DIN EN ISO/IEC 30111:2020-07 (D)

Informationstechnik - IT-Sicherheitsverfahren - Prozesse für die Behandlung von Schwachstellen (ISO/IEC 30111:2019); Deutsche Fassung EN ISO/IEC 30111:2020

Inhalt

Seite

Europäisches Vorwort ... 3

Vorwort ... 4

Einleitung ... 5

1 Anwendungsbereich ... 6

2 Normative Verweisungen ... 6

3 Begriffe ... 6

4 Abkürzungen ... 6

5 Beziehungen zu anderen Internationalen Normen ... 6
5.1 ISO/IEC 29147 ... 6
5.2 ISO/IEC 27034 (alle Teile) ... 7
5.3 ISO/IEC 27036-3 ... 7
5.4 ISO/IEC 15408-3 ... 8

6 Richtlinie und organisatorisches Rahmenwerk ... 8
6.1 Allgemeines ... 8
6.2 Führung ... 8
6.2.1 Führung und Verpflichtung ... 8
6.2.2 Richtlinie ... 9
6.2.3 Organisatorische Rollen, Verantwortlichkeiten und Befugnisse ... 9
6.3 Entwicklung der Schwachstellenbehandlungsrichtlinie ... 9
6.4 Entwicklung eines organisatorischen Rahmenwerks ... 10
6.5 CSIRT oder PSIRT des Lieferanten ... 10
6.5.1 Allgemeines ... 10
6.5.2 Auftrag des PSIRT ... 10
6.5.3 Verantwortlichkeiten des PSIRT ... 10
6.5.4 Fähigkeiten von Mitarbeitern ... 12
6.6 Verantwortlichkeiten des Produkt-Geschäftsbereichs ... 12
6.7 Verantwortlichkeiten des Kundendienstes und der Öffentlichkeitsarbeit ... 13
6.8 Rechtsberatung ... 13

7 Prozess für die Behandlung von Schwachstellen ... 13
7.1 Schwachstellenbehandlungsphasen ... 13
7.1.1 Allgemeines ... 13
7.1.2 Vorbereitung ... 14
7.1.3 Eingang ... 14
7.1.4 Verifizierung ... 15
7.1.5 Entwicklung von Abhilfemaßnahmen ... 16
7.1.6 Veröffentlichung ... 17
7.1.7 Nachveröffentlichung ... 17
7.2 Prozessüberwachung ... 17
7.3 Vertraulichkeit der Informationen über die Schwachstelle ... 18

8 Betrachtung der Lieferkette ... 18

Literaturhinweise ... 19