DIN EN ISO/IEC 27043:2016-12 (D)

Informationstechnik - IT-Sicherheitsverfahren - Grundsätze und Prozesse für die Untersuchung von Vorfällen (ISO/IEC 27043:2015); Deutsche Fassung EN ISO/IEC 27043:2016

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 Digitale Untersuchungen 14
5.1 Allgemeine Grundsätze 14
5.2 Rechtsgrundsätze 14

6 Digitale Untersuchungsprozesse 16
6.1 Allgemeiner Überblick über die Prozesse 16
6.2 Klassen der digitalen Untersuchungsprozesse 16

7 Bereitschaftsprozesse 18
7.1 Überblick über die Bereitschaftsprozesse 18
7.2 Prozess zur Definition des Szenarios 20
7.3 Prozess zur Identifikation von potentiellen Quellen für digitale Beweismittel 21
7.4 Prozess zur Planung der Sammlung, Speicherung und Bearbeitung von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen 22
7.5 Planung der Analyse von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen 22
7.6 Prozess zur Planung der Vorfallerkennung 22
7.7 Prozess zur Definition der Systemarchitektur 23
7.8 Prozess zur Umsetzung der Systemarchitektur 23
7.9 Prozess zur Umsetzung der Sammlung, Speicherung und Bearbeitung von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen 23
7.10 Prozess zur Umsetzung der Analyse von Daten aus dem Zeitraum vor dem Vorfall, die potentielle digitale Beweismittel darstellen 23
7.11 Prozess zur Umsetzung der Vorfallerkennung 24
7.12 Prozess zur Beurteilung der Umsetzung 24
7.13 Prozess zur Umsetzung der Beurteilungsergebnisse 24

8 Initialisierungsprozesse 25
8.1 Überblick über die Initialisierungsprozesse 25
8.2 Prozess zur Vorfallerkennung 26
8.3 Prozess zur ersten Reaktion 26
8.4 Prozess zur Planung 27
8.5 Prozess zur Vorbereitung 27

9 Sicherungsprozesse 27
9.1 Überblick über die Sicherungsprozesse 27
9.2 Prozess zur Identifikation von potentiellen digitalen Beweismitteln 28
9.3 Prozess zur Mitnahme von potentiellen digitalen Beweismitteln 28

9.4 Prozess zur Sicherung von potentiellen digitalen Beweismitteln 29
9.5 Prozess zum Transport von potentiellen digitalen Beweismitteln 29
9.6 Prozess zur Speicherung und Erhaltung von potentiellen digitalen Beweismitteln 29

10 Untersuchungsprozesse 30
10.1 Überblick über die Untersuchungsprozesse 30
10.2 Prozess zur Sicherung von potentiellen digitalen Beweismitteln 31
10.3 Prozess zur Prüfung und Analyse von potentiellen digitalen Beweismitteln 31
10.4 Prozess zur Interpretation von digitalen Beweismitteln 31
10.5 Prozess zur Berichterstattung 31
10.6 Prozess zur Präsentation 32
10.7 Prozess zum Untersuchungsabschluss 32

11 Parallele Prozesse 33
11.1 Überblick über die parallelen Prozesse 33
11.2 Prozess zum Einholen von Berechtigungen 33
11.3 Prozess zur Dokumentation 33
11.4 Prozess zur Steuerung des Informationsflusses 34
11.5 Prozess zur Erhaltung der Obhutskette 34
11.6 Prozess zur Erhaltung der digitalen Beweismittel 34
11.7 Prozess zur Interaktion mit den physischen Untersuchungen 34

12 Musterschema eines digitalen Untersuchungsprozesses 34

Anhang A (informativ) Digitale Untersuchungsprozesse: Gründe für die Harmonisierung 37

Literaturhinweise 44

Bilder

Bild 1 — Anwendbarkeit der Normen auf die Untersuchungsprozessklassen und Untersuchungstätigkeiten 10
Bild 2 — Die verschiedenen Prozessklassen von digitalen Untersuchungen 18
Bild 3 — Gruppen der Bereitschaftsprozesse 19
Bild 4 — Bereitschaftsprozesse 21
Bild 5 — Initialisierungsprozesse 25
Bild 6 — Sicherungsprozesse 28
Bild 7 — Untersuchungsprozesse 30
Bild 8 — Harmonisiertes Schema eines digitalen Untersuchungsprozesses 36

Tabellen

Tabelle 1 — Vergleich von bestehenden Modellen mit dem harmonisierten Modell 39