TCVN | **TIÊU CHUẨN QUỐC GIA**

DỰ THẢO

TCVN XXXXX:2026

ISO/IEC 27040:2024

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN — KỸ THUẬT AN TOÀN — BẢO MẬT TRONG LƯU TRỮ

Information technology — Security techniques — Storage security

HÀ NỘI – 2026

MỤC LỤC

Lời nói đầu

TCVN XXXXX:2026 hoàn toàn tương đương với ISO/IEC 27040:2024.

TCVN XXXXX:2026 do Ban Cơ yếu Chính phủ biên soạn, Bộ trưởng Bộ Quốc phòng đề nghị, Ủy ban tiêu chuẩn đo lường chất lượng quốc gia thẩm định, Bộ Khoa học và Công nghệ công bố.

TIÊU CHUẨN QUỐC GIA **TCVN XXXXX:2026**

Công nghệ thông tin — Kỹ thuật an toàn — Bảo mật trong lưu trữ

Information technology — Security techniques — Storage security

1 Phạm vi áp dụng

Tiêu chuẩn này cung cấp các yêu cầu kỹ thuật chi tiết và hướng dẫn về cách các tổ chức có thể đạt được mức độ giảm thiểu rủi ro phù hợp thông qua cách tiếp cận nhất quán và đã được kiểm chứng trong lập kế hoạch, thiết kế, lập tài liệu và triển khai bảo mật lưu trữ dữ liệu. Bảo mật lưu trữ áp dụng cho việc bảo vệ dữ liệu cả khi được lưu trữ trong các hệ thống công nghệ thông tin và truyền thông (CNTT-TT) và khi đang truyền qua các liên kết truyền thông liên quan đến lưu trữ. Bảo mật lưu trữ bao gồm an toàn của thiết bị và phương tiện, các hoạt động quản lý liên quan đến thiết bị và phương tiện, ứng dụng và dịch vụ, và kiểm soát hoặc giám sát hoạt động của người dùng trong suốt vòng đời của thiết bị và phương tiện, và sau khi kết thúc sử dụng hoặc hết vòng đời.

Bảo mật lưu trữ liên quan đến bất kỳ ai tham gia vào việc sở hữu, vận hành hoặc sử dụng các thiết bị, phương tiện và mạng lưu trữ dữ liệu. Điều này bao gồm các nhà quản lý cấp cao, người mua sản phẩm và dịch vụ lưu trữ, và các nhà quản lý hoặc người dùng phi kỹ thuật khác, ngoài các nhà quản lý và quản trị viên có trách nhiệm cụ thể về an toàn thông tin hoặc lưu trữ, hoạt động lưu trữ, hoặc chịu trách nhiệm về chương trình an toàn tổng thể và phát triển chính sách an toàn của tổ chức. Tiêu chuẩn này cũng liên quan đến bất kỳ ai tham gia vào việc lập kế hoạch, thiết kế và triển khai các khía cạnh kiến trúc của an toàn mạng lưu trữ.

Tiêu chuẩn này cung cấp cái nhìn tổng quan về các khái niệm bảo mật lưu trữ và các định nghĩa liên quan. Tiêu chuẩn này bao gồm các yêu cầu và hướng dẫn về các mối đe dọa, thiết kế và các khía cạnh kiểm soát liên quan đến các kịch bản lưu trữ điển hình và các lĩnh vực công nghệ lưu trữ. Ngoài ra, tiêu chuẩn này cung cấp các tham chiếu đến các tiêu chuẩn quốc tế và báo cáo kỹ thuật khác đề cập đến các thực tiễn và kỹ thuật hiện có có thể được áp dụng cho bảo mật lưu trữ.

2 Tài liệu viện dẫn

Các tài liệu sau đây được viện dẫn trong văn bản này theo cách mà một phần hoặc toàn bộ nội dung của chúng tạo thành yêu cầu của tiêu chuẩn này. Đối với các tài liệu viện dẫn có ghi năm công bố, chỉ áp dụng phiên bản được viện dẫn. Đối với các tài liệu viện dẫn không ghi năm công bố, áp dụng phiên bản mới nhất của tài liệu đó (bao gồm mọi sửa đổi).

- TCVN ISO/IEC 27000 (ISO/IEC 27000), Công nghệ thông tin - Kỹ thuật an toàn - Hệ thống quản lý an toàn thông tin - Tổng quan và từ vựng

3 Thuật ngữ và định nghĩa

3.1 Tổng quát

Đối với mục đích của tiêu chuẩn này, áp dụng các thuật ngữ và định nghĩa trong TCVN ISO/IEC 27000 (ISO/IEC 27000) và các thuật ngữ và định nghĩa sau đây.

3.2 Thuật ngữ liên quan đến công nghệ lưu trữ

3.2.1

khối (block)

đơn vị mà trong đó dữ liệu được *lưu trữ* (3.2.17) và truy xuất trên *thiết bị lưu trữ* (3.2.14) và *phương tiện lưu trữ* (3.2.16).

3.2.2

nén (compression)

giảm số lượng bit được sử dụng để biểu diễn một mục dữ liệu.

CHÚ THÍCH 1: Đối với lưu trữ (3.2.12), nén không mất dữ liệu (tức là nén bằng kỹ thuật bảo toàn toàn bộ nội dung của dữ liệu gốc và từ đó dữ liệu gốc có thể được khôi phục chính xác) được sử dụng.

3.2.3

dữ liệu tĩnh (data at rest)

dữ liệu được ghi trên phương tiện lưu trữ bền vững, không tạm thời (3.2.11).

3.2.4

dữ liệu động (data in motion)

dữ liệu đang được truyền từ vị trí này sang vị trí khác.

CHÚ THÍCH 1: Các hoạt động truyền này thường liên quan đến các giao diện có thể truy cập được và không bao gồm các hoạt động truyền nội bộ (tức là không bao giờ lộ ra ngoài giao diện, chip hoặc thiết bị).

3.2.5

khử trùng lặp (deduplication)

phương pháp giảm nhu cầu dung lượng *lưu trữ* (3.2.12) bằng cách loại bỏ dữ liệu dư thừa, được thay thế bằng một con trỏ đến bản sao dữ liệu duy nhất.

CHÚ THÍCH 1: Khử trùng lặp đôi khi được coi là một hình thức giảm dữ liệu.

3.2.6

thiết bị (device)

dụng cụ cơ khí, điện hoặc điện tử với một mục đích cụ thể.

[NGUỒN: ISO/IEC 14776-372:2011, 3.1.10]

3.2.7

Fibre Channel

kết nối vào/ra nối tiếp có khả năng hỗ trợ nhiều giao thức, bao gồm truy cập vào *lưu trữ* (3.2.12) của hệ thống mở, truy cập vào lưu trữ máy chủ lớn và truy cập mạng.

CHÚ THÍCH 1: Fibre Channel hỗ trợ các cấu trúc liên kết điểm-điểm, vòng lặp phân xử và chuyển mạch với nhiều loại liên kết cáp đồng và cáp quang chạy ở tốc độ từ 1 gigabit/giây đến hơn 128 gigabit/giây.

3.2.8

Giao thức Fibre Channel (Fibre Channel Protocol)

Giao thức vận chuyển Giao diện Hệ thống Máy tính Nhỏ Nối tiếp (Serial Small Computer System Interface - SCSI) được sử dụng trên các kết nối *Fibre Channel* (3.2.7).

3.2.9

cấp phát dư thừa (over provision)

kỹ thuật được sử dụng bởi các *thiết bị lưu trữ* (3.2.14) trong đó một tập hợp con của *phương tiện lưu trữ* (3.2.16) có sẵn được hiển thị thông qua giao diện.

CHÚ THÍCH 1: Phương tiện lưu trữ được sử dụng nội bộ và độc lập bởi thiết bị lưu trữ để cải thiện hiệu suất, độ bền hoặc độ tin cậy.

3.2.10

lưu trữ gắn mạng (network attached storage - NAS)

thiết bị lưu trữ (3.2.14) hoặc hệ thống kết nối với mạng và cung cấp dịch vụ truy cập tệp cho các hệ thống máy tính.

3.2.11

lưu trữ bền vững (non-volatile storage)

lưu trữ (3.2.12) giữ lại nội dung của nó sau khi nguồn điện bị ngắt.

3.2.12

lưu trữ (storage)

thiết bị (3.2.6), chức năng hoặc dịch vụ hỗ trợ nhập hoặc truy xuất dữ liệu.

3.2.13

mạng khu vực lưu trữ (storage area network - SAN)

mạng có mục đích chính là truyền dữ liệu giữa các hệ thống máy tính với các *thiết bị lưu trữ* (3.2.14) và giữa các thiết bị lưu trữ với nhau.

CHÚ THÍCH 1: Mạng khu vực lưu trữ bao gồm cơ sở hạ tầng truyền thông cung cấp các kết nối vật lý, và một lớp quản lý tổ chức các kết nối, thiết bị lưu trữ và hệ thống máy tính sao cho việc truyền dữ liệu được an toàn và mạnh mẽ.

3.2.14

thiết bị lưu trữ (storage device)

thành phần hoặc tập hợp các thành phần được tạo thành từ một hoặc nhiều *thiết bị* (3.2.6) chứa *phương tiện lưu trữ* (3.2.16), được thiết kế và chế tạo chủ yếu cho mục đích truy cập *lưu trữ bền vững* (3.2.11).

3.2.15

hệ sinh thái lưu trữ (storage ecosystem)

hệ thống các thành phần phụ thuộc lẫn nhau hoạt động cùng nhau để cho phép các dịch vụ và khả năng *lưu trữ* (3.2.12).

CHÚ THÍCH 1: Các thành phần thường bao gồm *thiết bị lưu trữ* (3.2.14), mạng lưu trữ, quản lý lưu trữ và cơ sở hạ tầng công nghệ thông tin và truyền thông (CNTT-TT) khác.

3.2.16

phương tiện lưu trữ (storage medium)

vật liệu mà trên nó dữ liệu số được, hoặc có thể được ghi hoặc truy xuất.

3.2.17

lưu giữ (store)

ghi dữ liệu trên *lưu trữ tạm thời* (3.2.20) hoặc *lưu trữ bền vững* (3.2.11).

3.2.18

dữ liệu mục tiêu (target data)

thông tin là đối tượng của một quy trình nhất định, thường bao gồm hầu hết hoặc toàn bộ thông tin đang *lưu trữ* (3.2.12).

3.2.19

lưu trữ ảo hóa (virtualized storage)

lưu trữ logic (logical storage)

sự trừu tượng hóa của các *thiết bị lưu trữ* (3.2.14) vật lý hoặc *phương tiện lưu trữ* (3.2.16) che giấu các đặc trưng và ranh giới của *lưu trữ* (3.2.12) vật lý.

CHÚ THÍCH 1: Lưu trữ được ảo hóa có thể sử dụng nhiều cấp độ ảo hóa trước khi cung cấp lưu trữ được ảo hóa cho một hệ thống hoặc ứng dụng.

3.2.20

lưu trữ tạm thời (volatile storage)

lưu trữ (3.2.12) không giữ lại nội dung của nó sau khi nguồn điện bị ngắt.

3.3 Thuật ngữ liên quan đến làm sạch (sanitization)

3.3.1

xóa sạch (clear)

làm sạch (3.3.12) bằng cách sử dụng các kỹ thuật logic trên dữ liệu người dùng ở tất cả các vị trí lưu trữ có thể định địa chỉ để bảo vệ chống lại các kỹ thuật khôi phục dữ liệu đơn giản không xâm lấn bằng cách sử dụng cùng một giao diện máy chủ có sẵn cho người dùng.

3.3.2

khử từ (degauss)

làm cho dữ liệu được lưu trữ bằng từ tính không thể đọc được bằng cách áp dụng một từ trường mạnh vào *phương tiện lưu trữ* (3.2.16) với cường độ trường được tổ chức phê duyệt.

3.3.3

tiêu hủy (destruct)

làm sạch (3.3.12) bằng cách sử dụng các kỹ thuật vật lý làm cho việc khôi phục *dữ liệu mục tiêu* (3.2.18) trở nên không khả thi bằng các kỹ thuật phòng thí nghiệm hiện đại và dẫn đến việc không thể sử dụng *phương tiện lưu trữ* (3.2.16) để *lưu trữ* (3.2.12) sau đó.

CHÚ THÍCH 1: *Phân rã* (3.3.5), *thiêu hủy* (3.3.6), *làm nóng chảy* (3.3.7), *nghiền thành bột* (3.3.9), và *cắt nhỏ* (3.3.13) là các hình thức tiêu hủy của *làm sạch phương tiện* (3.3.16).

CHÚ THÍCH 2: Nếu không thể tháo phương tiện lưu trữ, thì *thiết bị lưu trữ* (3.2.14) có thể bị áp dụng kỹ thuật tiêu hủy; một thiết bị lưu trữ có thể chứa nhiều phương tiện lưu trữ.

3.3.4

sự tiêu hủy (destruction)

kết quả của các hành động *tiêu hủy* (3.3.3) được thực hiện để đảm bảo rằng *phương tiện lưu trữ* (3.2.16) không thể được tái sử dụng như dự định ban đầu và dữ liệu người dùng hầu như không thể hoặc quá tốn kém để khôi phục.

3.3.5

phân rã (disintegrate)

tiêu hủy (3.3.3) bằng cách tách *phương tiện lưu trữ* (3.2.16) thành các bộ phận cấu thành của nó.

3.3.6

thiêu hủy (incinerate)

tiêu hủy (3.3.3) bằng cách đốt cháy hoàn toàn *phương tiện lưu trữ* (3.2.16).

3.3.7

làm nóng chảy (melt)

tiêu hủy (3.3.3) bằng cách thay đổi *phương tiện lưu trữ* (3.2.16) từ trạng thái rắn sang trạng thái lỏng thường bằng cách tác dụng nhiệt.

3.3.8

xóa bằng mật mã (cryptographic erase)

phương pháp làm sạch trong đó khóa mã hóa cho *dữ liệu mục tiêu* (3.2.18) được mã hóa bị *làm sạch* (3.3.12), làm cho việc khôi phục dữ liệu mục tiêu đã giải mã trở nên không khả thi.

3.3.9

nghiền thành bột (pulverize)

tiêu hủy (3.3.3) bằng cách nghiền *phương tiện lưu trữ* (3.2.16) thành bột hoặc các hạt nhỏ thích hợp.

3.3.10

thanh lọc (purge)

làm sạch (3.3.12) bằng cách sử dụng các kỹ thuật vật lý hoặc logic làm cho việc khôi phục *dữ liệu mục tiêu* (3.2.18) trở nên không khả thi bằng các kỹ thuật phòng thí nghiệm hiện đại, nhưng vẫn bảo toàn *phương tiện lưu trữ* (3.2.16) và *thiết bị lưu trữ* (3.2.14) ở trạng thái có thể tái sử dụng.

3.3.11

sự làm sạch (sanitization)

quy trình hoặc phương pháp để *làm sạch* (3.3.12).

3.3.12

làm sạch (sanitize)

làm cho việc truy cập vào *dữ liệu mục tiêu* (3.2.18) trên *lưu trữ* (3.2.12) trở nên không khả thi đối với một mức độ nỗ lực nhất định.

3.3.13

cắt nhỏ (shred)

tiêu hủy (3.3.3) bằng cách cắt hoặc xé *phương tiện lưu trữ* (3.2.16) thành các hạt nhỏ.

3.3.14

làm sạch lưu trữ (storage sanitization)

làm sạch lưu trữ logic (3.3.15) hoặc làm sạch phương tiện (3.3.16).

3.3.15

làm sạch lưu trữ logic (logical storage sanitization)

làm sạch lưu trữ ảo (virtual storage sanitization)

sự làm sạch (3.3.11) của lưu trữ ảo hóa (3.2.19).

CHÚ THÍCH 1: Xóa sạch (3.3.1) và thanh lọc (3.3.10) là các hành động có thể được thực hiện để làm sạch (3.3.12) lưu trữ ảo hóa.

CHÚ THÍCH 2: Làm sạch lưu trữ logic là một tập hợp con của làm sạch lưu trữ (3.3.14).

3.3.16

làm sạch phương tiện lưu trữ (media sanitization)

sự làm sạch (3.3.11) của phương tiện lưu trữ (3.2.16).

CHÚ THÍCH 1: Xóa sạch (3.3.1), thanh lọc (3.3.10), và tiêu hủy (3.3.3) là các hành động có thể được thực hiện để làm sạch (3.3.12) phương tiện lưu trữ (3.2.16).

CHÚ THÍCH 2: Làm sạch phương tiện là một tập hợp con của *làm sạch lưu trữ* (3.3.14).

3.4 Thuật ngữ liên quan đến tính sẵn sàng

3.4.1

khả năng phục hồi (resilience)

khả năng dự đoán và thích ứng, chống lại hoặc nhanh chóng phục hồi sau một sự kiện có khả năng gây gián đoạn, dù là tự nhiên hay do con người gây ra.

[NGUỒN: ISO 15392:2019, 3.21]

3.5 Thuật ngữ liên quan đến an toàn và mật mã

3.5.1

chu kỳ mật mã (cryptoperiod)

khoảng thời gian xác định trong đó một khóa mật mã cụ thể được phép sử dụng hoặc trong lúc đó các khóa mật mã trong một hệ thống nhất định có thể vẫn còn hiệu lực.

[NGUỒN: ISO 16609:2022, 3.6]

3.5.2

vi phạm dữ liệu (data breach)

sự xâm phạm an toàn dẫn đến việc *tiêu hủy* (3.3.4), mất mát, thay đổi, tiết lộ trái phép hoặc truy cập vào dữ liệu được bảo vệ đã truyền, *lưu trữ* (3.2.17), hoặc xử lý theo cách khác một cách vô ý hoặc bất hợp pháp.

3.5.3

tính toàn vẹn dữ liệu (data integrity)

thuộc tính mà dữ liệu chưa bị thay đổi hoặc tiêu hủy một cách trái phép.

[NGUỒN: ISO 7498-2:1989, 3.3.21]

3.5.4

xác thực đa yếu tố (multi-factor authentication)

xác thực bằng cách sử dụng hai hoặc nhiều yếu tố sau:

- yếu tố kiến thức, điều mà một cá nhân biết;
- yếu tố sở hữu, thứ mà một cá nhân có;
- yếu tố sinh trắc học, điều mà một cá nhân là hoặc có thể làm.

[NGUỒN: ISO 19092:2008, 4.42]

3.5.5

phần mềm độc hại (malware)

phần mềm có hại được thiết kế đặc biệt để gây hại hoặc làm gián đoạn một hệ thống, tấn công tính bí mật, tính toàn vẹn và/hoặc tính sẵn sàng.

CHÚ THÍCH 1: Virus và Trojan horse là ví dụ về phần mềm độc hại.

[NGUỒN: TCVN 9801-1:2015 (ISO/IEC 27033-1:2015), 3.22]

3.5.6

điểm mã hóa (point of encryption)

vị trí trong cơ sở hạ tầng công nghệ thông tin và truyền thông nơi dữ liệu được mã hóa trên đường đến *lưu trữ* (3.2.12) và ngược lại, nơi dữ liệu được giải mã khi truy cập từ lưu trữ.

CHÚ THÍCH 1: Điểm mã hóa chỉ áp dụng cho *dữ liệu tĩnh* (3.2.3).

3.5.7

độ mạnh bảo mật (security strength)

con số liên quan đến khối lượng công việc cần thiết để phá vỡ một thuật toán hoặc hệ thống mật mã.

3.5.8

bảo mật lưu trữ (storage security)

việc áp dụng các kiểm soát vật lý, kỹ thuật và hành chính để bảo vệ các hệ thống và cơ sở hạ tầng lưu trữ cũng như dữ liệu *được lưu trữ* (3.2.17) bên trong chúng.

CHÚ THÍCH 1: Bảo mật lưu trữ tập trung vào việc bảo vệ dữ liệu (và cơ sở hạ tầng lưu trữ của nó) chống lại việc tiết lộ, sửa đổi hoặc tiêu hủy trái phép đồng thời đảm bảo tính sẵn sàng của nó cho người dùng được ủy quyền.

CHÚ THÍCH 2: Các kiểm soát này về mặt bản chất có thể mang tính phòng ngừa, phát hiện, khắc phục, răn đe, phục hồi hoặc bù trừ.

3.5.9

xác thực mạnh (strong authentication)

xác thực bằng các thông tin xác thực đa yếu tố có nguồn gốc mật mã.

[NGUỒN: ISO 22600-1:2014, 3.23]

3.6 Thuật ngữ liên quan đến lưu trữ và kho lưu trữ

3.6.1

kho lưu trữ (archive)

<tổ chức> tổ chức hoặc một phần của tổ chức chịu trách nhiệm lựa chọn, thu thập, *bảo quản* (3.6.5), và có tính sẵn sàng để sử dụng một hoặc nhiều *kho lưu trữ* (3.6.2).

[NGUỒN: ISO 5127:2017, 3.2.3.01, sửa đổi — CHÚ THÍCH 1 đến 4 đã bị bỏ qua; thuật ngữ đã được đổi thành số ít từ số nhiều "archives"; phạm vi <tổ chức> đã được thêm vào.]

3.6.2

kho lưu trữ (archive)

<tài liệu> tài liệu, vật phẩm, *hồ sơ* (3.6.6) hoặc tư liệu được tạo ra hoặc nhận bởi một cá nhân, gia đình hoặc tổ chức, công cộng hoặc tư nhân, trong quá trình hoạt động của chúng và được bảo quản vì giá trị lâu dài chứa trong chúng hoặc làm bằng chứng về chức năng và trách nhiệm của người tạo ra chúng, đặc biệt là những tài liệu được quản lý theo các nguyên tắc về xuất xứ, thứ tự ban đầu và quản lý tập thể.

[NGUỒN: ISO 5127:2017, 3.6.1.03, sửa đổi — đã thêm "tài liệu, vật phẩm, hồ sơ hoặc tư liệu" vào đầu định nghĩa; CHÚ THÍCH 1 đã bị bỏ qua; thuật ngữ đã được đổi thành số ít từ số nhiều "archives"; phạm vi <tài liệu> đã được thêm vào.]

3.6.3

định đoạt (disposition)

phạm vi các quy trình hồ sơ liên quan đến việc thực hiện các quyết định *lưu giữ* (3.6.9) các hồ sơ, *tiêu hủy* (3.6.7) hồ sơ hoặc chuyển giao được ghi lại trong các văn bản quy định thẩm quyền định đoạt hoặc các công cụ khác.

[NGUỒN: ISO 30300:2020, 3.4.8, sửa đổi — "sự tiêu hủy" đã được đổi thành "sự tiêu hủy hồ sơ".]

3.6.4

bằng chứng (evidence)

thông tin có thể được sử dụng riêng lẻ hoặc kết hợp với thông tin khác, để thiết lập chứng cứ về một sự kiện hoặc hành động.

[NGUỒN: ISO 30300:2020, 3.2.6, sửa đổi — CHÚ THÍCH 1 đã bị bỏ qua; trong bản gốc tiếng Anh, từ "could" đã được đổi thành "can".]

3.6.5

sự bảo quản (preservation)

các biện pháp được thực hiện để duy trì *khả năng sử dụng* (3.6.10), tính xác thực, độ tin cậy và tính toàn vẹn của *hồ sơ* (3.6.6) theo thời gian.

CHÚ THÍCH 1: Các biện pháp bao gồm các nguyên tắc, các chính sách, quy tắc, chiến lược, quy trình và hoạt động.

[NGUỒN: ISO 30300:2020, 3.4.11]

3.6.6

hồ sơ (record)

thông tin được tạo ra hoặc nhận và duy trì làm *bằng chứng* (3.6.4) và tài sản của một tổ chức, nhằm theo đuổi các nghĩa vụ pháp lý hoặc trong quá trình tiến hành công việc.

CHÚ THÍCH 1: Hồ sơ thường được sử dụng ở dạng số nhiều.

CHÚ THÍCH 2: Trong việc triển khai tiêu chuẩn hệ thống quản lý (MSS), các hồ sơ được tạo ra để vận hành và điều hành hệ thống quản lý cũng như để ghi lại quá trình thực hiện hệ thống đó được gọi là thông tin được ghi chép.

[NGUỒN: ISO 30300:2020, 3.2.10]

3.6.7

sự tiêu hủy hồ sơ (records destruction)

loại bỏ hoặc xóa một *hồ sơ* (3.6.6), vượt quá mọi khả năng tái tạo có thể.

[NGUỒN: ISO 30300:2020, 3.4.7, sửa đổi — đổi thuật ngữ "sự tiêu hủy" thành "sự tiêu hủy hồ sơ".]

3.6.8

yêu cầu hồ sơ (records requirement)

nhu cầu về *bằng chứng* (3.6.4) của một chức năng, hoạt động hoặc giao dịch công việc và các quy trình xử lý hồ sơ bao gồm cách thức, và trong bao lâu *hồ sơ* (3.6.6) cần được lưu giữ.

[NGUỒN: ISO 30300:2020, 3.3.2]

3.6.9

sự lưu giữ (retention)

giữ một *hồ sơ* (3.6.6) theo *yêu cầu hồ sơ* (3.6.8).

[NGUỒN: ISO 30300:2020, 3.4.14]

3.6.10

khả năng sử dụng (usability)

thuộc tính có thể được định vị, truy xuất, đưa ra và hiểu.

CHÚ THÍCH 1: Khả năng sử dụng cũng có thể đề cập đến mức độ mà một hệ thống, sản phẩm hoặc dịch vụ có thể được sử dụng bởi những người dùng cụ thể để đạt được các mục tiêu cụ thể với hiệu quả, hiệu suất và sự hài lòng trong một bối cảnh sử dụng cụ thể.

[NGUỒN: ISO 30300:2020, 3.2.12]

3.7 Các thuật ngữ khác

3.7.1

trong băng (in-band)

truyền thông hoặc truyền tải xảy ra trong một phương thức hay kênh liên lạc đã được thiết lập từ trước.

CHÚ THÍCH 1: Các truyền thông hoặc truyền tải thường có dạng một giao thức riêng biệt, chẳng hạn như giao thức quản lý trên cùng một phương tiện với giao thức dữ liệu chính.

3.7.2

siêu dữ liệu (metadata)

dữ liệu xác định và mô tả dữ liệu khác.

[NGUỒN: ISO/IEC 11179-1:2023, 3.2.26]

3.7.3

đa bên thuê (multi-tenancy)

việc phân bổ tài nguyên vật lý hoặc ảo theo cách mà nhiều bên thuê - cùng với các hoạt động tính toán và dữ liệu của họ - được cách ly với nhau và các bên không thể truy cập vào dữ liệu/tính toán của nhau.

[NGUỒN: ISO/IEC 22123-1:2023, 3.4.3]

3.7.4

ngoài băng (out-of-band)

truyền thông hoặc truyền tải xảy ra bên ngoài một phương thức hay kênh liên lạc đã được thiết lập từ trước.

3.7.5

đa bên thuê an toàn (secure multi-tenancy)

kiểu đa bên thuê (3.7.3) sử dụng các kiểm soát an toàn để bảo vệ một cách rõ ràng chống lại *vi phạm dữ liệu* (3.5.2) và cung cấp phê chuẩn của các kiểm soát này để quản trị đúng đắn.

CHÚ THÍCH 1: Đa bên thuê an toàn tồn tại khi hồ sơ rủi ro của từng bên thuê riêng lẻ không lớn hơn so với môi trường đơn bên thuê chuyên dụng.

CHÚ THÍCH 2: Trong các môi trường rất an toàn, ngay cả danh tính của bên thuê cũng được giữ bí mật.

4 Ký hiệu và thuật ngữ viết tắt

ACL	access control list	Danh sách kiểm soát truy cập
AES	Advanced Encryption Standard	Tiêu chuẩn Mã hóa Tiên tiến
API	application programming interface	Giao diện lập trình ứng dụng
BCM	business continuity management	Quản lý tính liên tục kinh doanh
BMC	baseboard management controller	Bộ điều khiển quản lý bo mạch chủ
CCM	counter with cipher block chaining message authentication code	Chế độ bộ đếm với mã xác thực thông điệp chuỗi khối mật mã
CDMI	Cloud Data Management Interface	Giao diện Quản lý Dữ liệu Đám mây

CHAP	Challenge Handshake Authentication Protocol	Giao thức Xác thực Bắt tay Thách thức
CLI	command line interface	Giao diện dòng lệnh
CNA	converged network adaptor	Bộ điều hợp mạng hội tụ
DAS	direct attached storage	Lưu trữ gắn trực tiếp
DDoS	distributed denial of service	Từ chối dịch vụ phân tán
DH-CHAP	Diffie Hellman - Challenge Handshake Authentication Protocol	Giao thức Xác thực Bắt tay Thách thức Diffie Hellman
DNS	domain name system	Hệ thống tên miền
DoS	denial of service	Từ chối dịch vụ
DRAM	dynamic random access memory	Bộ nhớ truy cập ngẫu nhiên động
ESP	encapsulating security payload	Tải trọng an toàn đóng gói
FC	fibre channel	Fibre Channel
FC-SP	fibre channel - security protocol	Giao thức an toàn Fibre Channel
FCIP	fibre channel over TCP/IP	Fibre Channel qua TCP/IP
FCP	fibre channel protocol	Giao thức Fibre Channel
GCM	Galois/Counter Mode	Chế độ Galois/Bộ đếm
HBA	host bus adapter	Bộ điều hợp bus máy chủ
HDD	hard disk drive	Ổ đĩa cứng
HMAC	hash-based message authentication code	Mã xác thực thông điệp dựa trên hàm băm
HTTPS	hypertext transfer protocol secure	Giao thức truyền siêu văn bản an toàn
IB	InfiniBand™	InfiniBand™
ICT	information and communications technology	Công nghệ thông tin và truyền thông (CNTT-TT)
ID	identifier	Định danh
IEEE	Institute of Electrical and Electronics Engineers	Viện Kỹ sư Điện và Điện tử
IETF	Internet Engineering Task Force	Lực lượng Đặc nhiệm Kỹ thuật Internet
IKE	Internet Key Exchange	Trao đổi Khóa Internet
IP	Internet Protocol	Giao thức Internet
IPMI	Intelligent Platform Management Interface	Giao diện Quản lý Nền tảng Thông minh
IPsec	Internet Protocol Security	An toàn Giao thức Internet
IRBC	ICT readiness for business continuity	Sự sẵn sàng CNTT-TT cho tính liên tục kinh doanh
iSCSI	Internet Small Computer Systems Interface	Giao diện Hệ thống Máy tính Nhỏ Internet
ISMS	information security management system	Hệ thống quản lý an toàn thông tin
iSNS	Internet Storage Name Service	Dịch vụ Tên Lưu trữ Internet

KMIP	key management interoperability protocol	Giao thức tương tác quản lý khóa
LAN	local area network	Mạng cục bộ
LUN	logical unit number	Số đơn vị logic
MTBF	mean time between failure	Thời gian trung bình giữa các lần hỏng hóc
MTTF	mean time to failure	Thời gian trung bình đến khi hỏng hóc
MTTR	mean time to repair	Thời gian trung bình để sửa chữa
NAS	network attached storage	Lưu trữ gắn mạng
NFS	network file system	Hệ thống tệp mạng
NTP	network time protocol	Giao thức thời gian mạng
NVM	non-volatile memory	Bộ nhớ bền vững
NVMe®	NVM Express®	NVM Express®
NVMe-oF™	NVM Express® over Fabric	NVM Express® qua Fabric
NVMe®/FC	NVMe® over Fibre Channel	NVMe® qua Fibre Channel
NVMe®/RDMA	NVMe® over RDMA	NVMe® qua RDMA
NVMe®/TCP	NVMe® over TCP	NVMe® qua TCP
OASIS	Organization for the Advancement of Structured Information Standards	Tổ chức vì sự Tiến bộ của Tiêu chuẩn Thông tin Cấu trúc
PCIe®	PCI Express®	PCI Express®
PII	personally identifiable information	Thông tin nhận dạng cá nhân
RADIUS	remote authentication dial in user service	Dịch vụ người dùng quay số xác thực từ xa
RAID	redundant array of independent disks	Mảng dự phòng gồm các đĩa độc lập
RDMA	remote direct memory access	Truy cập bộ nhớ trực tiếp từ xa
REST	representational state transfer	Chuyển trạng thái đại diện
RMCP	Remote Management Control Protocol	Giao thức Kiểm soát Quản lý Từ xa
SAN	storage area network	Mạng khu vực lưu trữ
SCSI	Small Computer System Interface	Giao diện Hệ thống Máy tính Nhỏ
SHA	Secure Hash Algorithm	Thuật toán Băm An toàn
SLP	Service Locator Protocol	Giao thức Định vị Dịch vụ
SMB	Server Message Block	Khối thông điệp máy chủ
SNMP	Simple Network Management Protocol	Giao thức Quản lý Mạng Đơn giản
SSD	solid state drive	Ổ đĩa thể rắn
SSH	Secure Shell	Secure Shell
TCP	Transmission Control Protocol	Giao thức Điều khiển Truyền tải
TLS	Transport Layer Security	An toàn Lớp Vận chuyển
UDP	User Datagram Protocol	Giao thức Gói dữ liệu Người dùng

VLAN	virtual local area network	Mạng cục bộ ảo
VM	virtual machine	Máy ảo
VPN	virtual private network	Mạng riêng ảo
WORM	write once read many	Ghi một lần đọc nhiều lần
WWN	worldwide name	Tên toàn cầu
XEX	Xor-Encrypt-Xor	Xor-Encrypt-Xor
XTS	XEX-based Tweaked-codebook mode with ciphertext Stealing	Chế độ sổ mã hiệu chỉnh dựa trên XEX với Đánh cắp bản mã

5 Cấu trúc của tiêu chuẩn này

5.1 Tổng quát

Cấu trúc cơ bản của tiêu chuẩn này bắt đầu bằng phần giới thiệu về bảo mật lưu trữ trong Điều 6, tiếp theo là các điều khoản riêng biệt đề cập đến các kiểm soát tổ chức (Điều 7), kiểm soát con người (Điều 8), kiểm soát vật lý (Điều 9), và kiểm soát công nghệ (Điều 10) liên quan đến các hệ thống và hệ sinh thái lưu trữ.

5.2 Kiểm soát

Các kiểm soát của TCVN ISO/IEC 27001 (ISO/IEC 27001) và ISO/IEC 27002 nói chung áp dụng cho các hệ sinh thái lưu trữ và các tổ chức mua sắm, quản lý và vận hành chúng. Tiêu chuẩn này cung cấp hướng dẫn và yêu cầu bổ sung mở rộng dựa trên các tiêu chuẩn này. Các yêu cầu được quy định trong tiêu chuẩn này đại diện cho một bộ kiểm soát bảo mật lưu trữ cơ bản. Để hỗ trợ việc xác định các kiểm soát cơ bản và hướng dẫn chính này, các tiêu đề phụ được sử dụng trong văn bản. Các tiêu đề phụ này bao gồm một nhãn kiểm soát với mô tả. Các nhãn kiểm soát có dạng xx-yyyy-cnn trong đó:

- xx là "OC" cho kiểm soát tổ chức, "SC" cho kiểm soát con người, "PC" cho kiểm soát vật lý, hoặc "TC" cho kiểm soát công nghệ;

- yyyy liên quan đến chủ đề;

- c là "R" cho yêu cầu hoặc "G" cho hướng dẫn;

- nn là số thứ tự khi có nhiều kiểm soát tồn tại cho một chủ đề duy nhất; các yêu cầu và hướng dẫn được đánh số độc lập với nhau.

Khi một điều khoản hoặc tiểu mục có nhiều tiêu đề phụ, các tiêu đề này được trình bày dưới dạng danh sách có thứ tự để dễ tham chiếu. Tóm tắt các kiểm soát được liệt kê trong Phụ lục A.

Mặc dù tiêu chuẩn này được viết từ góc độ của người dùng công nghệ lưu trữ, cần lưu ý rằng nhiều kiểm soát phụ thuộc vào việc các nhà cung cấp triển khai sẵn một số tính năng hoặc khả năng an toàn nhất định làm điều kiện tiên quyết. Sự có hay không có các tính năng và khả năng này có thể là yếu tố quan trọng cần xem xét khi lựa chọn sản phẩm.

6 Tổng quan và các khái niệm

6.1 Tổng quát

Lưu trữ dữ liệu hoặc lưu trữ thông tin, thường được gọi tắt là lưu trữ, đề cập đến các thành phần hệ thống, các thiết bị lưu trữ và các phương tiện lưu trữ dùng để duy trì dữ liệu số ở dạng bền vững (tức là

không tạm thời). Mặc dù cả hai dạng lưu trữ tạm thời và bền vững đều tồn tại, tiêu chuẩn này chủ yếu quan tâm đến lưu trữ bền vững. Lưu trữ là chức năng cốt lõi và thành phần nền tảng của các hệ thống CNTT-TT.

Để bảo đảm an toàn cơ sở hạ tầng lưu trữ, cần có sự hiểu biết rõ ràng về các công nghệ và khái niệm lưu trữ. Bên cạnh đó, các loại kiểm soát an toàn và sự hiểu biết về cách chúng tác động và tương tác với các công nghệ lưu trữ cũng rất quan trọng. Cuối cùng, các mối đe dọa đối với cơ sở hạ tầng này và các rủi ro chính phát sinh từ những mối đe dọa đó được tính đến trong bất kỳ nỗ lực nào nhằm giảm thiểu rủi ro cho cơ sở hạ tầng lưu trữ hoặc các hệ thống lưu trữ riêng lẻ.

6.2 Các khái niệm lưu trữ

Ở dạng cơ bản nhất, lưu trữ có thể là ổ đĩa cứng (HDD), ổ đĩa thể rắn (SSD) hoặc ổ băng từ gắn vào hệ thống CNTT-TT để lưu trữ dữ liệu. Cách tiếp cận này, thường được gọi là lưu trữ gắn trực tiếp (DAS), vẫn được sử dụng phổ biến trong các trung tâm dữ liệu doanh nghiệp cũng như môi trường văn phòng nhỏ/gia đình. Với sự tích hợp của công nghệ mạng, các hệ thống và hệ sinh thái lưu trữ có thể trở thành các công nghệ rất tinh vi, cung cấp giải pháp để quản lý, kết nối, bảo đảm an toàn, chia sẻ và tối ưu hóa việc lưu trữ dữ liệu. Các giải pháp này ngày càng khả thi và hiệu quả về chi phí hơn khi công nghệ lưu trữ phát triển từ DAS nội bộ và bên ngoài không thông minh sang lưu trữ nối mạng thông minh. Việc sử dụng mạng trong các giải pháp này làm tăng bề mặt tấn công và đòi hỏi phải chú ý nhiều hơn để giảm thiểu các rủi ro liên quan.

Các giải pháp lưu trữ hiện đại bao gồm một số hoặc tất cả các yếu tố sau:

- Thiết bị và phương tiện lưu trữ, bao gồm các vật liệu từ tính, thể rắn, v.v., trên đó dữ liệu có thể được ghi hoặc truy cập;

- Lưu trữ dựa trên khối, là dạng cơ bản và nền tảng nhất của lưu trữ dữ liệu số bền vững được sắp xếp theo một chuỗi các khối (mỗi khối bao gồm một chuỗi các byte hoặc bit) với các offset để biểu thị vị trí của các khối dữ liệu riêng lẻ;

- Lưu trữ dựa trên tệp, là lưu trữ dữ liệu mà tổ chức dữ liệu thành các tệp và thư mục trên một hệ thống tệp, đồng thời trừu tượng hóa phần cứng cơ bản để truy cập người dùng truy cập cục bộ hoặc qua mạng, thường là lưu trữ gắn mạng (NAS). NAS có thể cho phép nhiều hệ thống máy tính có quyền truy cập bình đẳng vào nội dung được lưu trữ bất kể hệ điều hành gốc của chúng;

- Giao diện lưu trữ, bao gồm các giao diện kết nối lưu trữ trực tiếp cụ thể cũng như các giao diện mạng lưu trữ;

- Lưu trữ đối tượng, là phương pháp lưu trữ và sau đó truy xuất các tập dữ liệu dưới dạng những tập hợp của các mục hoặc đối tượng đơn lẻ, không thể phân chia có thể định danh duy nhất. Phương pháp này áp dụng cho bất kỳ dạng dữ liệu nào có thể được đóng gói và quản lý như một đối tượng;

- Lưu trữ điện toán đám mây, có thể là một phần của lưu trữ dữ liệu như một dịch vụ (DSaaS), như được định nghĩa trong TCVN 13809-1 (ISO/IEC 22123-1) và được mô tả trong TCVN 13809-2 (ISO/IEC 22123-2). Lưu trữ đám mây có thể bao gồm việc lưu trữ cơ bản nhất các tệp hoặc khối dữ liệu nhị phân thô, cơ sở dữ liệu quan hệ và các nền tảng dữ liệu lớn tiên tiến cũng như cung cấp sao lưu tự động, khôi phục sau thảm họa, dự phòng địa lý, chuyển đổi dự phòng nâng cao và các tính năng phức tạp khác;

- Hệ thống bảo vệ dữ liệu tạo ra một hoặc nhiều bản sao dữ liệu sản xuất để cho phép khôi phục hệ thống hoặc dữ liệu của nó sau một biến cố thảm khốc;

- Bộ nhớ liên tục (bền vững), là bộ nhớ bền vững có mật độ lớn hơn hoặc bằng bộ nhớ truy cập ngẫu nhiên động (DRAM) nằm trên bus bộ nhớ và có quyền truy cập dữ liệu giống như DRAM với tốc độ và độ trễ gần như DRAM và tính bền vững của bộ nhớ flash NAND.

Lưu trữ đã trở thành một lớp hạ tầng nổi bật và độc lập trong CNTT-TT trong các môi trường máy tính cấp doanh nghiệp và tầm trung. Các yêu cầu đối với các môi trường này thường vượt xa khả năng lưu trữ dữ liệu đơn thuần. Một số ứng dụng và chức năng thúc đẩy sự ra đời của các công nghệ lưu trữ mới bao gồm:

- chia sẻ tài nguyên lưu trữ khổng lồ (được đo bằng petabyte, exabyte và yottabyte) giữa nhiều hệ thống thông qua các mạng;

- nhu cầu về tốc độ cao hơn (độ trễ thấp hơn);

- tăng dung lượng lưu trữ;

- mở rộng quyền truy cập máy khách lưu trữ (ví dụ: thiết bị di động và internet vạn vật);

- hỗ trợ các kiến trúc CNTT-TT phân tán (ví dụ: điện toán biên);

- hỗ trợ các môi trường ảo hóa;

- các hệ thống bảo vệ dữ liệu sao lưu dữ liệu mà không cần sử dụng mạng cục bộ (LAN);

- điều khiển từ xa, chống chịu thảm họa, nhân bản trực tuyến với dữ liệu tối quan trọng;

- Tổ chức thành cụm các ứng dụng có khả năng chịu lỗi và các hệ thống liên quan quanh một bản sao dữ liệu duy nhất;

- lưu giữ dài hạn thông tin kinh doanh nhạy cảm hoặc có giá trị cao;

- cơ sở dữ liệu và hệ thống tệp phân tán;

- hỗ trợ tuân thủ các yêu cầu pháp lý và quy định;

- hỗ trợ các kho dữ liệu tập trung để phục hồi nhanh chóng (ví dụ: sao lưu) và lưu trữ;

- khả năng phục hồi trước các cuộc tấn công mạng.

6.3 Giới thiệu về bảo mật lưu trữ

Bảo mật lưu trữ tập trung vào việc giảm thiểu rủi ro liên quan đến các hệ thống và cơ sở hạ tầng lưu trữ, như đã nêu trong 6.2, thông qua việc sử dụng các biện pháp bảo vệ và đối phó (nghĩa là kiểm soát). Các kiểm soát được phân loại theo ISO/IEC 27002:2022, 4.2. Bảo mật lưu trữ cũng có thể bắt buộc đưa vào các kiểm soát chuyên biệt để giải quyết các công nghệ như:

- củng cố an toàn hệ thống;
- làm sạch lưu trữ;
- an toàn ảo hóa;
- thiết bị lưu trữ tự mã hóa và phần mềm mã hóa dữ liệu;
- dịch vụ quản lý khóa;
- dịch vụ xác thực và toàn vẹn dữ liệu;
- bảo vệ dữ liệu động (mã hóa và giảm dữ liệu);
- dịch vụ thư mục và các hệ thống quản lý người dùng khác;
- lưu giữ và bảo quản dữ liệu;
- bảo vệ và phục hồi dữ liệu.

Việc nắm rõ cả cách thức và lý do sử dụng các công nghệ lưu trữ có thể hướng tới việc hiểu sâu hơn về các vấn đề và tác động an toàn đối với lưu trữ. Trước hết, cần xem xét các điểm sau đây.

- Các hệ thống lưu trữ có thể hoạt động như các nút trong mạng lưu trữ, có thể dựa trên, nhưng không giới hạn ở các công nghệ như Giao thức Điều khiển Truyền tải/Giao thức Internet (TCP/IP), Fibre Channel (FC), InfiniBand™ (IB), v.v.. Các mối đe dọa tiềm ẩn có thể thay đổi đáng kể dựa trên công nghệ mạng và cấu trúc mạng của các công nghệ đó.

- Khi được lưu trữ, dữ liệu thường được biểu thị và truy cập dưới dạng khối hoặc tệp/đối tượng, với sự khác biệt đáng kể giữa hai phương pháp này. Theo đó, các biện pháp an toàn áp dụng cũng có thể khác nhau một cách căn bản, đặc biệt về kiểm soát truy cập, mã hóa và tính toàn vẹn dữ liệu.

- Là một phần của các hoạt động lưu trữ thông thường, nhiều loại thiết bị lưu trữ có dung lượng phương tiện lưu trữ nội bộ lớn hơn dung lượng được hiển thị thông qua giao diện. SSD thường cấp phát dư thừa phương tiện lưu trữ, nơi dữ liệu có thể được di chuyển nội bộ giữa các vùng phương tiện lưu trữ vật lý để cải thiện độ trễ ghi và phân phối đồng đều hoạt động ghi. HDD thường có các vùng dự phòng nơi dữ liệu có thể được di chuyển nội bộ giữa các vùng phương tiện lưu trữ vật lý khi có sự cố truy cập. Dữ liệu người dùng có thể vẫn còn sót lại trên các vùng cấp phát dư thừa hoặc vùng dự phòng thậm chí ngay sau khi các lần ghi tiếp theo vào thiết bị diễn ra thông qua giao diện của nó. Dữ liệu như vậy không thể bị xóa sạch bằng cách ghi đè thông qua giao diện.

- Quản lý lưu trữ vừa là một yếu tố của cơ sở hạ tầng lưu trữ vừa là một hoạt động được thực hiện trên cơ sở hạ tầng đó. Thông thường, cơ sở hạ tầng này có những người dùng đặc quyền thực hiện các thay đổi cấu hình, cấp phát lưu trữ, tinh chỉnh, giám sát, v.v. Một số hoạt động quản lý có thể được thực hiện từ xa và có thể liên quan đến các bên thứ ba như nhân viên hỗ trợ của nhà cung cấp.

- Tính sẵn sàng và tính toàn vẹn dữ liệu là những yếu tố then chốt trong kiến trúc lưu trữ của một tổ chức, do đó các biện pháp an toàn cần mang tính bổ trợ lẫn nhau thay vì đánh đổi, và các biện pháp đó không được làm mất tính sẵn sàng cao bằng cách tạo ra các điểm nghẽn hay điểm lỗi đơn lẻ.

- Nhiều tổ chức triển khai các chiến lược phục hồi dữ liệu phức tạp, vốn là bộ phận không thể tách rời trong kế hoạch quản lý tính liên tục kinh doanh (BCM). Các cơ chế an toàn như mã hóa dữ liệu tĩnh có thể ảnh hưởng tiêu cực đến các chiến lược phục hồi này nếu không được triển khai thận trọng.

- Ảo hóa trong lưu trữ có thể có nhiều dạng và được triển khai tại các điểm khác nhau trong cơ sở hạ tầng lưu trữ. Việc ảo hóa này có thể che giấu các chi tiết vật lý liên quan đến việc trình bày của việc lưu trữ [ví dụ: một đơn vị logic (xem CHÚ THÍCH bên dưới) hoặc hệ thống tệp cho máy chủ], che giấu dung lượng thực của thiết bị, thực hiện di chuyển dữ liệu tự động theo chính sách (nghĩa là lưu trữ phân tầng), hoặc trừu tượng hóa hoàn toàn cơ sở hạ tầng lưu trữ (nghĩa là lưu trữ điện toán đám mây). Việc cân bằng các biện pháp an toàn và ảo hóa để đảm bảo chúng tương thích với nhau đòi hỏi phải lập kế hoạch cẩn thận và lựa chọn các công nghệ phù hợp.

CHÚ THÍCH: Trong lưu trữ máy tính, một đơn vị logic là một thiết bị được định địa chỉ bởi giao thức SCSI hoặc các giao thức đóng gói SCSI, chẳng hạn như Fibre Channel hoặc iSCSI. Số đơn vị logic (LUN) là một số được sử dụng để xác định một đơn vị logic. LUN có thể được sử dụng với bất kỳ thiết bị nào hỗ trợ các hoạt động đọc/ghi, chẳng hạn như ổ băng từ, nhưng thường được sử dụng nhất để chỉ một lưu trữ logic được tạo trên SAN. Mặc dù không hoàn toàn chính xác về mặt kỹ thuật, thuật ngữ LUN thường cũng được sử dụng để chỉ chính lưu trữ logic đó.

- Tốc độ tăng trưởng dữ liệu tại nhiều tổ chức đang thúc đẩy việc tăng cường sử dụng các công nghệ lưu trữ dữ liệu. Thay vì mua thêm dung lượng lưu trữ, các tổ chức đang sử dụng các công nghệ giảm thiểu dữ liệu như nén và khử trùng lặp. Tuy nhiên, các công nghệ giảm thiểu dữ liệu này có thể bị ảnh hưởng bởi các cơ chế mã hóa dữ liệu tĩnh và đến lượt mình, chúng có thể gây ra vấn đề về tính toàn vẹn dữ liệu trong các hoạt động BCM.

- Các bản sao dữ liệu bổ sung có thể được tạo ra như một sản phẩm phụ của các chiến lược bảo vệ dữ liệu như sao chép dữ liệu giữa các hệ thống và các địa điểm (xem 10.14.3), sao lưu (xem 10.14.2), và ảnh chụp nhanh (xem 10.14.4). Các bản sao dữ liệu và dữ liệu tồn dư như vậy có cùng những cân nhắc về mức độ nhạy cảm như dữ liệu gốc.

- Dữ liệu nhạy cảm và có giá trị cao thường được truyền giữa và trong các hệ thống (ví dụ: dữ liệu động), làm tăng những cân nhắc về bảo vệ dữ liệu (xem 10.5.4).

- Nhiều tổ chức đang triển khai mã hóa dữ liệu tĩnh (xem 10.5.5) để bảo vệ dữ liệu nhạy cảm và có giá trị cao. Các cơ chế mật mã cụ thể và điểm mã hóa là những yếu tố quan trọng trong việc bảo vệ dữ liệu thực tế cũng như đáp ứng các yêu cầu tuân thủ.

- Việc sử dụng mã hóa thành công thường phụ thuộc vào việc quản lý đúng nguyên liệu khóa trong suốt vòng đời của nó (xem 10.5.2). Điều này bao gồm việc tạo khóa chính xác, lưu trữ và truyền nguyên liệu khóa an toàn, sao chép khóa như một phần của chiến lược thông thường để đảm bảo tính sẵn sàng của dữ liệu, và thải bỏ đúng cách nguyên liệu khóa khi không còn cần thiết. Mức độ nhạy cảm và tầm quan trọng của dữ liệu cần được bảo vệ cũng có thể là yếu tố trong cách tiếp cận quản lý khóa.

Việc đảm bảo đầy đủ tính bí mật, tính toàn vẹn và tính sẵn sàng của dữ liệu được lưu trữ và truy cập trên các công nghệ lưu trữ hiện tại và mới nổi đòi hỏi một nỗ lực phối hợp trong phân lớp CNTT-TT này. Nhiều nỗ lực an toàn tập trung vào:

- bảo vệ quản lý lưu trữ (hoạt động và giao diện);

- đảm bảo quản lý thông tin xác thực và tin cậy đầy đủ;

- bảo vệ tài nguyên sao lưu và phục hồi dữ liệu;

- bảo vệ dữ liệu động;

- bảo vệ dữ liệu tĩnh;

- bảo vệ tính sẵn sàng của dữ liệu;

- hỗ trợ BCM;

- làm sạch lưu trữ và thải bỏ phương tiện lưu trữ đúng cách;

- di chuyển dữ liệu tự động an toàn;

- đa bên thuê an toàn.

6.4 Rủi ro bảo mật lưu trữ

6.4.1 Bối cảnh

Rủi ro bảo mật lưu trữ được tạo ra bởi việc tổ chức sử dụng các hệ thống hoặc cơ sở hạ tầng lưu trữ cụ thể. Rủi ro bảo mật lưu trữ phát sinh từ:

- các mối đe dọa nhắm vào dữ liệu được xử lý bởi các hệ thống và cơ sở hạ tầng lưu trữ;
- các lỗ hổng (cả kỹ thuật và phi kỹ thuật);
- khả năng thực hiện thành công việc khai thác lỗ hổng bởi các mối đe dọa;
- tác động của việc khai thác thành công lỗ hổng bởi các mối đe dọa.

Quản lý rủi ro là một khái niệm then chốt trong an toàn thông tin. Quy trình quản lý rủi ro an toàn thông tin được trình bày trong TCVN ISO/IEC 27005 (ISO/IEC 27005), bao gồm: thiết lập bối cảnh, đánh giá rủi ro, xử lý rủi ro, chấp nhận rủi ro, truyền thông về rủi ro, và giám sát và xem xét rủi ro.

Các mối đe dọa đối với hệ thống và cơ sở hạ tầng lưu trữ có thể bao gồm:

- sử dụng trái phép tài nguyên lưu trữ;
- truy cập trái phép;
- trách nhiệm pháp lý do không tuân thủ quy định;
- các cuộc tấn công Từ chối Dịch vụ (DoS) và Từ chối Dịch vụ Phân tán (DDoS) vào lưu trữ hoặc mạng;
- làm hỏng/sửa đổi và tiêu hủy dữ liệu, bao gồm cả các bản sao lưu hoặc khôi phục;
- tiết lộ trái phép có thể cấu thành vi phạm dữ liệu;
- trộm cắp hoặc vô tình làm thất lạc phương tiện lưu trữ;
- tấn công phần mềm độc hại hoặc đưa mã độc vào (ví dụ: ransomware);
- làm sạch hoặc thải bỏ không đúng cách sau khi hết sử dụng.

Những mối đe dọa này có thể làm phát sinh một loạt các rủi ro. Tuy nhiên, đối với các hệ thống và cơ sở hạ tầng lưu trữ, mối quan tâm chính là các rủi ro liên quan đến vi phạm dữ liệu, làm hỏng hoặc tiêu hủy dữ liệu, mất quyền truy cập/tính sẵn sàng tạm thời hoặc vĩnh viễn, và không đáp ứng các yêu cầu luật định, quy định hoặc pháp lý.

6.4.2 Vi phạm dữ liệu

Tiêu chuẩn này định nghĩa vi phạm dữ liệu là sự xâm phạm bảo mật dẫn đến việc vô ý hoặc trái pháp luật làm tiêu hủy, mất mát, thay đổi, tiết lộ trái phép hoặc truy cập trái phép vào dữ liệu được bảo vệ đã được truyền, lưu trữ hoặc xử lý theo cách khác. Định nghĩa này vượt xa đáng kể các định nghĩa vi phạm dữ liệu đơn giản hơn vốn chỉ tập trung vào việc truy cập hoặc tiết lộ trái phép một số loại dữ liệu nhất định.

Tùy thuộc vào khối lượng và loại dữ liệu liên quan và các luật và quy định hiện hành, vi phạm dữ liệu có thể khiến tổ chức đối mặt với rủi ro đáng kể phát sinh từ chi phí liên quan đến việc điều tra vi phạm dữ liệu, thực hiện các thông báo cần thiết cho các cá nhân bị ảnh hưởng, chi phí kiện tụng, tiền phạt theo quy định và các hình phạt pháp lý khác cũng như thiệt hại thương hiệu tích lũy từ việc công khai vi phạm dữ liệu. Có những rủi ro kinh tế và an toàn đối với thực thể bị mất thông tin được bảo mật của họ hoặc của người khác. Thông tin đó có thể bao gồm:

- sở hữu trí tuệ hoặc thông tin kinh doanh nhạy cảm khác;
- thông tin nhận dạng cá nhân (PII);
- thông tin tài khoản hoặc hồ sơ tài chính;
- thông tin hồ sơ sức khỏe có thể nhận dạng cá nhân.

Các thực thể không đáng tin cậy hoặc trái phép tìm kiếm thông tin này có thể có nguồn lực tài chính dồi dào và có động cơ đa dạng. Bảng 1 tóm tắt các mối đe dọa an toàn dựa trên lưu trữ có khả năng xảy ra và liệt kê các hình thức vi phạm dữ liệu có thể là kết quả của những xâm phạm này.

Bảng 1 - Các vi phạm dữ liệu theo hướng lưu trữ

Các mối đe dọa an toàn	Các hình thức vi phạm dữ liệu tiềm ẩn
Trộm cắp hoặc mất mát thiết bị lưu trữ hoặc phương tiện lưu trữ	Tiết lộ bất hợp pháp hoặc trái phép, mất dữ liệu hoặc tiêu hủy dữ liệu
Thay đổi cấu hình vô ý (ví dụ: quản lý lưu trữ, tài nguyên lưu trữ/mạng và quản lý bản vá không chính xác) bởi nhân viên được ủy quyền	Truy cập vô ý, tiết lộ vô ý, tiêu hủy dữ liệu vô ý, thay đổi dữ liệu vô ý hoặc loại bỏ/từ chối truy cập

Thay đổi cấu hình độc hại (quản lý lưu trữ, tài nguyên lưu trữ/mạng và giả mạo ứng dụng) bởi đối thủ bên ngoài hoặc nội bộ	Truy cập bất hợp pháp, tiết lộ bất hợp pháp, tiêu hủy dữ liệu bất hợp pháp, thay đổi dữ liệu bất hợp pháp
Lạm dụng đặc quyền người dùng bởi người dùng được ủy quyền (ví dụ: rình mò dữ liệu không phù hợp)	Truy cập hoặc tiết lộ bất hợp pháp/trái phép
Giả mạo dữ liệu độc hại bởi đối thủ bên ngoài hoặc nội bộ	Tiêu hủy hoặc thay đổi dữ liệu bất hợp pháp
Tấn công từ chối dịch vụ	Mất quyền truy cập bởi người dùng hợp pháp và không khả dụng của lưu trữ và dữ liệu
Giám sát lưu lượng mạng nhằm mục đích xấu	Tiết lộ bất hợp pháp/trái phép

6.4.3 Hỏng hoặc tiêu hủy dữ liệu

Hỏng dữ liệu là sự suy giảm hoặc hư hỏng dữ liệu (tức là các thay đổi ngoài ý muốn đối với dữ liệu gốc) do lỗi người dùng, phần cứng hoặc phần mềm. Hỏng dữ liệu có thể xảy ra trong quá trình ghi, đọc, lưu giữ, truyền hoặc xử lý. Phát hiện sớm tình trạng hỏng dữ liệu có thể cho phép khôi phục dữ liệu hoặc siêu dữ liệu trong điều kiện phù hợp. Nếu không được phát hiện hay khắc phục, hỏng dữ liệu có thể dẫn đến mất dữ liệu vĩnh viễn nếu nguyên nhân gốc rễ vẫn còn tồn tại. Mặt khác, tiêu hủy dữ liệu dẫn đến mất dữ liệu — có thể là vĩnh viễn nếu các cơ chế bảo vệ dữ liệu như sao lưu chưa được áp dụng. Cả hỏng dữ liệu và tiêu hủy dữ liệu đều có thể là kết quả của các sự kiện vô ý hoặc cố ý; trong trường hợp cố ý, chúng có thể được phân loại thêm thành có ác ý hoặc không có ác ý.

Các sự kiện như hỏa hoạn, lũ lụt, mất điện và lỗi người dùng đều là những ví dụ điển hình về nguồn gốc vô ý nói chung gây ra hỏng hoặc tiêu hủy dữ liệu. Bức xạ nền, hỏng đầu đọc/ghi của ổ đĩa cứng (HDD), và sự lão hóa hoặc hao mòn của phương tiện lưu trữ là những nguồn gây sự cố bổ sung mang tính đặc thù của lưu trữ hơn. Hỏng dữ liệu do lỗi thiết bị lưu trữ hoặc phương tiện lưu trữ nhìn chung có thể được phát hiện bằng cách sử dụng tổng kiểm tra (checksum), và thường có thể được khắc phục bằng cách sử dụng mã sửa lỗi; tuy nhiên, những sự khắc phục âm thầm này có thể dẫn đến các vấn đề khác nếu lưu trữ không được quản lý tốt (tức là các lỗi có thể khắc phục tạm thời có thể trở thành lỗi vĩnh viễn khi thiết bị hoặc phương tiện lưu trữ xuống cấp).

Các cuộc tấn công cố ý mang tính ác ý có thể do các bên bên ngoài hoặc người trong nội bộ thực hiện nhằm mục đích làm cho một phần hoặc toàn bộ dữ liệu bị ảnh hưởng trở nên không thể sử dụng được hoặc bị tiêu hủy. Trong bối cảnh này, không thể sử dụng được có thể có nghĩa là đã có các sửa đổi trái phép được áp dụng, nghi ngờ có sửa đổi, hoặc dữ liệu có thể bị mã hóa bằng một khóa hoặc cơ chế không xác định (hoặc khóa ban đầu được sử dụng để mã hóa dữ liệu có thể đã bị tiêu hủy). Các sự cố không ác ý thường xuất phát từ sự bất cẩn, thiếu hiểu biết, hoặc cố ý bỏ qua các biện pháp an toàn vì những lý do như để hoàn thành công việc nhanh chóng. Tuy nhiên, tác động của các sự cố không ác ý đối với dữ liệu có thể gây thiệt hại nghiêm trọng không kém gì các cuộc tấn công có ác ý.

Việc áp dụng các cơ chế phù hợp để phát hiện và khắc phục tình trạng hỏng dữ liệu là một biện pháp quan trọng để duy trì tính toàn vẹn dữ liệu. Tương tự, việc phát hiện mất dữ liệu và khôi phục dữ liệu đó bằng các cơ chế bảo vệ dữ liệu có thể giúp phòng ngừa việc mất dữ liệu.

6.4.4 Mất quyền truy cập/tính sẵn sàng tạm thời hoặc vĩnh viễn

Tính sẵn sàng liên quan đến việc đảm bảo rằng người dùng và hệ thống được ủy quyền có thể truy cập dữ liệu ở mức hiệu suất yêu cầu trong khoảng thời gian xác định. Mất quyền truy cập - dù chỉ tạm thời -

có thể gây thiệt hại đáng kể cho tổ chức. Hơn nữa, truy cập bị suy giảm (ví dụ: không đáp ứng ngưỡng hiệu suất tối thiểu) cũng có thể gây hậu quả tương tự. Mất quyền truy cập hoặc tính sẵn sàng có thể xảy ra do lỗi hay sự cố liên quan đến thiết bị lưu trữ, các thành phần mạng lưu trữ, dữ liệu lưu trữ, luồng dữ liệu, dịch vụ và ứng dụng, hoặc do các cuộc tấn công. Nhìn chung, tính sẵn sàng của dữ liệu được đảm bảo thông qua dự phòng.

6.4.5 Không đáp ứng các yêu cầu luật định, quy định hoặc pháp lý

Các tổ chức có thể phải chịu trách nhiệm pháp lý và các hình phạt đáng kể do không tuân thủ các yêu cầu luật định, quy định hoặc pháp lý. Đối với các tổ chức đa quốc gia, pháp luật riêng của từng quốc gia có ảnh hưởng trực tiếp và quan trọng đến các yêu cầu an toàn thông tin. Các vấn đề tuân thủ thường gặp bao gồm:

- vi phạm các yêu cầu về quyền riêng tư cụ thể của quốc gia;
- chuyển dữ liệu bất hợp pháp (ví dụ: di chuyển dữ liệu bị hạn chế ra khỏi một khu vực pháp lý cụ thể);
- vi phạm bảo mật;
- không phù hợp với chính sách của tổ chức (ví dụ: làm sạch);
- lưu giữ và bảo vệ dữ liệu không đầy đủ;
- không đủ bằng chứng về an toàn (ví dụ: nhật ký kiểm toán và bằng chứng về mã hóa/làm sạch).

Những vấn đề không tuân thủ này có thể dẫn đến các biện pháp trừng phạt và khắc phục tốn kém (ví dụ: thông báo vi phạm).

7 Các kiểm soát tổ chức đối với lưu trữ

7.1 Tổng quát

Các tổ chức có thể tham khảo bộ kiểm soát tổ chức mở rộng được liệt kê trong ISO/IEC 27002:2022, Điều 5. Một số hoặc tất cả các kiểm soát này có liên quan đến các hệ thống và hệ sinh thái lưu trữ.

7.2 Điều chỉnh lưu trữ và chính sách

Việc có hay không có chính sách đóng vai trò quan trọng trong việc đảm bảo cả an toàn và tuân thủ. Các hướng dẫn và yêu cầu chính sách sau đây được áp dụng.

a) OC-PLCY-G01 Kết hợp lưu trữ vào chính sách

Lưu trữ nên được kết hợp vào các chính sách để:

- xác định các loại dữ liệu nhạy cảm nhất (PII, sở hữu trí tuệ, bí mật thương mại, v.v.) và quan trọng đối với kinh doanh/nhiệm vụ cũng như các yêu cầu bảo vệ;
- tích hợp các chính sách cụ thể về lưu trữ với các chính sách khác (tức là tránh tạo tài liệu chính sách riêng cho hệ sinh thái lưu trữ);
- giải quyết việc lưu giữ và bảo vệ dữ liệu (ví dụ: WORM, tính xác thực và kiểm soát truy cập);
- giải quyết việc tiêu hủy dữ liệu và làm sạch phương tiện lưu trữ.

b) OC-PLCY-G02 Đảm bảo lưu trữ tuân thủ chính sách

Sự phù hợp với các chính sách nên:

- đảm bảo rằng tất cả các yếu tố của hệ sinh thái lưu trữ tuân thủ chính sách (ví dụ: TCVN ISO/IEC 27001 **(**ISO/IEC 27001:2022), 5.2 và TCVN ISO/IEC 27002 **(**ISO/IEC 27002:2022), 5.1);

- ưu tiên dữ liệu nhạy cảm nhất/quan trọng nhất.

c) OC-PLCY-R01 Bao gồm lưu trữ trong chính sách ghi nhật ký

Bao gồm lưu trữ trong chính sách ghi nhật ký sao cho chính sách ghi nhật ký phải:

- nêu rõ rằng các hệ thống và thiết bị lưu trữ tham gia vào ghi nhật ký kiểm toán;
- xác định các sự kiện quan trọng liên quan đến lưu trữ cần được thu thập;
- xác định các yêu cầu bảo quản đối với nhật ký sự kiện liên quan đến lưu trữ;
- xác định các yêu cầu lưu giữ và lưu trữ đối với nhật ký sự kiện liên quan đến lưu trữ;
- chỉ định yêu cầu đồng bộ hóa thời gian và sử dụng đối với nhật ký sự kiện liên quan đến lưu trữ;
- bao gồm các kỳ vọng về bằng chứng (tính xác thực, chuỗi hành trình, v.v.).

7.3 Quản lý tính liên tục kinh doanh

ISO 22301 quy định cấu trúc và các yêu cầu để triển khai và duy trì hệ thống quản lý tính liên tục kinh doanh, nhằm xây dựng khả năng liên tục kinh doanh phù hợp với quy mô và tính chất của các tác động mà tổ chức chấp nhận sau một sự gián đoạn. Các yêu cầu của ISO 22301 mang tính tổng quát và được thiết kế để áp dụng cho mọi tổ chức, hoặc các bộ phận của tổ chức, bất kể loại hình, quy mô hay bản chất. Phạm vi áp dụng các yêu cầu này tùy thuộc vào môi trường hoạt động và mức độ phức tạp của tổ chức. Các yêu cầu quy định trong ISO 22301 đề cập đến bối cảnh của tổ chức, vai trò lãnh đạo, hoạch định, hỗ trợ, vận hành, đánh giá kết quả hoạt động và cải tiến.

ISO/IEC 27002:2022, 5.30 xác định tầm quan trọng của sự sẵn sàng CNTT-TT cho tính liên tục kinh doanh (IRBC) để đảm bảo tính sẵn sàng của thông tin của tổ chức và các tài sản liên quan khác trong thời gian gián đoạn. ISO/IEC 27031 mô tả các khái niệm và nguyên tắc của IRBC. ISO/IEC 27031 cũng cung cấp một khuôn khổ các phương pháp và quy trình để xác định và chỉ định tất cả các khía cạnh (như tiêu chí hiệu suất, thiết kế và triển khai) để cải thiện sự sẵn sàng CNTT-TT của tổ chức nhằm đảm bảo liên tục kinh doanh. Khuôn khổ này áp dụng cho bất kỳ tổ chức nào (tư nhân, chính phủ và phi chính phủ, không phân biệt quy mô) đang phát triển chương trình sẵn sàng CNTT-TT cho liên tục kinh doanh của mình và yêu cầu các dịch vụ/cơ sở hạ tầng CNTT-TT của mình phải sẵn sàng hỗ trợ các hoạt động kinh doanh trong trường hợp xảy ra các sự kiện và sự cố mới nổi, và các gián đoạn liên quan, có thể ảnh hưởng đến tính liên tục (bao gồm cả an toàn) của các chức năng kinh doanh quan trọng. Khuôn khổ này cũng cho phép một tổ chức đo lường các thông số hiệu suất tương quan với IRBC của mình một cách nhất quán và được công nhận.

Lưu trữ thường là một yếu tố quan trọng trong chương trình IRBC của tổ chức hoặc các hoạt động BCM không chính thức. Các kiểm soát liên quan đến BCM như sau:

a) OC-IRBC-G01 Tính đến hệ sinh thái lưu trữ trong lập kế hoạch và triển khai BCM

Các tổ chức nên đảm bảo rằng hệ sinh thái lưu trữ được tính đến trong việc lập kế hoạch và triển khai BCM.

b) OC-IRBC-G02 Chuẩn bị cho các sự kiện gián đoạn hạn chế

Các tổ chức nên chuẩn bị cho các sự kiện gián đoạn hạn chế (lỗi hệ thống, tấn công đối thủ, lỗi vận hành).

c) OC-IRBC-G03 Xác định và ghi lại các yêu cầu về nhân sự và cơ sở vật chất duy nhất

Các tổ chức nên xác định và ghi lại các yêu cầu về nhân sự và cơ sở vật chất duy nhất liên quan đến hệ sinh thái lưu trữ.

d) OC-IRBC-G04 Thực hiện lập kế hoạch và kiểm tra BCM liên tục

Các tổ chức nên thực hiện lập kế hoạch liên tục và kiểm tra thường xuyên các giả định, vốn rất quan trọng đối với BCM thành công. Kết quả kiểm tra BCM nên được đưa trở lại vào việc bảo trì liên tục kế hoạch BCM.

7.4 Tuân thủ

Tầm quan trọng của việc tuân thủ các yêu cầu pháp lý và quy định thúc đẩy một phần đáng kể chương trình nghị sự và chiến lược an toàn của nhiều tổ chức. Các yếu tố sau đây là các khía cạnh tuân thủ chính của các hệ thống và cơ sở hạ tầng lưu trữ được kiểm toán viên hệ thống thông tin (IS) quan tâm. Các kiểm soát liên quan đến tuân thủ như sau:

a) OC-CPLC-R01 Đảm bảo lưu trữ đáp ứng nghĩa vụ trách nhiệm giải trình của người dùng

Đảm bảo rằng các nghĩa vụ trách nhiệm giải trình của người dùng được đáp ứng bằng cách đảm bảo rằng:

- người dùng, đặc biệt là người dùng đặc quyền, phải có ID người dùng duy nhất (tức là không có tài khoản dùng chung);
- quyền và đặc quyền của người dùng phải được cấp rõ ràng dựa trên nhiệm vụ của họ (ví dụ: vai trò) theo nguyên tắc đặc quyền tối thiểu (tức là người dùng được cấp tài nguyên hệ thống và quyền hạn tối thiểu mà họ cần để thực hiện chức năng của mình);
- tất cả các sự kiện và giao dịch quản lý đã cố gắng (thành công và không thành công) phải được ghi lại.

b) OC-CPLC-G01 Đảm bảo lưu trữ đáp ứng nghĩa vụ truy xuất nguồn gốc người dùng

Đảm bảo rằng lưu trữ đáp ứng nghĩa vụ truy xuất nguồn gốc người dùng, cụ thể:

- dữ liệu sự kiện/giao dịch được ghi lại nên chứa đủ chi tiết ứng dụng hoặc hệ thống để xác định rõ nguồn gốc;
- thông tin người dùng nên có thể truy xuất được đến một cá nhân cụ thể;
- khi thích hợp, các hồ sơ nhật ký nên được coi là bằng chứng (chuỗi hành trình, tính không thể chối cãi, tính xác thực, v.v.).

c) OC-CPLC-G02 Đảm bảo lưu trữ đáp ứng nghĩa vụ giám sát người dùng

Đảm bảo rằng lưu trữ đáp ứng nghĩa vụ giám sát người dùng, cụ thể:

- lớp lưu trữ nên tham gia vào các biện pháp ghi nhật ký kiểm toán bên ngoài;
- các sự kiện ghi nhật ký kiểm toán nên được giám sát và cảnh báo các vấn đề khi thích hợp.

d) OC-CPLC-G03 Đảm bảo lưu trữ đáp ứng nghĩa vụ lưu giữ và làm sạch dữ liệu

Đảm bảo rằng lưu trữ đáp ứng nghĩa vụ lưu giữ và làm sạch dữ liệu, cụ thể:

- các biện pháp lưu giữ dữ liệu thích hợp nên được thực hiện;
- các biện pháp toàn vẹn và xác thực dữ liệu thích hợp nên được thực hiện;
- việc làm sạch dữ liệu chính xác nên được thực hiện trước khi tái sử dụng hoặc ngừng hoạt động phần cứng;
- việc làm sạch chính xác các hình ảnh máy chủ ảo và các bản sao của chúng nên được thực hiện khi hết vòng đời.

e) OC-CPLC-G04 Đảm bảo lưu trữ đáp ứng nghĩa vụ về quyền riêng tư

Đảm bảo rằng lưu trữ đáp ứng nghĩa vụ về quyền riêng tư (xem ISO/IEC 27701), cụ thể:

- kiểm soát truy cập dữ liệu thích hợp, dựa trên đặc quyền tối thiểu, nên được thực hiện để kiểm soát quyền truy cập vào dữ liệu và siêu dữ liệu (ví dụ: kết quả tìm kiếm);
- các biện pháp bảo mật dữ liệu thích hợp nên được thực hiện để ngăn chặn việc tiết lộ trái phép.

f) OC-CPLC-G05 Lưu trữ xem xét nghĩa vụ pháp lý

Nghĩa vụ pháp lý có thể áp dụng cho lưu trữ, cụ thể:

- việc sử dụng khử trùng lặp dữ liệu không nên xung đột với các yêu cầu về tính xác thực của dữ liệu;
- việc sử dụng các cơ chế làm sạch dữ liệu và phương tiện lưu trữ không nên vi phạm các yêu cầu bảo quản;
- các thủ tục chuỗi hành trình phù hợp nên được tuân thủ khi xử lý dữ liệu chứng cứ (ví dụ: nhật ký kiểm toán, siêu dữ liệu, bản sao gương (mirror) và bản sao tại một thời điểm).

8 Kiểm soát con người đối với lưu trữ

Các tổ chức có thể tham khảo bộ kiểm soát con người mở rộng được liệt kê trong ISO/IEC 27002:2022, Điều 6. Một số hoặc tất cả các kiểm soát này có liên quan đến các hệ thống lưu trữ và hệ sinh thái lưu trữ. ISO/IEC 27002:2022, 6.3 nêu rõ rằng một tổ chức nên xác định, chuẩn bị và thực hiện một kế hoạch đào tạo thích hợp cho các nhóm kỹ thuật có vai trò đòi hỏi bộ kỹ năng và chuyên môn cụ thể. Đối với các cá nhân chịu trách nhiệm về các khía cạnh của bảo mật lưu trữ, kỹ năng và chuyên môn có thể rất chuyên biệt như được thể hiện trong tiêu chuẩn này. Các kiểm soát liên quan đến chuyên môn như sau:

a) SC-XPTS-G01 Đảm bảo chuyên môn bảo vệ lưu trữ đầy đủ

Các nhóm lưu trữ và quản lý nên hiểu các công nghệ và thực tiễn liên quan đến các công nghệ bảo vệ dữ liệu dựa trên lưu trữ (xem 10.14). Ngoài ra, sự hiểu biết này nên bao gồm khả năng áp dụng bảo vệ dữ liệu trong tổ chức.

b) SC-XPTS-G02 Đảm bảo chuyên môn bảo mật lưu trữ đầy đủ

Các nhóm lưu trữ và quản lý nên hiểu các công nghệ và thực tiễn để bảo mật các thiết bị, hệ thống và hệ sinh thái lưu trữ, cũng như tận dụng các kiểm soát an toàn dựa trên lưu trữ.

9 Kiểm soát vật lý đối với lưu trữ

9.1 Tổng quát

Các tổ chức có thể tham khảo bộ kiểm soát vật lý mở rộng được liệt kê trong ISO/IEC 27002:2022, Điều 7. Một số hoặc tất cả các kiểm soát này có liên quan đến các hệ thống và hệ sinh thái lưu trữ.

9.2 Bảo mật vật lý lưu trữ

Các hệ thống và hệ sinh thái lưu trữ đặc biệt dễ bị tổn thương trước các mối đe dọa vật lý. Chúng có thể bị trộm cắp, tiêu hủy và bị truy cập trái phép nếu không được bảo vệ đúng cách khi không sử dụng hoặc không có người giám sát. Kích thước của phương tiện, thiết bị và hệ thống lưu trữ rất đa dạng, do đó các phương pháp bảo mật vật lý cũng cần phù hợp theo từng trường hợp. Các kiểm soát liên quan đến bảo mật vật lý lưu trữ như sau:

a) PC-PHYS-G01 Bảo mật vật lý phương tiện lưu trữ

Tất cả các phương tiện lưu trữ có dữ liệu đã ghi nên được lưu trữ trong một môi trường an toàn, bảo mật theo phân loại thông tin của chúng và bảo vệ chúng khỏi các mối đe dọa môi trường (như nhiệt, độ ẩm, trường điện từ hoặc lão hóa), theo thông số kỹ thuật của nhà sản xuất.

b) PC-PHYS-G02 Bảo mật vật lý thiết bị lưu trữ

Tùy thuộc vào kích thước và vị trí của chúng, các thiết bị lưu trữ nên được bảo mật vật lý:

- các đơn vị kích thước nhỏ trong môi trường văn phòng có thể được buộc vào đồ đạc hoặc tường cũng như được cất giữ trong tủ hoặc két sắt có khóa khi không sử dụng;
- hoặc các đơn vị kích thước lớn có thể được gắn vào giá đỡ và đặt trong phòng thí nghiệm hoặc trung tâm dữ liệu nơi chúng được hưởng lợi từ các biện pháp an toàn của cơ sở (ví dụ: vỏ hoặc lồng có khóa).

9.3 Bảo vệ giao diện vật lý đến lưu trữ

Việc bảo vệ các giao diện quản lý khỏi truy cập trái phép và trinh sát là vô cùng quan trọng. Truy cập trái phép vào giao diện quản lý do thiếu các kiểm soát phù hợp có thể dẫn đến tiêu hủy, làm hỏng dữ liệu hoặc từ chối truy cập.

Giao diện quản lý cho các hệ thống lưu trữ có thể có một số dạng vật lý bao gồm cổng nối tiếp, mạng cục bộ, modem và thậm chí cả các công nghệ được sử dụng cho đường dẫn dữ liệu (ví dụ: Fibre Channel). Giao diện lai (ví dụ: cổng nối tiếp được cắm vào bộ tập trung cổng console cung cấp giao diện trên mạng LAN) cũng tương đối phổ biến.

Các kiểm soát liên quan đến việc bảo vệ giao diện lưu trữ vật lý như sau:

PC-PHYS-R01 Bảo vệ giao diện vật lý

Để bảo vệ các giao diện vật lý này, tổ chức phải:

- hạn chế quyền truy cập vật lý vào giao diện quản lý;
- vô hiệu hóa và ngắt kết nối các cổng quản lý nối tiếp khi không sử dụng;
- tách biệt các giao diện LAN được sử dụng để quản lý khỏi lưu lượng LAN khác, lưu ý rằng cách ly vật lý được ưu tiên, nhưng cách ly logic (chẳng hạn như VLAN) được coi là một thực hành tốt nhất;
- vô hiệu hóa các cổng modem khi không cần thiết.

9.4 Cách ly hệ thống lưu trữ

Cách ly vật lý và logic các thiết bị lưu trữ (ví dụ: trong SAN) cũng có thể đóng vai trò quan trọng. Các kiểm soát liên quan đến cách ly lưu trữ như sau:

a) PC-PHYS-G03 Cách ly vật lý hệ thống lưu trữ

Cách ly vật lý nên được sử dụng để:

- tách biệt sản xuất khỏi các lớp hệ thống khác (ví dụ: đảm bảo chất lượng, phát triển) bao gồm:

  + nếu có thể, tránh kết nối mạng giữa các lớp (ví dụ: máy chủ sản xuất được kết nối với cả mạng sản xuất và phát triển),

  + tách biệt mạng và lưu trữ theo lớp khi thích hợp,

  + tách biệt vật lý các hệ thống trong mỗi lớp;

- cách ly các thiết bị lưu trữ khỏi các thiết bị trung tâm dữ liệu khác, nếu thực tế.

b) PC-PHYS-G04 Cách ly logic hệ thống lưu trữ

Cách ly logic nên được sử dụng để:

- tách biệt lưu lượng lưu trữ khỏi lưu lượng máy chủ thông thường bằng cách sử dụng:
  + các kiểm soát mạng có sẵn để tạo các miền logic độc lập trên cơ sở hạ tầng vật lý chung,
  + các kiểm soát tin cậy và truy cập để quản lý tư cách thành viên trong các miền logic;
- tách biệt lưu lượng quản lý lưu trữ khỏi tất cả các lưu lượng khác;
- cấu hình cổng mạng để phân tách mạng thích hợp.

10 Kiểm soát công nghệ đối với lưu trữ

10.1 Tổng quát

Người dùng có thể tham khảo bộ kiểm soát công nghệ mở rộng được liệt kê trong ISO/IEC 27002:2022, Điều 8. Một số hoặc tất cả các kiểm soát này có liên quan đến các hệ thống lưu trữ và hệ sinh thái lưu trữ.

10.2 Thiết kế và triển khai bảo mật lưu trữ

10.2.1 Tổng quát

Trước sự tăng trưởng mạnh mẽ về khối lượng dữ liệu trọng yếu, nhiều tổ chức đã áp dụng các kiến trúc lấy lưu trữ làm trung tâm cho cơ sở hạ tầng CNTT-TT. Do đó, bảo mật lưu trữ đóng vai trò quan trọng trong việc bảo vệ dữ liệu này và trong nhiều trường hợp là tuyến phòng thủ cuối cùng. Hiệu quả của bảo mật lưu trữ thường chịu ảnh hưởng lớn từ các quyết định thiết kế. Các kiểm soát liên quan đến thiết kế và triển khai lưu trữ như sau:

a) TC-DSGN-G01 Tuân thủ các nguyên tắc thiết kế an toàn cốt lõi

Việc thiết kế và triển khai các giải pháp bảo mật lưu trữ đòi hỏi phải tuân thủ các nguyên tắc thiết kế an toàn cốt lõi. Ngoài ra, các kiểm soát và hướng dẫn được mô tả trong Điều 7, 8 và 9 nên được tích hợp vào thiết kế và triển khai các giải pháp bảo mật lưu trữ để chống lại các mối đe dọa hiện hành. Độ nhạy cảm, mức độ trọng yếu và giá trị của dữ liệu cũng có thể là một yếu tố cân nhắc quan trọng trong thiết kế (xem 10.2.2).

b) TC-DSGN-G02 Xem xét các mối đe dọa liên quan trong thiết kế

Các lĩnh vực rủi ro phổ biến liên quan đến kiến trúc bảo mật lưu trữ là lỗi thiết kế do thiết kế kém hoặc thiếu cân nhắc thích hợp cho việc lập kế hoạch quản lý liên tục kinh doanh, hoặc thiếu sự tương ứng với mức độ đe dọa hiện tại hoặc dự kiến. Một thiết kế nên xem xét tất cả các mối đe dọa và lỗ hổng liên quan trong hệ thống lưu trữ như được mô tả trong 6.4. Thông tin về đánh giá rủi ro an toàn và các mối đe dọa liên quan cũng có thể được tìm thấy trong TCVN ISO/IEC 27001 (ISO/IEC 27001), ISO/IEC 27002 và TCVN ISO/IEC 27005 **(**ISO/IEC 27005).

10.2.2 Nguyên tắc thiết kế bảo mật lưu trữ

10.2.2.1 Phòng thủ theo chiều sâu

Ngày càng nhiều tổ chức tiếp cận an toàn theo mô hình phân lớp, toàn diện trên toàn bộ ứng dụng, hệ thống, mạng, lưu trữ và thiết bị. Cách tiếp cận phân lớp như vậy được gọi là phòng thủ theo chiều sâu,

đặc biệt khi kết hợp đồng thời chính sách, thiết kế, quản lý và công nghệ. Mức độ áp dụng phòng thủ theo chiều sâu khác nhau tùy từng tổ chức, phụ thuộc vào các yếu tố như giá trị và độ nhạy cảm của dữ liệu, yêu cầu tuân thủ, năng lực và chiến thuật của đối thủ. Một nguyên tắc quan trọng của phòng thủ theo chiều sâu là sử dụng nhiều kiểm soát an toàn để giảm thiểu rủi ro khi một thành phần trong hệ thống phòng thủ bị xâm phạm hoặc bị vượt qua.

Các kiểm soát liên quan đến phòng thủ theo chiều sâu như sau:

TC-DSGN-G03 Triển khai phòng thủ theo chiều sâu

Các hệ thống và giải pháp lưu trữ nên:

- đảm bảo tập trung cân bằng vào ba yếu tố chính: con người, công nghệ và hoạt động;
- thực hiện đầy đủ các chính sách và thủ tục đảm bảo thông tin hiệu quả, phân công vai trò và trách nhiệm, cam kết nguồn lực, đào tạo nhân sự chủ chốt và trách nhiệm cá nhân;
- triển khai các cơ chế bảo vệ tại nhiều địa điểm để chống lại nhiều loại tấn công;
- triển khai nhiều lớp cơ chế phòng thủ giữa các đối thủ tiềm năng và mục tiêu;
- bao gồm cả cơ chế phát hiện và bảo vệ;
- tận dụng các cơ sở hạ tầng an toàn mạnh mẽ (ví dụ: hỗ trợ nhiều trường hợp sử dụng và khối lượng lớn) và có khả năng chống tấn công cao (ví dụ: kiến trúc không tin cậy) (ví dụ: quản lý khóa, cơ sở hạ tầng khóa công khai và quản lý danh tính) được quản lý và giám sát tập trung;
- duy trì các chính sách an toàn hệ thống rõ ràng và cập nhật;
- chủ động quản lý tình trạng an toàn của công nghệ lưu trữ và cơ chế bảo vệ (ví dụ: cài đặt bản vá an toàn, cập nhật chống vi-rút và duy trì ACL);
- thực hiện đánh giá mối đe dọa an toàn thường xuyên để đánh giá sự sẵn sàng về an toàn;
- giám sát và phản ứng với các mối đe dọa hiện tại.

Đối với lưu trữ, nhiều cơ chế phòng thủ theo lớp có nghĩa là các kiểm soát an toàn được triển khai và sử dụng trong toàn bộ cơ sở hạ tầng lưu trữ, bao gồm bộ điều hợp mạng hội tụ (CNA) trong máy tính chủ, bộ chuyển mạch/bộ định tuyến mạng lưu trữ, hệ thống lưu trữ chuyên dụng và thiết bị lưu trữ.

CHÚ THÍCH: CNA là một thiết bị giao diện mạng duy nhất cung cấp chức năng của cả bộ điều hợp bus máy chủ FC (HBA) và thẻ giao diện mạng Ethernet TCP/IP.

10.2.2.2 Miền an toàn

Miền an toàn dựa trên nguyên tắc phân tách các tài nguyên hệ thống có mức độ nhạy cảm khác nhau (tức là có giá trị, mức chịu đựng rủi ro và khả năng bị đe dọa khác nhau). Điều này đảm bảo rằng mỗi hệ thống chỉ cung cấp dữ liệu cần thiết để thực hiện các tác vụ trong miền cụ thể đó. Theo nguyên tắc thiết kế này, kiến trúc thực thi sự phân tách miền để bảo đảm rằng các tài nguyên mà một thực thể có quyền truy cập không thể bị truy cập hay bị ảnh hưởng bởi thực thể thuộc miền khác.

Đối với cơ sở hạ tầng lưu trữ, một miền an toàn thường được biểu diễn dưới dạng SAN, đặc biệt khi dữ liệu nhạy cảm đang được lưu trữ và xử lý. Trong các tình huống mà độ nhạy cảm của dữ liệu thấp, việc sử dụng phân vùng (zoning) và VLAN có thể được coi là chấp nhận được, nhưng cần lưu ý rằng khả năng phân vùng thông thường không phải là một cơ chế an toàn theo nghĩa chặt chẽ như FC-SP-2 Zoning.

Dựa trên nguyên tắc phân vùng được mô tả trong TCVN 9801-2 (ISO/IEC 27033-2), các khuyến nghị thiết kế bảo mật lưu trữ sau đây có liên quan:

a) TC-DSGN-G04 Tính đến độ nhạy cảm của dữ liệu trong thiết kế miền an toàn

Độ nhạy cảm của dữ liệu nên được tính đến trong thiết kế miền an toàn, cụ thể:

- lưu trữ và mạng lưu trữ có các mức độ nhạy cảm khác nhau nên được đặt ở các miền an toàn khác nhau;
- các thiết bị và hệ thống máy tính cung cấp dịch vụ cho các mạng bên ngoài (ví dụ: Internet) nên được đặt ở các miền khác nhau (vùng phi quân sự) so với các thiết bị mạng nội bộ và hệ thống máy tính;
- các tài sản chiến lược nên được đặt ở các miền an toàn chuyên dụng;
- các thiết bị và hệ thống máy tính không đáng tin cậy nên có quyền truy cập hạn chế hoặc không có quyền truy cập vào tài sản lưu trữ.

b) TC-DSGN-G05 Tính đến mục đích trong thiết kế miền an toàn

Mục đích nên được tính đến trong thiết kế miền an toàn, cụ thể:

- lưu trữ và mạng lưu trữ được sử dụng cho các mục đích khác nhau (ví dụ: phát triển, sản xuất và quản lý) và sử dụng các công nghệ khác nhau (ví dụ: SMB, NFS, iSCSI và CDMI) nên được đặt ở các miền an toàn riêng biệt;
- mạng lưu trữ nên ở các miền an toàn khác với mạng thông thường sử dụng cùng công nghệ (ví dụ: mạng IP mang lưu lượng iSCSI nên được tách biệt khỏi mạng LAN công ty thông thường);
- các hệ thống quản lý thiết bị lưu trữ và mạng lưu trữ nên được đặt ở các miền an toàn chuyên dụng;
- hệ thống phát triển nên ở các miền khác với hệ thống sản xuất.

c) TC-DSGN-G06 Sử dụng cách ly hơn nữa trong một miền an toàn

Các thiết bị lưu trữ được phép nằm trong một miền an toàn duy nhất, nhưng được sử dụng cho nhiều mục đích hoặc chứa nhiều mức độ dữ liệu nhạy cảm, nên được cách ly hơn nữa để giảm thiểu các tương tác có thể xảy ra.

10.2.2.3 Khả năng phục hồi thiết kế

Các kiểm soát liên quan đến khả năng phục hồi thiết kế như sau:

TC-DSGN-G07 Bao gồm khả năng phục hồi trong thiết kế

Thiết kế bảo mật lưu trữ nên kết hợp một số lớp dự phòng để loại bỏ các điểm lỗi đơn lẻ và tối đa hóa tính sẵn sàng của cơ sở hạ tầng lưu trữ. Điều này bao gồm việc sử dụng các giao diện dự phòng, mô-đun dự phòng, thiết bị dự phòng và các đường dẫn dự phòng về mặt cấu trúc liên kết. Ngoài ra, các thiết kế cũng nên sử dụng một loạt các phương pháp nhằm làm cho lưu trữ có khả năng phục hồi tốt hơn trước các cuộc tấn công và lỗi mạng.

10.2.2.4 Khởi tạo an toàn

Các kiểm soát liên quan đến khởi tạo an toàn như sau:

TC-DSGN-G08 Hỗ trợ chuỗi khởi tạo an toàn

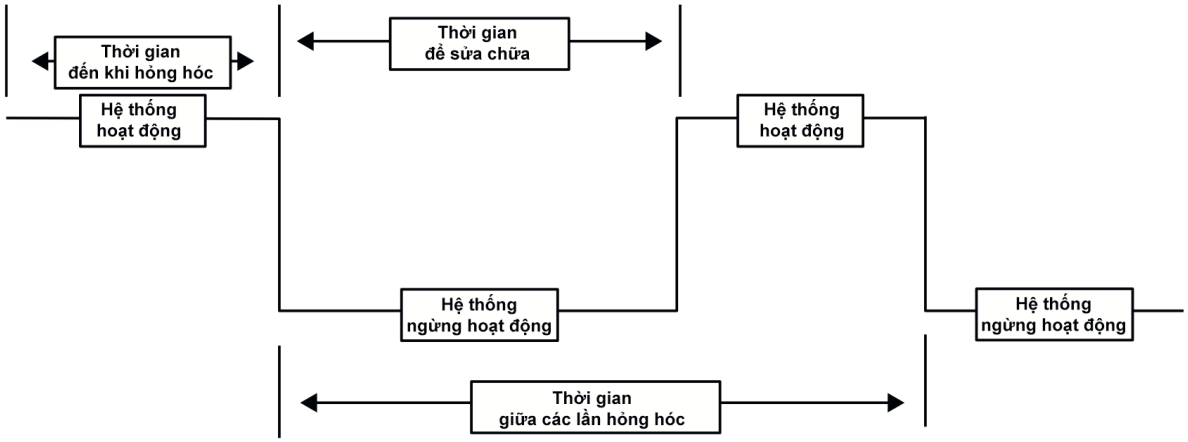
Là một nguyên tắc thiết kế, kiến trúc nên hỗ trợ một chuỗi khởi tạo an toàn trong quá trình chuyển đổi từ trạng thái tắt sang trạng thái hoạt động (ví dụ: sau khi bật nguồn hoặc đặt lại). Trong giai đoạn khởi tạo, các quy trình và giao diện mạng có thể truy cập từ bên ngoài nên bị từ chối truy cập hoặc không khả dụng cho đến khi các chủ thể được xác thực. Các quy trình tải phần mềm và hệ điều hành nên bắt đầu từ một trạng thái đã biết với các giá trị an toàn do quản trị viên hệ thống chỉ định khi hệ thống hoạt động lần cuối.

10.2.3 Thuộc tính chất lượng hệ thống lưu trữ

10.2.3.1 Độ tin cậy

TCVN ISO/IEC 27000 (ISO/IEC 27000) định nghĩa độ tin cậy là thuộc tính của hành vi và kết quả dự định nhất quán. Đối với lưu trữ, độ tin cậy thường được coi là xác suất một thiết bị thực hiện chức năng yêu cầu của nó trong các điều kiện đã nêu trong một khoảng thời gian cụ thể và được định lượng là:

- MTBF (thời gian trung bình giữa các lần hỏng hóc) đối với sản phẩm có thể sửa chữa, là thời gian dự kiến giữa các lần hỏng hóc liên tiếp trong một hệ thống hoặc thành phần và đôi khi được coi là thời gian trung bình có sẵn để một hệ thống hoặc thành phần thực hiện các hoạt động bình thường của nó giữa các lần hỏng hóc (xem Hình 1):
- MTTR (thời gian trung bình để sửa chữa) đối với sản phẩm có thể sửa chữa, là thời gian dự kiến hoặc quan sát được để đưa một hệ thống hoặc thành phần bị trục trặc trở lại hoạt động bình thường và đôi khi được coi là thời gian trung bình để sửa chữa một thành phần bị hỏng;
- MTTF (thời gian trung bình đến khi hỏng hóc) đối với sản phẩm không thể sửa chữa, là thời gian trung bình có sẵn để một hệ thống hoặc thành phần thực hiện các hoạt động bình thường của nó cho đến khi nó bị hỏng.



Hình 1 - Định lượng độ tin cậy

Trong bối cảnh lưu trữ, các xâm phạm và tấn công hệ thống (chẳng hạn như DDoS) có thể có tác động tiêu cực đến MTBF, MTTR (ví dụ: MTTR cũng có thể liên quan đến các hoạt động phục hồi sau một cuộc tấn công) và MTTF. Ngoài ra, việc bao gồm các tính năng an toàn, áp dụng các bản vá hệ thống hoặc ứng dụng, hoặc các biện pháp củng cố hệ thống khác như được mô tả trong 10.3.1 cũng có thể có tác động. Ví dụ, việc áp dụng không chính xác các bản cập nhật hoặc sử dụng các bản cập nhật từ các nguồn không được phê duyệt hoặc không đáng tin cậy có thể có tác động bất lợi. Các kiểm soát liên quan đến độ tin cậy như sau:

TC-DSGN-G09 Giảm thiểu tác động đến độ tin cậy của lưu trữ

Hướng dẫn về độ tin cậy cụ thể bao gồm:

- độ tin cậy của hệ thống và cơ sở hạ tầng lưu trữ không nên bị ảnh hưởng bất lợi bởi việc bao gồm các tính năng an toàn;
- các lỗ hổng lưu trữ nên được quản lý chủ động để giảm thiểu tác động của chúng đến độ tin cậy của hệ thống;
- các kiểm soát nên được đánh giá để xác định liệu chúng có thể đảm bảo độ tin cậy và an toàn của dữ liệu hay không.

10.2.3.2 Tính sẵn sàng

Trong bối cảnh lưu trữ, tính sẵn sàng của dữ liệu thường đề cập đến mức độ dễ dàng truy cập dữ liệu khi được lưu giữ ở một dạng nào đó — thường liên quan đến lưu trữ dữ liệu từ xa qua mạng hoặc

phương tiện lưu trữ bên ngoài. Thuật ngữ này thường bao hàm một số khái niệm khác nhau, chủ yếu là mức độ tin cậy mà dữ liệu sẵn sàng để người dùng được ủy quyền truy cập, xét về cả thời gian hoạt động lẫn tốc độ truy cập.

Tính sẵn sàng được đo bằng tỷ lệ thời gian mà hệ thống hoạt động và sẵn sàng để người dùng được ủy quyền truy cập với các đảm bảo hiệu suất nhất định (ví dụ: không quá 5 mili giây để truy xuất một phần thông tin). Ví dụ, một mảng lưu trữ chỉ có khoảng 5 phút ngừng hoạt động trong một năm (giả sử vận hành liên tục 24/7) thì có tính sẵn sàng đạt 0,999 99 (99,999 %).

Để đạt được tính sẵn sàng cao của dữ liệu, một lượng đáng kể dự phòng phần cứng và phần mềm (ví dụ: chuyển đổi dự phòng đường dẫn vào/ra tự động, các thành phần dự phòng, phụ tùng nóng toàn cầu và bộ đệm dữ liệu được nhân bản có pin dự phòng) được triển khai trong các hệ thống lưu trữ đương đại cũng như cơ sở hạ tầng lưu trữ. Ngoài ra, các cơ chế dự phòng dữ liệu (ví dụ: nhân bản và sao chép) cũng như các cơ chế bảo vệ dữ liệu (ví dụ: sao lưu) thường được sử dụng để đảm bảo phục hồi dữ liệu nhanh chóng trong trường hợp xảy ra lỗi.

Các kiểm soát liên quan đến tính sẵn sàng như sau:

TC-DSGN-G10 Giảm thiểu tác động đến tính sẵn sàng của dữ liệu

Do tầm quan trọng của tính sẵn sàng, cần giảm thiểu các tác động đến tính sẵn sàng của dữ liệu phát sinh từ:

- thiết kế và triển khai bảo mật lưu trữ không đầy đủ (ví dụ: giảm thiểu các điểm lỗi đơn lẻ);
- quản lý không đầy đủ các khóa mã hóa dữ liệu có thể gây ra sự cố khi khóa không khả dụng ở nơi cần thiết hoặc chúng bị tiêu hủy vô tình;
- cơ chế phục hồi dữ liệu không đầy đủ để bảo vệ chống lại mất dữ liệu lớn hoặc ngừng hoạt động lưu trữ.

10.2.3.3 Khả năng phục hồi

Khả năng phục hồi là năng lực cung cấp và duy trì mức dịch vụ chấp nhận được — thường liên quan đến bảo toàn tính toàn vẹn và tính sẵn sàng của dữ liệu — khi đối mặt với lỗi hệ thống và các thách thức đối với hoạt động bình thường (như tấn công, sự cố hoặc thảm họa tự nhiên quy mô lớn). Đây thường là yếu tố quan trọng cần cân nhắc khi triển khai các hệ thống và cơ sở hạ tầng lưu trữ, do ảnh hưởng trực tiếp đến tính sẵn sàng tổng thể của dữ liệu.

Khi xem xét khả năng phục hồi, lỗi của các thành phần riêng lẻ có thể chấp nhận được, nếu dịch vụ vẫn đang được cung cấp và tính toàn vẹn của dịch vụ đó vẫn còn. Tuy nhiên, khả năng phục hồi của một hệ thống lưu trữ hoặc cơ sở hạ tầng lưu trữ thường được xác định bởi thành phần kém phục hồi nhất trong hệ thống, và chi phí/hiệu suất hoặc các yếu tố khác có thể hạn chế mức độ khả năng phục hồi có thể hoặc thực tế.

Các kiểm soát liên quan đến khả năng phục hồi như sau:

TC-DSGN-G11 Giảm thiểu tác động đến khả năng phục hồi của lưu trữ

Cần giảm thiểu các tác động đến khả năng phục hồi phát sinh từ:

- việc không đưa bảo mật vào như một phần không thể thiếu của chiến lược phục hồi có tính đến lỗi thành phần, tấn công và xâm phạm cả công nghệ lưu trữ lẫn công nghệ bảo mật;
- không đủ dự phòng các thành phần lưu trữ;
- sử dụng không đầy đủ các thành phần đa dạng dễ sửa chữa;
- triển khai không phù hợp các tính năng và chức năng an toàn (ví dụ: mã hóa và xác thực tập trung) làm giảm khả năng phục hồi chung của hệ thống lưu trữ và cơ sở hạ tầng của nó.

10.2.3.4 Tính toàn vẹn

Tính toàn vẹn dữ liệu là tiêu chí thiết kế quan trọng hàng đầu đối với hầu hết các hệ thống và cơ sở hạ tầng lưu trữ, chỉ đứng sau tính sẵn sàng về mức độ ưu tiên đối với nhân viên quản lý lưu trữ. Dữ liệu được lưu trữ hoặc truyền qua mạng có thể bị hỏng do lỗi phần cứng hoặc phần mềm. Lỗi phần cứng cũng có thể gây ra hành vi sai lệch của phần mềm, dẫn đến thiệt hại nghiêm trọng cho dữ liệu. Lỗi trong phần mềm, chẳng hạn như trình điều khiển thiết bị, cũng có thể gây ra sửa đổi dữ liệu ngoài ý muốn. Mạng không đáng tin cậy có thể làm hỏng dữ liệu trong quá trình truyền.

Ngoài ra, thông tin quan trọng có thể bị sửa đổi bởi các chương trình độc hại hoặc người dùng độc hại, hoặc các thành phần hệ thống bị lỗi. Ví dụ, mã vi-rút có thể được chèn vào các tệp thực thi nhị phân, có khả năng dẫn đến mất tất cả dữ liệu được lưu trữ trên hệ thống. Các hệ điều hành cho phép truy cập vào đĩa thô có thể vô tình hỗ trợ kẻ tấn công bỏ qua kiểm tra an toàn trong hệ thống tệp và gây thiệt hại cho dữ liệu được lưu trữ.

Lỗi người dùng có thể làm tổn hại tính toàn vẹn dữ liệu ở cấp ứng dụng. Ví dụ, việc vô tình xóa một tệp quan trọng (ví dụ: tệp lược đồ cơ sở dữ liệu) có thể dẫn đến hỏng dữ liệu.

Các kiểm soát liên quan đến tính toàn vẹn như sau:

TC-DSGN-G12 Giảm thiểu tác động đến tính toàn vẹn dữ liệu

Để giải quyết các vấn đề về tính toàn vẹn dữ liệu, các tổ chức nên sử dụng các kỹ thuật đảm bảo tính toàn vẹn phổ biến, bao gồm sao chép hoặc nhân bản dữ liệu, RAID parity hoặc checksum. Các cơ chế đảm bảo tính toàn vẹn thực hiện các bước phòng ngừa để tránh các loại vi phạm tính toàn vẹn cụ thể (ví dụ: lưu trữ chỉ đọc và hệ thống tệp ghi nhật ký) hoặc có khả năng phục hồi sau khi phát hiện sự cố cũng nên được sử dụng.

10.2.4 Lưu giữ, bảo quản và thải bỏ dữ liệu

Lưu giữ tập trung vào việc duy trì hồ sơ theo các yêu cầu hồ sơ nhằm làm bằng chứng về chức năng, hoạt động hoặc giao dịch kinh doanh, bao gồm cách thức và thời gian cần lưu giữ. Bảo quản, mặt khác, tập trung vào các biện pháp đảm bảo khả năng sử dụng, tính xác thực, độ tin cậy và tính toàn vẹn của hồ sơ theo thời gian. Hai thuật ngữ "lưu giữ" và "bảo quản" thường bị dùng lẫn lộn không chính xác, dẫn đến các yêu cầu hồ sơ mâu thuẫn và xung đột về cách duy trì cùng một thông tin, thời gian lưu giữ và phương thức bảo vệ.

Các kiểm soát liên quan đến việc lưu giữ, bảo quản và thải bỏ dữ liệu như sau:

a) TC-DSGN-G13 Đảm bảo lưu giữ và bảo quản dữ liệu

Các tổ chức có nghĩa vụ lưu giữ và bảo quản dữ liệu nên lưu trữ dữ liệu theo cách chặn việc tiêu hủy hoặc thay đổi hồ sơ (tức là bất biến) cùng với xác minh tính toàn vẹn (ví dụ: băm) và thực thi các khoảng thời gian lưu giữ rõ ràng (ví dụ: giữ pháp lý). Để đáp ứng các yêu cầu về tính bất biến (không thể chỉnh sửa), các tổ chức nên sử dụng lưu trữ dựa trên WORM (ghi một lần đọc nhiều lần) hoặc triển khai lưu trữ dựa trên đối tượng (xem 10.12) kết hợp WORM với siêu dữ liệu có thể được sử dụng để thực hiện kiểm tra tính toàn vẹn rõ ràng cũng như thực thi việc hết hạn dữ liệu.

b) TC-DSGN-G14 Đảm bảo thải bỏ dữ liệu đúng cách

Trong các khuôn khổ quản lý hồ sơ và thông tin phổ biến (xem CHÚ THÍCH 1 bên dưới), định đoạt (disposition) là giai đoạn cuối cùng trong vòng đời của hồ sơ. Trong các khuôn khổ này, định đoạt không nhất thiết có nghĩa là tiêu hủy hồ sơ, mà là chuyển đến kho lưu trữ (xem 10.15). Trong trường hợp sau, điều này có thể chỉ đơn giản là trì hoãn thời điểm xảy ra việc tiêu hủy hồ sơ đối với hầu hết các hồ sơ

(rất ít hồ sơ ngoài chính phủ nên được lưu giữ vô thời hạn). Khi hồ sơ (dữ liệu) không còn cần thiết, việc tiêu hủy dữ liệu trở thành một thành phần quan trọng và thường cần thiết của một chương trình quản trị dữ liệu hiệu quả. Các tổ chức nên sử dụng một quy trình tiêu hủy dữ liệu loại bỏ thông tin theo cách làm cho nó không thể đọc được đối với hồ sơ giấy hoặc không thể truy xuất được đối với hồ sơ số (xem CHÚ THÍCH 2 bên dưới). Trong trường hợp sau, các kỹ thuật làm sạch lưu trữ (xem 10.6) thường được sử dụng.

CHÚ THÍCH 1: ISO 15489-1 là một trong nhiều khuôn khổ để lập kế hoạch và triển khai chương trình quản lý hồ sơ.

CHÚ THÍCH 2: Trong thế giới số, việc làm cho dữ liệu không thể truy xuất được được cảnh báo đến một mức độ nỗ lực cụ thể để truy xuất nó.

10.3 An toàn hệ thống lưu trữ

10.3.1 Củng cố hệ thống

Tất cả các hệ điều hành, trình siêu giám sát và ứng dụng cần được củng cố trong bối cảnh sử dụng hệ thống lưu trữ. Ngoài hướng dẫn quản lý lỗ hổng kỹ thuật trong ISO/IEC 27002:2022, 8.8, còn có nhiều thực hành tốt nhất hiện hành cho các hệ điều hành khác nhau có thể được tham khảo tùy theo hệ điều hành đang sử dụng. Trong các hệ thống lưu trữ, hệ điều hành tồn tại trong nhiều loại thiết bị (ví dụ: mảng lưu trữ, bộ chuyển mạch SAN, thiết bị ảo hóa, thiết bị sao lưu và lưu trữ). Các thiết bị cấp thấp hơn (ví dụ: HBA, bộ điều khiển lưu trữ, bộ điều hợp mạng) cũng cần cập nhật phần mềm và phần sụn định kỳ. Một số tính năng an toàn của hệ điều hành lưu trữ không được bật theo mặc định, và việc bảo trì, cập nhật định kỳ có thể vô tình xóa các thiết lập củng cố đã được quản trị viên lưu trữ thực hiện trước đó.

Các kiểm soát liên quan đến củng cố hệ thống như sau:

a) TC-HARD-G01 Thực hiện củng cố hệ điều hành cơ bản

Là một phần của thực hành vệ sinh bảo mật (security hygiene) hệ thống lưu trữ, các tổ chức nên:

- loại bỏ phần mềm, dịch vụ và giao thức không cần thiết/không sử dụng;
- loại bỏ các tài khoản không cần thiết;
- đổi tên hoặc vô hiệu hóa các tài khoản được xác định trước hoặc mặc định khi có thể cũng như thay đổi tất cả mật khẩu mặc định;
- chỉ mở các cổng mạng cần thiết;
- cài đặt các bản vá mới nhất từ một nguồn đáng tin cậy;
- cập nhật phần sụn từ một nguồn đáng tin cậy;
- cài đặt và duy trì các biện pháp bảo vệ chống phần mềm độc hại (xem ISO/IEC 27002:2022, 8.7);
- áp dụng các cấu hình an toàn do nhà cung cấp đề xuất.

b) TC-HARD-G02 Sử dụng các bản cập nhật phần mềm và bản vá từ các nguồn đáng tin cậy

Khi các yếu tố của cơ sở hạ tầng lưu trữ nhận được bản cập nhật (ví dụ: phần sụn) hoặc bản vá, nên có một số đảm bảo rằng phần mềm sẽ được áp dụng là từ một nguồn đáng tin cậy. Nếu không, những kẻ tấn công có thể viết bản cập nhật của riêng chúng thay vào đó chứa mã độc hại mà chúng chọn, chẳng hạn như rootkit, botnet hoặc phần mềm độc hại khác.

10.3.2 Kiểm toán, thống kê sự kiện và giám sát bảo mật

Các quy định tuân thủ và điều khoản hợp đồng thường bao gồm các yêu cầu về giám sát và báo cáo. Ghi nhật ký sự kiện và kiểm toán hệ thống là những năng lực chính để đáp ứng các yêu cầu này. Trong

hai loại trên, ghi nhật ký sự kiện có lẽ hữu ích hơn từ góc độ bảo mật lưu trữ vì có thể sử dụng cả trong thời gian thực lẫn trong điều tra sự cố. Trong các hệ thống và cơ sở hạ tầng lưu trữ, có nhiều loại giao dịch và sự kiện có thể tạo ra các hồ sơ nhật ký sự kiện thông qua cơ chế ghi nhật ký. Từ góc độ an toàn hoặc tuân thủ, điều quan trọng là phải ghi nhận đầy đủ các hồ sơ nhật ký cần thiết nhằm: chứng minh bằng chứng về hoạt động (ví dụ: mã hóa và lưu giữ), thực thi trách nhiệm giải trình và khả năng truy xuất nguồn gốc, đáp ứng các yêu cầu chứng cứ, và giám sát hệ thống hiệu quả. Tập hợp con này của ghi nhật ký sự kiện nói chung thường được gọi là ghi nhật ký kiểm toán.

Không phải mọi hồ sơ nhật ký sự kiện đều có giá trị như nhau — một số chỉ hữu ích cho mục đích gỡ lỗi, theo dõi tình trạng hệ thống, hoặc cảnh báo về các sự cố cấu hình nhỏ, v.v. Từ góc độ ghi nhật ký kiểm toán, các sự kiện quản lý (tức là hành động của người dùng) luôn là đối tượng quan tâm hàng đầu; các sự kiện truy cập dữ liệu thường ít được quan tâm hơn (trừ khi các tệp và thư mục quan trọng được theo dõi chặt chẽ); còn các sự kiện kiểm soát thường được quan tâm ít nhất — mặc dù chúng có thể cung cấp thông tin hữu ích trong quá trình phân tích nguyên nhân gốc rễ sau một sự cố.

Ngoài ra, ghi nhật ký kiểm toán thường yêu cầu các mục nhập sự kiện quan tâm phải được xử lý khác biệt và tách biệt khỏi hầu hết các mục nhập nhật ký sự kiện khác do thiết bị tạo ra. Việc xử lý đặc biệt này có thể được thực hiện bằng cách cho các thiết bị gửi các mục nhập nhật ký kiểm toán đến cơ sở hạ tầng nhật ký đặc biệt hoặc chúng có thể được chọn lọc ra khỏi luồng nhật ký chung, sử dụng cơ chế lọc nhật ký (một cách tiếp cận thách thức hơn vì nó yêu cầu tất cả các mục nhập sự kiện quan tâm phải được biết trước). Một khía cạnh khác của việc xử lý đặc biệt này là một tổ chức thường được yêu cầu chứng minh rằng họ đang giám sát (ví dụ: tạo cảnh báo cho các sự kiện bất thường) và báo cáo; những hành động này thường yêu cầu một số dạng cơ sở hạ tầng ghi nhật ký tập trung ngoài các bộ thu thập đơn giản.

Các yêu cầu và hướng dẫn về kiểm toán, thống kê sự kiện và giám sát bảo mật sau đây áp dụng cho các hệ thống lưu trữ:

a) TC-HARD-R01 Thực hiện ghi nhật ký trên lưu trữ

Thực hiện ghi nhật ký trên lưu trữ, cụ thể:

- ghi nhật ký phải được bật trên các hệ thống và thiết bị lưu trữ nếu có thể;
- các hệ thống và thiết bị lưu trữ phải sử dụng ghi nhật ký sự kiện bên ngoài hoặc tập trung và có thể sử dụng ghi nhật ký cục bộ;
- một nguồn thời gian chung, chính xác phải được sử dụng trên toàn môi trường để đảm bảo rằng các hồ sơ sự kiện từ các nguồn khác nhau có thể được tương quan;
- nếu có thể, các hệ thống và thiết bị lưu trữ phải ghi nhật ký sự kiện nguyên bản bằng các giao thức ghi nhật ký tiêu chuẩn như syslog hỗ trợ phân phối đáng tin cậy và vận chuyển an toàn (ví dụ: TLS);

CHÚ THÍCH 1: Syslog được định nghĩa trong IETF RFC 5424 với các chi tiết bổ sung có trong IETF RFC 3195, IETF RFC 5425, IETF RFC 5426, IETF RFC 5427, IETF RFC 5848, IETF RFC 6012 và IETF RFC 6587.

- ghi nhật ký sự kiện bên ngoài hoặc tập trung nên được sử dụng với một nguồn từ xa đáng tin cậy;

CHÚ THÍCH 2: Nguồn ghi nhật ký sự kiện bên ngoài đáng tin cậy là một sản phẩm quản lý an toàn CNTT-TT nằm trong vùng hoặc miền an toàn chuyên dụng và được giả định là thực thi chính xác các chức năng an toàn của nó.

- việc sử dụng nhật ký thiết bị cho bất cứ điều gì khác ngoài giám sát sức khỏe hệ thống và gỡ lỗi nên được tránh vì nhật ký lưu trên thiết bị dễ bị giả mạo hoặc tiêu hủy hơn, có không gian lưu trữ hạn chế cho nhật ký và chúng loại trừ việc sử dụng phân tích, cảnh báo và lưu trữ tự động tập trung;
- các hệ thống và thiết bị lưu trữ nên sử dụng nhiều máy chủ nhật ký bên ngoài;

CHÚ THÍCH 3: Một số giao thức ghi nhật ký sử dụng các giao thức mạng không đáng tin cậy như Giao thức Gói dữ liệu Người dùng (UDP) và do đó các thông điệp nhật ký có thể bị mất do hiệu suất mạng hoặc máy chủ. Gửi thông điệp đến nhiều đích nhật ký giúp giảm nguy cơ mất mát vô tình.

– các hệ thống và thiết bị lưu trữ nên được cấu hình để ghi nhật ký các sự kiện khi chúng xảy ra (tức là không có bộ đệm) khi các yếu tố thúc đẩy chính cho ghi nhật ký kiểm toán là tuân thủ, trách nhiệm giải trình hoặc an toàn.

b) TC-HARD-G03 Đảm bảo tính đầy đủ của ghi nhật ký kiểm toán lưu trữ

Tính hữu ích của việc ghi nhật ký sự kiện phần nào phụ thuộc vào thông tin được ghi lại (ví dụ: dấu thời gian, nguồn, loại sự kiện, v.v.).

Đối với các hệ thống lưu trữ, việc đảm bảo tính đầy đủ của các mục nhập nhật ký kiểm toán bao gồm:

– sau khi các loại sự kiện cần ghi nhật ký đã được xác định, thì tất cả các lần xuất hiện của các sự kiện này nên được ghi nhật ký một cách nhất quán (dù là trong băng hay ngoài băng);
– các loại sự kiện sau đây nên được ghi nhật ký (một bộ sự kiện an toàn tối thiểu):

+ các lần đăng nhập thất bại và thành công;

+ các lần truy cập tệp và đối tượng thất bại đối với dữ liệu nhạy cảm và có giá trị cao;

+ thêm, thay đổi và xóa hồ sơ tài khoản và nhóm;

+ thay đổi cấu hình an toàn hệ thống (ví dụ: ghi nhật ký kiểm toán, lọc mạng, thay đổi phân vùng);

+ thay đổi việc sử dụng máy chủ an toàn (ví dụ: syslog, Giao thức Thời gian Mạng hoặc NTP, Hệ thống Tên Miền hoặc DNS, xác thực);

+ tắt và khởi động lại hệ thống;

+ các hoạt động đặc quyền (tức là các thay đổi do quản trị viên khởi tạo);

+ sử dụng các tiện ích nhạy cảm (ví dụ: lệnh leo thang đặc quyền);

+ truy cập vào các tệp dữ liệu quan trọng;

+ di chuyển máy chủ ảo giữa các máy chủ vật lý.

– mỗi mục nhập nhật ký nên bao gồm:

+ dấu thời gian (ngày và giờ);

+ mức độ nghiêm trọng;

+ nguồn của mục nhập nhật ký (tên phân biệt, địa chỉ IP, v.v.);

+ ID sự kiện cũng như mô tả văn bản (cần thiết để cho phép bản địa hóa/quốc tế hóa các sự kiện, trong đó ID sự kiện vẫn giữ nguyên nhưng mô tả văn bản có thể được dịch sang các ngôn ngữ khác nhau);

+ mô tả sự kiện.

c) TC-HARD-G04 Thực hiện giám sát lưu trữ thích hợp

Thực hiện giám sát thích hợp, cụ thể:

- việc sử dụng cẩn thận bộ lọc (ví dụ: trên các trường như mức độ nghiêm trọng) tuân thủ chính sách ghi nhật ký nên được sử dụng bởi các hệ thống lưu trữ và cơ sở hạ tầng nhật ký kiểm toán;
- một giao thức phân tích nên được triển khai để tương quan các hồ sơ nhật ký kiểm toán trên các nguồn sự kiện để xác định các sự kiện an toàn quan trọng cung cấp dấu hiệu về các sự cố an toàn;
- việc ghi nhật ký lưu trữ nên được bao gồm trong các giải pháp quản lý sự kiện và thông tin an toàn, khi công nghệ đó được triển khai;
- các hệ thống và thiết bị lưu trữ nên được bao gồm trong các giải pháp giám sát liên tục an toàn thông tin (ISCM), khi công nghệ đó được triển khai.

d) TC-HARD-G05 Sử dụng lưu giữ và bảo vệ nhật ký cho lưu trữ

Thực hiện lưu giữ và bảo vệ thích hợp, cụ thể:

- dữ liệu nhật ký kiểm toán có thể có giá trị chứng cứ nên được xử lý đúng cách (tức là duy trì chuỗi hành trình, và tính toàn vẹn và xác thực có thể kiểm chứng);
- dữ liệu nhật ký kiểm toán có yêu cầu lưu giữ cụ thể (ví dụ: để tuân thủ quy định) nên được bảo quản bằng giải pháp lưu giữ dữ liệu của tổ chức;
- các biện pháp thích hợp để bảo toàn tính toàn vẹn của nhật ký và ngăn chặn việc sửa đổi hoặc tiêu hủy chúng (dù là độc hại hay vô tình) nên được thực hiện;
- khi các mục nhập nhật ký kiểm toán chứa thông tin nhạy cảm, dữ liệu nhật ký kiểm toán nên được bảo vệ bằng các cơ chế bảo đảm tính bí mật thích hợp;

CHÚ THÍCH 4: Một số mục nhập nhật ký có thể làm lộ những thứ như mật khẩu (ví dụ: khi người dùng nhập mật khẩu thay vì ID người dùng), nhưng các sự cố tinh vi hơn cũng có thể tồn tại (ví dụ: lệnh tìm kiếm làm lộ tên cụ thể và các vấn đề sức khỏe).

- đối với các yêu cầu ghi nhật ký kiểm toán duy nhất (ví dụ: khối lượng lớn, bảo quản đặc biệt và ký sự kiện) nên sử dụng các hệ thống chuyên dụng và được củng cố và cấu hình đặc biệt;
- chuyển tiếp nhật ký và lọc nhật ký nên được tận dụng để giảm thiểu tác động của các yêu cầu lưu trữ chuyên biệt (ví dụ: ghi một lần đọc nhiều lần (WORM)).

10.3.3 Quản lý lỗ hổng lưu trữ

ISO/IEC 27002:2022, 8.8, xác định tầm quan trọng của việc quản lý các lỗ hổng kỹ thuật cũng như cung cấp hướng dẫn cụ thể. Hướng dẫn này đề cập đến việc xác định, đánh giá và khắc phục các lỗ hổng kỹ thuật.

Các kiểm soát liên quan đến quản lý lỗ hổng lưu trữ như sau:

TC-HARD-G06 Bao gồm lưu trữ trong các chương trình quản lý lỗ hổng

Do tính chất chuyên biệt của các công nghệ lưu trữ, các hệ thống lưu trữ không phải lúc nào cũng được bao gồm trong chương trình quản lý lỗ hổng của tổ chức. Ngoài ra, nhiều công cụ được sử dụng để xác định lỗ hổng không cung cấp phạm vi bao phủ rộng rãi cho các hệ điều hành và ứng dụng lưu trữ. Các tổ chức nên bao gồm các hệ thống lưu trữ trong các chương trình quản lý lỗ hổng của họ.

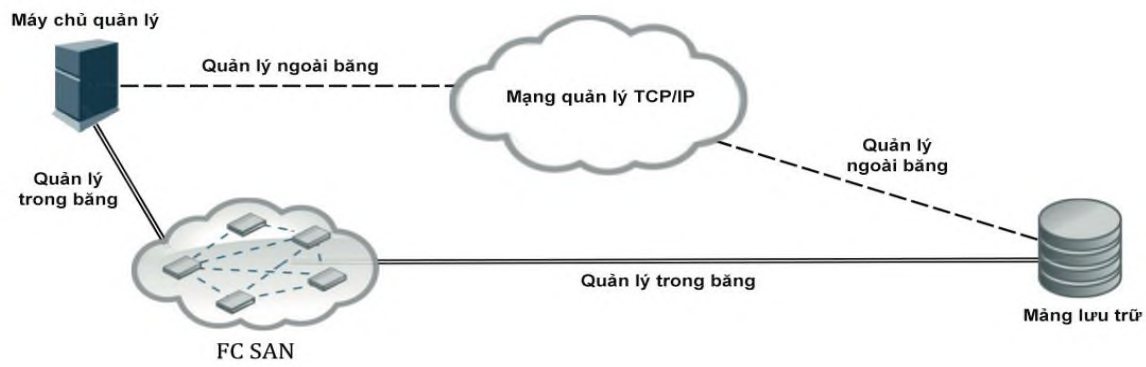
10.4 Quản lý lưu trữ

10.4.1 Bối cảnh

Mạng lưu trữ và các yếu tố cơ sở hạ tầng là các kiến trúc phức tạp có thể đặt ra các yêu cầu quản lý nghiêm ngặt đối với quản trị viên. Để giải quyết những yêu cầu này, các tổ chức triển khai các công cụ

và quy trình quản lý cơ sở hạ tầng lưu trữ để đảm bảo tính sẵn sàng và hiệu suất của tất cả các thiết bị lưu trữ, bảo vệ và bảo mật dữ liệu tốt hơn, kiểm toán tập trung và đáp ứng các nghĩa vụ tuân thủ.

Các hệ thống lưu trữ có thể được quản lý bằng các cơ chế trong băng hoặc ngoài băng (xem Hình 2). Trong bối cảnh này, quản lý trong băng thường có nghĩa là hệ thống lưu trữ được quản lý thông qua đường dẫn mà dữ liệu người dùng được truyền qua. Lệnh quản lý lưu trữ được gửi qua kết nối đầu vào/đầu ra bằng SCSI gắn nối tiếp (SAS), Fibre Channel hoặc iSCSI (Internet SCSI), PCI Express®, v.v.. Mặt khác, quản lý ngoài băng sử dụng một đường dẫn thay thế, khác với đường dẫn được sử dụng bởi lưu lượng dữ liệu người dùng, để truy cập giao diện quản lý của hệ thống lưu trữ. Quản lý ngoài băng gửi lệnh qua kết nối mạng hoặc giao diện băng tần phụ. Chức năng quản lý và các cân nhắc về an toàn có thể khác nhau đáng kể giữa hai loại quản lý lưu trữ này, ngay cả khi cả hai đều có sẵn trên một hệ thống lưu trữ.



Hình 2 - Ví dụ quản lý lưu trữ

Tương tự như mô tả quản lý mạng trong TCVN 9801-2 (ISO/IEC 27033-2), quản lý lưu trữ cũng đề cập đến các hoạt động, phương pháp, thủ tục và công cụ áp dụng cho các hệ thống lưu trữ, chẳng hạn như:

- Vận hành giải quyết việc giữ cho lưu trữ (và các dịch vụ mà cơ sở hạ tầng lưu trữ cung cấp) hoạt động trơn tru. Hoạt động này bao gồm việc giám sát lưu trữ để phát hiện sự cố càng sớm càng tốt, lý tưởng nhất là trước khi người dùng bị ảnh hưởng;
- Quản trị giải quyết việc theo dõi các tài nguyên trong cơ sở hạ tầng lưu trữ và cách chúng được gán. Hoạt động này bao gồm tất cả các công việc nội bộ cần thiết để giữ cho lưu trữ được kiểm soát;
- Bảo trì liên quan đến việc thực hiện sửa chữa và nâng cấp, ví dụ: khi thiết bị được thay thế, khi phần sụn mảng lưu trữ được cập nhật, hoặc khi một bộ chuyển mạch mới được thêm vào mạng lưu trữ. Bảo trì cũng bao gồm các biện pháp khắc phục và phòng ngừa để làm cho lưu trữ hoạt động tốt hơn, chẳng hạn như điều chỉnh các tham số cấu hình thiết bị;
- Cấp phát giải quyết quy trình xác định tài sản lưu trữ sẽ được gán cho một máy chủ;
- Làm sạch (xem 10.6) giải quyết việc bảo vệ tính bí mật của dữ liệu còn lại trên phương tiện lưu trữ khi nó bị loại khỏi dịch vụ hoặc được tái sử dụng bằng cách làm cho dữ liệu không thể truy xuất được.

Việc thực hiện các hoạt động quản lý lưu trữ này một cách an toàn đòi hỏi các kiểm soát liên quan đến xác thực và ủy quyền (xem 10.4.2), bảo vệ giao diện quản lý lưu trữ (xem 10.4.3), duy trì trách nhiệm giải trình và truy xuất nguồn gốc của hệ thống và người dùng (xem 10.3.2), và đảm bảo các hệ thống cơ bản được sử dụng để quản lý lưu trữ được củng cố đầy đủ (xem 10.3.1).

10.4.2 Xác thực và ủy quyền

10.4.2.1 Xác thực

Các cá nhân quản lý hệ thống và cơ sở hạ tầng lưu trữ thường là người dùng đặc quyền. Việc sử dụng không phù hợp các đặc quyền quản trị hệ thống (bất kỳ tính năng hoặc cơ sở nào của hệ thống thông tin cho phép người dùng ghi đè các kiểm soát hệ thống hoặc ứng dụng) có thể là một yếu tố đóng góp chính vào sự thất bại hoặc xâm phạm hệ thống. Để giúp giảm thiểu những rủi ro này, có thể sử dụng các thủ tục đăng nhập an toàn như được mô tả trong ISO/IEC 27002:2022, 8.5 cùng với các biện pháp xác thực bổ sung khi cần thiết.

Các kiểm soát liên quan đến xác thực như sau:

a) TC-MGMT-R01 Biện pháp xác thực người dùng tối thiểu

Quản lý lưu trữ thường liên quan đến các hoạt động đặc quyền được thực hiện bởi những người dùng có mức xác thực tối thiểu bao gồm:

- tất cả người dùng phải có một định danh duy nhất (ID người dùng) chỉ dành cho mục đích sử dụng cá nhân của họ;
- để chứng minh danh tính đã khai báo của người dùng, một trong các kỹ thuật xác thực phù hợp sau đây phải được sử dụng:

  + mật khẩu có độ phức tạp và bí mật đủ để kẻ tấn công không thể đoán hoặc khám phá bằng cách khác;

  + xác thực mạnh (ví dụ: giao thức thách thức-phản hồi); hoặc

  + xác thực đa yếu tố, chẳng hạn như dữ liệu sinh trắc học (ví dụ: xác minh vân tay hoặc quét võng mạc) và sử dụng mã thông báo phần cứng (ví dụ: thẻ thông minh).

- tất cả truy cập từ xa phải sử dụng xác thực mạnh hoặc xác thực đa yếu tố cùng với các kênh an toàn.

b) TC-MGMT-G01 Sử dụng các giải pháp xác thực tập trung

Một giải pháp xác thực tập trung, chẳng hạn như Dịch vụ Người dùng Quay số Xác thực Từ xa (RADIUS), đăng nhập một lần, Ủy quyền Mở (OAuth), Ngôn ngữ Đánh dấu Khẳng định Bảo mật (SAML), v.v. nên được sử dụng để cải thiện việc giám sát và kiểm soát.

c) TC-MGMT-G02 Sử dụng xác thực đa yếu tố

Xác thực đa yếu tố nên được sử dụng khi quản lý dữ liệu nhạy cảm và có giá trị cao.

d) TC-MGMT-G03 Vô hiệu hóa đăng nhập vào tài khoản root hoặc admin

Việc đăng nhập vào tài khoản root hoặc admin nên được vô hiệu hóa.

e) TC-MGMT-G04 Ghi nhật ký từ xa tất cả các hoạt động leo thang đặc quyền

Tất cả các hoạt động leo thang đặc quyền nên được ghi nhật ký từ xa.

f) TC-MGMT-G05 Sử dụng các cơ chế xác thực thực thể

Ngoài xác thực người dùng, các hệ thống lưu trữ đôi khi sử dụng xác thực thực thể, là quá trình mà một tác nhân trong hệ thống phân tán có được sự tin cậy vào danh tính của đối tác truyền thông. Xác thực thực thể này có thể diễn ra trong các kết nối Transport Layer Security (TLS) và IPsec cũng như trong các giao thức lưu trữ như Giao thức Xác thực Bắt tay Thách thức (CHAP) với iSCSI, Giao thức Xác thực Bắt tay Thách thức Diffie-Hellman (DH-CHAP) trong FCP, v.v.. Khi có thể, các cơ chế xác thực thực thể này nên được sử dụng.

10.4.2.2 Ủy quyền và kiểm soát truy cập

Trong các lĩnh vực thị trường như dịch vụ tài chính và chăm sóc sức khỏe, có xu hướng điều chỉnh ủy quyền và kiểm soát truy cập theo nguyên tắc đặc quyền tối thiểu bằng cách tận dụng các vai trò cụ thể.

Các kiểm soát liên quan đến ủy quyền và kiểm soát truy cập như sau:

TC-MGMT-G06 Tách biệt vai trò an toàn và phi an toàn

Các vai trò sau đây nên được triển khai và sử dụng trong các công nghệ lưu trữ:

- Quản trị viên bảo mật. Vai trò này có quyền chỉ đọc/xem và sửa đổi để thiết lập và quản lý tài khoản, tạo và liên kết vai trò/quyền, cho cấu hình và nội dung ghi nhật ký kiểm toán (các mục nhập nhật ký sự kiện kiểm toán không bao giờ có thể thay đổi), thiết lập mối quan hệ tin cậy với cơ sở hạ tầng CNTT (ví dụ: bí mật chia sẻ cho RADIUS), quản lý kho chứng chỉ và khóa, quản lý mã hóa và quản lý khóa, và đặt kiểm soát truy cập;
- Quản trị viên Lưu trữ. Vai trò này có quyền xem và sửa đổi đối với tất cả các khía cạnh của hệ thống lưu trữ ngoại trừ các yếu tố hoặc dữ liệu liên quan đến an toàn (tức là những yếu tố được bao phủ bởi quản trị viên an toàn);
- Kiểm toán viên bảo mật. Vai trò này có quyền xem cho phép xem xét quyền hạn, xác minh các tham số và cấu hình an toàn, và kiểm tra nhật ký kiểm toán. Không cấp quyền truy cập vào lưu trữ, cấu hình hoặc dữ liệu;
- Kiểm toán viên Lưu trữ. Vai trò này có quyền xem cho phép xác minh các tham số và cấu hình lưu trữ và kiểm tra nhật ký sức khỏe/lỗi. Không cấp quyền truy cập vào các yếu tố hoặc dữ liệu liên quan đến an toàn.

Mỗi giao dịch quản lý lưu trữ nên được liên kết với một vai trò an toàn hoặc lưu trữ. Các vai trò này có thể là các kiểm soát quan trọng để đảm bảo phân tách nhiệm vụ đối với các khả năng quản lý.

10.4.3 Bảo mật giao diện quản lý

Ngoài các giao diện vật lý (xem 9.3), các hệ thống lưu trữ sử dụng nhiều loại phần mềm và phần sụn để cho phép quản lý hệ thống lưu trữ. Các giao diện phần mềm này có thể bao gồm giao diện dòng lệnh đơn giản (CLI), giao diện dựa trên Web, bao gồm giao diện người dùng đồ họa hoặc giao diện lập trình ứng dụng (API) REST, hỗ trợ Giao thức Quản lý Mạng Đơn giản (SNMP), và các proxy dựa trên máy chủ xử lý quản lý trong băng (tức là qua đường dẫn dữ liệu).

Các kiểm soát liên quan đến việc bảo mật giao diện quản lý như sau:

a) TC-MGMT-G07 Bảo mật giao diện mạng đến phần mềm/phần sụn quản lý

Giao diện phần mềm/phần sụn quản lý lưu trữ thường được bảo mật bằng những cách sau:

- tường lửa và trình bao bọc TCP nên được sử dụng để hạn chế quyền truy cập vào mạng quản lý đối với các hệ thống và giao thức được ủy quyền;
- xác thực thực thể nên được sử dụng để thiết lập mối quan hệ tin cậy giữa các hệ thống lưu trữ và hệ thống quản lý (ví dụ: sử dụng FC-SP-2 AUTH-A1 để xác thực các thực thể thực hiện quản lý trong băng);
- cơ chế hệ thống phát hiện xâm nhập và hệ thống ngăn chặn xâm nhập nên được tận dụng để xác định các hành vi bất thường và bảo vệ chống lại chúng;
- cơ sở hạ tầng CNTT-TT như Hệ thống Tên Miền (DNS), Giao thức Định vị Dịch vụ (SLP), hoặc Giao thức Thời gian Mạng (NTP) nên được sử dụng với các kiểm soát an toàn thích hợp để tránh các cuộc tấn công gián tiếp;

- các kiểm soát người dùng đặc quyền thích hợp, bao gồm xác thực (xem 10.4.2.1), ủy quyền (xem 10.4.2.2), và kiểm toán/giám sát an toàn (xem 10.3.2) nên được sử dụng;
- hệ điều hành và ứng dụng nên được cập nhật và củng cố đủ mạnh chống lại các cuộc tấn công (xem 10.3.1).

b) TC-MGMT-R02 Bảo mật quản lý từ xa

Khi các hệ thống lưu trữ được quản lý từ xa, các biện pháp an toàn bổ sung sau đây phải được sử dụng:

- sử dụng các kênh an toàn như mạng riêng ảo (VPN), TLS, Secure Shell (SSH), hoặc Giao thức Truyền Siêu văn bản An toàn (HTTPS) cho tất cả truy cập từ xa;
- sử dụng xác thực mạnh hoặc xác thực đa yếu tố;
- hạn chế đặc quyền ở mức tối thiểu cần thiết (tức là đặc quyền tối thiểu).

Tổ chức nên xây dựng các kiểm soát tổ chức và kỹ thuật để hạn chế giao diện quản lý được sử dụng cho các phiên bảo trì từ xa (không cục bộ) của nhà cung cấp. Các hoạt động bảo trì từ xa của nhà cung cấp được thực hiện bởi các cá nhân giao tiếp thông qua mạng bên ngoài như internet gây ra rủi ro đáng kể cho tính sẵn sàng, tính toàn vẹn và tính bí mật.

c) TC-MGMT-R03 Hạn chế quản lý từ xa của nhà cung cấp

Các kiểm soát kỹ thuật phải hạn chế lưu lượng truyền thông (tức là hệ thống, cổng và giao thức) ở mức tối thiểu cần thiết cho các hoạt động bảo trì từ xa của nhà cung cấp. Sau khi bên truy cập được xác thực, các kiểm soát bổ sung tại điểm truy cập nên được xây dựng để ủy quyền cho phiên bảo trì của nhà cung cấp. Chúng bao gồm việc chấp nhận, yêu cầu phê duyệt hoặc từ chối phiên được yêu cầu. Các nhật ký thích hợp chứa các hồ sơ kiểm toán về hành động của nhà cung cấp phải được tạo ra.

d) TC-MGMT-R04 Hạn chế sử dụng truy cập quay số

Tổ chức phải hạn chế các đường truy cập quay số đối với các bên truy cập được ủy quyền. Điều này bao gồm việc thực thi giao thức gọi lại modem và vô hiệu hóa việc thiết lập kết nối cho đến khi nhà cung cấp yêu cầu một phiên bảo trì và yêu cầu đó được tổ chức ủy quyền.

e) TC-MGMT-R05 Bảo mật IPMI

Một số hệ thống lưu trữ bao gồm các hệ thống quản lý nền tảng dựa trên phần cứng giúp có thể kiểm soát và giám sát các hệ thống một cách tập trung, bao gồm khả năng quản lý máy chủ ở các vị trí vật lý từ xa bất kể hệ điều hành được cài đặt. Phần mềm này không yêu cầu quyền từ hệ điều hành của hệ thống lưu trữ vì nó chạy trên phần cứng riêng biệt được gắn vào bo mạch chủ hoặc máy chủ.

Trong một số triển khai, bộ điều khiển quản lý bo mạch chủ (BMC) nằm giữa các cảm biến và giao diện trên bo mạch và các giao diện truyền thông ngoài băng như Ethernet. Giao diện Quản lý Nền tảng Thông minh (IPMI) giải quyết một loạt các giao diện, bao gồm cả BMC, cung cấp quyền truy cập cấp thấp vào một hệ thống có thể ghi đè các kiểm soát hệ điều hành. Thông điệp IPMI có thể được truyền đến và đi từ BMC trong các gói dữ liệu UDP Giao thức Kiểm soát Quản lý Từ xa (RMCP) (cổng đích UDP 623 cho asf-rmcp) được đóng gói. Chức năng này còn được gọi là "IPMI-qua-LAN". IPMI cũng định nghĩa các cài đặt cấu hình cụ thể cho LAN, hơi giống với các cài đặt cho địa chỉ IP. Một định dạng gói bổ sung (RMCP+) cũng đã được định nghĩa trong IPMI 2.0. RMCP+ hỗ trợ truyền dữ liệu được mã hóa ngoài các phần mở rộng khác nhau để xác thực.

Khi IPMI được sử dụng, các biện pháp an toàn bổ sung sau đây là cần thiết:

- IPMI phải được vô hiệu hóa làm cài đặt cấu hình mặc định và IPMI chỉ nên được bật tạm thời khi cần thiết;

- Lưu lượng IPMI (thường là cổng UDP 623) phải được hạn chế đối với các mạng nội bộ đáng tin cậy như một phân đoạn VLAN quản lý với các kiểm soát mạng mạnh mẽ;
- Mật khẩu mạnh, duy nhất phải được đặt và sử dụng cho dịch vụ IPMI trên các thiết bị chạy IPMI;
- Mã hóa nên được bật trên IPMI (ví dụ: với các giao thức RMCP hoặc RMCP+), nếu có thể;
- "Cipher 0" (được bật theo mặc định trên nhiều thiết bị hỗ trợ IPMI) và đăng nhập ẩn danh phải được vô hiệu hóa để ngăn kẻ tấn công bỏ qua xác thực và gửi các lệnh IPMI tùy ý;
- Mật khẩu được lưu trữ phải được loại bỏ khi hết vòng đời của hệ thống.

10.5 Tính bí mật dữ liệu

10.5.1 Tổng quát

Trong cơ sở hạ tầng lưu trữ, tính bí mật dữ liệu thường được duy trì bằng một phương pháp mã hóa nào đó. Các phương pháp này chủ yếu liên quan đến việc bảo vệ dữ liệu khi đang được truyền (đôi khi gọi là dữ liệu đang truyền hoặc dữ liệu động) trong cơ sở hạ tầng lưu trữ, hoặc khi đang được lưu giữ (dữ liệu tĩnh) trong thiết bị hoặc trên phương tiện lưu trữ.

Quá trình mã hóa là vấn đề áp dụng một thuật toán mã hóa (hoặc mật mã) cho dữ liệu bản rõ tạo ra dữ liệu được mã hóa (hoặc bản mã). Ngược lại, giải mã biến đổi bản mã trở lại thành bản rõ ban đầu của nó. Định nghĩa và đặc tả của nhiều mật mã quan trọng liên quan đến lưu trữ có thể được tìm thấy trong loạt TCVN 11367 (ISO/IEC 18033), NIST FIPS 197 và IEEE 1619.2-2021. Đối với một số loại mật mã (ví dụ: mật mã khối n-bit), có nhiều cách (được gọi là chế độ hoạt động) trong đó mật mã có thể được sử dụng để mã hóa bản rõ. Định nghĩa và đặc tả của các chế độ hoạt động phổ biến có thể được tìm thấy trong TCVN 12213 (ISO/IEC 10116), NIST Special Publication 800-38A, NIST Special Publication 800-38C, NIST Special Publication 800-38D, NIST Special Publication 800-38E và IEEE 1619-2018.

Mật mã hoạt động kết hợp với một khóa và có thể cả nguyên liệu khóa khác (ví dụ: vectơ khởi tạo). Trong mật mã đối xứng, cùng một khóa được sử dụng với cả thuật toán mã hóa và giải mã. Trong mật mã bất đối xứng, các khóa khác nhau nhưng có liên quan được sử dụng để mã hóa và giải mã. Việc quản lý và bảo vệ khóa (được gọi là quản lý khóa) cực kỳ quan trọng trong việc duy trì tính bí mật dữ liệu.

Mục đích của quản lý khóa là cung cấp các thủ tục để xử lý nguyên liệu khóa mật mã được sử dụng với các cơ chế mật mã đối xứng hoặc bất đối xứng. Định nghĩa và đặc tả các khía cạnh khác nhau của quản lý khóa có thể được tìm thấy trong loạt TCVN 7817 (ISO/IEC 11770) và NIST Special Publication

10.5.2 Các vấn đề về mã hóa và quản lý khóa

Việc sử dụng công nghệ mật mã gây ra một số vấn đề nhất định không thể bỏ qua. Việc không giải quyết các vấn đề này có thể khiến một tổ chức phải chịu các hình phạt theo quy định cũng như gây ra tổn thất thảm khốc trong một số điều kiện nhất định.

Các kiểm soát liên quan đến mã hóa và quản lý khóa như sau:

a) TC-CNFD-G01 Tuân thủ quy định nhập/xuất khẩu đối với mật mã

Các công nghệ mật mã có thể có các quy định nghiêm ngặt chi phối việc nhập/xuất khẩu công nghệ. Để tránh các vấn đề, các tổ chức dự kiến sẽ:

- hiểu và tuân thủ các quy định nhập khẩu của chính phủ liên quan đến mã hóa và quản lý khóa;
- hiểu và tuân thủ các quy định xuất khẩu của chính phủ liên quan đến mã hóa và quản lý khóa.

b) TC-CNFD-G02 Tuân thủ các yêu cầu ký gửi và tiết lộ khóa

Một số tổ chức sử dụng dịch vụ ủy thác khóa để quản lý quyền truy cập của bên thứ ba, bao gồm cả việc tiết lộ khóa bắt buộc, vào một số phần nhất định trong hệ thống của họ. Khi dịch vụ ủy thác khóa được sử dụng, mặc định rằng tổ chức sẽ:

- tuân thủ các yêu cầu ký gửi khóa của công ty hoặc chính phủ;
- hiểu và tuân theo bất kỳ yêu cầu nào của công ty hoặc chính phủ về việc cung cấp khóa mã hóa cho các quan chức công ty, cơ quan thực thi pháp luật, v.v. để cho phép truy cập và khôi phục dữ liệu được mã hóa.

c) TC-CNFD-G03 Lập kế hoạch cho các lỗi khóa

Việc mất hoặc hỏng khóa mã hóa có thể làm cho dữ liệu không thể sử dụng được, vì vậy các tổ chức thường có các điều khoản để bảo vệ khóa mã hóa của họ (ví dụ: sao lưu khóa của máy chủ quản lý khóa). Sao lưu khóa thường được triển khai trong bối cảnh của một giải pháp mã hóa/quản lý khóa cụ thể và tập trung vào việc cung cấp cho giải pháp quyền truy cập vào các khóa được sử dụng để mã hóa dữ liệu trong giải pháp.

Để đảm bảo có sự bảo vệ đầy đủ chống lại việc mất hoặc xâm phạm khóa, các tổ chức nên có:

- một kế hoạch phục hồi trong trường hợp mất hoặc xâm phạm khóa;
- một kế hoạch sao lưu khóa để đảm bảo quyền truy cập liên tục vào dữ liệu kinh doanh/nhiệm vụ quan trọng được mã hóa.

d) TC-CNFD-G04 Hạn chế tác động hoạt động của mật mã

Việc sử dụng mật mã, đặc biệt là mã hóa, có thể có tác động hoạt động có thể ảnh hưởng đến hiệu quả hoặc hiệu suất của cơ sở hạ tầng CNTT-TT.

Các tổ chức nên giảm thiểu những tác động này, bao gồm:

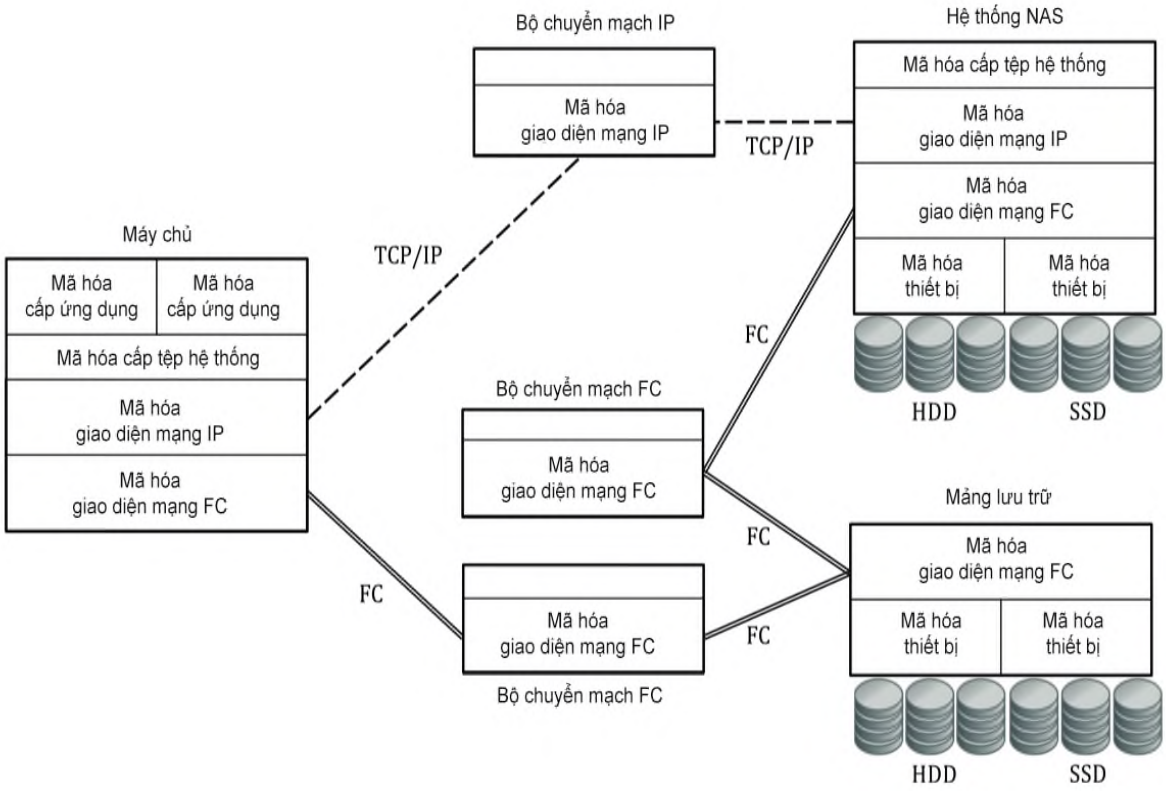
- sự suy giảm hiệu quả của các công nghệ ngăn chặn mất dữ liệu dựa trên mạng do sử dụng mã hóa đầu cuối trên truyền thông;
- sự gia tăng sử dụng mạng hoặc lưu trữ do không thể áp dụng các công nghệ giảm dữ liệu (kỹ thuật khử trùng lặp và nén) trên bản mã;
- việc không thể áp dụng quét phần mềm độc hại tập trung trên dữ liệu được mã hóa.

10.5.3 Mã hóa lưu trữ

Có nhiều cân nhắc cần giải quyết khi đánh giá việc triển khai giải pháp mã hóa dựa trên lưu trữ, bao gồm, nhưng không giới hạn ở:

- mã hóa có khả năng tác động đến các khía cạnh an toàn khác (ví dụ: kiểm tra dữ liệu và chống vi-rút);
- mã hóa mang rủi ro làm cho dữ liệu không khả dụng nếu có bất cứ điều gì sai sót xảy ra với việc xử lý dữ liệu, chuyển đổi dữ liệu, quản lý khóa hoặc mã hóa thực tế;
- mã hóa có thể yêu cầu tài nguyên tính toán không nhỏ;
- mã hóa có thể đòi hỏi quản lý khóa tập trung đặc biệt khi mã hóa được sử dụng kết hợp với sao chép ngoài khu vực cho mục đích BCM;
- mã hóa có thể làm giảm hoặc phủ nhận lợi ích của các công nghệ giảm dữ liệu (ví dụ: nén và khử trùng lặp) vì dữ liệu được mã hóa không dễ nén;
- chất lượng của mật mã (độ mạnh an toàn và các thuật toán được kiểm tra và chấp nhận trong ngành) có thể ảnh hưởng đến sự bảo vệ thực tế được cung cấp.

Không phải tất cả dữ liệu đều đáng để mã hóa. Đánh giá rủi ro có thể giúp xác định dữ liệu nhạy cảm và có giá trị cao cần sử dụng mã hóa cũng như hỗ trợ phân tích lợi ích chi phí (tức là liệu việc giảm rủi ro có đáng giá chi phí hay không). Điều quan trọng cần lưu ý là có các cơ chế khác để bảo vệ tính bí mật của dữ liệu khi dữ liệu được coi là tài sản quan trọng.



Hình 3 - Ví dụ về các điểm mã hóa

Bảo vệ dữ liệu đang truyền thường đòi hỏi hai hoặc nhiều thực thể thiết lập một kênh mã hóa để truyền dữ liệu (xem 10.5.4). Kết nối này thường mang tính tạm thời và các thông số an toàn thường được thỏa thuận mỗi khi cần thiết.

Việc bảo vệ dữ liệu tĩnh (xem 10.5.5) thường liên quan đến một điểm duy nhất trong đường dẫn dữ liệu (điểm mã hóa) được sử dụng để mã hóa/giải mã dữ liệu. Điểm mã hóa rất quan trọng vì nó đại diện cho vị trí trong đường dẫn dữ liệu nơi dữ liệu được mã hóa (bản mã) và nơi nó có thể sử dụng được (dạng rõ). Một quan điểm an toàn phổ biến là mã hóa càng gần nguồn hoặc nơi sử dụng càng tốt, vì điều này có xu hướng tối đa hóa sự bảo vệ được cung cấp, nhưng có thể có nhiều tùy chọn trong việc chọn điểm mã hóa (xem Hình 3), bao gồm:

- Cấp ứng dụng, ví dụ: một ứng dụng hoặc cơ sở dữ liệu cụ thể, cung cấp mức độ kiểm soát chi tiết nhất và hiểu biết sâu sắc nhất về dữ liệu (loại, người dùng, độ nhạy cảm).
- Cấp hệ thống tệp, ví dụ: hệ điều hành hoặc ứng dụng cấp hệ điều hành, cung cấp kiểm soát ở cấp độ tệp với hiểu biết sâu sắc về người dùng.
- Cấp mạng, ví dụ: HBA, bộ điều khiển mảng hoặc bộ chuyển mạch, trong đó:

+ dựa trên tệp (NAS) cung cấp kiểm soát ở cấp chia sẻ/hệ thống tệp (có thể là cấp tệp) với hiểu biết vừa phải về người dùng;

+ dựa trên khối cung cấp kiểm soát ở cấp đơn vị logic với hiểu biết hạn chế về cộng đồng người dùng.

CHÚ THÍCH 1: Cộng đồng người dùng cụ thể không xác định, cũng như quyền truy cập cá nhân của họ. Cộng đồng được xác định bởi các máy chủ có quyền truy cập vào các đơn vị logic riêng lẻ.

- Cấp thiết bị, ví dụ: ổ băng từ, mảng lưu trữ và ổ đĩa, cung cấp kiểm soát ở cấp phương tiện lưu trữ (và có thể ở cấp đơn vị logic) với hiểu biết hạn chế về cộng đồng người dùng.

Nếu không có thiết kế cẩn thận và giám sát liên tục các thay đổi đối với hệ sinh thái lưu trữ, nhiều điểm mã hóa có thể sẽ được triển khai ngoài dự kiến. Tình huống như vậy có thể có tác động tiêu cực, đặc biệt khi nhân viên CNTT-TT không biết về việc triển khai mã hóa dữ liệu tĩnh.

Những điều sau đây có thể được sử dụng để bảo vệ dữ liệu trên lưu trữ bằng mã hóa dữ liệu tĩnh (xem thêm 10.5.5):

a) TC-CNFD-R01 Sử dụng mật mã có độ mạnh an toàn ít nhất 128 bit

Mật mã có độ mạnh an toàn ít nhất 128 bit phải được sử dụng trong toàn bộ giải pháp mã hóa.

b) TC-CNFD-G05 Tránh sử dụng mã hóa lưu trữ làm biện pháp bảo vệ chính cho dữ liệu nhạy cảm

Mã hóa dựa trên lưu trữ không nên là biện pháp bảo vệ bảo mật chính cho dữ liệu nhạy cảm.

CHÚ THÍCH 2: Mã hóa lưu trữ thường chỉ hoạt động khi dữ liệu nằm trên hệ thống hoặc phương tiện lưu trữ (tức là nó là bản rõ sau khi đi qua điểm mã hóa, xảy ra bất cứ khi nào dữ liệu được truy cập).

c) TC-CNFD-G06 Chọn điểm mã hóa thích hợp

Việc lựa chọn và triển khai điểm mã hóa nên tương thích với BCM (xem 7.3), giảm dữ liệu (xem 10.13), bảo vệ dữ liệu (xem 10.14), và các yêu cầu bảo mật dữ liệu (xem 10.5).

d) TC-CNFD-G07 Sử dụng mã hóa và quản lý khóa thích hợp tương thích với các yêu cầu lưu giữ và bảo quản dữ liệu

Các giải pháp mã hóa và quản lý khóa nên tương thích với các yêu cầu lưu giữ và bảo quản dữ liệu.

e) TC-CNFD-G08 Sử dụng các mô-đun mật mã đã được xác nhận cho dữ liệu nhạy cảm hoặc được quản lý

Các mô-đun mật mã được sử dụng để bảo vệ dữ liệu nhạy cảm hoặc được quản lý nên được xác nhận bằng các tiêu chí được công nhận (ví dụ: TCVN 11295 (ISO/IEC 19790), loạt TCVN 8709 (ISO/IEC 15408) và NIST FIPS 140-3).

f) TC-CNFD-G09 Tạo và lưu giữ hồ sơ mã hóa lưu trữ

Giống như việc làm sạch, điều quan trọng là một tổ chức duy trì hồ sơ về mã hóa dữ liệu tĩnh của mình để ghi lại phương tiện lưu trữ đã được bảo vệ, cũng như thời gian và cách thức chúng được mã hóa. Khi một tổ chức bị nghi ngờ mất kiểm soát đối với phương tiện lưu trữ của mình, chứa dữ liệu nhạy cảm, những hồ sơ này hoặc bằng chứng về mã hóa có thể là công cụ để chứng minh rằng không có vi phạm dữ liệu nào xảy ra, do đó tránh được các thông báo vi phạm dữ liệu tốn kém và các trách nhiệm pháp lý khác.

Những điều sau đây nên được bao gồm để làm bằng chứng về mã hóa:

- đảm bảo rằng các cơ chế mã hóa tạo ra các mục nhập nhật ký kiểm toán thích hợp (kích hoạt, xác minh, kiểm tra tính toàn vẹn, đổi khóa, v.v.);
- thực hiện kiểm tra thường xuyên và được kiểm toán rằng mã hóa đã được thực hiện đúng cách và xem xét công nhận bên ngoài.

g) TC-CNFD-G10 Tuân thủ các nguyên tắc quản lý khóa cơ bản

Việc sử dụng mật mã thành công phụ thuộc vào việc tuân thủ các nguyên tắc cơ bản liên quan đến nguyên liệu khóa cũng như quản lý khóa.

Các hệ thống và thiết bị lưu trữ tích hợp mã hóa dữ liệu tĩnh và quản lý khóa có thể cải thiện hơn nữa tính bí mật bằng những điều sau:

- quản lý khóa tập trung nên được sử dụng cho quản lý vòng đời khóa;
- quản lý khóa nên được tự động hóa bất cứ khi nào có thể;
- các khóa có tuổi thọ dài (tức là gần đạt đến chu kỳ mật mã tối đa được khuyến nghị, thường không quá 1 đến 2 năm, tùy thuộc vào loại khóa) nên được sử dụng một cách hạn chế;
- kiểm soát truy cập nghiêm ngặt nên được sử dụng để hạn chế khả năng của người dùng và các ràng buộc phân tách nhiệm vụ (ví dụ: vai trò an toàn) đối với việc tạo, thay đổi và phân phối khóa.

10.5.4 Mã hóa dữ liệu được truyền

10.5.4.1 Tổng quát

Trong cơ sở hạ tầng lưu trữ, tính bí mật hoặc toàn vẹn dữ liệu (chữ ký số hoặc mã xác thực) của dữ liệu đang được truyền giữa hai điểm có thể được quan tâm, đặc biệt đối với dữ liệu rời khỏi giới hạn của một trung tâm dữ liệu được kiểm soát vật lý. Ngoài ra, việc truyền dữ liệu trong các hệ thống lưu trữ có thể là mối quan tâm. Các giao thức như FC ESP_Header, IPsec (xem 10.5.4.3), TLS (xem 10.5.4.2), hoặc thậm chí các kỹ thuật mã hóa dựa trên máy tính có thể cung cấp sự bảo vệ bổ sung cho dữ liệu khi nó được truyền. Các phương pháp này thường liên quan đến việc bảo vệ dữ liệu khi nó đang di chuyển (còn được gọi là in-flight hoặc in-transit).

bao gồm các tiêu chuẩn an toàn Fibre Channel, RFC IPsec và RFC TLS trình bày chi tiết các phương án thay thế để bảo mật dữ liệu đang di chuyển.

Đối với một số giao thức, có nhiều chế độ hoặc tùy chọn hoạt động trong các tiêu chuẩn. Ngoài ra, có nhiều chế độ mật mã hoặc thuật toán chữ ký số (toàn vẹn). Định nghĩa và đặc tả của các chế độ hoạt động có thể được tìm thấy trong ISO/IEC 10116.

Việc bảo vệ dữ liệu đang di chuyển hoạt động kết hợp với một quy trình hoặc giao thức thiết lập khóa hoặc thỏa thuận khóa. Việc quản lý và bảo vệ các khóa xác thực ban đầu cực kỳ quan trọng trong việc duy trì tính bí mật và toàn vẹn dữ liệu đang di chuyển. Các tiêu chuẩn được trích dẫn trước đây trình bày chi tiết thông tin bổ sung về các tham số an toàn quan trọng cần được bảo vệ khi sử dụng các phương pháp bảo vệ dữ liệu đang di chuyển.

Các kiểm soát liên quan đến mã hóa dữ liệu được truyền như sau:

a) TC-CNFD-G11 Cung cấp bảo vệ an toàn đầu cuối cho dữ liệu đang di chuyển

Khi yêu cầu bảo vệ dữ liệu đang di chuyển, nó nên cung cấp bảo vệ đầu cuối (tức là một phương pháp bảo mật truyền thông ngăn chặn các bên thứ ba truy cập dữ liệu khi nó được truyền từ một hệ thống hoặc thiết bị đầu cuối này sang hệ thống hoặc thiết bị đầu cuối khác).

b) TC-CNFD-G12 Bù đắp cho tác động tính toán của mã hóa dữ liệu đang di chuyển

Mã hóa dữ liệu đang di chuyển có thể gây ra gánh nặng tính toán đáng kể cho các thực thể giao tiếp, vì vậy nên thực hiện các biện pháp bù đắp thích hợp để giảm thiểu tác động.

10.5.4.2 An toàn Lớp Vận chuyển (TLS)

TLS là một giao thức an toàn được thiết kế để tạo điều kiện thuận lợi cho quyền riêng tư và an toàn dữ liệu cho các giao tiếp qua internet. Phiên bản giao thức TLS 1.3 được quy định trong IETF RFC 8446.

Các kiểm soát liên quan đến TLS như sau:

TC-CNFD-R02 Yêu cầu tối thiểu TLS

Khi TLS được sử dụng để bảo vệ dữ liệu đang di chuyển, việc triển khai:

- phải sử dụng TLS cho quản lý lưu trữ sao cho máy khách và máy chủ lưu trữ tuân thủ hồ sơ TLS được tổ chức phê duyệt (ví dụ: ISO/IEC 20648 hoặc Tài liệu tham khảo [71]);
- nên sử dụng TLS phiên bản 1.3 trở lên để truy cập dữ liệu.

10.5.4.3 An toàn IP (IPsec)

Có một số RFC của IETF liên quan đến đặc tả An toàn Giao thức Internet (IPsec). IETF RFC 6071 cung cấp một cái nhìn tổng quan tuyệt vời về các RFC liên quan đến IPsec- và IKE.

IPsec có thể có tác động bất lợi đến việc sử dụng một số công nghệ nhất định như dịch địa chỉ mạng, hệ thống phát hiện xâm nhập, hệ thống ngăn chặn xâm nhập hoặc các hệ thống khác xem xét sâu hơn vào các khung lưu lượng mạng. Việc dựa vào IPsec hay các giao thức bảo vệ dữ liệu đang di chuyển khác có thể phụ thuộc vào sự đánh đổi về khả năng vô hiệu hóa giá trị của các công nghệ khác.

Các kiểm soát liên quan đến IPsec như sau:

TC-CNFD-R03 Yêu cầu tối thiểu IPsec

Khi IPsec được sử dụng để bảo vệ dữ liệu đang di chuyển, việc triển khai phải:

- hỗ trợ IPsec, phiên bản 3;
- hỗ trợ chế độ đường hầm (tunnel) hoặc chế độ truyền tải (transport) của IPsec;
- hỗ trợ ít nhất một Cơ sở dữ liệu Chính sách Bảo mật (SPD) (ví dụ: IETF RFC 4301);
- hỗ trợ IPsec ESP sử dụng các thuật toán mật mã (ví dụ: IETF RFC 4303);
- hỗ trợ các thuật toán trao đổi khóa Trao đổi Khóa Internet (IKE) phiên bản 2 (hoặc các phiên bản mới hơn);
- hỗ trợ tải trọng được mã hóa bằng IKEv2;
- đảm bảo rằng các giao thức IKE thực hiện xác thực ngang hàng bằng thuật toán RSA/ECDSA sử dụng chứng chỉ X.509v3 tuân thủ phương pháp khóa chia sẻ trước (ví dụ: IETF RFC 4945).

10.5.5 Mã hóa dữ liệu tĩnh

Với lượng dữ liệu nhạy cảm và được quản lý ngày càng tăng đang được lưu trữ, các tổ chức đang thực hiện các bước để đảm bảo dữ liệu này được lưu trữ ở dạng mã hóa. Mặc dù mã hóa dữ liệu càng gần nguồn gốc và nơi sử dụng của nó càng tốt là tình huống lý tưởng, việc mã hóa dữ liệu tĩnh trong cơ sở hạ tầng lưu trữ cung cấp một mức độ bảo vệ cơ bản chống lại các vi phạm xuất phát từ việc mất kiểm soát phương tiện lưu trữ, đặc biệt là băng từ. Do đó, các cơ chế mã hóa trong các thiết bị lưu trữ (ổ đĩa tự mã hóa cũng như các công nghệ dựa trên bộ điều khiển), bộ chuyển mạch, thiết bị chuyên dụng, HBA, v.v. có thể cung cấp sự bảo vệ hữu ích.

Các kiểm soát liên quan đến mã hóa dữ liệu tĩnh như sau:

a) TC-CNFD-G13 Sử dụng điểm mã hóa thích hợp

Việc triển khai mã hóa dữ liệu đòi hỏi nhiều hơn là chỉ mua một thiết bị có tính năng mã hóa và kết nối nó với cơ sở hạ tầng lưu trữ hiện có. Vị trí của cơ chế mã hóa (điểm mã hóa) trong cơ sở hạ tầng nên được chọn để giải quyết các rủi ro đã xác định, và các sắp xếp được thực hiện để cung cấp vị trí đó bằng nguyên liệu khóa. Dữ liệu cần xử lý nên được xác định, và trong một số trường hợp, vị trí của nó nên được thay đổi.

b) TC-CNFD-G14 Tạo bằng chứng mã hóa thích hợp

Ngoài ra, bằng chứng mã hóa đầy đủ, có khả năng dưới dạng nhật ký, nên được tạo và tích hợp vào cơ sở hạ tầng nhật ký kiểm toán. Xem 10.5.3 để biết thêm thông tin.

c) TC-CNFD-R04 Bảo vệ khóa được sử dụng để mã hóa lưu trữ

Việc sử dụng tất cả các loại mã hóa cho lưu trữ phụ thuộc vào việc quản lý các khóa mật mã. Quản lý khóa kém có thể dễ dàng làm tổn hại dữ liệu bất kể mã hóa mạnh đến đâu. Cuối cùng, tính bí mật của dữ liệu được bảo vệ bằng mật mã trực tiếp phụ thuộc vào độ mạnh của khóa, hiệu quả của các cơ chế và giao thức liên quan đến khóa, và sự bảo vệ dành cho khóa. Tất cả các khóa phải được bảo vệ chống lại sửa đổi. Khóa bí mật (để mã hóa đối xứng) và khóa riêng tư (để mã hóa bất đối xứng hoặc khóa công khai) phải được bảo vệ chống lại việc tiết lộ trái phép. Quản lý khóa cung cấp nền tảng cho việc tạo, lưu trữ, phân phối và tiêu hủy khóa an toàn. Các khuôn khổ tổng thể cho quản lý khóa được đưa ra trong loạt TCVN 7817 (ISO/IEC 11770).

d) TC-CNFD-R05 Sử dụng các thuật toán mã hóa và chế độ hoạt động thích hợp cho lưu trữ

Các thuật toán mã hóa và chế độ hoạt động phù hợp với công nghệ lưu trữ phải được sử dụng và có thể bao gồm:

- đối với HDD và SSD, AES với chế độ XTS như được mô tả trong IEEE 1619-2018;
- đối với băng từ, AES với chế độ bộ đếm với mã xác thực thông điệp chuỗi khối mật mã (CCM) hoặc chế độ Galois/Bộ đếm (GCM) như được mô tả trong IEEE 1619.1-2018.

e) TC-CNFD-G15 Hạn chế lộ khóa ở dạng rõ

Lượng thời gian một khóa ở dạng rõ nên được hạn chế và người dùng nên bị ngăn không cho xem khóa ở dạng rõ.

f) TC-CNFD-R06 Sử dụng khóa mật mã cho một mục đích

Khóa mật mã chỉ được phép sử dụng cho một mục đích. Không sử dụng khóa mã hóa khóa (còn được gọi là khóa bao bọc khóa) để mã hóa dữ liệu hoặc sử dụng khóa mã hóa dữ liệu để mã hóa các khóa khác.

g) TC-CNFD-R07 Tạo khóa ngẫu nhiên bằng toàn bộ không gian khóa

Khóa phải được tạo ngẫu nhiên từ toàn bộ không gian khóa. Thực hành tốt nhất khuyến nghị một bộ tạo số giả ngẫu nhiên an toàn về mặt mật mã đảm bảo rằng, khi có đầy đủ kiến thức về thuật toán và một chuỗi đầu ra, cả các số đứng trước chuỗi lẫn các số đứng sau chuỗi đều không thể được xác định bằng các phương tiện tính toán thực tế.

h) TC-CNFD-R08 Việc sử dụng khóa bị giới hạn trong chu kỳ mật mã hữu hạn hoặc lượng dữ liệu xử lý tối đa

Nếu thích hợp, việc sử dụng khóa mã hóa dữ liệu phải được giới hạn trong một chu kỳ mật mã hữu hạn (thường không quá 2 năm) hoặc một lượng dữ liệu xử lý tối đa.

CHÚ THÍCH 1: Không phải tất cả các khóa đều có thể được thay thế (ví dụ: khóa chứng thực tĩnh trong mô-đun nền tảng đáng tin cậy).

i) TC-CNFD-G16 Sử dụng cơ sở hạ tầng quản lý khóa tập trung

Khi có thể, các hệ thống và cơ sở hạ tầng lưu trữ nên sử dụng cơ sở hạ tầng quản lý khóa tập trung, tương thích (ví dụ: tạo và lưu trữ khóa mã hóa).

j) TC-CNFD-G17 Sử dụng OASIS KMIP để truy cập và sử dụng cơ sở hạ tầng quản lý khóa tập trung

Đặc tả và hồ sơ Giao thức Tương thích Quản lý Khóa (KMIP) của Tổ chức vì sự Tiến bộ của Tiêu chuẩn Thông tin Cấu trúc (OASIS) xác định cơ chế chủ đạo để truy cập quản lý khóa tập trung trong cơ sở hạ tầng lưu trữ.

CHÚ THÍCH 2: OASIS KMIP được quy định trong Tài liệu tham khảo [75] và [76]. Các hệ thống và cơ sở hạ tầng lưu trữ nên sử dụng các máy khách tuân thủ OASIS KMIP Phiên bản 2.0 (hoặc mới hơn) để truy cập và sử dụng cơ sở hạ tầng quản lý khóa.

10.6 Làm sạch lưu trữ

10.6.1 Tổng quát

ISO/IEC 27002:2022, 7.10 và 7.14 cung cấp hướng dẫn về việc thải bỏ và tái sử dụng phương tiện lưu trữ để ngăn chặn rò rỉ thông tin. ISO/IEC 27002:2022, 8.10 cũng cung cấp hướng dẫn liên quan về việc xóa thông tin. Nói chung, dữ liệu nhạy cảm được ghi trên phương tiện lưu trữ nên được loại bỏ trước khi tái sử dụng hoặc thải bỏ phương tiện lưu trữ. Để giải quyết các yếu tố chính của hướng dẫn có trong ISO/IEC 27002 về thải bỏ và tái sử dụng, có thể sử dụng một chương trình làm sạch lưu trữ phù hợp với lược đồ phân loại dữ liệu được tổ chức áp dụng.

Một chương trình như vậy thường bao gồm:

- Đặc tả phương pháp làm sạch tối thiểu chấp nhận được (xem 10.6.2):
- Các bước xác minh cần thiết để xác định tính đầy đủ của việc làm sạch đã thực hiện (xem 10.6.6):
- Xác định các hồ sơ hoặc bằng chứng cần thiết để đáp ứng các nghĩa vụ tuân thủ (xem 10.6.7).

Làm sạch lưu trữ đề cập đến quy trình chung làm cho dữ liệu đã ghi trước đó trong lưu trữ không thể truy xuất được, sao cho có sự đảm bảo hợp lý rằng dữ liệu không thể dễ dàng được truy xuất hoặc tái tạo lại. Việc làm sạch lưu trữ được thực hiện trong lưu trữ có thể ở dạng làm sạch logic (xem 10.6.4) hoặc làm sạch dựa trên phương tiện (xem 10.6.3). Do tầm quan trọng của việc làm sạch lưu trữ, có thể có các nghĩa vụ bổ sung để xác nhận kết quả của các hoạt động làm sạch cũng như tạo hồ sơ (bằng chứng) về các hoạt động làm sạch (xem 10.6.7).

Các kiểm soát liên quan đến làm sạch lưu trữ như sau:

a) TC-SNTZ-G01 Bao gồm làm sạch lưu trữ như một phần của quản trị dữ liệu

Làm sạch lưu trữ nên là một yếu tố của quy trình quản trị dữ liệu của tổ chức. Quyết định sử dụng làm sạch lưu trữ nên dựa trên phân loại dữ liệu của tổ chức, tập trung vào dữ liệu được phân loại là nhạy cảm. Các ví dụ phổ biến về dữ liệu nhạy cảm bao gồm dữ liệu cá nhân, PII và hồ sơ chăm sóc sức khỏe điện tử cũng như một số dữ liệu kinh doanh nhất định (ví dụ: bí mật thương mại, sở hữu trí tuệ, hồ sơ khách hàng và hồ sơ tài chính) hoặc dữ liệu quan trọng cho nhiệm vụ (ví dụ: an ninh quốc gia). Việc không làm sạch lưu trữ hoặc không lưu giữ hồ sơ đầy đủ về các hoạt động làm sạch có thể kích hoạt thông báo vi phạm dữ liệu khi một tổ chức mất kiểm soát đối với các thiết bị lưu trữ hoặc phương tiện lưu trữ.

CHÚ THÍCH: Dữ liệu nhạy cảm trong ngữ cảnh này là dữ liệu mà việc tiết lộ có thể có tác động đến nhiệm vụ của tổ chức, dẫn đến thiệt hại cho tài sản của tổ chức, hoặc dẫn đến tổn thất tài chính hoặc tổn hại cho tổ chức hoặc cá nhân.

b) TC-SNTZ-R01 Làm sạch lưu trữ trước khi thải bỏ

Lưu trữ logic (xem 10.6.4) hoặc lưu trữ dựa trên phương tiện (xem 10.6.3) đã được sử dụng để ghi dữ liệu nhạy cảm phải được làm sạch trước khi thải bỏ hoặc chuyển giao cho một bên bên ngoài tổ chức

(tức là tổ chức mất kiểm soát đối với lưu trữ). Làm sạch phải được sử dụng trước khi chuyển giao lưu trữ nội bộ trong cùng một tổ chức (ví dụ: từ bộ phận nhân sự sang bộ phận kỹ thuật) khi độ nhạy cảm của dữ liệu đòi hỏi các biện pháp bảo vệ bảo mật (ví dụ: nghĩa vụ tuân thủ hoặc chính sách của tổ chức).

c) TC-SNTZ-R02 Xác minh kết quả làm sạch lưu trữ

Việc xác minh kết quả làm sạch lưu trữ phải được thực hiện, khi việc làm sạch đó là bắt buộc, trước khi thải bỏ hoặc chuyển giao lưu trữ để đảm bảo các rủi ro của tổ chức đã được giải quyết đầy đủ.

10.6.2 Lựa chọn phương pháp làm sạch

Nhiều phương pháp làm sạch có thể được sử dụng, tùy thuộc vào lưu trữ (logic hoặc dựa trên phương tiện), và chúng có dạng:

- **Xóa sạch (Clear):** Liên quan đến việc sử dụng phần mềm hoặc phần cứng để ghi đè dữ liệu mục tiêu bằng dữ liệu không nhạy cảm.
- **Thanh lọc (Purge):** Liên quan đến việc sử dụng các kỹ thuật vật lý hoặc logic làm cho việc khôi phục trở nên không khả thi, bằng các kỹ thuật phòng thí nghiệm hiện đại, đồng thời bảo toàn lưu trữ ở trạng thái có thể tái sử dụng.
- **Tiêu hủy (Destruct):** Liên quan đến việc sử dụng các kỹ thuật vật lý (ví dụ: phân rã, thiêu hủy, làm nóng chảy, nghiền thành bột và cắt nhỏ) để tiêu hủy lưu trữ. Phương pháp làm sạch này không áp dụng cho lưu trữ logic.

Mỗi phương pháp làm sạch trên cung cấp các mức độ đảm bảo khác nhau rằng dữ liệu không thể dễ dàng được truy xuất hoặc tái tạo lại, và chúng dựa trên mức độ nỗ lực mà kẻ tấn công bỏ ra để đánh bại các biện pháp bảo vệ.

Từ góc độ này, phương pháp xóa sạch cung cấp mức độ đảm bảo thấp nhất và phương pháp tiêu hủy cung cấp mức độ đảm bảo cao nhất khi phương pháp làm sạch được thực hiện đúng cách. Không phải tất cả các phương pháp làm sạch đều áp dụng được cho tất cả các loại lưu trữ logic (xem 10.6.4) hoặc lưu trữ dựa trên phương tiện (xem 10.6.3).

Các kiểm soát liên quan đến việc lựa chọn phương pháp làm sạch lưu trữ như sau:

a) TC-SNTZ-R03 Chọn phương pháp làm sạch lưu trữ tối thiểu chấp nhận được

Phương pháp làm sạch lưu trữ được chọn phải được chỉ định là mức tối thiểu chấp nhận được. Một phương pháp làm sạch cung cấp mức độ đảm bảo mạnh hơn được phép sử dụng (ví dụ: khi sử dụng tiêu hủy, nhưng xóa sạch là mức tối thiểu yêu cầu). Một phương pháp làm sạch cung cấp mức độ đảm bảo yếu hơn không được sử dụng.

b) TC-SNTZ-G02 Xem xét chi phí và tác động môi trường của việc làm sạch lưu trữ

Loại làm sạch lưu trữ được chọn nên được đánh giá về các yếu tố như chi phí và tác động môi trường, và nên đưa ra quyết định giảm thiểu tốt nhất rủi ro đối với tính bí mật và đáp ứng tốt nhất các ràng buộc khác đặt ra cho quy trình.

10.6.3 Làm sạch dựa trên phương tiện

Các công nghệ lưu trữ dữ liệu thay đổi và phát triển với tốc độ nhanh chóng, cũng như các cuộc tấn công chống lại lưu trữ. Do đó, các kỹ thuật làm sạch cụ thể liên quan đến ba phương pháp làm sạch (xem 10.6.2) cho các loại thiết bị lưu trữ hoặc phương tiện lưu trữ khác nhau được cập nhật thường xuyên. Tiêu chuẩn này không cung cấp chi tiết về cách các loại phương tiện cụ thể có thể được làm

sạch, mà thay vào đó, chuyển sang các tài nguyên khác cung cấp thông tin đó. Các kiểm soát liên quan đến làm sạch dựa trên phương tiện như sau:

a) TC-SNTZ-R04 Làm sạch phương tiện phù hợp với các tiêu chuẩn chấp nhận được

Khi yêu cầu làm sạch thiết bị lưu trữ hoặc phương tiện lưu trữ đã được thiết lập, thì việc làm sạch phải được thực hiện dựa trên phương pháp làm sạch đã chọn (xóa sạch, thanh lọc hoặc tiêu hủy) và theo cách phù hợp với tiêu chuẩn được xác định là chấp nhận được theo chính sách của tổ chức (ví dụ: IEEE 2883, cung cấp thông tin bổ sung về việc lựa chọn các phương pháp làm sạch thích hợp để sử dụng, cũng như các kỹ thuật làm sạch cụ thể theo công nghệ). Khi sử dụng phương pháp thanh lọc bằng xóa bằng mật mã, xem 10.6.5 để biết các cân nhắc hoặc yêu cầu bổ sung.

b) TC-SNTZ-R05 Xác minh tính đầy đủ của kết quả làm sạch phương tiện

Việc xác minh (xem 10.6.6) tính đầy đủ của kết quả làm sạch phải được thực hiện trên lưu trữ dựa trên phương tiện.

10.6.4 Làm sạch logic

Nhiều thiết bị lưu trữ ảo hóa phương tiện lưu trữ cơ bản và trình bày nó dưới dạng lưu trữ logic (xem 10.16.1). Một ví dụ nổi tiếng là đơn vị logic trên một mảng lưu trữ có thể có kích thước vượt xa dung lượng của một thiết bị lưu trữ duy nhất; lưu trữ điện toán đám mây (xem 10.11) có thể đưa sự ảo hóa này lên các cấp độ trừu tượng hóa cao hơn nữa. Tình hình có thể phức tạp hơn nữa khi lưu trữ logic được sao chép (tức là tồn tại nhiều bản sao dữ liệu) để hỗ trợ ảo hóa máy chủ (xem 10.16.2) và BCM (xem 7.3). Đối với các loại tình huống này, hầu như không thể xác định tất cả các phương tiện lưu trữ cơ bản mà dữ liệu nhạy cảm được ghi trên đó. Hơn nữa, việc làm sạch tất cả các phương tiện vật lý thường không phù hợp hoặc không được phép vì nhiều phiên bản lưu trữ logic có thể cùng tồn tại trên phương tiện vật lý dùng chung.

Các kiểm soát liên quan đến làm sạch logic như sau:

a) TC-SNTZ-R06 Làm sạch lưu trữ logic phù hợp với các tiêu chuẩn chấp nhận được

Nếu lưu trữ logic (ví dụ: đơn vị logic, hệ thống tệp, kho đối tượng hoặc lưu trữ điện toán đám mây) có thể ghi, thì việc làm sạch có thể được thực hiện bằng phương pháp xóa sạch hoặc, khi mã hóa đã được sử dụng thích hợp, phương pháp thanh lọc bằng xóa bằng mật mã (xem 10.6.5).

Khi yêu cầu làm sạch lưu trữ logic đã được thiết lập, thì việc làm sạch phải được thực hiện bằng bất kỳ cách nào sau đây, khi thích hợp:

- Xóa sạch bằng cách ghi đè (thay thế) tất cả không gian lưu trữ logic có thể định địa chỉ, thông qua các giao diện được cung cấp, bằng dữ liệu không nhạy cảm đã biết (thường là số không); hoặc
- Thanh lọc bằng cách sử dụng xóa bằng mật mã như được mô tả trong 10.6.5.

b) TC-SNTZ-R07 Xác minh tính đầy đủ của kết quả làm sạch lưu trữ logic

Xác minh (xem 10.6.6) tính đầy đủ của kết quả làm sạch phải được thực hiện trên lưu trữ logic.

c) TC-SNTZ-G03 Xem xét làm sạch lưu trữ bổ sung cho các cơ chế bảo vệ dữ liệu

Các công nghệ bảo vệ dữ liệu (xem 10.14), có thể bao gồm sao chép và sao lưu, thường được sử dụng kết hợp với lưu trữ logic, vì vậy các hoạt động làm sạch riêng biệt nên được thực hiện trên lưu trữ liên quan đến các cơ chế bảo vệ dữ liệu.

10.6.5 Xóa bằng mật mã

Ở cấp độ cơ bản, xóa bằng mật mã tận dụng việc mã hóa dữ liệu mục tiêu bằng cách cho phép làm sạch khóa mã hóa được sử dụng để mã hóa dữ liệu mục tiêu. Điều này chỉ để lại bản mã trên lưu trữ, làm sạch dữ liệu một cách hiệu quả. Các kiểm soát liên quan đến xóa bằng mật mã như sau:

a) TC-SNTZ-R08 Sử dụng xóa bằng mật mã để thanh lọc trong điều kiện chính xác

Để sử dụng xóa bằng mật mã như một phương pháp thanh lọc, các điều kiện sau đây phải được đáp ứng, tối thiểu:

- tất cả dữ liệu dự định xóa bằng mật mã phải được mã hóa trước khi ghi vào lưu trữ;
- độ mạnh của thuật toán mật mã (bao gồm cả chế độ hoạt động) được sử dụng để mã hóa dữ liệu mục tiêu phải ít nhất là 128 bit;
- số bit entropy phải ít nhất bằng số bit được sử dụng bởi khóa mã hóa được sử dụng để mã hóa dữ liệu mục tiêu;
- tất cả các bản sao của khóa mã hóa được sử dụng để mã hóa dữ liệu mục tiêu phải được làm sạch;
- nếu các khóa mã hóa của dữ liệu mục tiêu, bản thân chúng, được mã hóa bằng một hoặc nhiều khóa bao bọc, thì có thể chấp nhận thực hiện xóa bằng mật mã bằng cách làm sạch một khóa bao bọc tương ứng.

CHÚ THÍCH: Mặc dù có thể hấp dẫn khi kết hợp xóa bằng mật mã với một phương pháp làm sạch khác (ví dụ: xóa sạch), cách tiếp cận như vậy không cải thiện tính bí mật, nhưng có thể làm chậm đáng kể hoạt động làm sạch cũng như có khả

b) TC-SNTZ-G04 Tìm kiếm sự đảm bảo về chất lượng mật mã được sử dụng để xóa bằng mật mã

Những người chọn áp dụng xóa bằng mật mã nên tìm kiếm xác nhận độc lập về các lĩnh vực đảm bảo sau đây hoặc yêu cầu nhà cung cấp xác định các cơ chế nào được sử dụng để đảm bảo rằng các lĩnh vực quan tâm này đã được giải quyết:

- Tạo khóa: mức độ entropy của các nguồn số ngẫu nhiên và chất lượng của các quy trình làm trắng được áp dụng cho dữ liệu ngẫu nhiên. Điều này áp dụng cho các khóa mật mã, và có khả năng cho các khóa bao bọc bị ảnh hưởng bởi hoạt động xóa bằng mật mã.
- Mã hóa phương tiện: độ mạnh an toàn và tính hợp lệ của việc triển khai thuật toán/chế độ mã hóa được sử dụng để bảo vệ dữ liệu mục tiêu.
- Cấp độ khóa và bao bọc: làm sạch khóa được sử dụng để bao bọc (nghĩa là mã hóa) khóa mã hóa phương tiện hoặc một khóa khác có thể làm tăng tầm quan trọng của độ mạnh an toàn và mức độ đảm bảo của các kỹ thuật bao bọc được sử dụng (ví dụ: tương xứng với mức độ mạnh của hoạt động xóa bằng mật mã). Các cơ chế được chấp nhận chung và (nếu có thể) được tiêu chuẩn hóa nên được sử dụng. Ví dụ, các yêu cầu mật mã được quy định trong TCVN 11295 (ISO/IEC 19790) và các yêu cầu kiểm tra đối với các mô-đun mật mã được quy định trong TCVN 12211 **(**ISO/IEC 24759). Các yêu cầu kiểm tra và kiểm tra này bao gồm một số (nhưng không phải tất cả) các lĩnh vực quan tâm.

c) TC-SNTZ-G05 Xác định xem khóa mã hóa bị tiêu hủy có thể khôi phục được không

Khi quyết định có nên dựa vào xóa bằng mật mã hay không, cũng nên xem xét liệu các khóa mã hóa có thể được khôi phục nội bộ hoặc bên ngoài hay không (ví dụ: được nạp từ máy chủ quản lý khóa hoặc từ dịch vụ ký gửi khóa). Nếu khóa mã hóa (hoặc bất kỳ khóa nào ở cấp độ hoặc thấp hơn cấp độ khóa được làm sạch trong quá trình xóa bằng mật mã) tồn tại bên ngoài lưu trữ, có khả năng khóa đó có thể được sử dụng trong tương lai để khôi phục dữ liệu được lưu trữ trên lưu trữ được mã hóa.

10.6.6 Xác minh việc làm sạch lưu trữ

Việc xác minh kết quả làm sạch là một yếu tố quan trọng của chương trình làm sạch lưu trữ khi cần xác định tính đầy đủ hoặc hiệu quả của việc làm sạch lưu trữ. Việc xác minh này khác nhau tùy thuộc vào phương pháp làm sạch. Đối với xóa sạch hoặc thanh lọc, giao diện thiết bị được sử dụng để kiểm tra kết quả của hoạt động làm sạch. Đối với tiêu hủy, kiểm tra vật lý được sử dụng để kiểm tra kết quả làm sạch. Việc xác minh này rất quan trọng vì có thể có lỗi hoặc bất thường đòi hỏi các hành động bổ sung để hoàn thành việc làm sạch hoặc quyết định của tổ chức chấp nhận mọi rủi ro còn lại.

Để chứng minh tầm quan trọng của việc xác minh, có thể xem xét một kịch bản giả định trong đó phương pháp làm sạch bằng cách tiêu hủy, sử dụng kỹ thuật cắt nhỏ, được thực hiện trên một đĩa quang (PII được ghi lại). Ngoài ra, các mảnh kết quả từ việc cắt nhỏ không được lớn hơn kích thước 3 mm x 3 mm. Tuy nhiên, việc cắt nhỏ đĩa quang tạo ra các mảnh có kích thước 5 mm x 5 mm. Với khả năng tồn tại dữ liệu PII nhạy cảm trên đĩa quang, tổ chức phải đối mặt với quyết định chấp nhận kết quả (tức là tổ chức chấp nhận rủi ro với các mảnh kích thước lớn) hoặc không chấp nhận kết quả và sau đó sử dụng một phương pháp làm sạch thay thế bằng cách tiêu hủy (ví dụ: thiêu hủy, làm nóng chảy hoặc nghiền thành bột) trên các mảnh đó. Trong kịch bản này, tổ chức chấp nhận kết quả cắt nhỏ, nhưng ghi lại các sai lệch so với kích thước cắt nhỏ tối đa 3 mm x 3 mm.

Các kiểm soát liên quan đến việc xác minh làm sạch lưu trữ như sau:

a) TC-SNTZ-G06 Xác minh kết quả phương pháp làm sạch bằng cách xóa sạch

Đối với phương pháp làm sạch bằng cách xóa sạch, nên thực hiện lấy mẫu đại diện để xác minh việc làm sạch phương tiện lưu trữ. IEEE 2883 xác định hai tùy chọn lấy mẫu đại diện, bao gồm lấy mẫu ngẫu nhiên một tỷ lệ phần trăm không gian người dùng có thể định địa chỉ và một phương pháp chia không gian người dùng có thể định địa chỉ thành một số lượng băng được xác định trước, sau đó được lấy mẫu ngẫu nhiên.

b) TC-SNTZ-G07 Xác minh kết quả phương pháp làm sạch bằng cách thanh lọc

Đối với phương pháp làm sạch bằng cách thanh lọc, nên thực hiện xác minh đầy đủ phương tiện lưu trữ. Nếu xóa bằng mật mã được sử dụng để thực hiện việc làm sạch, có thể không thực hiện được việc xác minh vì phương tiện lưu trữ không thể truy cập được hoặc mẫu bit ngẫu nhiên còn lại trên phương tiện lưu trữ không cung cấp cơ sở để so sánh.

Các thiết bị lưu trữ được bảo vệ bằng các cơ chế kiểm soát truy cập có các cân nhắc xác minh bổ sung; các thiết bị lưu trữ nên có thể truy cập được cả trước và sau khi làm sạch để cho phép quá trình xác minh. Điều này có thể là một vấn đề vì một số hoạt động thanh lọc nhất định có thể dẫn đến việc dữ liệu mục tiêu trên các thiết bị lưu trữ không thể truy cập được.

c) TC-SNTZ-R09 Xác minh kết quả phương pháp làm sạch bằng cách tiêu hủy

Kiểm tra vật lý là tùy chọn duy nhất khi tiêu hủy là phương pháp làm sạch vì lưu trữ không thể sử dụng được (theo định nghĩa). Khi yêu cầu xác minh đối với việc làm sạch dựa trên tiêu hủy, kết quả phải được kiểm tra và so sánh với một tiêu chuẩn được xác định là chấp nhận được theo chính sách của tổ chức để xác định tính đầy đủ (ví dụ: IEEE 2883). Nếu sau khi xem xét các phát hiện xác minh liên quan đến kết quả tiêu hủy, người ta xác định rằng kết quả làm sạch không đầy đủ, việc làm sạch dựa trên tiêu hủy phải được lặp lại với việc xem xét sử dụng một hình thức tiêu hủy thay thế.

10.6.7 Bằng chứng về việc làm sạch

Các tổ chức nên duy trì hồ sơ về các hoạt động làm sạch để ghi lại phương tiện lưu trữ nào đã được làm sạch, thời gian và cách thức chúng được làm sạch, và việc định đoạt cuối cùng đối với phương tiện lưu trữ. Thông thường khi một tổ chức bị nghi ngờ mất kiểm soát thông tin của mình, đó là do việc lưu

giữ hồ sơ không đầy đủ về việc làm sạch phương tiện lưu trữ. Các kiểm soát liên quan đến bằng chứng về việc làm sạch như sau:

a) TC-SNTZ-G08 Tạo và lưu giữ hồ sơ làm sạch lưu trữ

Bằng chứng về việc làm sạch có ít nhất hai dạng: 1) dấu vết nhật ký kiểm toán và 2) giấy chứng nhận làm sạch ghi lại việc làm sạch. Những hồ sơ làm sạch này là bằng chứng mà các tổ chức nên lưu giữ cho các mục đích tuân thủ/pháp lý, để ngăn ngừa rủi ro bị xử phạt hoặc thông báo vi phạm dữ liệu tốn kém. Tầm quan trọng của bằng chứng này, cùng với các yêu cầu về nguồn gốc hoặc chuỗi hành trình liên quan đến bằng chứng ghi lại việc làm sạch, đóng vai trò là động lực chính để đặt việc làm sạch dưới sự kiểm soát của nhân viên an toàn.

b) TC-SNTZ-G09 Ghi lại thông tin tối thiểu để chứng nhận việc làm sạch

Để tạo giấy chứng nhận làm sạch, một số thông tin nhất định phải được thu thập, nếu có thể trước khi thực hiện việc làm sạch (ví dụ: tiêu hủy HDD).

Thông tin tối thiểu được ghi lại cho giấy chứng nhận làm sạch nên bao gồm:

- nhà sản xuất;
- kiểu máy (model);
- số sê-ri;
- loại phương tiện lưu trữ (ví dụ: từ tính, flash và lai);
- nguồn phương tiện lưu trữ (tức là người dùng hoặc hệ thống mà phương tiện lưu trữ đến từ đó);
- phương pháp làm sạch được sử dụng (tức là xóa sạch, thanh lọc hoặc tiêu hủy);
- mô tả kỹ thuật làm sạch được sử dụng (ví dụ: khử từ, ghi đè, xóa khối và xóa bằng mật mã);
- mô tả kết quả làm sạch (ví dụ: thành công/thất bại và lỗi/bất thường);
- đối với xác minh làm sạch bằng cách xóa sạch hoặc thanh lọc:

    + công cụ được sử dụng (bao gồm cả phiên bản);

    + phương pháp xác minh (ví dụ: đầy đủ và lấy mẫu nhanh).

- đối với cả làm sạch và xác nhận:

    + tên người;

    + vị trí/chức danh của người;

    + ngày và giờ hoàn thành;

    + địa điểm;

    + thông tin liên hệ (ví dụ: số điện thoại và địa chỉ email);

    + trường dành cho chữ ký của người thực hiện làm sạch.

Ngoài các chi tiết liên quan đến giấy chứng nhận làm sạch, dấu vết kiểm toán nên ghi lại các giao dịch và tiến trình có dấu thời gian liên quan đến việc làm sạch. Ví dụ, việc bắt đầu và kết thúc hoạt động làm sạch, cũng như tiến trình ghi đè và xác minh trung gian, nên được phản ánh.

10.7 Lưu trữ gắn trực tiếp

Thiết bị lưu trữ gắn trực tiếp (DAS) là một thiết bị lưu trữ (ví dụ: HDD, SSD và băng từ) được kết nối trực tiếp với máy tính chủ mà không qua mạng lưu trữ trung gian (tức là không có thiết bị mạng như hub, bộ định tuyến hoặc bộ chuyển mạch). Thiết bị DAS có thể ở dạng lưu trữ nội bộ (tức là một phần không thể

thiếu của hệ thống máy tính) hoặc lưu trữ bên ngoài (tức là lưu trữ phụ trợ), có thể bao gồm các bộ mở rộng làm tăng số lượng ổ đĩa có thể kết nối. DAS cũng có thể bao gồm các thiết bị lưu trữ có phương tiện di động (ví dụ: đĩa quang, đĩa flash, thẻ Secure Digital) sao cho phương tiện lưu trữ có thể được thêm hoặc bớt mà không cần tắt nguồn thiết bị lưu trữ hoặc hệ thống. Mặc dù chúng thường dành riêng cho hệ thống mà chúng được gắn vào, một thiết bị DAS có thể được chia sẻ giữa nhiều máy tính, nếu nó cung cấp nhiều giao diện (cổng) cho phép truy cập đồng thời và trực tiếp.

Các thiết bị lưu trữ này có các giao diện truy cập dữ liệu và quản lý hạn chế (giao diện quản lý thường là trong băng).

Các kiểm soát liên quan đến DAS như sau:

a) TC-DASS-G01 Bảo vệ DAS chống lại truy cập trái phép

Để tránh truy cập trái phép dữ liệu nhạy cảm hoặc có giá trị cao trên DAS, nên sử dụng một số hình thức kiểm soát truy cập được xác thực (khóa ổ đĩa) và mã hóa thiết bị lưu trữ để bảo vệ dữ liệu tĩnh.

b) TC-DASS-G02 Làm sạch DAS trước khi tái sử dụng hoặc thải bỏ

Trước khi tái sử dụng hoặc thải bỏ, DAS được sử dụng với dữ liệu nhạy cảm hoặc có giá trị cao nên được làm sạch như sau:

- sử dụng chức năng làm sạch lưu trữ tích hợp trong các thiết bị lưu trữ (xem 10.6.2);
- sử dụng làm sạch dựa trên máy tính hoặc dựa trên ứng dụng.

c) TC-DASS-G03 Sao lưu DAS để đảm bảo khôi phục sau khi mất dữ liệu

Để bảo vệ chống mất hoặc hỏng dữ liệu do tai nạn hoặc cố ý, nên thực hiện sao lưu (xem 10.14.2) nội dung DAS một cách thường xuyên và được bảo mật đúng cách ở một địa điểm khác.

10.8 Mạng lưu trữ

10.8.1 Bối cảnh

Mạng đóng vai trò quan trọng trong cơ sở hạ tầng lưu trữ và có thể bao gồm các công nghệ mạng phổ biến (ví dụ: LAN và mạng diện rộng), các giao thức mạng dành riêng cho lưu trữ sử dụng các công nghệ đó cũng như các công nghệ dành riêng cho lưu trữ (ví dụ: Fibre Channel). Trong trường hợp đầu tiên, hướng dẫn bảo mật được cung cấp trong loạt TCVN 9801 (ISO/IEC 27033) là công cụ để bảo vệ tài nguyên lưu trữ sử dụng các công nghệ này. Các giao thức và công nghệ mạng dành riêng cho lưu trữ được đề cập trong tiêu chuẩn này.

Hệ thống lưu trữ sử dụng mạng cho ba mục đích chính: 1) lưu trữ và truy xuất dữ liệu, 2) bảo vệ dữ liệu và 3) quản lý hệ thống lưu trữ. Không có mục đích sử dụng nào bắt buộc một công nghệ hoặc phương pháp mạng cụ thể. Ví dụ, một số quản lý lưu trữ có thể được thực hiện qua cùng một giao diện Fibre Channel (tức là trong băng) được máy chủ sử dụng để truy cập dữ liệu và qua kết nối TCP/IP đến giao diện quản lý (ngoài băng) của hệ thống lưu trữ.

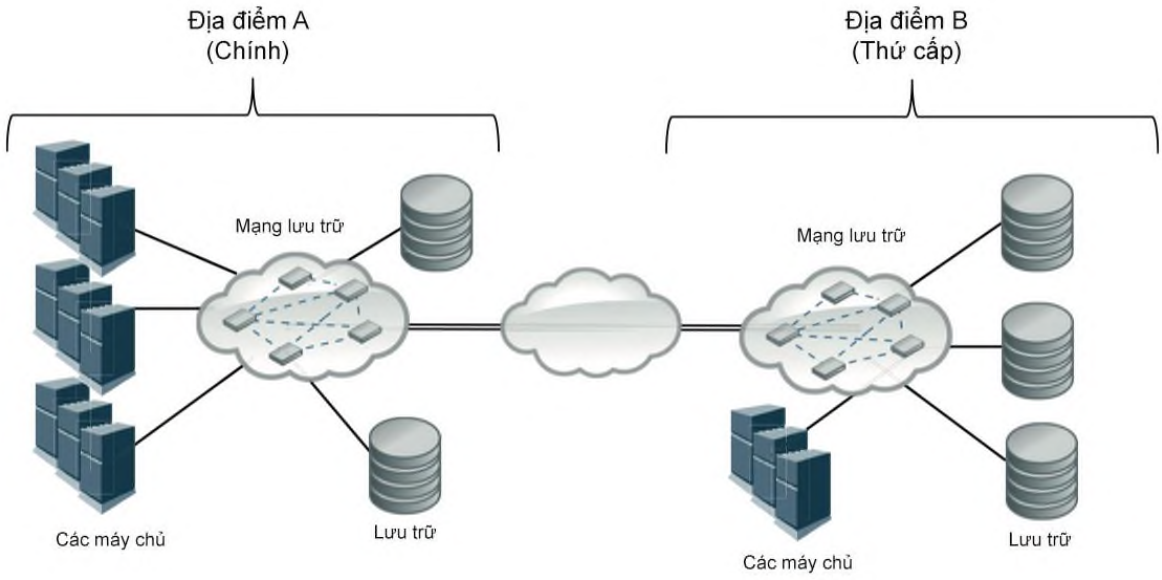
10.8.2 Mạng khu vực lưu trữ

10.8.2.1 Tổng quát

Mạng khu vực lưu trữ (SAN) là một mạng chuyên dụng, tốc độ cao cung cấp quyền truy cập mạng cấp khối vào lưu trữ. SAN thường bao gồm máy chủ, bộ chuyển mạch và thiết bị lưu trữ được kết nối với nhau bằng nhiều công nghệ, cấu trúc liên kết và giao thức khác nhau. SAN cũng có thể trải rộng trên nhiều địa điểm.

SAN thường được sử dụng để cải thiện tính sẵn sàng của ứng dụng (ví dụ: nhiều đường dẫn dữ liệu), nâng cao hiệu suất ứng dụng (ví dụ: giảm tải chức năng lưu trữ và sử dụng mạng riêng), tăng cường sử dụng và hiệu quả lưu trữ (ví dụ: hợp nhất tài nguyên lưu trữ và lưu trữ theo tầng), và cải thiện bảo vệ và bảo mật dữ liệu. Ngoài ra, SAN thường đóng vai trò quan trọng trong các hoạt động BCM (xem 7.3) của một tổ chức.

Hình 4 cho thấy một ví dụ về một SAN duy nhất được phân phối về mặt địa lý. Một SAN như vậy cho phép các máy tính ở một trong hai địa điểm truy cập tài nguyên lưu trữ ở cả hai địa điểm (ví dụ: thuận lợi cho phản hồi cục bộ hóa và chuyển đổi dự phòng). Ngoài ra, các hệ thống lưu trữ có thể sao chép dữ liệu sang các hệ thống lưu trữ khác độc lập với vị trí của chúng. Các cơ chế kết nối giữa hai địa điểm có thể đưa ra các cân nhắc bảo mật bổ sung.



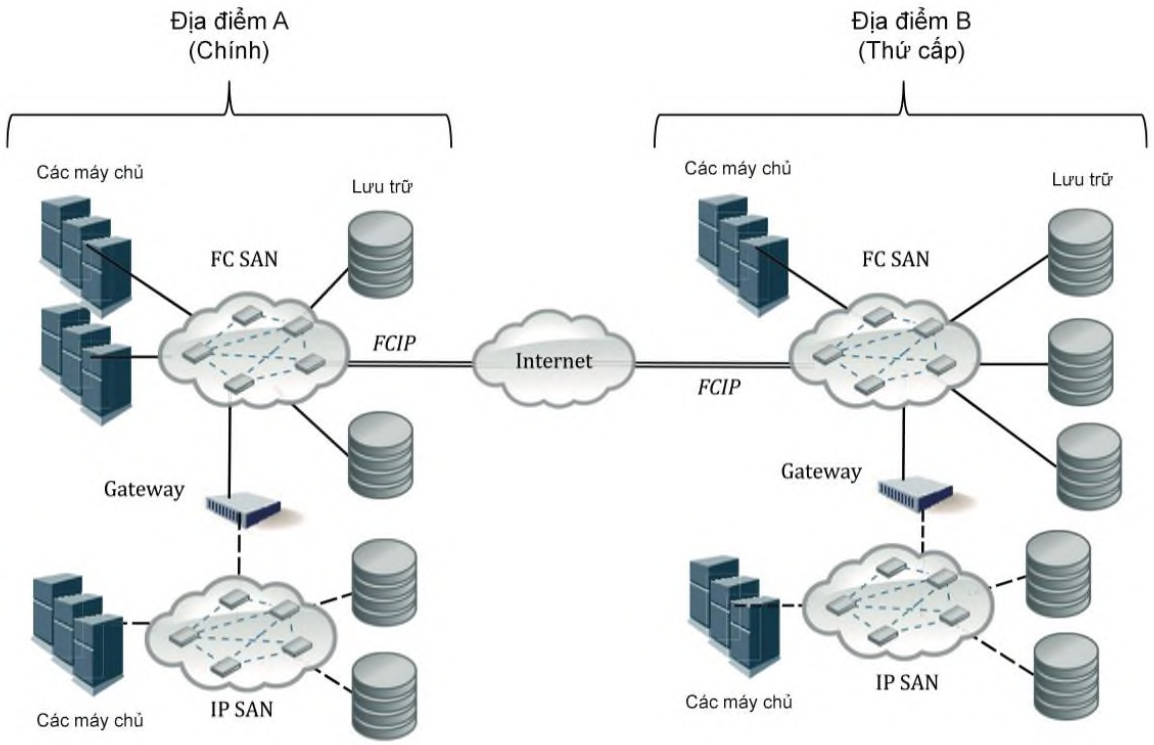
Hình 4 - Ví dụ về mạng khu vực lưu trữ

SAN trình bày các thiết bị lưu trữ (chẳng hạn như mảng đĩa và thư viện băng) cho hệ điều hành máy chủ sao cho, đối với máy chủ, lưu trữ dường như được gắn cục bộ. Việc trình bày lưu trữ đơn giản hóa này cho máy chủ được thực hiện bằng các loại ảo hóa khác nhau.

SAN thường dựa trên:

- Các công nghệ Fibre Channel (FC) sử dụng Giao thức Fibre Channel (FCP) cho SCSI cho các hệ thống mở và các biến thể độc quyền cho máy chủ lớn;
- Giao diện Hệ thống Máy tính Nhỏ Internet (iSCSI), thường được sử dụng trong các tổ chức vừa và nhỏ như một giải pháp thay thế ít tốn kém hơn cho FC;
- InfiniBand, thường được sử dụng trong môi trường điện toán hiệu năng cao;
- NVMe® qua Fabric (NVMe-oF™), sử dụng các phương tiện truyền tải fabric khác nhau (xem 10.8.2.5), được sử dụng cho tốc độ đa nhiệm với độ trễ thấp và thông lượng cao;
- Các kết nối tận dụng bộ mở rộng và bộ chuyển mạch cũng mang các đặc điểm của SAN.

Ngoài ra, có thể di chuyển dữ liệu giữa các công nghệ SAN khác nhau bằng cách sử dụng cổng mạng (xem Hình 5). Việc kết nối như vậy có thể quan trọng để hỗ trợ quản lý liên tục kinh doanh.



Hình 5 - Ví dụ về SAN đa địa điểm và chủng loại

Chiến lược phòng thủ theo chiều sâu (xem 10.2.2.1) giúp giảm thiểu rủi ro liên quan đến lỗi của một kiểm soát an toàn (có thể là điểm lỗi đơn lẻ) làm tổn hại tài sản được bảo vệ.

10.8.2.2 SAN Fibre Channel

Mạng khu vực lưu trữ Fibre Channel là một công nghệ mạng tốc độ nhiều gigabit được sử dụng cho lưu trữ dựa trên khối (xem 10.9). Có ba cấu trúc liên kết Fibre Channel chính, mô tả cách nhiều cổng được kết nối với nhau: điểm-điểm (hai thiết bị được kết nối trực tiếp), vòng lặp phân xử và fabric chuyển mạch. Cấu trúc liên kết fabric chuyển mạch cùng với Giao thức Fibre Channel (FCP), là giao thức giao diện được sử dụng để truyền lưu lượng SCSI trên công nghệ mạng này, đáng quan tâm hơn từ góc độ bảo mật.

Các kiểm soát an toàn liên quan đến SAN FC có thể được nhóm thành kiểm soát truy cập, xác thực và mã hóa (xem Tài liệu tham khảo [73] để biết tóm tắt hữu ích về an toàn FC cho các hệ thống và hệ sinh thái lưu trữ).

Kiểm soát truy cập trên SAN được thực hiện thông qua việc áp dụng các cơ chế phân vùng (zoning), che giấu số đơn vị logic (LUN masking) và ràng buộc cổng (port binding):

- Ràng buộc cổng: Các định danh duy nhất toàn cầu được gọi là tên toàn cầu (WWN) cho FC được sử dụng để nhận dạng trong SAN. Ràng buộc cổng là một cơ chế bảo mật SAN liên kết ID cổng vật lý và WWN của thiết bị được kết nối. Liên kết này có thể giảm thiểu các nỗ lực rình mò của một kẻ tấn công tiềm năng.
- Phân vùng (Zoning): Fabric SAN có thể được phân đoạn thành các vùng riêng biệt để hạn chế khả năng hiển thị các phần của SAN đối với các máy chủ và thiết bị lưu trữ cụ thể. Phân vùng mềm dựa trên việc giới hạn phản hồi của máy chủ tên fabric SAN đối với các truy vấn dựa trên giả định rằng máy chủ không liên hệ với các thiết bị lưu trữ không được khám phá thông qua máy chủ tên. Phân vùng cứng sử dụng số cổng vật lý trên bộ chuyển mạch SAN để hạn chế chuyển tiếp lưu lượng và

là phương pháp phân vùng an toàn hơn vì nó không dựa vào hành vi chính xác của máy chủ và đặc biệt, không dễ bị giả mạo danh tính máy chủ.

- **Che giấu và ánh xạ LUN:** Thiết bị lưu trữ có thể được chia thành các đơn vị logic khác nhau được xác định bằng LUN. Ánh xạ LUN đề cập đến việc gán một số cho LUN, và nó thường diễn ra trong một mảng lưu trữ, nhưng nó cũng có thể xảy ra như một phần của việc chuyển hướng (địa chỉ ban đầu đến địa chỉ mới) trong bộ chuyển mạch, HBA hoặc CNA, và lớp ảo hóa. Che giấu LUN đề cập đến việc làm cho LUN hiển thị với một số máy chủ và không hiển thị với những máy chủ khác.

Đối với SAN, điều quan trọng là một bộ chuyển mạch phải xác minh danh tính của các bộ chuyển mạch khác trong SAN mà nó giao tiếp. Nếu xác thực bộ chuyển mạch không được thực hiện, một bộ chuyển mạch giả mạo có thể tham gia SAN và có khả năng làm tổn hại dữ liệu SAN. Tương tự như vậy, các nút trong SAN (ví dụ: thiết bị lưu trữ và máy chủ) có thể sử dụng xác thực để hạn chế quyền truy cập vào dữ liệu SAN.

Có hai thành phần chính của tính bí mật dữ liệu trên SAN: dữ liệu đang di chuyển và dữ liệu tĩnh. Các biện pháp bảo vệ mật mã có thể được sử dụng cho dữ liệu nhạy cảm và có giá trị cao trong SAN khi dữ liệu đang di chuyển cũng như khi ở trạng thái tĩnh trên thiết bị lưu trữ. Việc bảo vệ này có thể yêu cầu sử dụng phần cứng chuyên dụng có thể mã hóa dữ liệu đang được gửi đến thiết bị lưu trữ. Tham khảo 10.5.4 để biết hướng dẫn bổ sung về bảo vệ dữ liệu đang di chuyển và 10.5.5 để biết hướng dẫn về bảo vệ dữ liệu tĩnh.

Các kiểm soát liên quan đến SAN Fibre Channel như sau:

a) TC-FCSS-G01 Kiểm soát truy cập nút FCP

Truy cập nút FCP nên được kiểm soát bằng cách hạn chế quyền truy cập máy chủ trên các bộ chuyển mạch bằng các kỹ thuật như danh sách kiểm soát truy cập (ACL), danh sách ràng buộc và chính sách fabric FC-SP-2.

b) TC-FCSS-G02 Sử dụng các kiểm soát dựa trên bộ chuyển mạch FC

Các kiểm soát dựa trên bộ chuyển mạch nên được thực hiện để:

- hạn chế kết nối bộ chuyển mạch bằng các kỹ thuật như ACL, danh sách ràng buộc và chính sách fabric FC-SP-2;
- thiết lập phân vùng để sử dụng trong fabric FC SAN với ưu tiên phân vùng cứng;
- xác định xem phân vùng cơ bản có phải là biện pháp bảo mật đủ mạnh cho môi trường mục tiêu hay không, và nếu không, sử dụng các kỹ thuật mạnh hơn như Phân vùng FC-SP-2 nếu được nhà cung cấp hỗ trợ;
- vô hiệu hóa các cổng không sử dụng;
- cẩn thận sử dụng các vùng và bộ vùng mặc định (theo nguyên tắc đặc quyền tối thiểu).

c) TC-FCSS-G03 Cấu hình thiết bị FC để đáp ứng yêu cầu bảo mật

Khi cấu hình bộ chuyển mạch, bộ mở rộng, bộ định tuyến và cổng (ví dụ: FCIP) để kết nối các mạng lưu trữ, cấu hình nên đáp ứng các yêu cầu bảo mật. Phần 10.9.1 cung cấp hướng dẫn về lưu trữ Fibre Channel dựa trên khối.

10.8.2.3 SAN IP

Mạng khu vực lưu trữ Internet SCSI (iSCSI), được mô tả trong IETF RFC 7143, là một giao thức lệnh/phản hồi hướng kết nối chạy trên TCP, và được sử dụng để truy cập mạng vào đĩa, băng từ và các thiết bị khác. Các kiểm soát liên quan đến SAN IP như sau:

a) TC-IPSS-G01 Sử dụng truy cập mạng và giao thức iSCSI

Truy cập mạng và giao thức iSCSI nên được kiểm soát bằng cách:

- tách biệt các giao diện iSCSI khỏi các mạng LAN đa năng để cung cấp bảo mật và hiệu suất tốt hơn;
- sử dụng mạng cục bộ ảo (VLAN) khi việc sử dụng mạng LAN cách ly vật lý không phải là một tùy chọn.

Fibre Channel qua IP (FCIP), được định nghĩa trong IETF RFC 3821, là một giao thức đóng gói Fibre Channel thuần túy. FCIP cho phép kết nối các đảo Mạng Khu vực Lưu trữ Fibre Channel thông qua các mạng dựa trên IP để tạo thành một SAN thống nhất.

b) TC-IPSS-G02 Sử dụng truy cập mạng và giao thức FCIP

Truy cập mạng và giao thức FCIP nên được kiểm soát bằng cách:

- thiết lập mối quan hệ ngang hàng giữa các thực thể FCIP, nhận biết rằng các chính sách bảo mật được áp dụng thống nhất;
- sử dụng mạng IP riêng, được các thực thể FCIP sử dụng độc quyền, bất cứ khi nào có thể.

c) TC-IPSS-G03 Sử dụng IPsec để bảo mật FCIP

Các biện pháp bảo mật IPsec (xem 10.5.4.3) nên được thực hiện kết hợp với FCIP bằng cách:

- thực hiện xác thực mật mã và toàn vẹn dữ liệu ở mức tối thiểu;
- bảo vệ dữ liệu nhạy cảm bằng các biện pháp bảo mật thích hợp.

IETF RFC 3723 cung cấp thông tin hữu ích bổ sung về cả iSCSI và FCIP. Phần 10.9.2 cung cấp hướng dẫn về lưu trữ IP dựa trên khối. Ngoài ra, IETF RFC 7146 cung cấp các cập nhật bảo mật quan trọng cho IETF RFC 3723 và IETF RFC 3821.

10.8.2.4 InfiniBand

InfiniBand là một kết nối có độ trễ thấp, băng thông cao, yêu cầu chi phí xử lý thấp và lý tưởng để mang nhiều loại lưu lượng (phân cụm, truyền thông, lưu trữ, quản lý) qua một kết nối duy nhất. InfiniBand là một kiến trúc kết nối điểm-điểm dựa trên bộ chuyển mạch hoạt động cả trên bảng mạch in như một kết nối thành phần-với-thành phần, cũng như một kết nối khung-với-khung.

Kiến trúc InfiniBand định nghĩa nhiều thiết bị cho giao tiếp hệ thống: bộ điều hợp kênh (xem CHÚ THÍCH 1), bộ chuyển mạch, bộ định tuyến và trình quản lý mạng con (xem CHÚ THÍCH 2). Trong một mạng con, InfiniBand yêu cầu phải có ít nhất một bộ điều hợp kênh cho mỗi nút cuối và một trình quản lý mạng con để thiết lập và duy trì liên kết. Ngoài ra, InfiniBand yêu cầu tất cả các bộ điều hợp kênh và bộ chuyển mạch phải chứa một tác nhân quản lý mạng con để xử lý giao tiếp với trình quản lý mạng con.

CHÚ THÍCH 1: Bộ điều hợp kênh kết nối InfiniBand với các thiết bị khác. Có hai loại bộ điều hợp kênh, bộ điều hợp kênh máy chủ và bộ điều hợp kênh đích.

CHÚ THÍCH 2: Trình quản lý mạng con cấu hình mạng con cục bộ và đảm bảo hoạt động liên tục của nó. InfiniBand yêu cầu phải có ít nhất một trình quản lý mạng con trong mạng con để quản lý tất cả các thiết lập bộ chuyển mạch và bộ định tuyến và để cấu hình lại mạng con khi một liên kết bị ngắt hoặc một liên kết mới được thiết lập.

Các kiểm soát liên quan đến SAN InfiniBand như sau:

TC-IBSS-G01 Bảo vệ SAN InfiniBand

SAN InfiniBand nên được bảo vệ bằng cách:

- giữ an toàn cho tất cả các máy chủ IB được gắn vào fabric IB vì fabric IB chỉ an toàn như máy chủ IB kém an toàn nhất được gắn vào nó;

- duy trì an toàn vật lý vì kẻ tấn công có thể kết nối máy chủ giả mạo với bộ chuyển mạch IB có thể được sử dụng để làm tổn hại đến an toàn của fabric IB.

10.8.2.5 NVMe qua Fabrics

NVM Express (NVMe) được bộ xử lý sử dụng để giao tiếp với bộ nhớ bền vững qua bus PCI Express (PCIe), bao gồm cả các ổ đĩa thể rắn (SSD) gắn NVMe ở nhiều dạng thức. NVMe được thiết kế để tận dụng độ trễ thấp và tính song song nội bộ của các phương tiện nhanh hơn, chẳng hạn như SSD và các công nghệ dựa trên lưu trữ flash.

NVMe qua Fabric (NVMe-oF™) là một giao thức truyền thông để hiển thị các mục tiêu NVMe từ một hệ thống từ xa cho máy khách thông qua việc đóng gói các lệnh Quản trị và vào/ra NVMe qua nhiều phương tiện truyền tải khác nhau được gọi là fabric. Các fabric này có thể là các phương tiện truyền tải dựa trên lưu trữ, ví dụ: truy cập bộ nhớ trực tiếp từ xa (RDMA), và các phương tiện truyền tải dựa trên thông điệp, ví dụ: TCP và FC. NVMe-oF quy định ba họ fabric:

- NVMe qua Fibre Channel (NVMe/FC);
- NVMe qua TCP (NVMe/TCP);
- NVMe qua RDMA (NVMe/RDMA), bao gồm:

    + NVMe qua RDMA qua Ethernet hội tụ (RoCE);

    + NVMe qua InfiniBand;

    + NVMe qua iWARP (qua Ethernet truyền thống).

Các kiểm soát liên quan đến NVMe-oF như sau:

a) TC-NVSS-G01 Sử dụng xác thực NVMe-oF

NVMe-oF hỗ trợ hai loại xác thực cấp cao (kênh an toàn fabric và xác thực trong băng). Nên sử dụng một hoặc cả hai cơ chế xác thực.

b) TC-NVSS-G02 Sử dụng các kiểm soát an toàn NVMe/FC

Các kiểm soát an toàn cho NVMe/FC có thể bao gồm một số kiểm soát được sử dụng với các kiểm soát SAN FC (xem 10.8.2.2).

Đối với NVMe/FC, nên sử dụng những điều sau:

- an toàn vật lý đầy đủ, bao gồm các mạng tách biệt;
- phân vùng FC để phân vùng các fabric FC;
- che giấu LUN trên lưu trữ để hạn chế quyền truy cập vào LUN cụ thể;
- xác thực các thiết bị Fibre Channel, trao đổi khóa an toàn và giao tiếp an toàn (tức là được mã hóa) giữa các thiết bị Fibre Channel.

CHÚ THÍCH: Tiêu chuẩn NVMe-oF chuyển các mối quan tâm bảo mật cụ thể của NVMe/FC sang tiêu chuẩn kỹ thuật FC-SP-2, bao gồm các giao thức để tăng cường bảo mật Fibre Channel trong một số lĩnh vực.

c) TC-NVSS-G03 Sử dụng các kiểm soát an toàn NVMe/TCP

Nên sử dụng các kiểm soát an toàn cho NVMe/TCP, bao gồm:

- chỉ xác thực (yêu cầu cung cấp bí mật xác thực, một cho mỗi thực thể) với DH-HMAC-CHAP;
- kênh an toàn được nối với một giao dịch xác thực (trong đó giao dịch xác thực tạo ra một khóa chia sẻ trước tạm thời để được sử dụng bởi giao thức kênh an toàn);
- chỉ kênh an toàn (yêu cầu cung cấp khóa chia sẻ trước cho mỗi cặp thực thể được phép giao tiếp);

– bảo mật truyền thông thích hợp với các giải pháp NVMe-oF, cụ thể:

+ TLS được sử dụng và không có phiên bản nào của Giao thức Lớp Socket Bảo mật (SSL) được sử dụng;

+ các giải pháp NVMe-oF dựa trên NVMe-oF Bản sửa đổi 1.1 không sử dụng các phiên bản giao thức TLS thấp hơn 1.2;

+ các giải pháp NVMe-oF dựa trên đặc tả NVMe Base Revision 2.0 và đặc tả NVMe qua TCP Revision 1.0 không sử dụng các phiên bản giao thức TLS thấp hơn 1.3.

d) TC-NVSS-G04 Sử dụng các kiểm soát an toàn NVMe/RDMA

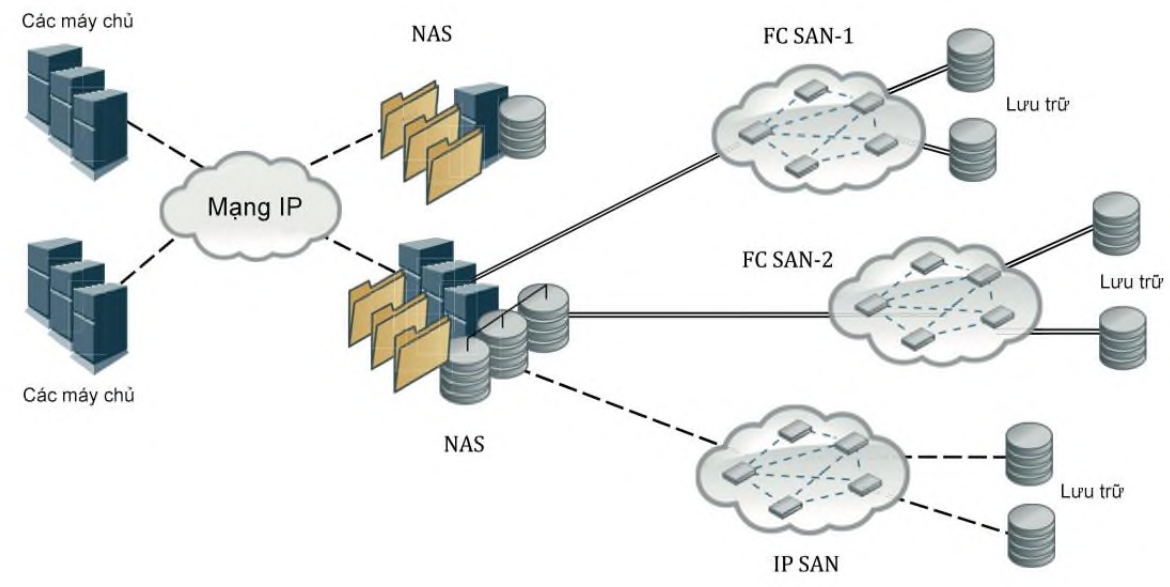
Các Kiểm soát An toàn cho NVMe/RDMA nên sử dụng xác thực trong băng được cung cấp bởi DH-HMAC-CHAP.

10.8.3 Giao thức Lưu trữ Gắn mạng

10.8.3.1 Tổng quát

Lưu trữ gắn mạng (NAS) là một công nghệ lưu trữ dữ liệu cung cấp quyền truy cập cấp tệp cho các máy khách không đồng nhất qua mạng. NAS cho phép một hệ thống tệp vật lý nằm trên một máy chủ hoặc thiết bị được truy cập bởi các máy tính khách từ xa, xuất hiện cho người dùng như một hệ thống tệp cục bộ. Hệ thống NAS thường được thiết kế và xây dựng đặc biệt cho mục đích NAS, nhưng các máy tính máy chủ đa năng cũng có thể được sử dụng.

Hệ thống NAS có thể được triển khai dưới dạng các máy chủ lưu trữ riêng lẻ hoặc dưới dạng một tập hợp các máy chủ lưu trữ được phân cụm, phân phối động các kết nối máy khách bằng cách cắt lát hoặc phân dải (striping) dữ liệu và siêu dữ liệu trên các máy chủ lưu trữ được phân cụm (xem Hình 6). Ngoài ra, hệ thống NAS có thể sử dụng một hoặc nhiều SAN để lưu trữ dữ liệu cục bộ hoặc ngoài khu vực (được hiển thị là FC SAN-1 và FC SAN-2 trong Hình 6).



Hình 6 - Ví dụ về lưu trữ gắn mạng

Các triển khai hệ thống tệp phổ biến bao gồm Hệ thống Tệp Mạng (NFS) và Hệ thống tệp Internet chung sử dụng Khối thông điệp máy chủ (SMB), ngoài các công nghệ khác như Lưu trữ Dựa trên Đối tượng và lưu trữ điện toán đám mây. Các giao thức này có thể được cấu hình để giúp bảo mật NAS.

Tham khảo 10.10 để biết các kiểm soát bổ sung cho NAS và lưu trữ dựa trên tệp.

10.8.3.2 Hệ thống Tệp Mạng

Hệ thống tệp mạng (NFS) là một ứng dụng máy khách/máy chủ, giao tiếp bằng giao thức dựa trên lệnh gọi thủ tục từ xa. Nhiều phiên bản NFS được quy định và đang được sử dụng, bao gồm NFS phiên bản 3 (được quy định trong IETF RFC 1813), NFS phiên bản 4 (được quy định trong IETF RFC 7530) và NFS phiên bản 4.1 (được quy định trong IETF RFC 8881). Từ góc độ bảo mật, NFS phiên bản 3 (NFSv3) được coi là kém an toàn hơn và cần phải cẩn thận hơn khi sử dụng nó với dữ liệu nhạy cảm hoặc có giá trị cao.

Các kiểm soát liên quan đến NFS như sau:

a) TC-NASP-G01 Sử dụng truy cập mạng và giao thức NFS

Truy cập mạng và giao thức NFS nên được kiểm soát bằng cách:

- chỉ bật NFS nếu được yêu cầu để loại bỏ nó như một vectơ tấn công có thể có sẵn cho đối thủ;
- sử dụng NFSv4 (hoặc các phiên bản mới hơn) bất cứ khi nào có thể và hạn chế sử dụng NFSv3;
- lọc quyền truy cập máy khách và quản lý theo địa chỉ IP để tăng cường bảo mật.

b) TC-NASP-G02 Sử dụng mã hóa để bảo mật NFS

Truy cập dữ liệu máy khách NFS nên sử dụng mã hóa (ví dụ: IPsec hoặc TLS).

10.8.3.3 Khối thông điệp máy chủ (SMB)

SMB 3 là một giao thức nhằm cung cấp một cơ chế đa nền tảng mở cho các hệ thống máy khách yêu cầu dịch vụ tệp từ các hệ thống máy chủ qua mạng. Giao thức này dựa trên giao thức SMB tiêu chuẩn được sử dụng rộng rãi bởi các máy tính cá nhân và máy trạm chạy nhiều loại hệ điều hành khác nhau.

Các kiểm soát liên quan đến SMB như sau:

TC-NASP-G03 Sử dụng truy cập mạng và giao thức SMB

Hướng dẫn mạng sau đây áp dụng cho NAS dựa trên SMB và nên được sử dụng:

- sử dụng các phiên bản mới hơn của giao thức SMB;

- tắt các giao thức đàm phán phiên bảo mật thấp và sử dụng Kerberos thay thế;

- duy trì các cấp bản vá cập nhật;

- sử dụng ký SMB;

- duy trì các dịch vụ thư mục một cách an toàn;

- sử dụng các mối quan hệ tin cậy một chiều, từ các miền lá đến các miền cha, khi có thể;

- kiểm soát truy cập mạng và giao thức SMB bằng cách:

+ chỉ bật SMB nếu cần thiết. Điều này loại bỏ nó như một vectơ tấn công có thể có sẵn cho đối thủ;

+ mã hóa truy cập dữ liệu máy khách khi cần thiết.

10.9 Lưu trữ dựa trên khối

10.9.1 Lưu trữ Fibre Channel (FC)

Hệ thống lưu trữ Fibre Channel sử dụng mạng chuyên dụng (xem 10.8.2.2) để trình bày các tài nguyên lưu trữ dựa trên khối cho máy tính. Các tài nguyên này thường có dạng đơn vị logic (lưu trữ logic) và thiết bị băng từ (bao gồm cả băng từ ảo).

Các kiểm soát liên quan đến lưu trữ FC như sau:

a) TC-BBFC-G01 Sử dụng che giấu và ánh xạ LUN FC

Che giấu và ánh xạ LUN (lọc tên cổng toàn cầu) cũng như các cơ chế kiểm soát truy cập khác nên được sử dụng để hạn chế quyền truy cập vào lưu trữ.

b) TC-BBFC-G02 Sử dụng các biện pháp bảo mật FCP cho SCSI

Nên sử dụng các biện pháp bảo mật FCP cho SCSI, bao gồm:

- xác thực lẫn nhau bằng FC-SP-2 AUTH-A với tất cả các máy chủ và bộ chuyển mạch, tận dụng các dịch vụ xác thực tập trung khi có thể;
- mã hóa các kết nối Fibre Channel rời khỏi khu vực được bảo vệ (ví dụ: giới hạn của một trung tâm dữ liệu được kiểm soát vật lý) bằng ESP_Header.

CHÚ THÍCH 1: Tính toàn vẹn hoặc bảo mật khung Fibre Channel có thể được cung cấp bằng các tiêu đề tùy chọn ESP_Header, được định nghĩa trong Tài liệu tham khảo [60].

c) TC-BBFC-G03 Sử dụng mã hóa dữ liệu tĩnh cho lưu trữ FC

Nên sử dụng các biện pháp mã hóa dữ liệu tĩnh (xem 10.5.5) để:

- bảo vệ tính bí mật của dữ liệu nhạy cảm hoặc có giá trị cao được ghi trên các thiết bị hoặc phương tiện lưu trữ FC;

CHÚ THÍCH 2: Mã hóa trong các hệ sinh thái lưu trữ FC cung cấp bảo vệ cấp phương tiện và có thể là một mạng lưới an toàn cho dữ liệu thường được mã hóa bởi máy chủ, ứng dụng, v.v. làm hình thức bảo vệ chính.

- tạo điều kiện loại bỏ nhanh chóng dữ liệu trên lưu trữ FC bằng cách xóa bằng mật mã (xem 10.6.5).

d) TC-BBFC-G04 Sử dụng làm sạch lưu trữ cho lưu trữ FC

Nên sử dụng các biện pháp làm sạch lưu trữ (xem 10.6) dưới dạng:

- làm sạch phù hợp với phương tiện (xem 10.6.3) cho phương tiện lưu trữ FC và thiết bị lưu trữ đối với dữ liệu nhạy cảm và được quản lý;
- làm sạch logic (xem 10.6.4) cho lưu trữ FC được ảo hóa (xem 10.16.1), đặc biệt khi không thể xác định được các thiết bị và phương tiện lưu trữ thực tế.

10.9.2 Lưu trữ IP

Không giống như lưu trữ FC, lưu trữ IP sử dụng mạng TCP/IP (xem 10.8.2.3), cụ thể là iSCSI, để trình bày các tài nguyên lưu trữ dựa trên khối cho máy tính.

Các kiểm soát liên quan đến lưu trữ IP như sau:

a) TC-BBIP-G01 Lọc truy cập trình khởi tạo iSCSI

Truy cập trình khởi tạo iSCSI nên được kiểm soát bằng cách lọc dựa trên địa chỉ IP nguồn và giao thức.

b) TC-BBIP-G02 Sử dụng các biện pháp bảo mật iSCSI

Nên sử dụng các biện pháp bảo mật iSCSI, bao gồm:

- xác thực CHAP hai chiều, sử dụng các thách thức ngẫu nhiên (tức là không lặp lại), cho cả trình khởi tạo và mục tiêu;
- IPsec để bảo mật kênh truyền thông khi dữ liệu nhạy cảm hoặc có giá trị cao có thể bị lộ (xem 10.5.4.3);
- cơ sở hạ tầng Dịch vụ Tên Lưu trữ Internet (iSNS), SLP, DNS với các kiểm soát an toàn thích hợp để tránh các cuộc tấn công gián tiếp.

c) TC-BBIP-G03 Sử dụng mã hóa dữ liệu tĩnh cho lưu trữ IP

Nên sử dụng các biện pháp mã hóa dữ liệu tĩnh (xem 10.5.5) để:

- bảo vệ tính bí mật của dữ liệu nhạy cảm hoặc có giá trị cao được ghi trên các thiết bị hoặc phương tiện lưu trữ IP;

CHÚ THÍCH: Mã hóa trong các hệ sinh thái lưu trữ FC cung cấp bảo vệ cấp phương tiện và có thể là một mạng lưới an toàn cho dữ liệu thường được mã hóa bởi máy chủ, ứng dụng, v.v. làm hình thức bảo vệ chính.

- tạo điều kiện loại bỏ nhanh chóng dữ liệu trên lưu trữ IP bằng cách xóa bằng mật mã (xem 10.6.5).

d) TC-BBIP-G04 Sử dụng làm sạch lưu trữ cho lưu trữ IP

Nên sử dụng các biện pháp làm sạch lưu trữ (xem 10.6) dưới dạng:

- làm sạch phù hợp với phương tiện (xem 10.6.3) cho phương tiện lưu trữ IP và thiết bị lưu trữ đối với dữ liệu nhạy cảm và được quản lý;
- làm sạch logic (xem 10.6.4) cho lưu trữ IP được ảo hóa (xem 10.16.1), đặc biệt khi không thể xác định được các thiết bị và phương tiện lưu trữ thực tế.

10.10 Lưu trữ dựa trên tệp

10.10.1 Tổng quát

Các kiểm soát an toàn liên quan đến lưu trữ dựa trên tệp (thường là NAS) được nhóm thành các loại sau:

- kiểm soát ủy quyền, chẳng hạn như ACL, hạn chế quyền truy cập của người dùng vào tài nguyên tệp và thư mục do thiết bị NAS cung cấp;
- mã hóa dữ liệu tĩnh;
- kiểm soát xác thực, chẳng hạn như Kerberos, để xác minh danh tính của người dùng cố gắng truy cập dữ liệu NAS.

10.10.2 NAS dựa trên NFS

Loại lưu trữ này về cơ bản là một máy chủ tệp được gắn vào mạng LAN trình bày các tệp bằng giao thức mạng, NFS (xem 10.8.3.2). Loại lưu trữ này bao gồm một công cụ thực hiện các dịch vụ tệp và một hoặc nhiều thiết bị lưu trữ, trên đó dữ liệu được lưu trữ. Hệ thống NAS cũng có thể được gắn vào nút, trong trường hợp đó hệ thống NAS được coi giống như bất kỳ máy chủ nào khác trên SAN (ví dụ: được cấp quyền truy cập vào lưu trữ và sao lưu không qua mạng LAN). Hệ thống NAS dựa trên NFS có thể có nhiều dạng khác nhau (ví dụ: từ máy chủ NAS đơn giản đến các cụm có khả năng mở rộng cao), và chúng có xu hướng được tối ưu hóa cao để xử lý số lượng lớn các truy cập tệp đồng thời. Các kiểm soát liên quan đến NAS dựa trên NFS như sau:

a) TC-FBNF-R01 Áp dụng kiểm soát truy cập NFS

Kiểm soát truy cập phải được áp dụng cho các hệ thống tệp được xuất NFS để:

- sử dụng xác thực cấp người dùng bất cứ khi nào có thể (ví dụ: NFSv4 với Kerberos V5);
- cấu hình máy chủ NFS để xuất các hệ thống tệp một cách rõ ràng cho những người dùng được ủy quyền;
- cấu hình máy chủ NFS để xuất các hệ thống tệp với các đặc quyền yêu cầu tối thiểu;
- tránh cấp quyền truy cập root hoặc quản trị viên vào các tệp trên hệ thống tệp mạng;
- đảm bảo ACL NFSv4 (danh sách kiểm soát truy cập) được gán chính xác;
- sử dụng xác thực Kerberos cho NFSv3;
- khi thích hợp, sử dụng các chế độ Kerberos An toàn và Riêng tư để ký và mã hóa lưu lượng NFS.

b) TC-FBNF-R02 Hạn chế hành vi máy khách NFS

Hành vi máy khách NFS phải bị hạn chế để:

- lọc quyền truy cập máy khách vào các chia sẻ NFS bất cứ khi nào có thể;
- không cho phép máy khách NFS chạy các chương trình cung cấp quyền được nâng cao tạm thời trong quá trình thực thi trên các hệ thống tệp được xuất.

c) TC-FBNF-G01 Bảo mật dữ liệu trên máy chủ NFS

Dữ liệu trên máy chủ NFS nên được bảo mật bằng cách:

- đảm bảo các hệ thống tệp được xuất nằm trong các phân vùng riêng của chúng để ngăn chặn sự suy giảm hệ thống do kẻ tấn công ghi vào hệ thống tệp được xuất cho đến khi đầy;
- mã hóa dữ liệu tĩnh khi cần thiết;
- không cho phép xuất NFS các hệ thống tệp quản trị;
- bảo vệ chống lại phần mềm độc hại (ví dụ: vi-rút, sâu và rootkit);
- liên tục giám sát nội dung được đặt trong các chia sẻ NFS và các kiểm soát truy cập liên quan.

10.10.3 NAS dựa trên SMB

Giống như NAS dựa trên NFS (xem 10.10.2), NAS dựa trên SMB là một máy chủ tệp được gắn vào mạng LAN phục vụ các tệp, nhưng nó khác ở việc sử dụng các giao thức mạng, SMB (xem 10.8.3.3). Các kiểm soát liên quan đến NAS dựa trên SMB như sau:

a) TC-FBSM-R01 Giao thức SMB tối thiểu chấp nhận được

Đối với NAS dựa trên SMB, phải sử dụng SMB phiên bản 3 trở lên và tất cả các phiên bản trước đó phải bị vô hiệu hóa.

b) TC-FBSM-R02 Áp dụng kiểm soát truy cập SMB

Kiểm soát truy cập phải được áp dụng cho các hệ thống tệp được xuất SMB để:

- vô hiệu hóa quyền truy cập không được xác thực vào các chia sẻ SMB và thiết bị NAS (tức là hạn chế quyền truy cập Vô danh);
- vô hiệu hóa quyền truy cập Khách và Mọi người vào tất cả các chia sẻ SMB;
- thực hiện xác thực và kiểm soát truy cập thông qua một cơ chế tập trung (RADIUS, Giao thức Truy cập Thư mục Nhẹ).

c) TC-FBSM-R03 Hạn chế hành vi máy khách SMB

Hành vi máy khách SMB phải bị hạn chế bằng cách bật ký SMB cho máy khách và thiết bị NAS.

d) TC-FBSM-G01 Bảo mật dữ liệu trên máy chủ SMB

Dữ liệu trên máy chủ SMB nên được bảo mật bằng cách:

- bật kiểm toán SMB bất cứ khi nào có thể;
- liên tục xem xét nội dung được đặt trong các chia sẻ SMB và các kiểm soát truy cập liên quan;
- mã hóa dữ liệu tĩnh khi cần thiết;
- bảo vệ chống lại phần mềm độc hại (ví dụ: vi-rút, sâu và rootkit);
- sử dụng SMB với xác thực mạnh (Kerberos).

10.11 Lưu trữ điện toán đám mây

10.11.1 Bảo mật lưu trữ điện toán đám mây

Cả các dịch vụ lưu trữ điện toán đám mây độc quyền và dựa trên tiêu chuẩn đều đang được sử dụng và thường cung cấp các khả năng sao chép (ví dụ: nhân bản một phần hoặc toàn bộ lưu trữ trên một hệ thống), khả năng sao lưu và phục hồi, khả năng lưu giữ dài hạn (ví dụ: kho lưu trữ) và khả năng đồng bộ hóa đa hệ thống (ví dụ: cho phép người dùng đồng bộ hóa dữ liệu trên nhiều thiết bị và có thể khác loại). Tuy nhiên, các cá nhân và tổ chức ngần ngại giao phó dữ liệu của họ cho lưu trữ điện toán đám mây trừ khi họ có sự đảm bảo rằng các mối đe dọa và thách thức bảo mật liên quan đã được giải quyết (xem Tài liệu tham khảo [77] để biết tóm tắt hữu ích về các mối đe dọa và thách thức bảo mật điện toán đám mây).

Một số triển khai điện toán đám mây này dựa trên đối tượng và thường phụ thuộc vào HTTPS (HTTP qua TLS) để bảo mật các giao tiếp cơ bản. Các tính năng bảo mật bổ sung có thể được chỉ định, nhưng có thể có sự khác biệt đáng kể về những gì được triển khai so với những gì cuối cùng được sử dụng.

Các kiểm soát liên quan đến bảo mật lưu trữ điện toán đám mây như sau:

a) TC-CCSS-G01 Sử dụng bảo mật truyền tải cho các giao dịch đám mây

Bảo mật truyền tải như IPsec hoặc Transport Layer Security (TLS) nên được sử dụng cho tất cả các giao dịch (xem 10.5.4).

b) TC-CCSS-G02 Sử dụng mã hóa dữ liệu tĩnh cho lưu trữ đám mây

Mã hóa dữ liệu tĩnh (và các quy trình quản lý khóa thích hợp) nên được sử dụng để ngăn chặn truy cập bởi các bên trái phép (ví dụ: nhân viên nhà cung cấp dịch vụ đám mây, những bên thuê khác và đối thủ).

c) TC-CCSS-G03 Sử dụng xác thực mạnh để truy cập lưu trữ đám mây

Đăng ký người dùng nên được bảo mật và xác thực mạnh nên được sử dụng để bảo vệ quyền truy cập vào dữ liệu.

d) TC-CCSS-G04 Sử dụng kiểm soát truy cập để bảo vệ dữ liệu trên lưu trữ đám mây

Nên sử dụng kiểm soát truy cập để bảo vệ chống lại truy cập trái phép từ những bên thuê khác đồng thời cung cấp các đặc quyền truy cập thích hợp cho những người dùng được phép truy cập dữ liệu.

e) TC-CCSS-G05 Sử dụng làm sạch lưu trữ cho lưu trữ đám mây

Nên sử dụng các khả năng làm sạch lưu trữ được cung cấp để loại bỏ dữ liệu nhạy cảm khỏi lưu trữ điện toán đám mây.

CHÚ THÍCH: Ở một số khu vực pháp lý, các yêu cầu về quyền riêng tư như quyền xóa bỏ hoặc quyền được lãng quên có thể yêu cầu các kiểm soát bảo mật bổ sung. Các triển khai điện toán đám mây thường tận dụng các dạng ảo hóa khác nhau, vì vậy hướng dẫn trong 10.16 cũng có thể liên quan.

10.11.2 Bảo mật CDMI

Lưu trữ điện toán đám mây, dựa trên đặc tả về giao diện quản lý dữ liệu đám mây (CDMI) có trong TCVN 13575 (ISO/IEC 17826), là một công nghệ lưu trữ dựa trên đối tượng sử dụng giao diện HTTP dựa trên RESTful. Các biện pháp bảo mật trong CDMI có thể được tóm tắt là bảo mật truyền tải, xác thực người dùng và thực thể, ủy quyền và kiểm soát truy cập, toàn vẹn dữ liệu, làm sạch dữ liệu và phương tiện, lưu giữ dữ liệu, bảo vệ chống phần mềm độc hại, mã hóa dữ liệu tĩnh và truy vấn khả năng bảo mật. Ngoại trừ cả bảo mật truyền tải và truy vấn khả năng bảo mật (cơ chế xác định những gì được hỗ trợ), bắt buộc phải triển khai (việc sử dụng luôn là tùy chọn), các biện pháp bảo mật có thể khác nhau đáng kể giữa các triển khai.

Các kiểm soát liên quan đến bảo mật CDMI như sau:

a) TC-CDMI-R01 Sử dụng TLS cho tất cả các giao dịch CDMI

Transport Layer Security (TLS) phải được sử dụng cho tất cả các giao dịch CDMI (xem 10.5.4.2).

b) TC-CDMI-R02 Xác thực lẫn nhau tất cả các thực thể CDMI

Các thực thể CDMI (chứng chỉ cho máy chủ và xác thực cơ bản HTTP cho máy khách) phải được xác thực.

c) TC-CDMI-G01 Sử dụng truy vấn khả năng CDMI để đánh giá tính đầy đủ về bảo mật

Tính đầy đủ của các khả năng bảo mật của việc triển khai CDMI của nhà cung cấp dịch vụ đám mây nên được xác định bằng các truy vấn khả năng CDMI để xác định chức năng bảo mật được cung cấp.

d) TC-CDMI-G02 Sử dụng các miền CDMI

Các miền CDMI nên được sử dụng để cung cấp một nơi cho các ánh xạ xác thực đến các nhà cung cấp xác thực bên ngoài.

e) TC-CDMI-G03 Tích hợp ghi nhật ký CDMI vào nhật ký kiểm toán

Ghi nhật ký bảo mật CDMI nên được bật và dữ liệu sự kiện bảo mật có trong các hàng đợi ghi nhật ký thích hợp nên được truy xuất một cách thường xuyên và kịp thời.

f) TC-CDMI-G04 Cấu hình lưu giữ CDMI để điều chỉnh việc tự động xóa với chính sách

Khả năng xóa tự động (xóa CDMI) nên được điều chỉnh phù hợp với chính sách lưu giữ dữ liệu của tổ chức.

g) TC-CDMI-G05 Xác minh khả năng gỡ bỏ giữ CDMI trước khi sử dụng khả năng này

Trước khi sử dụng giữ CDMI, quy trình và cơ chế gỡ bỏ giữ CDMI nên được hiểu rõ.

h) TC-CDMI-G06 Sử dụng mã hóa dữ liệu tĩnh cho lưu trữ CDMI

Nên sử dụng các biện pháp mã hóa dữ liệu tĩnh để bảo vệ dữ liệu nhạy cảm và có giá trị cao.

i) TC-CDMI-G07 Sử dụng làm sạch lưu trữ cho lưu trữ CDMI

Nên sử dụng làm sạch lưu trữ được cung cấp để loại bỏ dữ liệu nhạy cảm khỏi lưu trữ của nhà cung cấp dịch vụ đám mây.

10.12 Lưu trữ dựa trên đối tượng

Lưu trữ dựa trên đối tượng là một kiến trúc lưu trữ dữ liệu để xử lý lượng lớn dữ liệu phi cấu trúc. Các đơn vị dữ liệu rời rạc (đối tượng) được lưu trữ trong một môi trường dữ liệu phẳng về mặt cấu trúc. Mỗi đối tượng là một kho lưu trữ đơn giản, độc lập bao gồm dữ liệu, siêu dữ liệu (thông tin mô tả, tùy chỉnh liên quan đến một đối tượng) và một số ID nhận dạng duy nhất (thay vì tên tệp và đường dẫn tệp). Siêu dữ liệu hoặc ID có thể được ứng dụng sử dụng để định vị và truy cập các đối tượng. Các đối tượng (dữ liệu) trong hệ thống lưu trữ đối tượng được truy cập thông qua API. API gốc cho lưu trữ đối tượng thường là API dựa trên HTTP RESTful (còn được gọi là dịch vụ web RESTful).

Các kiểm soát liên quan đến lưu trữ dựa trên đối tượng như sau:

a) TC-OBSS-G01 Sử dụng bảo mật truyền tải cho các giao dịch lưu trữ dựa trên đối tượng

Bảo mật truyền tải như IPsec hoặc Transport Layer Security (TLS) nên được sử dụng cho tất cả các giao dịch lưu trữ dựa trên đối tượng (xem 10.5.4).

b) TC-OBSS-G02 Sử dụng mã hóa dữ liệu tĩnh cho lưu trữ dựa trên đối tượng

Mã hóa dữ liệu tĩnh (ở cấp độ đối tượng hoặc cấp độ bên thuê) nên được sử dụng để ngăn chặn truy cập bởi các bên trái phép (ví dụ: nhân viên nhà cung cấp dịch vụ và đối thủ).

c) TC-OBSS-G03 Bật tính bất biến dữ liệu cho lưu trữ dựa trên đối tượng

Các đối tượng dữ liệu nên được bật các biện pháp bảo vệ tính bất biến dữ liệu thích hợp để bảo vệ chống lại việc xóa hoặc mã hóa độc hại do tai nạn (ví dụ: ransomware).

d) TC-OBSS-G04 Điều chỉnh các cơ chế bảo mật với bên thuê trên lưu trữ dựa trên đối tượng

Cơ chế bảo mật (ví dụ: xác thực và quản lý khóa) nên được điều chỉnh phù hợp với bên thuê trên lưu trữ dựa trên đối tượng.

e) TC-OBSS-G05 Sử dụng làm sạch lưu trữ cho lưu trữ dựa trên đối tượng

Nên sử dụng làm sạch lưu trữ được cung cấp để loại bỏ dữ liệu nhạy cảm khỏi lưu trữ dựa trên đối tượng.

10.13 Giảm dữ liệu

Trong quá trình kinh doanh thông thường, các tổ chức thường cố gắng giảm lượng dữ liệu họ lưu trữ và truyền đi nhằm nỗ lực giảm chi phí. Hai trong số các phương pháp phổ biến hơn là nén dữ liệu và khử trùng lặp dữ liệu. Nén dữ liệu tìm cách giảm lượng dữ liệu bằng cách mã hóa nó bằng một thuật toán đã biết để tạo ra một biểu diễn dữ liệu sử dụng ít bit lưu trữ hơn so với biểu diễn chưa được mã hóa. Mặt khác, khử trùng lặp dữ liệu cố gắng thay thế nhiều bản sao dữ liệu bằng các tham chiếu đến một bản sao dùng chung. Hai kỹ thuật này có thể được sử dụng cùng nhau để tối đa hóa việc giảm dữ liệu.

CHÚ THÍCH: Các thuật toán nén bao gồm các phương pháp mất dữ liệu (trong đó một phần thông tin gốc bị mất) và các phương pháp không mất dữ liệu (bảo toàn toàn bộ nội dung của dữ liệu gốc), nhưng trong ngành công nghiệp lưu trữ chỉ sử dụng các thuật toán không mất dữ liệu. Việc áp dụng một thuật toán nén cụ thể cho nhiều phiên bản dữ liệu có thể dẫn đến dữ liệu được mã hóa/nén giống hệt nhau nếu tồn tại các điều kiện bắt đầu giống nhau (ví dụ: bộ đệm lịch sử).

Nén dữ liệu thường được sử dụng kết hợp với lưu trữ băng từ để giảm số lượng băng cần thiết cho những việc như sao lưu. Ngoài ra, nén có thể là một phần không thể thiếu của các cổng mạng được sử dụng trong sao chép từ xa để giảm yêu cầu băng thông cho hỗ trợ BCM. Nén dữ liệu thường được thực hiện bằng phần cứng nên cần phải cẩn thận để đảm bảo dữ liệu được mã hóa có thể được giải mã sau

này (ví dụ: khi băng được đọc bởi một ổ băng khác hoặc khi dữ liệu nén được nhận bởi một cổng mạng).

Khử trùng lặp dữ liệu có thể diễn ra tại nhiều điểm khác nhau trong cơ sở hạ tầng lưu trữ, bao gồm ở cấp hệ thống tệp, nội tuyến với mạng lưu trữ và thiết bị lưu trữ. Bản thân các công nghệ giảm dữ liệu không đại diện cho các cơ chế bảo mật. Tuy nhiên, sự hiện diện của chúng có thể đòi hỏi những điều chỉnh đối với các hoạt động bảo mật lưu trữ.

Các kiểm soát liên quan đến giảm dữ liệu như sau:

a) TC-DRDC-G01 Sử dụng nén trước khi mã hóa

Khi mã hóa được sử dụng cùng với nén, việc nén nên được áp dụng trước khi mã hóa vì bản mã không nén hiệu quả; thứ tự ngược lại nên được sử dụng ở đầu kia (tức là giải mã sau đó là giải nén).

b) TC-DRDC-G02 Sử dụng khử trùng lặp trước khi mã hóa

Khi mã hóa được sử dụng cùng với khử trùng lặp, việc khử trùng lặp nên được áp dụng trước khi mã hóa trước khi ghi dữ liệu vì khử trùng lặp thường không hiệu quả trên bản mã; khi đọc dữ liệu, nên sử dụng thứ tự ngược lại.

c) TC-DRDC-G03 Sử dụng thứ tự chính xác cho nhiều lần giảm dữ liệu và mã hóa

Khi cả nén và khử trùng lặp được sử dụng cùng với mã hóa, thứ tự sử dụng nên là:

- khử trùng lặp, nén và mã hóa trước khi ghi dữ liệu (với thứ tự ngược lại được sử dụng khi đọc dữ liệu); hoặc
- nén, khử trùng lặp và mã hóa trước khi ghi dữ liệu (với thứ tự ngược lại được sử dụng khi đọc dữ liệu).

d) TC-DRDC-G04 Sử dụng giảm dữ liệu tương thích với BCM

Nén hoặc khử trùng lặp có thể tác động đến việc triển khai BCM, vì vậy chúng nên được tính đến trong thiết kế, tài liệu hóa và kiểm tra các giải pháp BCM.

10.14 Bảo vệ và phục hồi dữ liệu

10.14.1 Tổng quát

Từ góc độ lưu trữ, bảo vệ dữ liệu là quá trình bảo vệ dữ liệu quan trọng khỏi bị hỏng hoặc mất mát. Phục hồi dữ liệu là quá trình khôi phục dữ liệu đã bị mất, vô tình bị xóa, bị hỏng hoặc không thể truy cập được. Các tổ chức sử dụng các cơ chế và quy trình bảo vệ dữ liệu thường triển khai chúng theo cách cho phép phục hồi dữ liệu nhanh chóng và hoàn chỉnh (xem Tài liệu tham khảo [72] để biết tóm tắt hữu ích về bảo vệ dữ liệu với các hệ thống và hệ sinh thái lưu trữ). Do sự phụ thuộc ngày càng tăng vào tính sẵn sàng và toàn vẹn của dữ liệu, nhiều tổ chức sử dụng một loạt các cơ chế bảo vệ dữ liệu như sao lưu (xem 10.14.2) và sao chép (xem 10.14.3) để tăng khả năng phục hồi dữ liệu. Thật không may, trọng tâm thường là tạo ra các bản sao lưu và bộ dữ liệu sao chép thay vì khả năng sử dụng chúng để khắc phục sự cố. Tất cả các giải pháp bảo vệ dữ liệu có thể được xem là cơ chế phục hồi dữ liệu.

TC-PROT-G01 Thiết kế cơ chế bảo vệ dữ liệu để phục hồi nhanh chóng

Các cơ chế bảo vệ dữ liệu (như sao lưu và sao chép) nên được thiết kế với mục tiêu phục hồi nhanh chóng, thay vì chỉ bảo quản dữ liệu. Các mục tiêu thời gian phục hồi và mục tiêu điểm phục hồi cụ thể nên được bao gồm trong các thiết kế này.

10.14.2 Sao lưu lưu trữ

Mặc dù mất dữ liệu do lỗi công nghệ ít phổ biến hơn do phần cứng và phần mềm đáng tin cậy hơn, nhưng số lượng mối đe dọa lớn hơn đã xuất hiện từ vi-rút và ransomware. Rủi ro mất dữ liệu này đã buộc các tổ chức phải sử dụng một công nghệ được gọi là sao lưu lưu trữ. Các bản sao lưu này thường có dạng:

- sao lưu đầy đủ, sao chép tất cả các tệp trong một thư mục vào phương tiện lưu trữ bất kể các bản sao lưu trước đó;
- sao lưu tăng dần, chỉ sao chép những tệp trong thư mục đã thay đổi kể từ lần sao lưu cuối cùng (đầy đủ hoặc tăng dần), vào phương tiện lưu trữ;
- sao lưu khác biệt, sao chép tất cả các tệp trong một thư mục đã thay đổi kể từ lần sao lưu đầy đủ cuối cùng, vào phương tiện lưu trữ.

Một thách thức lớn với các bản sao lưu truyền thống (đầy đủ, tăng dần hoặc khác biệt) là chúng liên quan đến việc di chuyển các khối dữ liệu lớn, chẳng hạn như terabyte hoặc petabyte. Việc di chuyển các bộ dữ liệu lớn là một quá trình tốn thời gian và cuối cùng có thể dẫn đến việc vượt quá thời gian phục hồi yêu cầu của tổ chức.

ISO/IEC 27002:2022, 8.13 cung cấp thông tin hữu ích về sao lưu.

Các kiểm soát liên quan đến sao lưu lưu trữ như sau:

a) TC-PROT-G02 Sử dụng các biện pháp và hoạt động sao lưu dữ liệu một cách an toàn

Bảo mật sao lưu nên:

- đảm bảo rằng phương pháp sao lưu, đặc biệt đối với dữ liệu quan trọng cho kinh doanh/nhiệm vụ, phù hợp với chiến lược khôi phục liên quan của nó;
- đảm bảo rằng phương pháp sao lưu cung cấp sự bảo vệ đầy đủ và thích hợp chống lại truy cập trái phép (ví dụ: mã hóa hoặc xác thực người dùng);
- thiết lập một chuỗi các cá nhân (và nhà cung cấp) đáng tin cậy xử lý phương tiện lưu trữ;
- thực hiện xác thực sao lưu để chứng minh rằng các yêu cầu khôi phục đang được đáp ứng.

b) TC-PROT-G03 Sử dụng sao lưu phục hồi sau tấn công mạng

Trong khi nhiều tổ chức triển khai sao lưu cho mục đích phục hồi sau thảm họa và liên tục kinh doanh (không độc hại), một số tổ chức cũng đang thực hiện các bản sao lưu đặc biệt để hỗ trợ phục hồi sau tấn công mạng (ví dụ: tấn công ransomware). Ngoài các biện pháp bảo mật sao lưu thông thường, các bản sao lưu phục hồi sau tấn công mạng nên:

- không thể truy cập được bởi nhân viên CNTT thông thường, mà là một nhóm rất hẹp gồm những nhân viên được ủy quyền cụ thể;
- được lưu giữ trong khoảng thời gian dài hơn nhiều để cho phép điều tra và đối phó với các cuộc tấn công tiềm ẩn cho đến khi được kích hoạt sau đó;
- được lưu trữ ngoài địa điểm và tách biệt khỏi nơi lưu trữ các bản sao lưu lưu trữ sản xuất;
- sử dụng các bản sao lưu đầy đủ, độc lập một cách thường xuyên (tức là không phụ thuộc vào dữ liệu cơ sở sản xuất);
- được khôi phục vào một môi trường dàn dựng bị cô lập (hoặc cách ly không khí) thay vì trực tiếp vào máy chủ hoặc ứng dụng đích;
- sử dụng lưu trữ bất biến.

10.14.3 Sao chép lưu trữ

Sao chép liên quan đến việc tạo một bản sao của dữ liệu sản xuất sẵn sàng để sử dụng ngay lập tức mà không cần di chuyển hoặc thay đổi thêm. Sao chép là một quá trình phức tạp và tốn kém, và nó chỉ có thể sử dụng được trong các kịch bản hạn chế. Sao chép đã trở thành công nghệ hàng đầu trong các giải pháp phục hồi sau thảm họa vì nó có thể cung cấp khả năng không mất dữ liệu. Tuy nhiên, sao chép không bảo vệ khỏi việc xóa, hỏng hoặc sự kiện ransomware. Do đó, mặc dù hiệu quả, sao chép không phải là sự thay thế cho sao lưu.

Các kiểm soát liên quan đến sao chép lưu trữ như sau:

TC-PROT-G04 Sử dụng các biện pháp và hoạt động sao chép dữ liệu một cách an toàn

Bảo mật sao chép nên:

- đảm bảo rằng phương pháp sao chép, đặc biệt đối với dữ liệu quan trọng cho kinh doanh/nhiệm vụ, phù hợp với các yêu cầu về độ tin cậy, khả năng chịu lỗi hoặc hiệu suất liên quan của nó;
- đảm bảo rằng phương pháp sao chép cung cấp sự bảo vệ đầy đủ chống lại truy cập trái phép (ví dụ: mã hóa dữ liệu đang di chuyển).

10.14.4 Ảnh chụp nhanh lưu trữ

Ảnh chụp nhanh lưu trữ có thể là của một ổ đĩa lưu trữ, tệp hoặc cơ sở dữ liệu như chúng xuất hiện tại một thời điểm nhất định. Trong trường hợp xảy ra lỗi, người dùng có thể khôi phục dữ liệu của họ từ ảnh chụp nhanh gần đây nhất (hoặc bất kỳ ảnh chụp nhanh nào khác đã lưu trước đó) trước khi xảy ra lỗi. Không giống như sao lưu liên quan đến việc tạo bản sao dữ liệu, ảnh chụp nhanh duy trì các con trỏ đến dữ liệu và ghi lại các thay đổi đối với dữ liệu này (xóa, thêm, di chuyển, v.v.). Ảnh chụp nhanh thường không chiếm nhiều dung lượng lưu trữ riêng lẻ, nhưng tổng dung lượng của chúng có thể tăng lên, đặc biệt nếu có nhiều khối/tệp bị xóa, vì vậy các nhà cung cấp thường giới hạn số lượng ảnh chụp nhanh có thể được lưu giữ.

Các kiểm soát liên quan đến ảnh chụp nhanh lưu trữ như sau:

TC-PROT-G05 Sử dụng ảnh chụp nhanh kết hợp với sao lưu

Ảnh chụp nhanh nên được sử dụng kết hợp với chiến lược sao lưu để cung cấp bảo vệ thường xuyên hơn, được đo bằng phút hoặc giờ, trong khi sao lưu được sử dụng để bảo vệ hàng ngày. Khoảng thời gian của ảnh chụp nhanh nên dựa trên các yêu cầu về độ chi tiết để khôi phục từ một thời điểm cụ thể. Thời gian lưu giữ ảnh chụp nhanh nên cho phép một hoặc hai lần sao lưu diễn ra trong khoảng thời gian đó (tức là trước khi ảnh chụp nhanh bị xóa).

TC-PROT-G06 Sử dụng bảo mật ảnh chụp nhanh Bảo mật ảnh chụp nhanh nên:

- đảm bảo rằng phương pháp ảnh chụp nhanh, đặc biệt đối với dữ liệu quan trọng cho kinh doanh/nhiệm vụ, phù hợp với chiến lược phục hồi liên quan của nó;
- đảm bảo rằng ảnh chụp nhanh được bảo vệ khỏi các thay đổi (ví dụ: chỉ đọc);
- đảm bảo rằng phương pháp ảnh chụp nhanh cung cấp sự bảo vệ đầy đủ chống lại truy cập trái phép (ví dụ: mã hóa).

10.15 Kho lưu trữ và kho chứa dữ liệu

10.15.1 Tổng quát

Mặc dù có thể lập luận rằng kho lưu trữ dữ liệu chỉ đơn giản là một loại cơ sở dữ liệu đặc biệt, nhưng thường có sự khác biệt về trọng tâm giữa cơ sở dữ liệu và kho lưu trữ. Cả hai đều phục vụ các chức năng truy cập và bảo quản, nhưng cơ sở dữ liệu thường nhấn mạnh vào quyền truy cập, trong khi kho

lưu trữ thường nhấn mạnh vào việc bảo quản. Từ góc độ lưu trữ và bảo mật, sự khác biệt này có ý nghĩa lớn đối với công nghệ cơ bản và các kiểm soát cần thiết để bảo vệ dữ liệu.

10.15.2 Kho lưu trữ dữ liệu

10.15.2.1 Tổng quát

ISO 14721 chỉ ra rằng thuật ngữ "kho lưu trữ" đã được sử dụng để chỉ nhiều chức năng và hệ thống lưu trữ và bảo quản khác nhau. Hơn nữa, các kho lưu trữ truyền thống được hiểu là các cơ sở hoặc tổ chức bảo quản hồ sơ, ban đầu được tạo ra bởi hoặc cho một tổ chức chính phủ, viện hoặc tập đoàn, để cộng đồng công cộng hoặc tư nhân truy cập. Kho lưu trữ thực hiện nhiệm vụ này bằng cách sở hữu hồ sơ, đảm bảo rằng chúng dễ hiểu đối với cộng đồng truy cập, và quản lý chúng để bảo tồn nội dung thông tin và tính xác thực của chúng.

vì phục hồi ứng dụng. Ngoài ra, các yêu cầu lưu giữ có thể thay đổi (ví dụ: ngắn hạn, trung hạn và dài hạn), nhưng kho lưu trữ nên đảm bảo tính toàn vẹn, tính bất biến, tính xác thực, tính bí mật và nguồn gốc thích hợp.

ISO/TR 18492 định nghĩa bảo quản dài hạn là khoảng thời gian, dao động từ vài năm đến hàng trăm năm, mà thông tin dựa trên tài liệu điện tử được duy trì dưới dạng bằng chứng có thể truy cập và xác thực. Thời gian lưu giữ thường được xác định bởi sự tuân thủ quy định, yêu cầu pháp lý và nhu cầu kinh doanh, vì vậy chúng có thể thay đổi đáng kể từ tổ chức này sang tổ chức khác.

Các kiểm soát liên quan đến kho lưu trữ dữ liệu như sau:

a) TC-DARS-G01 Giải quyết các vấn đề bảo quản chính trong kho lưu trữ dữ liệu

Các tổ chức nên xem xét và giải quyết các vấn đề chính sau đây đối với kho lưu trữ dữ liệu có trong ISO/TR 18492 khi phát triển chiến lược bảo quản dài hạn.

- Thông tin dựa trên tài liệu điện tử có thể đọc được. Luồng bit bao gồm thông tin dựa trên tài liệu điện tử phải có thể truy cập được trên hệ thống máy tính hoặc thiết bị ban đầu tạo ra nó, hiện đang lưu trữ nó, hiện đang truy cập nó, hoặc có thể được sử dụng để lưu trữ nó trong tương lai; sự lỗi thời của phương tiện và định dạng dữ liệu cũng là những cân nhắc.
- Thông tin dựa trên tài liệu điện tử có thể hiểu được. Khả năng hiểu được của thông tin dựa trên tài liệu điện tử là một chức năng của thông tin liên quan đến những gì luồng bit thực sự đại diện và khả năng của phần mềm xử lý để thực hiện hành động thích hợp dựa trên thông tin này.
- Thông tin dựa trên tài liệu điện tử có thể nhận dạng được. Thông tin dựa trên tài liệu nên được tổ chức, phân loại và mô tả theo cách mà người dùng và hệ thống thông tin có thể phân biệt giữa các đối tượng thông tin dựa trên một thuộc tính duy nhất như tên hoặc số ID. Việc tạo điều kiện tìm kiếm và truy xuất cũng là một cân nhắc.
- Thông tin dựa trên tài liệu có thể truy xuất được. Các đối tượng thông tin rời rạc (hoặc các phần của chúng) có thể được truy xuất và hiển thị. Khả năng truy xuất thường phụ thuộc vào phần mềm ở chỗ nó yêu cầu các khóa hoặc con trỏ liên kết cấu trúc logic của các đối tượng thông tin (ví dụ: các trường dữ liệu hoặc chuỗi văn bản) với vị trí lưu trữ vật lý của chúng.
- Thông tin dựa trên tài liệu có thể hiểu được. Truyền đạt thông tin cho cả máy tính và người dùng ngoài nội dung tài liệu, bao gồm bối cảnh tạo và sử dụng (tức là siêu dữ liệu) cũng như mối quan hệ giữa các tài liệu khác.
- Thông tin dựa trên tài liệu điện tử xác thực. Đảm bảo thông tin là những gì nó được cho là, nghĩa là, thông tin mà theo thời gian, chưa bị thay đổi, thay đổi hoặc bị hỏng theo cách khác.

b) TC-DARS-G02 Sử dụng các dịch vụ bảo mật để giải quyết các khía cạnh chứng cứ của kho lưu trữ

Các kho lưu trữ có khả năng liên quan đến chứng cứ nên giải quyết các khía cạnh xác thực dữ liệu, nguồn gốc và chuỗi hành trình, bao gồm lưu giữ, bảo vệ và duy trì một lượng lớn siêu dữ liệu. Các tổ chức nên sử dụng các dịch vụ bảo mật sau đây được xác định bởi ISO 14721 cho cả dữ liệu và siêu dữ liệu.

- Dịch vụ nhận dạng/xác thực xác nhận danh tính của người yêu cầu sử dụng tài nguyên hệ thống thông tin. Ngoài ra, xác thực có thể áp dụng cho các nhà cung cấp dữ liệu. Dịch vụ xác thực nên xảy ra khi bắt đầu một phiên hoặc trong một phiên.
- Dịch vụ kiểm soát truy cập ngăn chặn việc sử dụng trái phép tài nguyên hệ thống thông tin. Dịch vụ này cũng ngăn chặn việc sử dụng tài nguyên một cách trái phép. Dịch vụ này nên được áp dụng cho các khía cạnh khác nhau của việc truy cập tài nguyên (ví dụ: truy cập vào các giao tiếp đến tài nguyên, việc đọc, ghi hoặc xóa tài nguyên thông tin/dữ liệu, việc thực thi tài nguyên xử lý) hoặc cho tất cả các truy cập vào tài nguyên.
- Dịch vụ toàn vẹn dữ liệu đảm bảo rằng dữ liệu không bị thay đổi hoặc tiêu hủy một cách trái phép. Dịch vụ này áp dụng cho dữ liệu trong các kho dữ liệu cố định và cho dữ liệu trong các thông điệp truyền thông.
- Dịch vụ bảo mật dữ liệu đảm bảo rằng dữ liệu không được cung cấp hoặc tiết lộ cho các cá nhân hoặc quy trình máy tính trái phép. Dịch vụ này có thể được áp dụng cho các thiết bị cho phép tương tác giữa người dùng và hệ thống thông tin. Ngoài ra, dịch vụ này có thể đảm bảo rằng không thể quan sát được các mẫu sử dụng tài nguyên truyền thông.
- Dịch vụ không thể chối cãi đảm bảo rằng các thực thể tham gia trao đổi thông tin không thể phủ nhận việc tham gia vào đó. Dịch vụ này có thể có một hoặc cả hai dạng sau. Thứ nhất, người nhận dữ liệu được cung cấp bằng chứng về nguồn gốc của dữ liệu. Điều này bảo vệ chống lại mọi nỗ lực của người gửi nhằm phủ nhận sai việc gửi dữ liệu hoặc nội dung của nó. Thứ hai, người gửi dữ liệu được cung cấp bằng chứng về việc gửi dữ liệu. Điều này bảo vệ chống lại mọi nỗ lực tiếp theo của người nhận nhằm phủ nhận sai việc nhận dữ liệu hoặc nội dung của nó.

Các dịch vụ bảo mật này nên được áp dụng trong quá trình lưu trữ và truyền dữ liệu và siêu dữ liệu đến và từ kho lưu trữ. Quan trọng không kém, cần phải cẩn thận khi các dịch vụ/kiểm soát bảo mật được điều chỉnh/thay thế để tránh làm lộ dữ liệu lưu trữ cho các cuộc tấn công hoặc tiết lộ (tức là rủi ro).

Trong nhiều tiêu chuẩn và ấn phẩm, quyền riêng tư thường không được đề cập trực tiếp trong bối cảnh kho lưu trữ. Tuy nhiên, với sự gia tăng các quy định về quyền riêng tư (bảo vệ PII) trên toàn thế giới, đây là một khía cạnh quan trọng cần giải quyết. Nguồn gốc và tính xác thực là những yếu tố thiết yếu của hầu hết các kho lưu trữ, điều đó có nghĩa là cần phải xử lý siêu dữ liệu đúng cách. Các biện pháp chuỗi hành trình cũng có thể cần thiết để giải quyết các yêu cầu về chứng cứ, điều này có thể làm phức tạp bản chất của các giải pháp kho lưu trữ được sử dụng (ví dụ: lưu trữ dựa trên điện toán đám mây có thể không cung cấp được các chi tiết cần thiết).

Nhiều kho lưu trữ quan tâm đến việc "chứng minh" dữ liệu không bị thay đổi (tính xác thực), sử dụng các phương pháp xác minh tính toàn vẹn. Một chiến lược thay thế là sử dụng các biện pháp bất biến (ví dụ: lưu trữ WORM) để ngăn chặn các thay đổi.

10.15.2.2 Kho lưu trữ ngắn hạn đến trung hạn

Một số lượng lớn các tổ chức phải lưu giữ dữ liệu trong khoảng thời gian ngắn hơn các kho lưu trữ truyền thống (dưới 10 năm). Thông thường, các yếu tố thúc đẩy việc lưu giữ dựa trên các yêu cầu pháp lý, quy định hoặc luật định cũng bao gồm các điều khoản bảo mật. Việc không đáp ứng các yêu cầu có thể dẫn đến trách nhiệm pháp lý đáng kể cho tổ chức.

Việc lưu giữ và bảo quản dữ liệu thành công trong các khoảng thời gian lưu giữ ngắn hạn đến trung hạn có thể liên quan đến việc sử dụng các biện pháp bảo vệ dữ liệu, quản lý liên tục kinh doanh, và các thực

hành bảo quản và giám tuyển kỹ thuật số. Các biện pháp cụ thể thường tương xứng với giá trị của dữ liệu đang được lưu giữ, rủi ro mất mát từ tất cả các yếu tố, và mức độ mất mát chấp nhận được trong khoảng thời gian lưu giữ. Từ góc độ lưu trữ, các kịch bản lưu giữ dữ liệu ngắn hạn và trung hạn này thường kéo dài một hoặc nhiều thế hệ công nghệ và yêu cầu thu thập và lưu giữ siêu dữ liệu liên quan.

Các kiểm soát liên quan đến kho lưu trữ ngắn hạn đến trung hạn như sau:

a) TC-DARS-G03 Tạo nhiều bản sao vật lý hoặc logic của dữ liệu được lưu giữ trong kho lưu trữ

Nên tạo và bảo quản nhiều bản sao vật lý hoặc logic của dữ liệu; dữ liệu lưu trữ không nên phụ thuộc vào dữ liệu cơ sở sản xuất hoặc phục hồi sau thảm họa. Các bản sao nên được tổ chức độc lập nhất có thể (ví dụ: về địa lý, hành chính/quản lý và nền tảng/hệ điều hành), và số lượng của chúng được chọn theo giá trị của dữ liệu và khả năng chịu rủi ro.

CHÚ THÍCH: Khía cạnh quan trọng cần xem xét là chất lượng và đặc điểm của quy trình lưu trữ kỹ thuật số, thay vì có bao nhiêu bản sao.

b) TC-DARS-G04 Thực hiện kiểm toán tính toàn vẹn thường xuyên đối với dữ liệu được lưu giữ trong kho lưu trữ

Nên thực hiện kiểm toán tính toàn vẹn theo lịch trình xác định, tìm kiếm cả lỗi rõ ràng và tiềm ẩn (ví dụ: kiểm tra tính toàn vẹn) và thiệt hại mà chúng gây ra. Dữ liệu bị hỏng nên được sửa chữa bằng dữ liệu tốt từ các bản sao khác trước khi thiệt hại đó lan rộng.

c) TC-DARS-G05 Kiểm soát truy cập đối với dữ liệu được lưu giữ trong kho lưu trữ phù hợp với các yêu cầu pháp lý và quy định

Là một phần của việc giải quyết các nghĩa vụ pháp lý và quy định (ví dụ: bảo vệ PII) liên quan đến truy cập dữ liệu, lược đồ kiểm soát truy cập nên đủ mạnh để bảo vệ chống lại truy cập không phù hợp ngay cả khi các nghĩa vụ thay đổi theo thời gian.

d) TC-DARS-G06 Sử dụng các biện pháp trách nhiệm giải trình và truy xuất nguồn gốc để truy cập dữ liệu của kho lưu trữ

Nên thực hiện và kiểm tra định kỳ các biện pháp trách nhiệm giải trình và truy xuất nguồn gốc để xác định xem chúng có đầy đủ và hoạt động hay không. Tất cả các truy cập dữ liệu nhạy cảm hoặc có giá trị cao nên được ghi lại trong các mục nhập nhật ký kiểm toán.

e) TC-DARS-G07 Sử dụng các cơ chế để giải quyết tính xác thực, nguồn gốc và chuỗi hành trình dữ liệu đối với dữ liệu được lưu giữ trong kho lưu trữ

Nên thực hiện các cơ chế để giải quyết tính xác thực, nguồn gốc và chuỗi hành trình dữ liệu, đặc biệt đối với dữ liệu có tính chất chứng cứ.

f) TC-DARS-G08 Đảm bảo quản lý vòng đời khóa thích hợp đối với dữ liệu được lưu giữ trong kho lưu trữ

Nếu sử dụng mã hóa, các khóa và nguyên liệu khóa nên được lưu trữ hoặc ký gửi. Dữ liệu nên được đổi khóa trong các chu kỳ mật mã được khuyến nghị hoặc khi thuật toán mật mã cơ bản đang được thay thế.

10.15.2.3 Kho lưu trữ dài hạn

Do tuổi thọ khá ngắn và độ tin cậy hạn chế của các thành phần lưu trữ truyền thống, dữ liệu có thể bị hỏng khi phương tiện lưu trữ xuống cấp theo thời gian. Vấn đề này được những người tham gia vào việc

lưu giữ dữ liệu dài hạn (ví dụ: quản lý kho lưu trữ dữ liệu) hiểu tương đối rõ. Vấn đề này được giải quyết trong các tiêu chuẩn sau, áp dụng cho cơ sở hạ tầng lưu trữ:

- ISO/TR 10255;
- ISO/TR 18492;
- ISO 16175-1;
- ISO/TS 16175-2.

Hệ thống lưu trữ dài hạn giới thiệu các mối đe dọa về tính toàn vẹn, xác thực và quyền riêng tư thường không tồn tại trong các hệ thống lưu trữ không lưu trữ. Ngoài ra, tuổi thọ dài của dữ liệu mang lại cho những kẻ tấn công một cửa sổ lớn hơn nhiều để họ có thể cố gắng xâm phạm hệ thống bảo mật. Với lưu trữ dài hạn, kẻ tấn công có thể có vài thập kỷ để tiến hành một cuộc tấn công (tấn công chậm).

Các kiểm soát liên quan đến kho lưu trữ ngắn hạn đến trung hạn (xem 10.15.2.2) áp dụng cho kho lưu trữ dài hạn. Các kiểm soát bổ sung dành riêng cho kho lưu trữ dài hạn cũng có thể áp dụng.

Các kiểm soát liên quan đến kho lưu trữ dài hạn như sau:

a) TC-DARS-G09 Chủ động kiểm tra tính toàn vẹn dữ liệu của kho lưu trữ dài hạn

Lưu trữ dài hạn giả định một mẫu truy cập ghi một lần, đọc hạn chế, do đó tính toàn vẹn của dữ liệu trong hệ thống nên được chủ động kiểm tra định kỳ thay vì đợi cho đến khi nó được đọc.

b) TC-DARS-G10 Nâng cấp bảo mật trong quá trình làm mới công nghệ của kho lưu trữ dài hạn

Khi di chuyển dữ liệu lưu trữ sang các công nghệ lưu trữ mới hơn, các khả năng bảo mật cung cấp các biện pháp bảo mật nâng cao để bảo mật dữ liệu tốt hơn ở vị trí mới của nó cũng nên được nâng cấp.

c) TC-DARS-G11 Quản lý người dùng và quyền truy cập vào kho lưu trữ dài hạn

Vì dữ liệu trong kho lưu trữ dài hạn có thể tồn tại lâu hơn chủ sở hữu dữ liệu, một hệ thống lưu trữ dài hạn, an toàn nên có khả năng xác thực người dùng mới và thiết lập mối quan hệ của họ với các tài nguyên và dữ liệu được gắn với người dùng hiện có.

d) TC-DARS-G12 Duy trì các biện pháp bảo mật dữ liệu trong khi được lưu giữ trong kho lưu trữ dài hạn

Các cơ chế bảo mật (ví dụ: mã hóa và chia sẻ khóa) nên hoạt động khi hoàn toàn không có người dùng đã lưu trữ dữ liệu (ví dụ: người dùng mới được cấp quyền đọc dữ liệu cũng nên được cấp khả năng giải mã dữ liệu).

e) TC-DARS-G13 Lưu giữ nhật ký bảo mật cho kho lưu trữ dài hạn

Ghi nhật ký bảo mật nên đầy đủ và có thời gian tồn tại đủ dài (được đo bằng thập kỷ) để hỗ trợ phát hiện các cuộc tấn công chậm và duy trì lịch sử tấn công có thể được sử dụng để đưa ra quyết định điều chỉnh các biện pháp bảo vệ dữ liệu.

f) TC-DARS-G14 Phát hiện và giải quyết các xâm phạm của kho lưu trữ dài hạn

Hệ thống kho lưu trữ nên giải quyết ngay lập tức mọi xâm phạm hoặc duy trì lịch sử các xâm phạm để lên lịch hành động khắc phục một cách thông minh.

g) TC-DARS-G15 Đảm bảo rằng các công nghệ giảm dữ liệu không ảnh hưởng đến tính toàn vẹn dữ liệu của kho lưu trữ dài hạn

Việc sử dụng các công nghệ giảm dữ liệu (ví dụ: nén và khử trùng lặp) nên được sử dụng theo cách tránh làm tổn hại tính toàn vẹn dữ liệu (ví dụ: được tính vào các bản sao không có bất kỳ liên kết nào với các công nghệ giảm dữ liệu).

10.15.3 Kho chứa dữ liệu

Khi dữ liệu trở nên quan trọng hơn đối với việc ra quyết định kinh doanh, nhu cầu về các nền tảng có thể thu thập, lưu trữ và phân tích dữ liệu ngày càng tăng. Kho chứa dữ liệu là một thực thể lưu trữ mà có thể giúp hợp nhất và quản lý dữ liệu doanh nghiệp quan trọng. Các dạng phổ biến của các kho chứa dữ liệu này bao gồm kho dữ liệu, hồ dữ liệu, chợ dữ liệu và khối dữ liệu.

Kho chứa dữ liệu có thể đưa ra những phức tạp bổ sung bao gồm:

- kho chứa dữ liệu thường bao gồm các thành phần không đồng nhất trong đó một lược đồ bảo mật duy nhất chưa được thiết kế ngay từ đầu;
- kho chứa dữ liệu ngày càng liên quan đến một hoặc nhiều nguồn dữ liệu được truyền trực tuyến được sử dụng kết hợp với dữ liệu tĩnh, tạo ra các kịch bản bảo mật và quyền riêng tư độc đáo;
- nhiều nguồn dữ liệu ban đầu không nhằm mục đích sử dụng cùng nhau có thể làm tổn hại đến quyền riêng tư, bảo mật hoặc cả hai;
- các vấn đề về tính xác thực, bối cảnh, nguồn gốc và khu vực pháp lý có thể bị phóng đại đáng kể trong các kho chứa dữ liệu;
- dữ liệu có thể được bảo quản vượt quá tuổi thọ của các biện pháp bảo mật được thiết kế để bảo vệ nó;
- luồng dữ liệu xuyên biên giới được tạo điều kiện bởi các kho chứa dữ liệu có thể đặt ra những thách thức tuân thủ cho các tổ chức khi dữ liệu di chuyển qua biên giới quốc gia.

Các kiểm soát liên quan đến kho chứa dữ liệu như sau:

TC-DARS-G16 Sử dụng các kiểm soát bảo mật cho kho chứa dữ liệu

Ngoài các kiểm soát trong 10.15.2, những điều sau đây nên được sử dụng cho các kho chứa dữ liệu:

- thông tin không nên được cung cấp hoặc tiết lộ cho các cá nhân, thực thể hoặc quy trình trái phép;
- tính chính xác và đầy đủ của dữ liệu nên được duy trì trong toàn bộ vòng đời của chúng;
- khả năng truy cập và sử dụng nên được đảm bảo theo yêu cầu của một thực thể được ủy quyền;
- việc sử dụng, lưu giữ và tiết lộ (bao gồm cả chuyển giao) PII nên được giới hạn ở mức cần thiết để thực hiện các mục đích cụ thể, rõ ràng và hợp pháp. Ngoài ra, dự kiến các mục đích của kho chứa dữ liệu tuân thủ luật hiện hành và dựa trên cơ sở pháp lý cho phép. Người ta giả định rằng việc thu thập PII nằm trong giới hạn của luật hiện hành và hoàn toàn cần thiết cho mục đích được chỉ định.

Dữ liệu lớn thường được sử dụng kết hợp với các kho chứa dữ liệu, vì vậy hướng dẫn về bảo mật và quyền riêng tư trong ISO/IEC 20547-4 có thể liên quan.

10.16 Ảo hóa

10.16.1 Ảo hóa lưu trữ

Ảo hóa lưu trữ tách biệt các trừu tượng lưu trữ logic được sử dụng bởi máy chủ và ứng dụng khỏi các hệ thống, thiết bị hoặc phương tiện lưu trữ vật lý nơi dữ liệu được lưu trữ theo cách cho phép mối quan hệ logic với vật lý đó thay đổi theo thời gian và có thể che giấu các chi tiết của các thực thể vật lý. Ví dụ, một trình quản lý ổ đĩa logic trong máy chủ hoặc mảng lưu trữ có thể trình bày các phần của nhiều ổ đĩa vật lý dưới dạng một ổ đĩa logic được nhân bản duy nhất và có khả năng xây dựng lại ổ đĩa được nhân bản để sử dụng một ổ đĩa khác sau khi một trong các ổ đĩa gốc bị lỗi. Một ví dụ khác là chức năng phân tầng tự động trong một mảng lưu trữ có thể thay đổi các ổ đĩa nơi dữ liệu được lưu trữ để đáp ứng các mẫu truy cập đã thay đổi (ví dụ: di chuyển dữ liệu được truy cập thường xuyên hơn đến các ổ đĩa hiệu suất cao hơn).

Sự có mặt của ảo hóa lưu trữ là một yếu tố cân nhắc quan trọng trong thiết kế và ứng dụng kiểm soát. Kiểm soát có thể được áp dụng cho các thực thể lưu trữ logic hoặc vật lý. Kiểm soát trên các thực thể lưu trữ logic thường không bị ảnh hưởng bởi việc di chuyển vật lý của dữ liệu. Việc áp dụng kiểm soát trên các thực thể vật lý có thể liên quan đến toàn bộ miền của các thực thể vật lý (ví dụ: hệ thống, thiết bị, phương tiện lưu trữ) nơi dữ liệu có khả năng được lưu trữ. Phạm vi bao phủ mở rộng này là cần thiết để tránh các tình huống trong đó việc di chuyển dữ liệu dẫn đến việc bỏ qua các kiểm soát.

Các kiểm soát liên quan đến ảo hóa lưu trữ như sau:

a) TC-SVSS-G01 Áp dụng các kiểm soát mạng lưu trữ cho tất cả các thực thể tham gia vào ảo hóa lưu trữ

Khi ảo hóa lưu trữ lưu trữ hoặc di chuyển dữ liệu qua một miền các thực thể phân tán (ví dụ: dữ liệu được lưu trữ trên một trong nhiều hệ thống lưu trữ và được di chuyển theo thời gian) và mạng lưu trữ đang được sử dụng, các kiểm soát mạng lưu trữ thích hợp (xem 10.8) nên được áp dụng cho toàn bộ miền đó. Nếu một kiểm soát mạng được áp dụng cho một tập hợp con của miền, có khả năng kiểm soát mạng bị bỏ qua khi dữ liệu được di chuyển hoặc dữ liệu mới thuộc đối tượng kiểm soát được lưu trữ trên một thực thể mà kiểm soát chưa được áp dụng.

b) TC-SVSS-G02 Hạn chế hoặc ngăn chặn truy cập trực tiếp vào các yếu tố vật lý không được ảo hóa

Nếu ảo hóa lưu trữ làm lộ các thực thể lưu trữ vật lý được ảo hóa (ví dụ: lưu trữ bên ngoài được ảo hóa bởi một mảng lưu trữ), các kiểm soát nên được áp dụng để hạn chế hoặc ngăn chặn truy cập trực tiếp vào các yếu tố vật lý không được ảo hóa, vì việc truy cập như vậy không tương đương với việc truy cập lưu trữ được ảo hóa.

c) TC-SVSS-G03 Sử dụng các kiểm soát bảo mật để bảo vệ dữ liệu trong lưu trữ được ảo hóa

Lưu trữ được ảo hóa và các thực thể lưu trữ vật lý cơ bản (ví dụ: hệ thống, thiết bị và phương tiện) nên sử dụng các kiểm soát thích hợp để bảo vệ dữ liệu nhạy cảm nhất có thể được lưu trữ trên chúng. Các kiểm soát này nên bao gồm:

- làm sạch lưu trữ (xem 10.6);
- mã hóa dữ liệu tĩnh (xem 10.5.5).

d) TC-SVSS-G04 Đáp ứng các mục tiêu cấp độ dịch vụ về tính sẵn sàng, bảo mật và quyền riêng tư cho lưu trữ được ảo hóa

Nên đáp ứng các mục tiêu cấp độ dịch vụ hướng bảo mật thích hợp cho lưu trữ được ảo hóa, bao gồm:

- phù hợp với mục tiêu sẵn có cho cơ sở hạ tầng lưu trữ với các yêu cầu ứng dụng;
- phù hợp các yêu cầu bảo mật và quyền riêng tư cho cơ sở hạ tầng lưu trữ với các loại dữ liệu được lưu trữ.

e) TC-SVSS-G05 Đảm bảo lưu trữ được ảo hóa giải quyết các yêu cầu bảo mật đa bên thuê

Nên giải quyết các yêu cầu bảo mật đa bên thuê, khi thích hợp (xem 10.17).

10.16.2 Lưu trữ cho các hệ thống được ảo hóa

Ảo hóa máy chủ mở rộng quyền truy cập chung vào tài nguyên của các hệ điều hành điển hình thành một mô hình trong đó phần mềm ảo hóa thay vào đó cung cấp ảo ảnh về nhiều hơn một máy tính, HDD, máy in, v.v. Máy chủ vật lý thường chạy một trình siêu giám sát có nhiệm vụ tạo, giải phóng và quản lý tài nguyên của các hệ điều hành khách, hoặc máy ảo (VM). Các hệ điều hành khách này được phân bổ

một phần tài nguyên của máy chủ vật lý, thường theo cách mà khách không biết về bất kỳ tài nguyên vật lý nào khác, ngoại trừ những tài nguyên được phân bổ cho nó bởi trình siêu giám sát.

Khi các hệ thống và cơ sở hạ tầng lưu trữ được sử dụng để hỗ trợ các máy chủ được ảo hóa, thường cần phải cẩn thận hơn để đảm bảo dữ liệu có sẵn, nhưng không bị lộ quá mức cho các vi phạm dữ liệu tiềm ẩn.

Các kiểm soát liên quan đến lưu trữ cho các hệ thống được ảo hóa như sau:

a) TC-SVSS-G06 Kiểm soát quyền truy cập VM vào mạng lưu trữ

Quyền truy cập VM vào mạng lưu trữ nên được kiểm soát thông qua việc sử dụng các kiểm soát truy cập trong phần mềm ảo hóa máy chủ (trình siêu giám sát).

b) TC-SVSS-G07 Kiểm soát di chuyển/di trú VM giữa các máy chủ vật lý

Việc di chuyển/di trú VM giữa các máy chủ vật lý trong một cơ sở hạ tầng nên được kiểm soát để tránh có những hậu quả bảo mật ngoài ý muốn, chẳng hạn như:

- di chuyển VM từ miền rủi ro thấp hơn (đáng tin cậy hơn) sang miền rủi ro cao hơn (ít tin cậy hơn) có thể làm lộ dữ liệu nhạy cảm mà máy chủ chứa hoặc được phép xử lý trừ khi cấu hình của nó được củng cố thích hợp;
- ngược lại, khi VM được di chuyển từ miền rủi ro cao hơn (ít tin cậy hơn) sang miền rủi ro thấp hơn (đáng tin cậy hơn), cấu hình được củng cố của nó có thể cản trở hoạt động bình thường trừ khi cấu hình của nó được thay đổi thích hợp cho miền bảo mật thấp hơn;
- VM có thể di chuyển đến các máy chủ vật lý bị xâm phạm do đó đặt dữ liệu vào rủi ro.

10.17 Đa bên thuê an toàn

Đa bên thuê, như định nghĩa trong TCVN 13809-1 (ISO/IEC 22123-1), tập trung vào việc phân bổ tài nguyên dùng chung sao cho các phép tính và dữ liệu của từng bên thuê được cách ly và không thể truy cập lẫn nhau. Đa bên thuê an toàn xây dựng dựa trên khái niệm này bằng cách bổ sung các kiểm soát an toàn nhằm tường minh bảo vệ chống vi phạm dữ liệu, đồng thời cho phép xác minh trạng thái hoạt động của các kiểm soát đó (ví dụ: kiểm tra chúng có đang hoạt động không) và kiểm nhận tính hiệu quả của chúng.

Các kiểm soát liên quan đến đa bên thuê an toàn như sau:

a) TC-SMTS-G01 Cung cấp đảm bảo cách ly an toàn cho đa bên thuê

Khi xem xét đa bên thuê an toàn, điều quan trọng là phải bao gồm quan điểm của bên thuê (bao gồm cả quản trị viên của họ). Do đó, một giải pháp đa bên thuê an toàn nên cung cấp các đảm bảo cách ly an toàn trong khi vẫn mang lại lợi ích quản lý và linh hoạt của tài nguyên dùng chung mà kết hợp đảm bảo:

- không bên thuê nào có thể xác định sự tồn tại hoặc danh tính của bất kỳ bên thuê nào khác;
- không bên thuê nào có thể truy cập dữ liệu đang di chuyển (mạng) của bất kỳ bên thuê nào khác;
- không bên thuê nào có thể truy cập dữ liệu tĩnh (lưu trữ) của bất kỳ bên thuê nào khác;
- không bên thuê nào có thể thực hiện một hoạt động ảnh hưởng đến hoạt động được thực hiện bởi bên thuê khác;
- không bên thuê nào có thể thực hiện một hoạt động có thể từ chối dịch vụ cho bên thuê khác;
- mỗi bên thuê có thể có một cấu hình độc lập với sự tồn tại và cấu hình của bên thuê khác (ví dụ: trong việc đặt tên hoặc địa chỉ);
- khi một tài nguyên (máy tính, lưu trữ hoặc mạng) được ngừng hoạt động khỏi một bên thuê, tài nguyên đó được làm sạch khỏi tất cả dữ liệu và thông tin cấu hình;

- các biện pháp trách nhiệm giải trình và truy xuất nguồn gốc có sẵn ở cấp độ bên thuê.

b) TC-SMTS-G02 Sử dụng các biện pháp bảo mật cho đa bên thuê an toàn

Trong các hệ thống và cơ sở hạ tầng lưu trữ được sử dụng một phần hoặc toàn bộ cho các giải pháp đa bên thuê an toàn, nên sử dụng các biện pháp bảo mật bổ sung sau đây:

- lưu trữ được mã hóa phù hợp với việc sử dụng tài nguyên của bên thuê;
- mã hóa đối xứng mạnh (tức là tối thiểu 128-bit độ mạnh bảo mật) để bảo vệ dữ liệu tĩnh;
- hủy cấp phát an toàn và nhanh chóng (xem 10.6 để biết về làm sạch phương tiện lưu trữ, bao gồm cả xóa bằng mật mã);
- quản lý lưu trữ dữ liệu của bên thứ ba đáng tin cậy (ví dụ: SNMPv3);
- quản lý khóa tự động cung cấp quản lý khóa do bên thuê kiểm soát (tận dụng các máy chủ tuân thủ KMIP);
- sao chép dữ liệu an toàn (ví dụ: mã hóa dữ liệu đang di chuyển và dữ liệu tĩnh);
- bảo vệ dữ liệu khỏi quản trị viên (ví dụ: thực thi mô hình truy cập đặc quyền tối thiểu và không truy cập vào nguyên liệu khóa);
- fabric mạng lưu trữ có tính sẵn sàng cao (đa đường và đường dẫn đa dạng);
- ghi nhật ký kiểm toán tập trung và an toàn (ví dụ: syslog qua TLS);
- xác nhận và chứng nhận (ví dụ: Common Criteria) của các mô-đun mật mã và các biện pháp bảo mật khác (ví dụ: làm sạch phương tiện lưu trữ và kiểm soát truy cập).

10.18 Di chuyển dữ liệu tự động an toàn

Nhiều hệ thống và cơ sở hạ tầng lưu trữ có thể di chuyển dữ liệu giữa các thiết bị lưu trữ khác nhau (ví dụ: lưu trữ theo tầng), giữa các trung tâm dữ liệu (ví dụ: sao chép dữ liệu đồng bộ và không đồng bộ), đến các cơ sở lưu trữ dữ liệu và đến các hệ thống bảo vệ dữ liệu (ví dụ: sao lưu trên robot băng từ hoặc băng từ ảo). Các kịch bản phức tạp hơn tồn tại trong các giải pháp quản lý vòng đời thông tin và quản lý vòng đời dữ liệu. Tuy nhiên, tất cả các kịch bản này đều giả định:

- việc di chuyển dữ liệu được điều khiển bởi chính sách;
- sự can thiệp của người vận hành hoặc hệ thống công nghệ thông tin không cần thiết để khởi tạo hoặc can thiệp trong suốt quá trình.

Vì di chuyển dữ liệu tự động có nhiều dạng, nhu cầu bảo mật có thể thay đổi đáng kể.

Các kiểm soát liên quan đến di chuyển dữ liệu tự động an toàn như sau:

a) TC-SADM-G01 Sử dụng trách nhiệm giải trình và truy xuất nguồn gốc cho di chuyển dữ liệu tự động an toàn

Các cân nhắc về trách nhiệm giải trình và truy xuất nguồn gốc đối với di chuyển dữ liệu tự động an toàn có thể bao gồm:

- việc cấu hình chính sách di chuyển dữ liệu nên được hạn chế đối với những người dùng đặc quyền đã được xác thực và ủy quyền;
- cá nhân thiết lập cấu hình nên thông thạo các thuộc tính bí mật của cả nguồn và đích;
- các thay đổi cấu hình để triển khai hoặc chấm dứt di chuyển dữ liệu tự động nên được phản ánh trong nhật ký kiểm toán;
- tất cả các giao dịch di chuyển dữ liệu tự động nên được phản ánh trong nhật ký kiểm toán của hệ thống tiến hành di chuyển dữ liệu.

b) TC-SADM-G02 Sử dụng tính toàn vẹn, xác thực và bất biến cho di chuyển dữ liệu tự động an toàn

Các cân nhắc về tính toàn vẹn, xác thực và bất biến đối với các giao dịch di chuyển dữ liệu tự động an toàn nên bao gồm:

- xác minh tính toàn vẹn của dữ liệu đã di chuyển (tốt nhất là bằng hàm băm mật mã có chữ ký);
- đảm bảo không ảnh hưởng đến tính xác thực của dữ liệu (ví dụ: siêu dữ liệu hệ thống gốc như ngày tạo và lần truy cập cuối cùng được biểu thị chính xác trong dữ liệu đã di chuyển);
- đảm bảo tính bất biến hoặc các kiểm soát bảo quản dữ liệu khác (ví dụ: hỗ trợ giữ pháp lý) không bị phủ nhận.

c) TC-SADM-G03 Sử dụng tính bí mật cho di chuyển dữ liệu tự động an toàn

Các cân nhắc về tính bí mật đối với các giao dịch di chuyển dữ liệu tự động an toàn nên bao gồm:

- đảm bảo các kiểm soát mã hóa liên quan đến dữ liệu không bị loại bỏ hoặc suy yếu;
- đảm bảo mã hóa dữ liệu đang di chuyển được sử dụng cho dữ liệu nhạy cảm hoặc có giá trị cao khi di chuyển giữa các hệ thống.

d) TC-SADM-G04 Sử dụng làm sạch kết hợp với di chuyển dữ liệu tự động an toàn

Các cân nhắc về làm sạch đối với các giao dịch di chuyển dữ liệu tự động an toàn nên bao gồm:

- đảm bảo làm sạch thích hợp (xem 10.6.3 và 10.6.4) dữ liệu nguồn hoặc phương tiện lưu trữ trước khi chúng được giải phóng để tái sử dụng;
- đảm bảo xác minh làm sạch (xem 10.6.6) và tạo ra một số hình thức bằng chứng về việc làm sạch (xem 10.6.7).

e) TC-SADM-G05 Sử dụng tính đáng tin cậy và an toàn vật lý cho di chuyển dữ liệu tự động an toàn

Các cân nhắc về tính đáng tin cậy và an toàn vật lý đối với các giao dịch di chuyển dữ liệu tự động an toàn nên bao gồm:

- đảm bảo dữ liệu không vượt qua các miền bảo mật (ví dụ: môi trường sản xuất sang môi trường phát triển);
- đảm bảo dữ liệu không di chuyển đến các hệ thống có chứng nhận và công nhận không đầy đủ (ví dụ: ISO/IEC 19790, loạt TCVN 8709 (ISO/IEC 15408) và NIST FIPS 140-3);
- đảm bảo dữ liệu không di chuyển đến các hệ thống có an toàn vật lý không đầy đủ.

Phụ lục A
(tham khảo)
Tóm tắt các kiểm soát bảo mật lưu trữ

A.1 Tổng quát

Phụ lục này cung cấp tóm tắt các kiểm soát bảo mật lưu trữ được liệt kê trong toàn bộ tiêu chuẩn này. Mục đích của phụ lục này là giúp các tổ chức xác định những kiểm soát phù hợp nhất cho cơ sở hạ tầng lưu trữ của họ. Một sự khác biệt quan trọng giữa tiêu chuẩn này và phiên bản trước (ISO/IEC 27040:2015) là việc bao gồm các yêu cầu lưu trữ (được tóm tắt trong A.2), có khả năng được coi là một bộ kiểm soát cơ bản. Điều khoản A.3 cung cấp tóm tắt cả yêu cầu và khuyến nghị, dựa trên từng loại kiểm soát (tổ chức, con người, vật lý và công nghệ).

A.2 Các yêu cầu bảo mật lưu trữ

Bảng A.1 liệt kê các nhãn kiểm soát liên quan đến các yêu cầu hoặc cụm yêu cầu được cung cấp trong tiêu chuẩn này.

Bảng A.1 - Yêu cầu bảo mật lưu trữ

Loại kiểm soát	Kiểm soát	Số điều khoản
Tổ chức	OC-PLCY-R01 Bao gồm lưu trữ trong chính sách ghi nhật ký	7.2
Tổ chức	OC-CPLC-R01 Đảm bảo lưu trữ đáp ứng nghĩa vụ trách nhiệm giải trình của người dùng	7.4
Vật lý	PC-PHYS-R01 Bảo vệ giao diện vật lý	9.3
Công nghệ	TC-HARD-R01 Thực hiện ghi nhật ký trên lưu trữ	10.3.2
Công nghệ	TC-MGMT-R01 Biện pháp xác thực người dùng tối thiểu	10.4.2.1
Công nghệ	TC-MGMT-R02 Bảo mật quản lý từ xa	10.4.3
Công nghệ	TC-MGMT-R03 Hạn chế quản lý từ xa của nhà cung cấp	10.4.3
Công nghệ	TC-MGMT-R04 Hạn chế sử dụng truy cập quay số	10.4.3
Công nghệ	TC-MGMT-R05 Bảo mật IPMI	10.4.3
Công nghệ	TC-CNFD-R01 Sử dụng mật mã có độ mạnh an toàn ít nhất 128 bit	10.5.3

Loại kiểm soát	Kiểm soát	Số điều khoản
Công nghệ	TC-CNFD-R02 Yêu cầu tối thiểu TLS	10.5.4.2
Công nghệ	TC-CNFD-R03 Yêu cầu tối thiểu IPsec	10.5.4.3
Công nghệ	TC-CNFD-R04 Bảo vệ khóa được sử dụng để mã hóa lưu trữ	10.5.5
Công nghệ	TC-CNFD-R05 Sử dụng các thuật toán mã hóa và chế độ hoạt động thích hợp cho lưu trữ	10.5.5
Công nghệ	TC-CNFD-R06 Sử dụng khóa mật mã cho một mục đích	10.5.5
Công nghệ	TC-CNFD-R07 Tạo khóa ngẫu nhiên bằng toàn bộ không gian khóa	10.5.5
Công nghệ	TC-CNFD-R08 Việc sử dụng khóa bị giới hạn trong chu kỳ mật mã hữu hạn hoặc lượng dữ liệu xử lý tối đa	10.5.5
Công nghệ	TC-SNTZ-R01 Làm sạch lưu trữ trước khi thải bỏ	10.6.1
Công nghệ	TC-SNTZ-R02 Xác minh kết quả làm sạch lưu trữ	10.6.1
Công nghệ	TC-SNTZ-R03 Chọn phương pháp làm sạch lưu trữ tối thiểu chấp nhận được	10.6.2
Công nghệ	TC-SNTZ-R04 Làm sạch phương tiện phù hợp với các tiêu chuẩn chấp nhận được	10.6.3
Công nghệ	TC-SNTZ-R05 Xác minh tính đầy đủ của kết quả làm sạch phương tiện	10.6.3
Công nghệ	TC-SNTZ-R06 Làm sạch lưu trữ logic phù hợp với các tiêu chuẩn chấp nhận được	10.6.4
Công nghệ	TC-SNTZ-R07 Xác minh tính đầy đủ của kết quả làm sạch lưu trữ logic	10.6.4
Công nghệ	TC-SNTZ-R08 Sử dụng xóa bằng mật mã để thanh lọc trong điều kiện chính xác	10.6.5

Loại kiểm soát	Kiểm soát	Số điều khoản
Công nghệ	TC-SNTZ-R09 Xác minh kết quả phương pháp làm sạch bằng cách tiêu hủy	10.6.6
Công nghệ	TC-FBNF-R01 Áp dụng kiểm soát truy cập NFS	10.10.2
Công nghệ	TC-FBNF-R02 Hạn chế hành vi máy khách NFS	10.10.2
Công nghệ	TC-FBSM-R01 Giao thức SMB tối thiểu chấp nhận được	10.10.3
Công nghệ	TC-FBSM-R02 Áp dụng kiểm soát truy cập SMB	10.10.3
Công nghệ	TC-FBSM-R03 Hạn chế hành vi máy khách SMB	10.10.3
Công nghệ	TC-CDMI-R01 Sử dụng TLS cho tất cả các giao dịch CDMI	10.11.2
Công nghệ	TC-CDMI-R02 Xác thực lẫn nhau tất cả các thực thể CDMI	10.11.2

A.3 Các kiểm soát bảo mật lưu trữ

Bảng A.2 liệt kê các nhãn kiểm soát liên quan đến các yêu cầu và khuyến nghị hoặc cụm yêu cầu và khuyến nghị được cung cấp trong Điều 7.

Bảng A.2 - Các kiểm soát tổ chức bảo mật lưu trữ

Chủ đề	Kiểm soát	Số điều khoản
Chính sách	OC-PLCY-G01 Kết hợp lưu trữ vào chính sách	7.2
	OC-PLCY-G02 Đảm bảo lưu trữ tuân thủ chính sách	7.2
	OC-PLCY-R01 Bao gồm lưu trữ trong chính sách ghi nhật ký	7.2
Quản lý tính liên tục kinh doanh	OC-IRBC-G01 Tính đến hệ sinh thái lưu trữ trong lập kế hoạch và triển khai BCM	7.3
	OC-IRBC-G02 Chuẩn bị cho các sự kiện gián đoạn hạn chế	7.3

Chủ đề	Kiểm soát	Số điều khoản
	OC-IRBC-G03 Xác định và ghi lại các yêu cầu về nhân sự và cơ sở vật chất duy nhất	7.3
	OC-IRBC-G04 Thực hiện lập kế hoạch và kiểm tra BCM liên tục	7.3
Tuân thủ	OC-CPLC-R01 Đảm bảo lưu trữ đáp ứng nghĩa vụ trách nhiệm giải trình của người dùng	7.4
	OC-CPLC-G01 Đảm bảo lưu trữ đáp ứng nghĩa vụ truy xuất nguồn gốc người dùng	7.4
	OC-CPLC-G02 Đảm bảo lưu trữ đáp ứng nghĩa vụ giám sát người dùng	7.4
	OC-CPLC-G03 Đảm bảo lưu trữ đáp ứng nghĩa vụ lưu giữ và làm sạch dữ liệu	7.4
	OC-CPLC-G04 Đảm bảo lưu trữ đáp ứng nghĩa vụ về quyền riêng tư	7.4
	OC-CPLC-G05 Lưu trữ xem xét nghĩa vụ pháp lý	7.4

Bảng A.3 liệt kê các nhãn kiểm soát liên quan đến các yêu cầu và khuyến nghị hoặc cụm yêu cầu và khuyến nghị được cung cấp trong Điều 8.

Bảng A.3 - Các kiểm soát con người bảo mật lưu trữ

Chủ đề	Kiểm soát	Số điều khoản
Chuyên môn bảo mật lưu trữ	SC-XPTS-G01 Đảm bảo chuyên môn bảo vệ lưu trữ đầy đủ	8
	SC-XPTS-G02 Đảm bảo chuyên môn bảo mật lưu trữ đầy đủ	8

Bảng A.4 liệt kê các nhãn kiểm soát liên quan đến các yêu cầu và khuyến nghị hoặc cụm yêu cầu và khuyến nghị được cung cấp trong Điều 9.

Bảng A.4 - Các kiểm soát vật lý bảo mật lưu trữ

Chủ đề	Kiểm soát	Vị trí
Vật lý	PC-PHYS-G01 Bảo mật vật lý phương tiện lưu trữ	9.3
	PC-PHYS-G02 Bảo mật vật lý thiết bị lưu trữ	9.3
	PC-PHYS-R01 Bảo vệ giao diện vật lý	9.3
	PC-PHYS-G03 Cách ly vật lý hệ thống lưu trữ	9.4
	PC-PHYS-G04 Cách ly logic hệ thống lưu trữ	9.4

Bảng A.5 liệt kê các nhãn kiểm soát liên quan đến các yêu cầu và khuyến nghị hoặc cụm yêu cầu và khuyến nghị được cung cấp trong Điều 10.

Bảng A.5 - Các kiểm soát công nghệ bảo mật lưu trữ

Chủ đề	Kiểm soát	Vị trí
Thiết kế và triển khai	TC-DSGN-G01 Tuân thủ các nguyên tắc thiết kế an toàn cốt lõi	10.2.1
	TC-DSGN-G02 Xem xét các mối đe dọa liên quan trong thiết kế	10.2.1
	TC-DSGN-G03 Triển khai phòng thủ theo chiều sâu	10.2.2.1
	TC-DSGN-G04 Tính đến độ nhạy cảm của dữ liệu trong thiết kế miền an toàn	10.2.2.2
	TC-DSGN-G05 Tính đến mục đích trong thiết kế miền an toàn	10.2.2.2
	TC-DSGN-G06 Sử dụng cách ly hơn nữa trong một miền an toàn	10.2.2.2
	TC-DSGN-G07 Bao gồm khả năng phục hồi trong thiết kế	10.2.2.3
	TC-DSGN-G08 Hỗ trợ chuỗi khởi tạo an toàn	10.2.2.4
	TC-DSGN-G09 Giảm thiểu tác động đến độ tin cậy của lưu trữ	10.2.3.1

Chủ đề	Kiểm soát	Vị trí
	TC-DSGN-G10 Giảm thiểu tác động đến tính sẵn sàng của dữ liệu	10.2.3.2
	TC-DSGN-G11 Giảm thiểu tác động đến khả năng phục hồi của lưu trữ	10.2.3.3
	TC-DSGN-G12 Giảm thiểu tác động đến tính toàn vẹn dữ liệu	10.2.3.4
	TC-DSGN-G13 Đảm bảo lưu giữ và bảo quản dữ liệu	10.2.4
	TC-DSGN-G14 Đảm bảo thải bỏ dữ liệu đúng cách	10.2.4
An toàn hệ thống	TC-HARD-G01 Thực hiện củng cố hệ điều hành cơ bản	10.3.1
	TC-HARD-G02 Sử dụng các bản cập nhật phần mềm và bản vá từ các nguồn đáng tin cậy	10.3.1
	TC-HARD-R01 Thực hiện ghi nhật ký trên lưu trữ	10.3.2
	TC-HARD-G03 Đảm bảo tính đầy đủ của ghi nhật ký kiểm toán lưu trữ	10.3.2
	TC-HARD-G04 Thực hiện giám sát lưu trữ thích hợp	10.3.2
	TC-HARD-G05 Sử dụng lưu giữ và bảo vệ nhật ký cho lưu trữ	10.3.2
	TC-HARD-G06 Bao gồm lưu trữ trong các chương trình quản lý lỗ hổng	10.3.3
Quản lý lưu trữ	TC-MGMT-R01 Biện pháp xác thực người dùng tối thiểu	10.4.2.1
	TC-MGMT-G01 Sử dụng các giải pháp xác thực tập trung	10.4.2.1
	TC-MGMT-G02 Sử dụng xác thực đa yếu tố	10.4.2.1
	TC-MGMT-G03 Vô hiệu hóa đăng nhập vào tài khoản root hoặc admin	10.4.2.1

Chủ đề	Kiểm soát	Vị trí
	TC-MGMT-G04 Ghi nhật ký từ xa tất cả các hoạt động leo thang đặc quyền	10.4.2.1
	TC-MGMT-G05 Sử dụng các cơ chế xác thực thực thể	10.4.2.1
	TC-MGMT-G06 Tách biệt vai trò an toàn và phi an toàn	10.4.2.2
	TC-MGMT-G07 Bảo mật giao diện mạng đến phần mềm/phần sụn quản lý	10.4.3
	TC-MGMT-R02 Bảo mật quản lý từ xa	10.4.3
	TC-MGMT-R03 Hạn chế quản lý từ xa của nhà cung cấp	10.4.3
	TC-MGMT-R04 Hạn chế sử dụng truy cập quay số	10.4.3
	TC-MGMT-R05 Bảo mật IPMI	10.4.3
Tính bí mật dữ liệu	TC-CNFD-G01 Tuân thủ quy định nhập/xuất khẩu đối với mật mã	10.5.2
	TC-CNFD-G02 Tuân thủ các yêu cầu ký gửi và tiết lộ khóa	10.5.2
	TC-CNFD-G03 Lập kế hoạch cho các lỗi khóa	10.5.2
	TC-CNFD-G04 Hạn chế tác động hoạt động của mật mã	10.5.2
	TC-CNFD-R01 Sử dụng mật mã có độ mạnh an toàn ít nhất 128 bit	10.5.3
	TC-CNFD-G05 Tránh sử dụng mã hóa lưu trữ làm biện pháp bảo vệ chính cho dữ liệu nhạy cảm	10.5.3
	TC-CNFD-G06 Chọn điểm mã hóa thích hợp	10.5.3
	TC-CNFD-G07 Sử dụng mã hóa và quản lý khóa thích hợp tương thích với các yêu cầu lưu giữ và bảo quản dữ liệu	10.5.3
	TC-CNFD-G08 Sử dụng các mô-đun mật mã đã được xác nhận cho dữ liệu nhạy cảm hoặc được quản lý	10.5.3

Chủ đề	Kiểm soát	Vị trí
	TC-CNFD-G09 Tạo và lưu giữ hồ sơ mã hóa lưu trữ	10.5.3
	TC-CNFD-G10 Tuân thủ các nguyên tắc quản lý khóa cơ bản	10.5.3
	TC-CNFD-G11 Cung cấp bảo vệ an toàn đầu cuối cho dữ liệu đang di chuyển	10.5.4.1
	TC-CNFD-G12 Bù đắp cho tác động tính toán của mã hóa dữ liệu đang di chuyển	10.5.4.1
	TC-CNFD-R02 Yêu cầu tối thiểu TLS	10.5.4.2
	TC-CNFD-R03 Yêu cầu tối thiểu IPsec	10.5.4.3
	TC-CNFD-G13 Sử dụng điểm mã hóa thích hợp	10.5.5
	TC-CNFD-G14 Tạo bằng chứng mã hóa thích hợp	10.5.5
	TC-CNFD-R04 Bảo vệ khóa được sử dụng để mã hóa lưu trữ	10.5.5
	TC-CNFD-R05 Sử dụng các thuật toán mã hóa và chế độ hoạt động thích hợp cho lưu trữ	10.5.5
	TC-CNFD-G15 Hạn chế lộ khóa ở dạng rõ	10.5.5
	TC-CNFD-R06 Sử dụng khóa mật mã cho một mục đích	10.5.5
	TC-CNFD-R07 Tạo khóa ngẫu nhiên bằng toàn bộ không gian khóa	10.5.5
	TC-CNFD-R08 Việc sử dụng khóa bị giới hạn trong chu kỳ mật mã hữu hạn hoặc lượng dữ liệu xử lý tối đa	10.5.5
	TC-CNFD-G16 Sử dụng cơ sở hạ tầng quản lý khóa tập trung	10.5.5
	TC-CNFD-G17 Sử dụng OASIS KMIP để truy cập và sử dụng cơ sở hạ tầng quản lý khóa tập trung	10.5.5

Chủ đề	Kiểm soát	Vị trí
Làm sạch lưu trữ	TC-SNTZ-G01 Bao gồm làm sạch lưu trữ như một phần của quản trị dữ liệu	10.6.1
	TC-SNTZ-R01 Làm sạch lưu trữ trước khi thải bỏ	10.6.1
	TC-SNTZ-R02 Xác minh kết quả làm sạch lưu trữ	10.6.1
	TC-SNTZ-R03 Chọn phương pháp làm sạch lưu trữ tối thiểu chấp nhận được	10.6.2
	TC-SNTZ-G02 Xem xét chi phí và tác động môi trường của việc làm sạch lưu trữ	10.6.2
	TC-SNTZ-R04 Làm sạch phương tiện phù hợp với các tiêu chuẩn chấp nhận được	10.6.3
	TC-SNTZ-R05 Xác minh tính đầy đủ của kết quả làm sạch phương tiện	10.6.3
	TC-SNTZ-R06 Làm sạch lưu trữ logic phù hợp với các tiêu chuẩn chấp nhận được	10.6.4
	TC-SNTZ-R07 Xác minh tính đầy đủ của kết quả làm sạch lưu trữ logic	10.6.4
	TC-SNTZ-G03 Xem xét làm sạch lưu trữ bổ sung cho các cơ chế bảo vệ dữ liệu	10.6.4
	TC-SNTZ-R08 Sử dụng xóa bằng mật mã để thanh lọc trong điều kiện chính xác	10.6.5
	TC-SNTZ-G04 Tìm kiếm sự đảm bảo về chất lượng mật mã được sử dụng để xóa bằng mật mã	10.6.5
	TC-SNTZ-G05 Xác định xem khóa mã hóa bị tiêu hủy có thể khôi phục được không	10.6.5
	TC-SNTZ-G06 Xác minh kết quả phương pháp làm sạch bằng cách xóa sạch	10.6.6
	TC-SNTZ-G07 Xác minh kết quả phương pháp làm sạch bằng cách thanh lọc	10.6.6

Chủ đề	Kiểm soát	Vị trí
	TC-SNTZ-R09 Xác minh kết quả phương pháp làm sạch bằng cách tiêu hủy	10.6.6
	TC-SNTZ-G08 Tạo và lưu giữ hồ sơ làm sạch lưu trữ	10.6.7
	TC-SNTZ-G09 Ghi lại thông tin tối thiểu để chứng nhận việc làm sạch	10.6.7
Lưu trữ gắn trực tiếp	TC-DASS-G01 Bảo vệ DAS chống truy cập trái phép	10.7
	TC-DASS-G02 Làm sạch DAS trước khi tái sử dụng hoặc thải bỏ	10.7
	TC-DASS-G03 Sao lưu DAS để đảm bảo khôi phục sau khi mất dữ liệu	10.7
SAN FC	TC-FCSS-G01 Kiểm soát truy cập nút FCP	10.8.2.2
	TC-FCSS-G02 Sử dụng các kiểm soát dựa trên bộ chuyển mạch FC	10.8.2.2
	TC-FCSS-G03 Cấu hình thiết bị FC để đáp ứng yêu cầu bảo mật	10.8.2.2
SAN IP	TC-IPSS-G01 Sử dụng truy cập mạng và giao thức iSCSI	10.8.2.3
	TC-IPSS-G02 Sử dụng truy cập mạng và giao thức FCIP	10.8.2.3
	TC-IPSS-G03 Sử dụng IPsec để bảo mật FCIP	10.8.2.3
SAN InfiniBand	TC-IBSS-G01 Bảo vệ SAN InfiniBand	10.8.2.4
NVMe-oF	TC-NVSS-G01 Sử dụng xác thực NVMe-oF	10.8.2.5
	TC-NVSS-G02 Sử dụng các kiểm soát an toàn NVMe/FC	10.8.2.5
	TC-NVSS-G03 Sử dụng các kiểm soát an toàn NVMe/TCP	10.8.2.5
	TC-NVSS-G04 Sử dụng các kiểm soát an toàn NVMe/RDMA	10.8.2.5

Chủ đề	Kiểm soát	Vị trí
Giao thức NAS	TC-NASP-G01 Sử dụng truy cập mạng và giao thức NFS	10.8.3.2
	TC-NASP-G02 Sử dụng mã hóa để bảo mật NFS	10.8.3.2
	TC-NASP-G03 Sử dụng truy cập mạng và giao thức SMB	10.8.3.3
Lưu trữ FC dựa trên khối	TC-BBFC-G01 Sử dụng che giấu và ánh xạ LUN FC	10.9.1
	TC-BBFC-G02 Sử dụng các biện pháp bảo mật FCP cho SCSI	10.9.1
	TC-BBFC-G03 Sử dụng mã hóa dữ liệu tĩnh cho lưu trữ FC	10.9.1
	TC-BBFC-G04 Sử dụng làm sạch lưu trữ cho lưu trữ FC	10.9.1
Lưu trữ IP dựa trên khối	TC-BBIP-G01 Lọc truy cập trình khởi tạo iSCSI	10.9.2
	TC-BBIP-G02 Sử dụng các biện pháp bảo mật iSCSI	10.9.2
	TC-BBIP-G03 Sử dụng mã hóa dữ liệu tĩnh cho lưu trữ IP	10.9.2
	TC-BBIP-G04 Sử dụng làm sạch lưu trữ cho lưu trữ IP	10.9.2
Lưu trữ NFS dựa trên tệp	TC-FBNF-R01 Áp dụng kiểm soát truy cập NFS	10.10.2
	TC-FBNF-R02 Hạn chế hành vi máy khách NFS	10.10.2
	TC-FBNF-G01 Bảo mật dữ liệu trên máy chủ NFS	10.10.2
Lưu trữ SMB dựa trên tệp	TC-FBSM-R01 Giao thức SMB tối thiểu chấp nhận được	10.10.3
	TC-FBSM-R02 Áp dụng kiểm soát truy cập SMB	10.10.3
	TC-FBSM-R03 Hạn chế hành vi máy khách SMB	10.10.3
	TC-FBSM-G01 Bảo mật dữ liệu trên máy chủ SMB	10.10.3

Chủ đề	Kiểm soát	Vị trí
Lưu trữ Điện toán Đám mây	TC-CCSS-G01 Sử dụng bảo mật truyền tải cho các giao dịch đám mây	10.11.1
	TC-CCSS-G02 Sử dụng mã hóa dữ liệu tĩnh cho lưu trữ đám mây	10.11.1
	TC-CCSS-G03 Sử dụng xác thực mạnh để truy cập lưu trữ đám mây	10.11.1
	TC-CCSS-G04 Sử dụng kiểm soát truy cập để bảo vệ dữ liệu trên lưu trữ đám mây	10.11.1
	TC-CCSS-G05 Sử dụng làm sạch lưu trữ cho lưu trữ đám mây	10.11.1
CDMI	TC-CDMI-R01 Sử dụng TLS cho tất cả các giao dịch CDMI	10.11.2
	TC-CDMI-R02 Xác thực lẫn nhau tất cả các thực thể CDMI	10.11.2
	TC-CDMI-G01 Sử dụng truy vấn khả năng CDMI để đánh giá tính đầy đủ về bảo mật	10.11.2
	TC-CDMI-G02 Sử dụng các miền CDMI	10.11.2
	TC-CDMI-G03 Tích hợp ghi nhật ký CDMI vào nhật ký kiểm toán	10.11.2
	TC-CDMI-G04 Cấu hình lưu giữ CDMI để điều chỉnh việc tự động xóa với chính sách	10.11.2
	TC-CDMI-G05 Xác minh khả năng gỡ bỏ giữ CDMI trước khi sử dụng khả năng này	10.11.2
	TC-CDMI-G06 Sử dụng mã hóa dữ liệu tĩnh cho lưu trữ CDMI	10.11.2
	TC-CDMI-G07 Sử dụng làm sạch lưu trữ cho lưu trữ CDMI	10.11.2
Lưu trữ dựa trên đối tượng	TC-OBSS-G01 Sử dụng bảo mật truyền tải cho các giao dịch lưu trữ dựa trên đối tượng	10.12

Chủ đề	Kiểm soát	Vị trí
	TC-OBSS-G02 Sử dụng mã hóa dữ liệu tĩnh cho lưu trữ dựa trên đối tượng	10.12
	TC-OBSS-G03 Bật tính bất biến dữ liệu cho lưu trữ dựa trên đối tượng	10.12
	TC-OBSS-G04 Điều chỉnh các cơ chế bảo mật với bên thuê trên lưu trữ dựa trên đối tượng	10.12
	TC-OBSS-G05 Sử dụng làm sạch lưu trữ cho lưu trữ dựa trên đối tượng	10.12
Giảm dữ liệu	TC-DRDC-G01 Sử dụng nén trước khi mã hóa	10.13
	TC-DRDC-G02 Sử dụng khử trùng lặp trước khi mã hóa	10.13
	TC-DRDC-G03 Sử dụng thứ tự chính xác cho nhiều lần giảm dữ liệu và mã hóa	10.13
	TC-DRDC-G04 Sử dụng giảm dữ liệu tương thích với BCM	10.13
Bảo vệ và phục hồi dữ liệu	TC-PROT-G01 Thiết kế cơ chế bảo vệ dữ liệu để phục hồi nhanh chóng	10.14.1
	TC-PROT-G02 Sử dụng các biện pháp và hoạt động sao lưu dữ liệu một cách an toàn	10.14.2
	TC-PROT-G03 Sử dụng sao lưu phục hồi sau tấn công mạng	10.14.2
	TC-PROT-G04 Sử dụng các biện pháp và hoạt động sao chép dữ liệu một cách an toàn	10.14.3
	TC-PROT-G05 Sử dụng ảnh chụp nhanh kết hợp với sao lưu	10.14.4
	TC-PROT-G06 Sử dụng bảo mật ảnh chụp nhanh	10.14.4
Lưu trữ dữ liệu và kho lưu trữ	TC-DARS-G01 Giải quyết các vấn đề bảo quản chính trong kho lưu trữ dữ liệu	10.15.2.1

Chủ đề	Kiểm soát	Vị trí
	TC-DARS-G02 Sử dụng các dịch vụ bảo mật để giải quyết các khía cạnh chứng cứ của kho lưu trữ	10.15.2.1
	TC-DARS-G03 Tạo nhiều bản sao vật lý hoặc logic của dữ liệu được lưu giữ trong kho lưu trữ	10.15.2.2
	TC-DARS-G04 Thực hiện kiểm toán tính toàn vẹn thường xuyên đối với dữ liệu được lưu giữ trong kho lưu trữ	10.15.2.2
	TC-DARS-G05 Kiểm soát truy cập đối với dữ liệu được lưu giữ trong kho lưu trữ phù hợp với các yêu cầu pháp lý và quy định	10.15.2.2
	TC-DARS-G06 Sử dụng các biện pháp trách nhiệm giải trình và truy xuất nguồn gốc để truy cập dữ liệu của kho lưu trữ	10.15.2.2
	TC-DARS-G07 Sử dụng các cơ chế để giải quyết tính xác thực, nguồn gốc và chuỗi hành trình dữ liệu đối với dữ liệu được lưu giữ trong kho lưu trữ	10.15.2.2
	TC-DARS-G08 Đảm bảo quản lý vòng đời khóa thích hợp đối với dữ liệu được lưu giữ trong kho lưu trữ	10.15.2.2
	TC-DARS-G09 Chủ động kiểm tra tính toàn vẹn dữ liệu của kho lưu trữ dài hạn	10.15.2.3
	TC-DARS-G10 Nâng cấp bảo mật trong quá trình làm mới công nghệ của kho lưu trữ dài hạn	10.15.2.3
	TC-DARS-G11 Quản lý người dùng và quyền truy cập vào kho lưu trữ dài hạn	10.15.2.3
	TC-DARS-G12 Duy trì các biện pháp bảo mật dữ liệu trong khi được lưu giữ trong kho lưu trữ dài hạn	10.15.2.3
	TC-DARS-G13 Lưu giữ nhật ký bảo mật cho kho lưu trữ dài hạn	10.15.2.3
	TC-DARS-G14 Phát hiện và giải quyết các xâm phạm của kho lưu trữ dài hạn	10.15.2.3

Chủ đề	Kiểm soát	Vị trí
	TC-DARS-G15 Đảm bảo rằng các công nghệ giảm dữ liệu không ảnh hưởng đến tính toàn vẹn dữ liệu của kho lưu trữ dài hạn	10.15.2.3
	TC-DARS-G16 Sử dụng các kiểm soát bảo mật cho cơ sở dữ liệu	10.15.3
Ảo hóa lưu trữ	TC-SVSS-G01 Áp dụng các kiểm soát mạng lưu trữ cho tất cả các thực thể tham gia vào ảo hóa lưu trữ	10.16.1
	TC-SVSS-G02 Hạn chế hoặc ngăn chặn truy cập trực tiếp vào các yếu tố vật lý không được ảo hóa	10.16.1
	TC-SVSS-G03 Sử dụng các kiểm soát bảo mật để bảo vệ dữ liệu trong lưu trữ được ảo hóa	10.16.1
	TC-SVSS-G04 Đáp ứng các mục tiêu cấp độ dịch vụ về tính sẵn sàng, bảo mật và quyền riêng tư cho lưu trữ được ảo hóa	10.16.1
	TC-SVSS-G05 Đảm bảo lưu trữ được ảo hóa giải quyết các yêu cầu bảo mật đa bên thuê	10.16.1
	TC-SVSS-G06 Kiểm soát quyền truy cập VM vào mạng lưu trữ	10.16.2
	TC-SVSS-G07 Kiểm soát di chuyển/di trú VM giữa các máy chủ vật lý	10.16.2
Đa bên thuê an toàn	TC-SMTS-G01 Cung cấp đảm bảo cách ly an toàn cho đa bên thuê	10.17
	TC-SMTS-G02 Sử dụng các biện pháp bảo mật cho đa bên thuê an toàn	10.17
Di chuyển dữ liệu tự động an toàn	TC-SADM-G01 Sử dụng trách nhiệm giải trình và truy xuất nguồn gốc cho di chuyển dữ liệu tự động an toàn	10.18
	TC-SADM-G02 Sử dụng tính toàn vẹn, xác thực và bất biến cho di chuyển dữ liệu tự động an toàn	10.18
	TC-SADM-G03 Sử dụng tính bí mật cho di chuyển dữ liệu tự động an toàn	10.18

Chủ đề	Kiểm soát	Vị trí
	TC-SADM-G04 Sử dụng làm sạch kết hợp với di chuyển dữ liệu tự động an toàn	10.18
	TC-SADM-G05 Sử dụng tính đáng tin cậy và an toàn vật lý cho di chuyển dữ liệu tự động an toàn	10.18

Thư mục tài liệu tham khảo

[1] ISO 5127:2017, Information and documentation — Foundation and vocabulary

[2] ISO 7498-2:1989, Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture

[3] ISO/TR 10255:2009, Document management applications — Optical disk storage technology, management and standards

[4] ISO 14721, Space data and information transfer systems — Open archival information system (OAIS) —

Reference model

[5] ISO 15392:2019, Sustainability in buildings and civil engineering works — General principles

[6] ISO 15489-1:2016, Information and documentation — Records management — Part 1: Concepts and principles

[7] ISO 16175-1, Information and documentation — Processes and functional requirements for software for managing records — Part 1: Functional requirements and associated guidance for any applications that manage digital records

[8] ISO/TS 16175-2, Information and documentation — Processes and functional requirements for software for managing records — Part 2: Guidance for selecting, designing, implementing and maintaining software for managing records

[9] ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection — Information security controls

[10] ISO 16609:2022, Financial services — Requirements for message authentication using symmetric techniques

[11] ISO/TR 18492:2005, Long-term preservation of electronic document-based information

[12] ISO 19092:20085), Financial services — Biometrics — Security framework

[13] ISO 22301, Security and resilience — Business continuity management systems — Requirements

[14] ISO/IEC 20648, Information technology — TLS specification for storage systems

[15] ISO 22600-1:2014, Health informatics — Privilege management and access control — Part 1: Overview and policy management

[16] ISO 30300:2020, Information and documentation — Records management — Core concepts and vocabulary

[17] ISO/IEC 10116:2017, Information technology — Security techniques — Modes of operation for an n-bit block cipher

[18] ISO/IEC 11179-1:2023, Information technology — Metadata registries (MDR) — Part 1: Framework

[19] ISO/IEC 11770 (all parts), Information security — Key management

[20] ISO/IEC 14776-372:2011, Information technology — Small Computer System Interface (SCSI) — Part 372: SCSI Enclosure Services - 2 (SES-2)

[21] ISO/IEC 15408 (all parts), Information security, cybersecurity and privacy protection — Evaluation criteria for IT security

[22] ISO/IEC 17826, Information technology — Cloud Data Management Interface (CDMI) Version 2.0.0

[23] ISO/IEC 18033 (all parts), Information security — Encryption algorithms

[24] ISO/IEC 19790:2012, Information technology — Security techniques — Security requirements for cryptographic modules

[25] ISO/IEC 20547-4, Information technology — Big data reference architecture — Part 4: Security and privacy

[26] ISO/IEC 22123-1, Information technology — Cloud computing — Part 1: Vocabulary

[27] ISO/IEC 22123-2, Information technology — Cloud computing — Part 2: Concepts

[28] ISO/IEC 24759:2017, Information technology — Security techniques — Test requirements for cryptographic modules

[29] ISO/IEC 27001:2022, Information technology — Security techniques — Information security management systems — Requirements

[30] ISO/IEC 27005, Information security, cybersecurity and privacy protection — Guidance on managing information security risks

[31] ISO/IEC 27031:2011, Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity

[32] ISO/IEC 27033-1:2015, Information technology — Security techniques — Network security — Part 1:

Overview and concepts

[33] ISO/IEC 27033-2:2012, Information technology — Security techniques — Network security — Part 2:

Guidelines for the design and implementation of network security

[34] ISO/IEC 27033-3:2010, Information technology — Security techniques — Network security — Part 3:

Reference networking scenarios — Threats, design techniques and control issues

[35] ISO/IEC 27701, Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

[36] IEEE 1619-2018, IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices

[37] IEEE 1619.1-2018, IEEE Standard for Authenticated Encryption with Length Expansion for Storage Devices

[38] IEEE 1619.2-2021, IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices

[39] IETF RFC 768, User Datagram Protocol

[40] IETF RFC 1813, NFS Version 3 Protocol Specification

[41] IETF RFC 3195, Reliable Delivery for syslog

[42] IETF RFC 3723, Securing Block Storage Protocols over IP

[43] IETF RFC 3821, Fibre Channel Over TCP/IP (FCIP)

[44] IETF RFC 4301, Security Architecture for the Internet Protocol

[45] IETF RFC 4303, IP Encapsulating Security Payload (ESP)

[46] IETF RFC 4945, The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX

[47] IETF RFC 5424, The Syslog Protocol

[48] IETF RFC 5425, TLS Transport Mapping for Syslog

[49] IETF RFC 5426, Transmission of Syslog Messages over UDP

[50] IETF RFC 5427, Textual Conventions for Syslog Management

[51] IETF RFC 5848, Signed Syslog Messages

[52] IETF RFC 6012, Datagram Transport Layer Security (DTLS) Transport Mapping for Syslog

[53] IETF RFC 6071 IP, Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap

[54] IETF RFC 6587, Transmission of Syslog Messages over TCP

[55] IETF RFC 7143, Internet Small Computer Systems Interface (iSCSI) Protocol (Consolidated)

[56] IETF RFC 7146, Securing Block Storage Protocols over IP: RFC 3723 Requirements Update for IPsec v3

[57] IETF RFC 7530, Network File System (NFS) version 4 Protocol

[58] IETF RFC 8446, The Transport Layer Security (TLS) Protocol Version 1.3

[59] IETF RFC 8881, Network File System (NFS) Version 4 Minor Version 1 Protocol

[60] ANSI INCITS 470–2019, Fibre Channel — Framing and Signaling-5 (FC-FS-5)

[61] ANSI INCITS 496–2012, Information Technology — Fibre Channel — Security Protocols — 2 (FC-SP-2)

[62] ANSI INCITS 556–2020, Information Technology — Non-Volatile Memory Express - 2 (FC-NVMe-2)

[63] NIST FIPS 140–3, Security Requirements for Cryptographic Modules

[64] NIST FIPS 197, Advanced Encryption Standard

[65] NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode modes of operations

[66] NIST Special Publication 800-38C, Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality modes of operations

[67] NIST Special Publication 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/ Counter Mode (GCM) and GMAC modes of operations Galois/Counter Mode

[68] NIST Special Publication 800-38E, Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices

[69] NIST Special Publication 800-57 Part 1, Recommendation for Key Management: Part 1: General (Revision 3)

[70] NIST Special Publication 800-57 Part 2, Recommendation for Key Management: Part 2: Best Practices for Key Management Organization

[71] SNIA, Technical Position: TLS Specification for Storage Systems, https://www.snia.org/tech_activities/ standards/curr_standards/tls

[72] SNIA, Technical White Paper, White Paper Data Protection Best Practices, https://www.snia.org/ educational-library

[73] SNIA, Technical White Paper, White Paper Storage Security: Fibre Channel Security, https://www.snia.org/educational-library

[74] SNIA, Technical White Paper, White Paper Storage Security: Encryption and Key Management, https:// www.snia.org/educational-library

[75] OASIS Key Management Interoperability Protocol Specification (Version 2.0 or later)

[76] OASIS Key Management Interoperability Protocol Profiles (Version 2.0 or later)

[77] RecoMMendatIon ITU-T X 1601 (2013), Security framework for cloud computing

[78] NVM Express Inc NVM Express® Base Specification, Revision 2.0

[79] NVM Express Inc NVM Express® NVM Command Set Specification, Revision 1.0

[80] NVM Express Inc NVM Express® over PCIe™ Transport Specification, Revision 1.0

[81] NVM Express Inc NVM Express® over TCP Transport Specification, Revision 1.0

[82] NVM Express Inc NVM Express® over RDMA Transport Specification, Revision 1.0

[83] IEEE 2883, IEEE Standard for Storage Sanitization