ISO/IEC 27040:2015-01 (E)

Information technology - Security techniques - Storage security

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 1

4 Symbols and abbreviated terms 7

5 Overview and concepts 11
5.1 General 11
5.2 Storage concepts 12
5.3 Introduction to storage security 12
5.4 Storage security risks 14
5.4.1 Background 14
5.4.2 Data breaches 15
5.4.3 Data corruption or destruction 16
5.4.4 Temporary or permanent loss of access/availability 16
5.4.5 Failure to meet statutory, regulatory, or legal requirements 17

6 Supporting controls 17
6.1 General 17
6.2 Direct Attached Storage (DAS) 17
6.3 Storage networking 18
6.3.1 Background 18
6.3.2 Storage Area Networks (SAN) 18
6.3.3 Network Attached Storage (NAS) 23
6.4 Storage management 24
6.4.1 Background 24
6.4.2 Authentication and authorization 26
6.4.3 Secure the management interfaces 27
6.4.4 Security auditing, accounting, and monitoring 28
6.4.5 System hardening 30
6.5 Block-based storage 31
6.5.1 Fibre Channel (FC) storage 31
6.5.2 IP storage 31
6.6 File-based storage 32
6.6.1 NFS-based NAS 32
6.6.2 SMB/CIFS-based NAS 33
6.6.3 Parallel NFS-based NAS 33
6.7 Object-based storage 34
6.7.1 Cloud computing storage 34
6.7.2 Object-based Storage Device (OSD) 35
6.7.3 Content Addressable Storage (CAS) 36
6.8 Storage security services 37
6.8.1 Data sanitization 37
6.8.2 Data confidentiality 40
6.8.3 Data reductions 42

7 Guidelines for the design and implementation of storage security 43
7.1 General 43
7.2 Storage security design principles 43
7.2.1 Defence in depth 43
7.2.2 Security domains 44
7.2.3 Design resilience 45
7.2.4 Secure initialization 45
7.3 Data reliability, availability, and resilience 45
7.3.1 Reliability 45
7.3.2 Availability 46
7.3.3 Backups and replication 46
7.3.4 Disaster Recovery and Business Continuity 47
7.3.5 Resilience 48
7.4 Data retention 48
7.4.1 Long-term retention 48
7.4.2 Short to medium-term retention 49
7.5 Data confidentiality and integrity 50
7.6 Virtualization 52
7.6.1 Storage virtualization 52
7.6.2 Storage for virtualized systems 53
7.7 Design and implementation considerations 54
7.7.1 Encryption and key management issues 54
7.7.2 Align storage and policy 55
7.7.3 Compliance 55
7.7.4 Secure multi-tenancy 56
7.7.5 Secure autonomous data movement 57

Annex A (normative) Media sanitization 60

Annex B (informative) Selecting appropriate storage security controls 75

Annex C (informative) Important security concepts 96

Bibliography 109