2.2 Sammlung, Erhebung und Erhaltung 42
7.3 Sammlung, Erhebung und Erhaltung von Daten aus CCTV-Systemen 44

Anhang A (informativ) Beschreibung von Schlüsselqualifikationen und Kompetenzen des DEFR 47

Anhang B (informativ) Mindestanforderungen an die Dokumentation für den Transfer von Beweismitteln 50

Literaturhinweise 51