E DIN EN ISO/IEC 27041:2016-03 (D/E)

Erscheinungsdatum: 2016-02-26

Informationstechnik - IT-Sicherheitsverfahren - Leitfaden zur Sicherung der Tauglichkeit und Eignung von Vorfall-Untersuchungsmethoden (ISO/IEC 27041:2015); Deutsche und Englische Fassung FprEN ISO/IEC 27041:2016

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

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 Entwicklung von Methoden und deren Sicherung 14
5.1 Überblick 14
5.2 Allgemeine Grundsätze 15
5.3 Allgemeines Entwicklungs- und Einsatzmodell 15
5.4 Sicherungsstufen 16
5.5 Erfassung und Analyse von Anforderungen 16
5.5.1 Allgemeine Grundsätze der Anforderungen 16
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 18
5.7 Prozessverwirklichung 19
5.7.1 Überblick 19
5.7.2 Auswahl des Tools — Hinweise für den Einsatz 19
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 20
5.9.1 Allgemeine Grundsätze der Validierung 20
5.9.2 Umfassende Validierung 21
5.9.3 Ausreichende Validierung 21
5.9.4 Vollständig validierte Prozesse 21
5.9.5 Nicht bestandene Validierung 21
5.10 Bestätigung 22
5.11 Einsatz 22
5.11.1 Auswahl der Tools 22
5.12 Überprüfung und Aufrechterhaltung 22

6 Sicherungsmodelle 22

6.1 Überblick 22
6.2 Interne Sicherung 23
6.3 Externe Sicherung 23
6.4 Kombinierte Sicherung 23

7 Erstellung von Sicherungsnachweisen 23
7.1 Überblick 23
7.2 Vorbereitung der Validierung 24
7.3 Erstellen von Validierungsnachweisen 24
7.4 Aufrechterhaltung der Validierung 24
7.5 Validierung von Untersuchungen 25
7.6 Validierung von Ermittlungen 25

Anhang A (informativ) Beispiele 26
A.1 Arbeitsanweisung 26
A.2 Validierungsplan 28
A.3 Validierungsnachweis 30
A.4 Aussage zur Bestätigung 31

Literaturhinweise 32