

E DIN EN ISO/IEC 27040:2016-04 (D/E)

Erscheinungsdatum: 2016-03-04

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

Information technology - Security techniques - Storage security (ISO/IEC 27040:2015); German and English version FprEN 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	18
5.1 Allgemeines	18
5.2 Speicherkonzepte	18
5.3 Einführung in die Speichersicherheit	19
5.4 Risiken der Speichersicherheit	21
5.4.1 Hintergrund	21
5.4.2 Bruch der Vertraulichkeit	22
5.4.3 Datenkorruption und Datenvernichtung	23
5.4.4 Vorübergehender oder dauerhafter Verlust des Zugriffs/der Verfügbarkeit	24
5.4.5 Versagen beim Erfüllen gesetzlicher, behördlicher oder rechtlicher Anforderungen	24
6 Unterstützende Maßnahmen	25
6.1 Allgemeines	25
6.2 Direct Attached Storage (DAS)	25
6.3 Speichernetzwerk	26
6.3.1 Hintergrund	26
6.3.2 Speichernetzwerke (SAN)	26
6.3.3 Netzwerkspeicher (NAS)	31
6.4 Speichermanagement	33
6.4.1 Hintergrund	33
6.4.2 Authentifizierung und Autorisierung	34
6.4.3 Schutz der Managementschnittstellen	35
6.4.4 Sicherheitsprüfung, Kontenführung und Überwachung	37
6.4.5 Härten von Systemen	39
6.5 Blockbasierter Speicher	40
6.5.1 Fibre-Channel-Speicher (FC-Speicher)	40
6.5.2 IP-Speicher	41
6.6 Dateibasierte Speicherung	42
6.6.1 NFS-basierte Netzwerkspeicher (NAS)	42
6.6.2 SMB/CIFS-basierte NAS	43
6.6.3 Parallele NFS-basierte NAS	43
6.7 Objekt-basierter Speicher	44
6.7.1 Cloud-Computing-Speicher	44
6.7.2 Objektbasiertes Speichergerät (OSD)	46

6.7.3	Content-Adressable-Storage (CAS)	47
6.8	Dienste für die Speichersicherheit	48
6.8.1	Sicheres Löschen von Daten	48
6.8.2	Vertraulichkeit von Daten	51
6.8.3	Daten-Reduzierung	54
7	Leitlinien für Design und Umsetzung der Speichersicherheit	55
7.1	Allgemeines	55
7.2	Designgrundsätze der Speichersicherheit	55
7.2.1	Konzept der gestaffelten Verteidigung	55
7.2.2	Sicherheits-Domains	56
7.2.3	Belastbarkeit des Designs	57
7.2.4	Sichere Initialisierung	57
7.3	Verlässlichkeit, Verfügbarkeit und Belastbarkeit von Daten	58
7.3.1	Verlässlichkeit	58
7.3.2	Verfügbarkeit	59
7.3.3	Backup und Vervielfältigung	59
7.3.4	Disaster-Recovery und Business Continuity (DR/BC)	60
7.3.5	Belastbarkeit	61
7.4	Datenhaltung	61
7.4.1	Langfristige Datenhaltung	61
7.4.2	Kurz- bis mittelfristige Datenhaltung	62
7.5	Vertraulichkeit und Integrität von Daten	63
7.6	Virtualisierung	66
7.6.1	Speichervirtualisierung	66
7.6.2	Speicher für virtualisierte Systeme	67
7.7	Überlegungen zu Design und Umsetzung	68
7.7.1	Themen zu Verschlüsselung und Schlüsselmanagement	68
7.7.2	Abgleichen von Speicher und Politik	69
7.7.3	Übereinstimmung	70
7.7.4	Sichere Mandantenfähigkeit	71
7.7.5	Sicherer autonomer Datenverkehr	72
Anhang A (normativ)	Sicheres Löschen von Datenträgern	74
A.1	Methoden zum sicheren Löschen von Datenträgern	74
A.2	Sicheres Löschen von verschiedenen Datenträgertypen	75
A.3	Leitlinien für Geräte zum kryptographischen Löschen	89
Anhang B (informativ)	Auswahl geeigneter Speichersicherheitsmaßnahmen	93
B.1	Kriterien zur Auswahl von Maßnahmen	93
B.1.1	Überblick	93
B.1.2	Datensensibilitätsklassen	94
B.1.3	Sicherheitsvorrangcodes	95
B.2	Zusammenfassung der Speichersicherheitsmaßnahmen	95
B.2.1	Unterstützende Maßnahmen für die Speichersicherheit	95
B.2.2	Leitfaden für Design und Umsetzung der Speichersicherheit	109
Anhang C (informativ)	Wichtige Sicherheitskonzepte	122
C.1	Authentifizierung	122
C.2	Autorisierung und Zugriffskontrolle	123
C.3	Selbstverschlüsselnde Festplatten (SED, en: Self-Encrypting Drives)	125
C.4	Sicheres Löschen	126
C.5	Protokollieren	128
C.6	N_Port_ID Virtualization (NPIV)	128
C.7	Fibre-Channel-Sicherheit	129
C.7.1	Überblick	129
C.7.2	DH-CHAP-Authentifizierung	131
C.7.3	ESP_Header	132
C.7.4	CT_Authentication	132
C.7.5	FC-SP-Zoning	133

C.8	OASIS Key Management Interoperability Protocol (KMIP)	133
Literaturhinweise		137