DIN EN ISO/IEC 27040:2017-03 (D)

Informationstechnik - IT-Sicherheitsverfahren - Speichersicherheit (ISO/IEC 27040:2015); Deutsche Fassung EN ISO/IEC 27040:2016

Inhalt

Seite

Europäisches Vorwort ... 4

Vorwort ... 5

Einleitung ... 6

1 Anwendungsbereich ... 7

2 Normative Verweisungen ... 7

3 Begriffe ... 7

4 Symbole und Abkürzungen ... 14

5 Überblick und Konzepte ... 17
5.1 Allgemeines ... 17
5.2 Speicherkonzepte ... 17
5.3 Einführung in die Speichersicherheit ... 18
5.4 Risiken der Speichersicherheit ... 20
5.4.1 Hintergrund ... 20
5.4.2 Bruch der Vertraulichkeit ... 21
5.4.3 Datenbeschädigung und Datenvernichtung ... 22
5.4.4 Vorübergehender oder dauerhafter Verlust des Zugriffs/der Verfügbarkeit ... 23
5.4.5 Versagen des Erfüllens gesetzlicher, behördlicher oder rechtlicher Anforderungen ... 23

6 Unterstützende Maßnahmen ... 24
6.1 Allgemeines ... 24
6.2 Direct Attached Storage (DAS) ... 24
6.3 Speichernetzwerk ... 25
6.3.1 Hintergrund ... 25
6.3.2 Speichernetzwerke (SAN) ... 25
6.3.3 Netzwerkspeicher (NAS) ... 30
6.4 Speichermanagement ... 32
6.4.1 Hintergrund ... 32
6.4.2 Authentifizierung und Autorisierung ... 33
6.4.3 Schutz der Managementschnittstellen ... 34
6.4.4 Sicherheitsprüfung, Kontenführung und Überwachung ... 36
6.4.5 Härten von Systemen ... 38
6.5 Blockbasierter Speicher ... 39
6.5.1 Fibre-Channel-Speicher (FC-Speicher) ... 39
6.5.2 IP-Speicher ... 40
6.6 Dateibasierte Speicherung ... 40
6.6.1 NFS-basierte NAS ... 40
6.6.2 SMB/CIFS-basierte NAS ... 41
6.6.3 Parallele NFS-basierte NAS ... 42
6.7 Objekt-basierter Speicher ... 43
6.7.1 Cloud-Computing-Speicher ... 43
6.7.2 Objektbasiertes Speichergerät (OSD) ... 45
6.7.3 Content Adressable Storage (CAS) ... 46
6.8 Dienste für die Speichersicherheit ... 47
6.8.1 Daten-Löschung ... 47
6.8.2 Vertraulichkeit von Daten ... 50

6.8.3 Daten-Reduzierung 53

7 Leitlinien für Design und Umsetzung der Speichersicherheit 54
7.1 Allgemeines 54
7.2 Designgrundsätze der Speichersicherheit 54
7.2.1 Konzept der gestaffelten Verteidigung 54
7.2.2 Sicherheits-Domains 55
7.2.3 Resilienz des Designs 56
7.2.4 Sichere Initialisierung 56
7.3 Verlässlichkeit, Verfügbarkeit und Resilienz von Daten 57
7.3.1 Verlässlichkeit 57
7.3.2 Verfügbarkeit 58
7.3.3 Backup und Vervielfältigung 58
7.3.4 Disaster Recovery und Business Continuity (DR/BC) 59
7.3.5 Resilienz 60
7.4 Datenaufbewahrung 60
7.4.1 Langfristige Datenaufbewahrung 60
7.4.2 Kurz- bis mittelfristige Datenaufbewahrung 61
7.5 Vertraulichkeit und Integrität von Daten 62
7.6 Virtualisierung 65
7.6.1 Speichervirtualisierung 65
7.6.2 Speicher für virtualisierte Systeme 66
7.7 Überlegungen zu Design und Umsetzung 67
7.7.1 Themen zu Verschlüsselung- und Schlüsselmanagement 67
7.7.2 Ausrichten von Speicher und Richtlinie 68
7.7.3 Compliance 69
7.7.4 Sichere Mandantenfähigkeit 70
7.7.5 Sichere autonome Datenverschiebung 71

Anhang A (normativ) Löschen von Datenträgern 73
A.1 Methoden zum Löschen von Datenträgern 73
A.2 Löschen von verschiedenen Datenträgertypen 74
A.3 Leitlinien zum kryptographischen Löschen von Geräten 87

Anhang B (informativ) Auswahl geeigneter Speichersicherheitsmaßnahmen 91
B.1 Kriterien zur Auswahl von Maßnahmen 91
B.1.1 Überblick 91
B.1.2 Datensensibilitätsklassen 92
B.1.3 Sicherheitsvorrangcodes 93
B.2 Zusammenfassung der Speichersicherheitsmaßnahmen 93
B.2.1 Unterstützende Maßnahmen für die Speichersicherheit 93
B.2.2 Leitfaden für Design und Umsetzung der Speichersicherheit 105

Anhang C (informativ) Wichtige Sicherheitskonzepte 117
C.1 Authentifizierung 117
C.2 Autorisierung und Zugriffskontrolle 118
C.3 Selbstverschlüsselnde Festplatten (SED) 120
C.4 Löschung 121
C.5 Logging 123
C.6 N_Port_ID Virtualization (NPIV) 123
C.7 Fibre-Channel-Sicherheit 124
C.7.1 Überblick 124
C.7.2 DH-CHAP-Authentifizierung 126
C.7.3 ESP_Header 127
C.7.4 CT_Authentication 127
C.7.5 FC-SP-Zoning 128
C.8 OASIS Key Management Interoperability Protocol (KMIP) 128

Literaturhinweise 132