TCVN

TIÊU CHUẨN QUỐC GIA

TCVN 14423:2026

Xuất bản lần 2

AN NINH MẠNG - HỆ THỐNG THÔNG TIN - YÊU CẦU CƠ BẢN

Cyber security - Information system - Baseline requirements

HÀ NỘI - 2026

Mục lục

Lời nói đầu 6

Lời giới thiệu 7

2.1 Thuật ngữ và định nghĩa 8

2.2 Chữ viết tắt 13

3 Yêu cầu cơ bản đối với hệ thống thông tin cấp độ 1 15

3.1 Quản lý rủi ro an ninh mạng 15

3.2 Quản lý tài sản phần cứng 15

3.3 Quản lý tài sản phần mềm 16

3.4 Quản lý tài sản thông tin 16

3.5 Cấu hình an toàn cho phần cứng và phần mềm 17

3.6 Quản lý tài khoản và quyền truy cập tài khoản của người dùng 18

3.7 Quản lý lỗ hổng bảo mật 19

3.8 Quản lý nhật ký an ninh mạng 20

3.9 Bảo vệ cho trình duyệt web, dịch vụ thư điện tử 21

3.10 Phòng chống phần mềm độc hại 21

3.11 Sao lưu và khôi phục dữ liệu 22

3.12 Quản lý hạ tầng mạng 22

3.13 Nhân sự vận hành, quản trị hệ thống, bảo vệ an ninh mạng 24

3.14 Quản lý nhà cung cấp sản phẩm, dịch vụ 24

3.15 Quản trị ứng phó sự cố an ninh mạng 25

4 Yêu cầu cơ bản đối với hệ thống thông tin cấp độ 2 25

4.1 Quản lý rủi ro an ninh mạng 25

4.2 Quản lý tài sản phần cứng 26

4.3 Quản lý tài sản phần mềm 26

4.4 Quản lý tài sản thông tin 27

4.5 Cấu hình an toàn cho phần cứng và phần mềm 28

4.6 Quản lý tài khoản và quyền truy cập tài khoản của người dùng 29

4.7 Quản lý lỗ hổng bảo mật 31

4.8 Quản lý nhật ký an ninh mạng 32

4.9 Bảo vệ cho trình duyệt web, dịch vụ thư điện tử 32

4.10 Phòng chống phần mềm độc hại 33

4.11 Sao lưu và khôi phục dữ liệu 33

4.12 Quản lý hạ tầng mạng 34

4.13 Nhân sự vận hành, quản trị hệ thống, bảo vệ an ninh mạng 36

4.14 Quản lý nhà cung cấp sản phẩm, dịch vụ 37

4.15 Quản trị ứng phó sự cố an ninh mạng 37

5 Yêu cầu cơ bản đối với hệ thống thông tin cấp độ 3 38
5.1 Quản lý rủi ro an ninh mạng 38
5.2 Quản lý tài sản phần cứng 39
5.3 Quản lý tài sản phần mềm 40
5.4 Quản lý tài sản thông tin 41
5.5 Cấu hình an toàn cho phần cứng và phần mềm 43
5.6 Quản lý tài khoản và quyền truy cập tài khoản của người dùng 44
5.7 Quản lý lỗ hổng bảo mật 46
5.8 Quản lý nhật ký an ninh mạng 46
5.9 Bảo vệ cho trình duyệt web, dịch vụ thư điện tử 47
5.10 Phòng chống phần mềm độc hại 48
5.11 Sao lưu và khôi phục dữ liệu 49
5.12 Quản lý hạ tầng mạng 50
5.13 Giám sát và phòng thủ an ninh mạng 52
5.14 Nhân sự vận hành, quản trị hệ thống, bảo vệ an ninh mạng 53
5.15 Quản lý nhà cung cấp sản phẩm, dịch vụ 53
5.16 Quản trị ứng phó sự cố an ninh mạng 54
5.17 Phát triển ứng dụng an toàn 55
5.18 Quản lý kiểm tra an ninh mạng 56
6 Yêu cầu cơ bản đối với hệ thống thông tin cấp độ 4 57
6.1 Quản lý rủi ro an ninh mạng 57
6.2 Quản lý tài sản phần cứng 58
6.3 Quản lý tài sản phần mềm 59
6.4 Quản lý tài sản thông tin 60
6.5 Cấu hình an toàn cho phần cứng và phần mềm 62
6.6 Quản lý tài khoản và quyền truy cập tài khoản của người dùng 63
6.7 Quản lý lỗ hổng bảo mật 66
6.8 Quản lý nhật ký an ninh mạng 66
6.9 Bảo vệ cho trình duyệt web, dịch vụ thư điện tử 68
6.10 Phòng chống phần mềm độc hại 69
6.11 Sao lưu và khôi phục dữ liệu 70
6.12 Quản lý hạ tầng mạng 71
6.13 Giám sát và phòng thủ an ninh mạng 74
6.14 Nhân sự vận hành, quản trị hệ thống, bảo vệ an ninh mạng 75
6.15 Quản lý nhà cung cấp sản phẩm, dịch vụ 76
6.16 Phát triển ứng dụng an toàn 77
6.17 Quản trị ứng phó sự cố an ninh mạng 78
6.18 Quản lý kiểm tra an ninh mạng 79

7 Yêu cầu cơ bản đối với hệ thống thông tin cấp độ 5 80
7.1 Quản lý rủi ro an ninh mạng 80
7.2 Quản lý tài sản phần cứng 82
7.3 Quản lý tài sản phần mềm 83
7.4 Quản lý tài sản thông tin 84
7.5 Cấu hình an toàn cho phần cứng và phần mềm 86
7.6 Quản lý tài khoản và quyền truy cập tài khoản của người dùng 88
7.7 Quản lý lỗ hổng bảo mật 90
7.8 Quản lý nhật ký an ninh mạng 91
7.9 Bảo vệ cho trình duyệt web, dịch vụ thư điện tử 92
7.10 Phòng chống phần mềm độc hại 93
7.11 Sao lưu và khôi phục dữ liệu 94
7.12 Quản lý hạ tầng mạng 95
7.13 Giám sát và phòng thủ an ninh mạng 98
7.14 Nhân sự vận hành, quản trị hệ thống, bảo vệ an ninh mạng 99
7.15 Quản lý nhà cung cấp sản phẩm, dịch vụ 100
7.16 Phát triển ứng dụng an toàn 101
7.17 Quản trị ứng phó sự cố an ninh mạng 103
7.18 Quản lý kiểm tra an ninh mạng 104
Phụ lục A Yêu cầu cơ bản về an toàn vật lý cho hệ thống thông tin theo cấp độ 106

Lời nói đầu

TCVN 14423:2026 thay thế TCVN 14423:2025 An ninh mạng - Yêu cầu đối với hệ thống thông tin quan trọng và TCVN 11930:2017 Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ.

TCVN 14423:2026 do Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao biên soạn, Bộ Công an đề nghị, Ủy ban Tiêu chuẩn Đo lường Chất lượng Quốc gia thẩm định, Bộ Khoa học và Công nghệ công bố.

Lời giới thiệu

Tiêu chuẩn này quy định các yêu cầu cần thiết để đảm bảo an ninh mạng, tăng cường khả năng phòng thủ cho hệ thống thông tin, đồng thời tạo cơ sở cho các công tác của lực lượng chuyên trách bảo vệ an ninh mạng (như giám sát bảo vệ, điều phối ứng phó sự cố, thẩm định, kiểm tra, đánh giá an ninh mạng…) và hoạt động bảo vệ hệ thống thông tin của cơ quan chủ quản.

Để hiệu quả đảm bảo an ninh mạng ở mức cao nhất, khuyến khích chủ quản của hệ thống thông tin triển khai các biện pháp đảm bảo an ninh mạng đáp ứng toàn bộ các yêu cầu đưa ra trong tiêu chuẩn.

An ninh mạng - Hệ thống thông tin - Yêu cầu cơ bản

Cyber security - Information system - Baseline requirements

1 Phạm vi áp dụng

Tiêu chuẩn này quy định các yêu cầu cơ bản về an ninh mạng cho hệ thống thông tin theo cấp độ. Hệ thống thông tin quan trọng về an ninh quốc gia áp dụng các yêu cầu về an ninh mạng tương đương hệ thống thông tin cấp độ 5.

2 Thuật ngữ, định nghĩa và chữ viết tắt

Tiêu chuẩn này sử dụng các thuật ngữ, định nghĩa và chữ viết tắt dưới đây.

2.1 Thuật ngữ và định nghĩa

2.1.1

An ninh mạng (cyber security)

Sự ổn định, an ninh, an toàn của không gian mạng; bảo vệ hệ thống thông tin và bảo đảm thông tin, dữ liệu, hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

2.1.2

Hệ thống thông tin (information system)

Tập hợp phần cứng, phần mềm và dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên không gian mạng.

2.1.3

Dữ liệu quan trọng (important data)

Dữ liệu quan trọng là dữ liệu có thể tác động đến quốc phòng, an ninh, đối ngoại, kinh tế vĩ mô, ổn định xã hội, sức khỏe và an toàn cộng đồng.

2.1.4

Giám sát an ninh mạng (cyber security monitoring)

Biện pháp theo dõi, thu thập, phân tích thông tin, dữ liệu về hoạt động của hệ thống thông tin nhằm phát hiện, cảnh báo các nguy cơ, rủi ro, sự cố an ninh mạng.

2.1.5

Giám sát hệ thống thông tin (information system monitoring)

Biện pháp giám sát, theo dõi trạng thái hoạt động của hệ thống để phát hiện, cảnh báo sớm các sự cố có thể gây gián đoạn hoạt động của hệ thống và làm mất tính khả dụng của hệ thống thông tin. Trạng thái giám sát bao gồm: RAM, CPU, ổ cứng,…

2.1.6

Nhật ký (log)

Bản ghi các sự kiện diễn ra bên trong hệ thống và mạng của tổ chức.

2.1.7

Phần mềm độc hại (malware)

Phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hoặc toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép dữ liệu lưu trữ trong hệ thống thông tin.

2.1.8

Phương tiện lưu trữ (media storage)

Các thiết bị, phương tiện được sử dụng để lưu trữ, sao chép, trao đổi dữ liệu giữa các thiết bị, máy tính một cách gián tiếp.

2.1.9

Xác thực đa yếu tố (multi-factor authentication)

Phương pháp xác thực kết hợp một số yếu tố liên quan đến người dùng, bao gồm: những thông tin mà người dùng biết (mật khẩu, mã số truy cập...), những thông tin mà người dùng sở hữu (chứng thư chữ ký số, thẻ thông minh...), những thông tin về sinh trắc học của người dùng (vân tay, mống mắt...).

2.1.10

Tiến trình (process)

Thực thể của một chương trình đang được thực thi bởi một hoặc nhiều luồng.

2.1.11

Khôi phục (recover)

Thao tác đưa hệ thống, dịch vụ bị ảnh hưởng trở lại trạng thái hoạt động bình thường sau khi sự cố đã bị ngăn chặn và loại bỏ.

2.1.12

Biện pháp kiểm soát (control)

Biện pháp điều chỉnh rủi ro.

CHÚ THÍCH 1: Biện pháp kiểm soát bao gồm bất kỳ quy trình, chính sách, thiết bị, thực hành hoặc các hành động khác nhằm điều chỉnh rủi ro.

CHÚ THÍCH 2: Biện pháp kiểm soát không phải lúc nào cũng có tác động như mong muốn hoặc như đã giả định.

2.1.13

Rủi ro (risk)

Tác động của sự không chắc chắn lên các mục tiêu.

2.1.14

Quản lý rủi ro an ninh mạng (cyber security risk management)

Hoạt động xác định, đánh giá, xử lý và kiểm soát rủi ro an ninh mạng.

2.1.15

Tăng cường bảo mật (hardening)

Quá trình nâng cao bảo mật, giảm thiểu bề mặt tấn công bằng cách vá lỗ hổng bảo mật và tắt các dịch vụ không cần thiết.

2.1.16

Phần mềm trái phép (unauthorized software)

Những phần mềm chưa được phê duyệt, không nằm trong danh sách phần mềm được phép sử dụng hoặc đã hết thời gian hỗ trợ của nhà cung cấp, nhà phát triển phần mềm.

2.1.17

Thiết bị di động (mobile device)

Thiết bị số có thể cầm tay, được thiết kế để hoạt động mà không cần kết nối vật lý, có bộ nhớ lưu trữ dữ liệu cục bộ, không thể tháo rời và hoạt động trong thời gian dài nhờ nguồn điện tích hợp sẵn như máy tính xách tay, máy tính bảng, điện thoại di động thông minh.

2.1.18

Lỗ hổng bảo mật (security vulnerability)

Điểm yếu trong hệ thống thông tin, quy trình bảo mật hệ thống, kiểm soát nội bộ hoặc triển khai, có thể bị khai thác hoặc kích hoạt bởi một mối đe dọa.

2.1.19

Bản sao lưu dữ liệu (data backup)

Tập hợp các dữ liệu, thông tin được sử dụng để khôi phục hệ thống, ứng dụng hoặc dữ liệu trong trường hợp xảy ra sự cố.

2.1.20

Phân quyền dữ liệu (data authorization)

Quá trình xác định và quản lý quyền truy cập của người dùng, nhóm người dùng hoặc hệ thống đối với các nguồn dữ liệu trong một tổ chức hoặc hệ thống thông tin thông qua danh sách kiểm soát truy cập.

2.1.21

Nhà cung cấp (supplier)

Tổ chức hoặc cá nhân thực hiện việc cung cấp sản phẩm, dịch vụ.

2.1.22

Phần mềm thuê khoán (outsourced software)

Phần mềm được đối tác phát triển, nâng cấp, chỉnh sửa theo các yêu cầu riêng của tổ chức hoặc người sử dụng nhằm đáp ứng yêu cầu đặc thù của tổ chức.

2.1.23

Vùng DMZ (demilitarized zone)

Vùng mạng được thiết lập để đặt các máy chủ công cộng, cho phép truy cập trực tiếp từ mạng bên ngoài và mạng Internet.

2.1.24

Vùng mạng biên (edge zone)

Vùng mạng được thiết lập để cung cấp các kết nối hệ thống ra bên ngoài Internet và các mạng khác.

2.1.25

Vùng máy chủ nội bộ (internal server zone)

Vùng mạng được thiết lập để đặt các máy chủ nội bộ, cung cấp ứng dụng, dịch vụ phục vụ hoạt động nội bộ của tổ chức và hoạt động khác mà không cho phép truy cập trực tiếp từ các mạng bên ngoài.

2.1.26

Vùng mạng nội bộ (local area network)

Vùng mạng được thiết lập để cung cấp kết nối mạng cho các máy trạm và các thiết bị đầu cuối và các thiết bị khác của người sử dụng vào hệ thống.

2.1.27

Vùng quản trị (management zone)

Vùng mạng được thiết lập để đặt các máy chủ, máy quản trị và thiết bị chuyên dụng khác phục vụ việc quản lý, vận hành và giám sát hệ thống.

2.1.28

Vùng quản trị thiết bị hệ thống (device management zone)

Vùng mạng riêng cho các địa chỉ quản trị của các thiết bị hệ thống cho phép thiết lập chính sách chung và quản lý tập trung các thiết bị hệ thống.

2.1.29

Vùng máy chủ cơ sở dữ liệu (database server zone)

Vùng mạng được thiết lập để đặt các máy chủ cơ sở dữ liệu. Máy chủ trong vùng này được triển khai tách biệt với các máy chủ ứng dụng nhằm tăng cường kiểm soát truy cập giữa các vùng máy chủ khác với vùng máy chủ này.

2.1.30

Vùng mạng lõi (core zone)

Vùng mạng quan trọng có độ tin cậy cao trong hệ thống thông tin, bất kỳ sự cố nào tại vùng mạng này đều sẽ gây hậu quả nghiêm trọng cho cơ quan, tổ chức và các bên liên quan (nếu có).

2.1.31

Khả năng xảy ra (likelihood)

Chỉ số thể hiện khả năng xảy ra của rủi ro an ninh mạng, có thể được định nghĩa, được đo lường hay được xác định một cách chủ quan hay khách quan, dưới dạng định tính hay định lượng và được mô tả bằng cách sử dụng thuật ngữ chung hoặc bằng toán học (như xác suất hoặc tần suất trong một khoảng thời gian nhất định).

2.1.32

Mức độ ảnh hưởng của rủi ro (impact)

Chỉ số thể hiện mức độ thiệt hại có thể xảy ra do hậu quả của rủi ro an ninh mạng.

2.1.33

Mức độ rủi ro (risk level)

Chỉ số thể hiện mức độ nghiêm trọng của rủi ro an ninh mạng, được xác định dựa trên khả năng xảy ra và mức độ ảnh hưởng của rủi ro.

2.1.34

Kiểm thử xâm nhập (penetration testing)

Phương pháp đánh giá an ninh mạng bằng cách mô phỏng các cuộc tấn công thực tế từ tác nhân độc hại vào hệ thống thông tin nhằm phát hiện lỗ hổng bảo mật có thể bị khai thác.

2.1.35

Tài sản vật lý (physical assets)

Thiết bị công nghệ thông tin, phương tiện truyền thông, vật mang tin và thiết bị khác phục vụ cho hoạt động của hệ thống thông tin.

2.1.36

Tài sản phần cứng (hardware asset)

Thiết bị vật lý được sử dụng để xử lý, lưu trữ hoặc truyền tải các chương trình hoặc dữ liệu máy tính.

2.1.37

Tài sản phần mềm (software asset)

Phần mềm hệ thống, phần mềm tiện ích, phần mềm lớp giữa, hệ quản trị cơ sở dữ liệu, chương trình ứng dụng, mã nguồn và công cụ phát triển.

2.1.38

Tài sản thông tin (information asset)

Dữ liệu, thông tin ở dạng số được xử lý, lưu trữ thông qua hệ thống thông tin.

2.1.39

Phân đoạn vi mô (microsegmentation)

Kỹ thuật trong an ninh mạng phục vụ chia tách mạng thành các phân đoạn nhỏ, biệt lập ở mức độ của từng dịch vụ, ứng dụng riêng lẻ.

2.1.40

Mối đe dọa (threat)

Bất kỳ tình huống hoặc sự kiện nào có khả năng tác động tiêu cực đến hoạt động, tài sản của tổ chức, cá nhân thông qua hệ thống thông tin bằng cách truy cập trái phép, phá hủy, tiết lộ, sửa đổi thông tin và/hoặc từ chối dịch vụ.

2.1.41

Mã hóa (encryption)

Quá trình biến đổi dữ liệu bằng kỹ thuật mật mã để tạo ra bản mã.

2.1.42

Sự cố an ninh mạng (cybersecurity incident)

Sự việc bất ngờ xảy ra trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

2.1.43

Dự phòng nóng (hot standby)

Khả năng thay thế ngay lập tức chức năng của thiết bị khi xảy ra sự cố mà không làm gián đoạn hoạt động của hệ thống.

2.1.44

Quy tắc sao lưu 3-2-1 (3-2-1 backup strategy)

Quy tắc sao lưu dữ liệu yêu cầu ít nhất 3 bản sao dữ liệu, lưu trữ trên 2 loại phương tiện khác nhau và 1 bản sao đặt ở vị trí cách biệt để tránh mất mát toàn bộ do sự cố vật lý hay phần mềm.

2.1.45

Diode dữ liệu (datadiode)

Thiết bị mạng cho phép dữ liệu chỉ truyền theo một chiều về mặt vật lý.

2.1.46

Cổng bảo mật một chiều (unidirectional security gateway)

Là thiết bị mạng bao gồm phần cứng và phần mềm, phần cứng cho phép dữ liệu chỉ truyền theo một chiều về mặt vật lý, phần mềm thực hiện mô phỏng các giao thức và triển khai các tác vụ kiểm soát dữ liệu liên quan.

2.1.47

Cổng bảo mật hai chiều (bilateral security gateway / bidirectional security gateway)

Là thiết bị mạng bao gồm phần cứng và phần mềm, phần cứng cho phép dữ liệu truyền theo hai chiều độc lập về mặt vật lý (thông qua hai kênh một chiều độc lập về mặt vật lý), phần mềm thực hiện mô phỏng các giao thức và triển khai các tác vụ kiểm soát dữ liệu liên quan.

2.2 Chữ viết tắt

ZTNA	Truy cập mạng theo mô hình không tin cậy mặc định	Zero Trust Network Access
VPN	Mạng riêng ảo	Virtual Private Network
DHCP	Giao thức cấp phát địa chỉ IP tự động	Dynamic Host Configuration Protocol
IP	Giao thức Internet	Internet Protocol

OT	Công nghệ vận hành	Operational Technology
IoT	Internet vạn vật	Internet of Things
SIEM	Quản lý nhật ký và sự kiện tập trung	Security Information and Event Management
CNTT	Công nghệ thông tin	
CPU	Bộ vi xử lý trung tâm	Central Processing Unit
DLP	Phòng chống thất thoát dữ liệu	Data Loss Prevention
DMARC	Giao thức xác thực, báo cáo và tuân thủ thư điện tử dựa trên tên miền	Domain-based Message Authentication, Reporting & Conformance
DMZ	Vùng phi quân sự	Demilitarized Zone
DNS	Hệ thống phân giải tên miền	Domain Name System
EDR	Phát hiện và phản hồi điểm cuối	Endpoint Detection and Response
IDS/IPS	Hệ thống phát hiện / Ngăn chặn xâm nhập	Intrusion Detection / Prevention System
LAN	Mạng nội bộ	Local Area Network
MAC	Địa chỉ vật lý	Media Access Control
MFA	Xác thực đa yếu tố	Multi-Factor Authentication
NTP	Giao thức đồng bộ thời gian mạng	Network Time Protocol
QoS	Chất lượng dịch vụ	Quality of Service
RAM	Bộ nhớ truy cập ngẫu nhiên	Random Access Memory
UPS	Bộ lưu điện	Uninterruptible Power Supply
URL	Địa chỉ định danh tài nguyên	Uniform Resource Locator
USB	Chuẩn kết nối phần cứng đa dụng	Universal Serial Bus
WAF	Tường lửa ứng dụng web	Web Application Firewall
DBF	Tường lửa cơ sở dữ liệu	Database Firewall
WAN	Mạng diện rộng	Wide Area Network
USG	Cổng bảo mật một chiều	Unidirectional Security Gateway
BSG	Cổng bảo mật hai chiều	Bilateral Security Gateway / Bidirectional Security Gateway

3 Yêu cầu cơ bản đối với hệ thống thông tin cấp độ 1

3.1 Quản lý rủi ro an ninh mạng

a) Có quy định, quy trình quản lý rủi ro an ninh mạng. Trong đó, yêu cầu thực hiện quản lý rủi ro an ninh mạng bao gồm tối thiểu các bước: xác định, phân tích, đánh giá và xử lý rủi ro an ninh mạng.

b) Đánh giá và cập nhật quy định, quy trình quản lý rủi ro an ninh mạng và các tài liệu liên quan tối thiểu 01 lần/ năm hoặc khi có thay đổi xảy ra trong tổ chức ảnh hưởng đến các văn bản đã ban hành có liên quan.

3.2 Quản lý tài sản phần cứng

3.2.1 Khái quát

a) Lập danh sách, theo dõi, cập nhật trạng thái của tất cả tài sản phần cứng thuộc hệ thống thông tin và các tài sản không thuộc quyền kiểm soát của tổ chức nhưng có kết nối vào hệ thống thông tin; xác định danh sách tài sản cần được giám sát, bảo vệ.

b) Xác định các tài sản vô chủ, tài sản trái phép để loại bỏ hoặc đưa ra phương án quản lý.

c) Thực hiện kiểm kê, rà soát và cập nhật danh sách cho tất cả tài sản phần cứng thuộc hệ thống thông tin định kỳ tối thiểu 01 lần/ năm.

3.2.2 Yêu cầu cụ thể

3.2.2.1 Thiết lập và duy trì hệ thống quản lý danh mục tài sản phần cứng

a) Lập danh sách, theo dõi, cập nhật trạng thái của tất cả tài sản phần cứng có khả năng lưu trữ hoặc xử lý dữ liệu, bao gồm: thiết bị của người dùng cuối, thiết bị di động, thiết bị lưu trữ ngoài, thiết bị văn phòng, thiết bị mạng, thiết bị OT/IoT và máy chủ trong môi trường vật lý, ảo hóa, truy cập từ xa và điện toán đám mây.

b) Danh sách tài sản phần cứng phải bao gồm tối thiểu các thông tin cơ bản sau: tên tài sản, địa chỉ mạng IP (đối với thiết bị đặt địa chỉ IP tĩnh), địa chỉ phần cứng MAC/ mã nhận diện serial, thời gian ngừng hỗ trợ kỹ thuật của hãng (nếu có), vị trí lắp đặt địa lý, vị trí lắp đặt trong hệ thống mạng, mục đích sử dụng, tình trạng sử dụng. Tài sản vật lý phải được giao, gán trách nhiệm cho cá nhân hoặc bộ phận quản lý, sử dụng.

c) Các thiết bị di động do tổ chức quản lý hoặc được tổ chức cho phép kết nối vào hệ thống thông tin phải được đăng ký để kiểm soát. Quy định trách nhiệm của cá nhân trong tổ chức khi sử dụng thiết bị di động để phục vụ công việc.

3.2.2.2 Xử lý các tài sản phần cứng chưa được quản lý

a) Có quy trình phát hiện và xử lý các tài sản phần cứng không có trong danh sách quản lý, đang kết nối trái phép vào hệ thống thông tin định kỳ tối thiểu 01 lần/ năm.

b) Có thể lựa chọn loại bỏ, từ chối kết nối hoặc cách ly tài sản trái phép.

3.3 Quản lý tài sản phần mềm

3.3.1 Khái quát

a) Lập danh sách, theo dõi, cập nhật trạng thái của tất cả tài sản phần mềm thuộc hệ thống thông tin của cơ quan, tổ chức, đảm bảo chỉ những phần mềm đã phê duyệt mới được phép cài đặt và sử dụng.

b) Thực hiện kiểm kê, rà soát và cập nhật danh sách cho tất cả tài sản phần mềm định kỳ tối thiểu 01 lần/ năm.

3.3.2 Yêu cầu cụ thể

3.3.2.1 Thiết lập và duy trì hệ thống quản lý danh mục tài sản phần mềm

a) Lập danh sách, theo dõi, cập nhật trạng thái của tất cả tài sản phần mềm hiện đang được cài đặt trên các tài sản phần cứng thuộc hệ thống thông tin của cơ quan, tổ chức.

b) Danh sách tài sản phần mềm phải bao gồm tối thiểu các thông tin cơ bản sau: tên tài sản, mục đích sử dụng, thời gian ngừng hỗ trợ kỹ thuật (nếu có), phạm vi sử dụng, chủ thể quản lý, thông tin về bản quyền, phiên bản, hệ thống thông tin thành phần (nếu có). Tài sản phần mềm phải được gắn trách nhiệm cho cá nhân hoặc bộ phận quản lý, sử dụng.

3.3.2.2 Xử lý các tài sản phần mềm trái phép

a) Có quy trình phát hiện và xử lý các phần mềm trái phép định kỳ tối thiểu 01 lần/ năm.

b) Những phần mềm trái phép nhưng vẫn cần thiết đối với hoạt động của cơ quan, tổ chức phải được đưa vào danh sách ngoại lệ để quản lý. Danh sách ngoại lệ này phải thể hiện chi tiết các biện pháp kiểm soát giảm thiểu nguy cơ an ninh mạng ảnh hưởng đến hệ thống.

c) Những phần mềm trái phép không nằm trong danh sách ngoại lệ phải có kế hoạch để xóa/ gỡ bỏ hoàn toàn khỏi các tài sản phần cứng của cơ quan, tổ chức trong thời gian sớm nhất.

3.4 Quản lý tài sản thông tin

3.4.1 Khái quát

Thực hiện quản lý tài sản thông tin và triển khai các biện pháp kiểm soát để phát hiện, phân loại, xử lý, lưu trữ và loại bỏ tài sản thông tin một cách an toàn.

3.4.2 Yêu cầu cụ thể

3.4.2.1 Thiết lập và duy trì quy định quản lý tài sản thông tin

a) Có quy định quản lý tài sản thông tin. Trong quy định, xác định danh sách tài sản thông tin, mức độ nhạy cảm, chủ sở hữu, các bước xử lý, thời gian lưu trữ và các yêu cầu khi tiêu hủy/xóa bỏ dựa trên các tiêu chuẩn về mức độ bảo mật của tài sản thông tin.

b) Có quy trình yêu cầu truy cập, thêm mới, sửa, xóa dữ liệu để kiểm soát truy cập dữ liệu.

c) Kiểm tra cấp độ phân quyền dữ liệu định kỳ tối thiểu 01 lần/ năm.

d) Đánh giá và cập nhật quy trình quản lý tài sản thông tin định kỳ tối thiểu 01 lần/ năm hoặc khi xảy ra các thay đổi trong tổ chức ảnh hưởng đến quy trình.

3.4.2.2 Thiết lập và duy trì bản danh sách tài sản thông tin

a) Lập danh sách các tài sản thông tin dựa trên quy trình quản lý tài sản thông tin.

b) Đánh giá và cập nhật danh sách tài sản thông tin tối thiểu 01 lần/ năm hoặc khi xảy ra thay đổi trong tổ chức ảnh hưởng đến danh sách.

3.4.2.3 Xây dựng danh sách kiểm soát truy cập tài sản thông tin

Xây dựng danh sách quyền truy cập của các tài khoản, người dùng đối với từng loại tài sản thông tin.

3.4.2.4 Mã hóa dữ liệu

Mã hóa thông tin xác thực được lưu trữ trong các tài sản phần cứng và phần mềm của cơ quan, tổ chức.

3.5 Cấu hình an toàn cho phần cứng và phần mềm

3.5.1 Khái quát

Có phương án thiết lập và duy trì cấu hình an toàn cho phần cứng (như thiết bị người dùng cuối bao gồm máy tính, thiết bị di động và cầm tay, thiết bị mạng, thiết bị OT/IoT, máy chủ...) và phần mềm (như hệ điều hành, ứng dụng…).

3.5.2 Yêu cầu cụ thể

3.5.2.1 Thiết lập và duy trì quy định, quy trình cấu hình an toàn cho tài sản phần cứng và phần mềm

a) Có quy định, quy trình cấu hình an toàn cho các tài sản phần cứng và phần mềm của cơ quan, tổ chức.

b) Có các tài liệu cấu hình tiêu chuẩn, tài liệu cấu hình tăng cường bảo mật cho các tài sản phần cứng và phần mềm của cơ quan, tổ chức. Đảm bảo sử dụng giao thức kết nối an toàn, thiết lập tường lửa cho máy chủ/ máy trạm.

c) Đánh giá và cập nhật quy định, quy trình quản lý cấu hình an toàn và các tài liệu liên quan tối thiểu 01 lần/ năm hoặc khi có thay đổi xảy ra trong tổ chức ảnh hưởng đến tài liệu.

3.5.2.2 Cấu hình tự động khóa phiên làm việc trên các tài sản phần cứng và phần mềm

a) Dựa trên yêu cầu sử dụng, kết quả đánh giá rủi ro, thực hiện cấu hình tự động khóa phiên làm việc trên các tài sản phần cứng và phần mềm. Có thể thực hiện cấu hình như sau:

- Tự động khóa phiên làm việc trên các tài sản sau một khoảng thời gian không sử dụng:

+ Đối với máy tính người dùng: không quá 15 phút.

+ Đối với các phiên quản trị phần mềm, máy chủ, thiết bị mạng, thiết bị IoT: không quá 05 phút.

+ Đối với thiết bị di động: không quá 05 phút.

- Tự động khóa thiết bị di động sau một số lần đăng nhập thất bại:

+ Đối với máy tính xách tay: tối đa 10 lần.

+ Đối với điện thoại: tối đa 10 lần.

+ Giới hạn thời gian mở khóa thiết bị sau khi bị khóa: tối thiểu 12 giờ, tối đa 30 ngày.

b) Có cơ chế mở khóa khẩn cấp dành cho quản trị viên/tài khoản đặc quyền.

3.6 Quản lý tài khoản và quyền truy cập tài khoản của người dùng

3.6.1 Khái quát

a) Có quy trình, công cụ để phân quyền và quản lý quyền truy cập của tài khoản người dùng bao gồm: tài khoản quản trị, tài khoản tác nghiệp (tài khoản của người dùng cuối tác nghiệp), tài khoản kỹ thuật (tài khoản dùng để kết nối giữa các hệ thống kỹ thuật), tài khoản dịch vụ (tài khoản cấp cho người thụ hưởng dịch vụ) trên các tài sản phần cứng và phần mềm.

b) Có quy trình tạo, gán, quản lý, thu hồi đặc quyền và quyền truy cập đối với các tài khoản người dùng cho tài sản phần cứng và phần mềm. Quyền truy cập của tài khoản quản trị, tài khoản tác nghiệp, tài khoản kỹ thuật, tài khoản dịch vụ phải nhất quán dựa trên vai trò và các yêu cầu cụ thể, đảm bảo người dùng chỉ có quyền truy cập vào dữ liệu, tài sản phù hợp.

c) Ghi nhật ký và giám sát tài khoản người dùng.

3.6.2 Yêu cầu cụ thể

3.6.2.1 Thiết lập và duy trì hệ thống quản lý tài khoản

a) Lập danh sách, theo dõi và cập nhật tất cả các tài khoản trên các tài sản phần cứng và phần mềm của tổ chức.

b) Danh sách tài khoản phải bao gồm tối thiểu các loại tài khoản sau: tài khoản quản trị, tài khoản tác nghiệp, tài khoản dịch vụ và tài khoản kỹ thuật.

c) Danh sách tài khoản phải bao gồm các thông tin tối thiểu: loại tài khoản, tên tài khoản, trạng thái tài khoản, tên tài sản/ hệ thống thông tin tương ứng, tên người quản lý, phòng ban, ngày kích hoạt tài khoản, ngày vô hiệu hóa tài khoản (nếu có). Đảm bảo tất cả tài khoản đang hoạt động là hợp lệ.

d) Danh sách tài khoản phải được rà soát định kỳ tối thiểu 01 lần/ năm.

3.6.2.2 Xây dựng và tuân thủ quy định sử dụng mật khẩu

a) Thiết lập cấu hình mật khẩu trên tài sản phần cứng, phần mềm để đảm bảo an toàn mật khẩu người sử dụng, bao gồm các yêu cầu sau:

- Yêu cầu thay đổi mật khẩu mặc định.

- Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự.

b) Dựa trên yêu cầu sử dụng, kết quả đánh giá rủi ro, triển khai quy định sử dụng mật khẩu an toàn trong tổ chức. Có thể thực hiện cấu hình như sau:

- Sử dụng mật khẩu duy nhất cho mỗi tài sản hoặc sử dụng giải pháp xác thực và quản lý tập trung.

- Yêu cầu thay đổi mật khẩu trong lần đăng nhập đầu tiên.

- Đối với các hệ thống sử dụng xác thực MFA, quy định mật khẩu có tối thiểu 08 ký tự.

- Đối với các hệ thống không sử dụng xác thực MFA, quy định mật khẩu có tối thiểu 14 ký tự, bao gồm ký tự viết thường, ký tự viết hoa, ký tự đặc biệt, chữ số.

- Đối với tài khoản quản trị cần thay đổi mật khẩu định kỳ tối thiểu 01 lần/ 02 tháng.

3.6.2.3 Xây dựng và tuân thủ quy định quản lý tài khoản

Có quy định quản lý tài khoản trong tổ chức đáp ứng các yêu cầu sau:

- Thay đổi hoặc vô hiệu hóa tài khoản mặc định trên phần mềm, thiết bị (như tài khoản root, administrator, tài khoản cấu hình sẵn của nhà cung cấp dịch vụ).

- Quản lý tách biệt giữa các loại tài khoản: tài khoản quản trị, tài khoản tác nghiệp, tài khoản kỹ thuật, tài khoản dịch vụ.

- Mỗi tài khoản truy cập hệ thống phải được gán cho một người sử dụng duy nhất; trường hợp chia sẻ tài khoản dùng chung phải được phê duyệt bởi cấp có thẩm quyền và làm rõ trách nhiệm cá nhân tại mỗi thời điểm sử dụng.

- Xóa hoặc vô hiệu hóa các tài khoản không hoạt động sau 45 ngày hoặc ngay khi có thay đổi về nhân sự quản lý, sử dụng, khai thác tài khoản.

- Định kỳ rà soát và cập nhật quy định quản lý tài khoản và các tài liệu liên quan tối thiểu 01 lần/ năm hoặc khi có thay đổi trong tổ chức có ảnh hưởng đến quy định.

3.6.2.4 Xây dựng và tuân thủ quy định quản lý truy cập

Có quy định về quản lý truy cập đáp ứng các yêu cầu sau:

- Nguyên tắc cấp quyền tối thiểu và phân tách nhiệm vụ đối với mọi loại tài khoản.

- Tài liệu hóa các quyền truy cập cần thiết tương ứng với các chức danh, bộ phận trong cơ quan, tổ chức.

- Yêu cầu xác thực MFA đối với truy cập của người dùng từ bên ngoài tổ chức, từ đối tác/ bên thứ ba, từ Internet và truy cập vào tài khoản có quyền quản trị hệ thống.

- Định kỳ rà soát và cập nhật quy định quản lý truy cập và các tài liệu liên quan tối thiểu 01 lần/ năm hoặc khi có thay đổi trong tổ chức có ảnh hưởng đến quy định.

3.7 Quản lý lỗ hổng bảo mật

3.7.1 Khái quát

a) Có kế hoạch đánh giá và theo dõi các lỗ hổng bảo mật thường xuyên để khắc phục và giảm thiểu nguy cơ bị tấn công mạng.

b) Theo dõi, cập nhật thông tin về các mối đe dọa, lỗ hổng bảo mật mới từ nhiều nguồn.

3.7.2 Yêu cầu cụ thể

3.7.2.1 Có quy trình quản lý lỗ hổng bảo mật

a) Có quy trình quản lý lỗ hổng bảo mật cho các tài sản công nghệ thông tin của tổ chức. Các nội dung tối thiểu bao gồm:

- Phát hiện lỗ hổng bảo mật: Xây dựng và triển khai giải pháp để rà quét lỗ hổng bảo mật cho các tài sản phần cứng và phần mềm của cơ quan, tổ chức.

- Đánh giá mức độ nghiêm trọng của lỗ hổng: Triển khai đánh giá mức độ nghiêm trọng của lỗ hổng, từ đó xác định mức độ ưu tiên của việc khắc phục lỗ hổng.

- Chia sẻ thông tin lỗ hổng: Có cơ chế để chia sẻ thông tin, tiếp nhận và phản hồi báo cáo lỗ hổng bảo mật từ bên liên quan hoặc các nguồn công khai khác.

- Triển khai các biện pháp khắc phục: Có phương án, biện pháp kiểm soát rủi ro, kế hoạch khắc phục cho các lỗ hổng đã phát hiện theo thứ tự ưu tiên và đánh giá lại hệ thống để đảm bảo lỗ hổng đã được khắc phục hoàn toàn.

b) Rà soát, cập nhật quy trình và rà quét lỗ hổng bảo mật tối thiểu 01 lần/ năm hoặc khi xảy ra thay đổi trong tổ chức ảnh hưởng đến quy trình này.

3.7.2.2 Có quy trình quản lý bản vá

Có quy trình quản lý bản vá. Các nội dung tối thiểu bao gồm:

- Thực hiện kiểm tra và cập nhật bản vá hệ điều hành, ứng dụng cho toàn bộ máy tính, thiết bị di động cấp cho người dùng tối thiểu 01 lần/ tháng (nếu có).

- Giám sát và duy trì hệ thống để đảm bảo phát hiện kịp thời các lỗ hổng mới xuất hiện và cập nhật bản vá.

3.8 Quản lý nhật ký an ninh mạng

3.8.1 Khái quát

Thực hiện thu thập, phân tích, giám sát và lưu trữ nhật ký an ninh mạng để phát hiện sớm và ứng phó sự cố tấn công mạng.

3.8.2 Yêu cầu cụ thể

3.8.2.1 Thiết lập quy trình quản lý nhật ký an ninh mạng

a) Có quy định quản lý nhật ký an ninh mạng, trong đó bao gồm:

- Quy định về cách thức ghi nhật ký.

- Quy định về việc thu thập, kiểm tra, lưu trữ nhật ký.

- Quy định các loại nhật ký được thu thập. Thu thập tối thiểu các loại nhật ký sau: Nhật ký truy cập tài sản phần cứng, nhật ký truy cập tài sản phần mềm, nhật ký cảnh báo của các thiết bị bảo mật.

- Sử dụng máy chủ thời gian để đồng bộ thời gian giữa các thiết bị mạng, thiết bị đầu cuối và các thành phần khác trong hệ thống tham gia giám sát.

- Định kỳ thực hiện rà soát nhật ký an ninh mạng tối thiểu 01 lần/ năm.

b) Kiểm tra và cập nhật tối thiểu 01 lần/ năm hoặc khi có thay đổi ảnh hưởng đến quy trình này.

3.9 Bảo vệ cho trình duyệt web, dịch vụ thư điện tử

3.9.1 Khái quát

Tăng cường bảo vệ và phát hiện các mối đe dọa từ dịch vụ thư điện tử, trình duyệt web thuộc hệ thống thông tin.

3.9.2 Yêu cầu cụ thể

3.9.2.1 Quản lý trình duyệt web và dịch vụ thư điện tử

a) Có danh sách các trình duyệt web và dịch vụ thư điện tử được phép sử dụng trong cơ quan, tổ chức.

b) Đảm bảo danh sách các trình duyệt web và dịch vụ thư điện tử trên đang trong thời gian hỗ trợ của nhà cung cấp.

c) Đảm bảo phiên bản trình duyệt web và dịch vụ thư điện tử được rà soát, cập nhật bản vá lỗ hổng bảo mật thường xuyên hoặc có biện pháp kiểm soát rủi ro tương đương.

3.9.2.2 Sử dụng dịch vụ lọc tên miền

Triển khai sử dụng dịch vụ lọc tên miền trong cơ quan, tổ chức để ngăn chặn các tên miền giả mạo và độc hại.

3.10 Phòng chống phần mềm độc hại

3.10.1 Khái quát

a) Có quy định để quản lý, phòng chống, khắc phục việc cài đặt, lây lan, thực thi các phần mềm và đoạn mã độc hại trong cơ quan, tổ chức.

b) Triển khai giải pháp phòng chống mã độc cho tất cả tài sản và các điểm kết nối giữa những hệ thống thông tin (bao gồm cả kết nối nội bộ và kết nối ra bên ngoài tổ chức). Giải pháp phòng chống mã độc phải phù hợp và tương thích với hệ thống thông tin của cơ quan, tổ chức, đồng thời có khả năng tự động dò quét, ngăn chặn khi phát hiện mã độc, cập nhật kịp thời các mẫu nhận diện mã độc mới và tích hợp với quy trình quản lý lỗ hổng, ứng phó sự cố.

3.10.2 Yêu cầu cụ thể

3.10.2.1 Triển khai và duy trì phần mềm, giải pháp phòng chống mã độc

a) Triển khai và duy trì phần mềm, giải pháp phòng, chống mã độc hoặc phương án tương đương trên máy chủ, máy tính người dùng.

b) Sử dụng giải pháp phòng, chống mã độc, bao gồm ít nhất các tính năng cơ bản như bảo vệ thời gian thực, tự động cập nhật các mẫu nhận diện mã độc mới.

3.10.2.2 Thực hiện phòng, chống mã độc đối với các thiết bị lưu trữ ngoài

Triển khai rà quét mã độc và vô hiệu hóa tính năng tự động thực thi (autorun, autoplay…) đối với các phương tiện lưu trữ di động như ổ cứng, thẻ nhớ, USB…

3.11 Sao lưu và khôi phục dữ liệu

3.11.1 Khái quát

Triển khai và duy trì phương án sao lưu, khôi phục dữ liệu, đảm bảo khôi phục các tài sản về trạng thái tin cậy trước khi có sự cố.

3.11.2 Yêu cầu cụ thể

3.11.2.1 Xây dựng và tuân thủ quy định sao lưu, khôi phục dữ liệu

a) Có quy định sao lưu và khôi phục dữ liệu. Các nội dung tối thiểu bao gồm:

- Định nghĩa các loại dữ liệu cần được sao lưu và khôi phục cơ bản sau: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu, dữ liệu, thông tin nghiệp vụ.

- Xác định tần suất sao lưu và khôi phục tương ứng với từng loại dữ liệu đã định nghĩa.

- Xác định phương pháp sao lưu và khôi phục tương ứng với từng loại dữ liệu đã định nghĩa.

- Quản lý vùng lưu trữ dữ liệu sao lưu, đảm bảo tính toàn vẹn của dữ liệu và khôi phục dữ liệu một cách nhanh, hiệu quả.

- Định kỳ thực hiện khôi phục dữ liệu đã sao lưu dựa trên mức độ nhạy cảm và tầm quan trọng của dữ liệu nhằm kiểm tra khả năng khôi phục của bản sao lưu.

b) Rà soát và cập nhật quy định tối thiểu 01 lần/ năm hoặc khi xảy ra thay đổi trong tổ chức ảnh hưởng đến quy định.

3.11.2.2 Thực hiện sao lưu dữ liệu tự động

Xác định danh sách dữ liệu cần sao lưu và phân loại tần suất sao lưu theo thời gian (ngày/tuần/tháng/năm…) đối với từng loại dữ liệu.

3.11.2.3 Bảo vệ bản sao lưu dữ liệu

Thực hiện bảo vệ bản sao lưu dữ liệu đảm bảo tính toàn vẹn, tính sẵn sàng và khả năng khôi phục của dữ liệu.

3.12 Quản lý hạ tầng mạng

3.12.1 Khái quát

Có phương án thiết lập, thực thi và quản lý thiết bị mạng để phòng ngừa tin tặc khai thác lỗ hổng dịch vụ mạng và các điểm truy cập dễ bị tấn công.

3.12.2 Yêu cầu cụ thể

3.12.2.1 Thiết lập, duy trì các sơ đồ kiến trúc hệ thống mạng và kiến trúc mạng an toàn

a) Có phương án thiết lập và duy trì sơ đồ kiến trúc mạng và các hồ sơ khác về hệ thống mạng.

b) Có phương án triển khai và duy trì một kiến trúc hệ thống mạng an toàn, đảm bảo thực hiện tối thiểu 03 nguyên tắc: phân vùng mạng, đặc quyền ít nhất và tính sẵn sàng.

c) Tài liệu hóa sơ đồ kiến trúc hệ thống mạng tối thiểu bao gồm:

- Tổng quan kiến trúc hệ thống mạng.

- Sơ đồ cấp chi tiết của hệ thống mạng.

- Ghi chú các tài liệu đặc tả kỹ thuật, tài liệu thống kê…

- Tài liệu mô tả phương án đảm bảo an ninh mạng.

d) Xem xét và cập nhật sơ đồ mạng 01 lần/ năm hoặc mỗi khi có thay đổi ảnh hưởng đến sơ đồ hệ thống.

3.12.2.2 Quản lý an toàn cơ sở hạ tầng mạng

Thực hiện quản lý an toàn cơ sở hạ tầng mạng, đảm bảo tối thiểu:

- Có phương án dự phòng cho các thiết bị mạng chính.

- Sử dụng giải pháp tường lửa có tích hợp chức năng phòng, chống xâm nhập hoặc có phương án tương đương phục vụ kiểm soát truy cập và phòng, chống xâm nhập giữa các vùng mạng; kiểm soát truy cập thiết bị đầu cuối, máy tính người dùng kết nối vào mạng.

- Định kỳ cập nhật cơ sở dữ liệu phát hiện tấn công mạng cho các giải pháp đảm bảo an ninh mạng trong hệ thống thông tin.

- Thực hiện quản lý thay đổi.

- Kiểm tra hiệu năng (RAM, CPU...), đảm bảo hoạt động bình thường của hệ thống.

3.12.2.3 Kiểm thử và nghiệm thu hệ thống

a) Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống.

b) Thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng.

c) Có nhân sự chịu trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống.

3.12.2.4 Kiểm soát truy cập

a) Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn (nếu hỗ trợ) khi truy cập thông tin nội bộ hoặc thực hiện quản trị từ xa đối với tài sản phần cứng và phần mềm.

b) Cấu hình chức năng xác thực trên các tài sản phần cứng, phần mềm (nếu hỗ trợ) để xác thực người dùng khi quản trị thiết bị trực tiếp hoặc từ xa.

c) Kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả truy cập tới các tài sản phần cứng và phần mềm mà hệ thống không cung cấp hoặc không cho phép truy cập.

d) Thiết lập giới hạn thời gian chờ (timeout) để tự động đóng các phiên kết nối khi không nhận được yêu cầu từ người dùng trong một khoảng thời gian quy định.

3.12.2.5 Xây dựng và áp dụng chính sách quản lý truy cập từ xa

Sử dụng mạng riêng ảo VPN hoặc phương án tương đương và yêu cầu xác thực cho việc truy cập từ xa vào hệ thống đối với người dùng quản trị, người dùng tác nghiệp hệ thống.

3.13 Nhân sự vận hành, quản trị hệ thống, bảo vệ an ninh mạng

3.13.1 Khái quát

a) Có nhân sự vận hành, quản trị, bảo vệ an ninh mạng.

b) Có chương trình đào tạo nâng cao nhận thức an ninh mạng và kỹ năng an ninh mạng.

3.13.2 Yêu cầu cụ thể

3.13.2.1 Có nhân sự phụ trách về vận hành, quản trị hệ thống và bảo vệ an ninh mạng

a) Có nhân sự phụ trách vận hành, quản trị hệ thống và bảo vệ an ninh mạng.

b) Nhân sự phụ trách về vận hành, quản trị hệ thống và bảo vệ an ninh mạng phải có trình độ về an ninh mạng, công nghệ thông tin; có cam kết bảo mật thông tin trong quá trình làm việc và sau khi nghỉ việc.

3.13.2.2 Thiết lập và duy trì chương trình đào tạo tổng quan để nâng cao nhận thức an ninh mạng cho cán bộ, nhân viên

a) Có chương trình nâng cao nhận thức an ninh mạng cho toàn bộ cán bộ, nhân viên có sử dụng hệ thống thông tin.

b) Tiến hành đào tạo tối thiểu 01 lần/ năm.

c) Chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của tổ chức.

3.14 Quản lý nhà cung cấp sản phẩm, dịch vụ

3.14.1 Khái quát

Có quy trình để đánh giá nhà cung cấp sản phẩm, dịch vụ an ninh mạng, lưu trữ, xử lý dữ liệu nhạy cảm hoặc chịu trách nhiệm về các quy trình, nền tảng quan trọng của hệ thống.

3.14.2 Yêu cầu cụ thể

Có phương án thiết lập và duy trì bản kiểm kê các nhà cung cấp sản phẩm, dịch vụ. Tối thiểu bao gồm:

- Lập danh sách, theo dõi, cập nhật trạng thái các nhà cung cấp sản phẩm, dịch vụ.

- Thực hiện phân loại các nhà cung cấp dịch vụ trong danh sách quản lý.

- Có văn bản xác định rõ phạm vi trách nhiệm của nhà cung cấp và tổ chức.

- Xem xét và cập nhật danh sách tối thiểu 01 lần/ năm hoặc khi xảy ra thay đổi ảnh hưởng đến danh sách này.

3.15 Quản trị ứng phó sự cố an ninh mạng

3.15.1 Khái quát

Có kế hoạch, chương trình để phát triển và duy trì khả năng ứng phó sự cố bao gồm chính sách, kế hoạch, thủ tục, vai trò, đào tạo, kênh liên lạc.

3.15.2 Yêu cầu cụ thể

3.15.2.1 Thành lập lực lượng ứng phó sự cố an ninh mạng

a) Chỉ định một người chủ chốt và ít nhất một người dự phòng để quản lý quy trình ứng phó sự cố an ninh mạng.

b) Thiết lập và duy trì đầu mối liên lạc để báo cáo sự cố. Xác minh thông tin liên hệ của các cơ quan, tổ chức hỗ trợ điều phối ứng phó sự cố hàng năm để đảm bảo thông tin được cập nhật.

c) Phân công vị trí, vai trò và trách nhiệm chính của từng thành viên trong lực lượng tham gia ứng phó sự cố.

d) Quy định về trách nhiệm phối hợp với lực lượng ứng phó sự cố an ninh mạng của các phòng ban có liên quan.

3.15.2.2 Thiết lập và duy trì quy trình nội bộ để báo cáo sự cố an ninh mạng

a) Có quy trình nội bộ để báo cáo sự cố an ninh mạng.

b) Thực hiện phân nhóm sự cố an ninh mạng.

c) Đánh giá và cập nhật quy trình tối thiểu 01 lần/ năm hoặc khi xảy ra các thay đổi ảnh hưởng đến quy trình.

3.15.2.3 Thiết lập và duy trì quy trình ứng phó sự cố an ninh mạng

a) Có quy trình ứng phó sự cố, đảm bảo có cơ chế phối hợp với các cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ khắc phục sự cố an ninh mạng.

b) Đánh giá và cập nhật quy trình tối thiểu 01 lần/ năm hoặc khi xảy ra các thay đổi ảnh hưởng đến quy trình.

4 Yêu cầu cơ bản đối với hệ thống thông tin cấp độ 2

4.1 Quản lý rủi ro an ninh mạng

a) Có quy định, quy trình quản lý rủi ro an ninh mạng. Trong đó, yêu cầu thực hiện quản lý rủi ro an ninh mạng bao gồm tối thiểu các bước: xác định, phân tích, đánh giá và xử lý rủi ro an ninh mạng.

b) Đánh giá và cập nhật quy định, quy trình quản lý rủi ro an ninh mạng và các tài liệu liên quan tối thiểu 01 lần/ năm hoặc khi có thay đổi xảy ra trong tổ chức ảnh hưởng đến các văn bản đã ban hành có liên quan.

4.2 Quản lý tài sản phần cứng

4.2.1 Khái quát

a) Lập danh sách, theo dõi, cập nhật trạng thái của tất cả tài sản phần cứng thuộc hệ thống thông tin và các tài sản không thuộc quyền kiểm soát của tổ chức nhưng có kết nối vào hệ thống thông tin; xác định danh sách tài sản cần được giám sát, bảo vệ.

b) Xác định các tài sản vô chủ, tài sản trái phép để loại bỏ hoặc đưa ra phương án quản lý.

c) Thực hiện kiểm kê, rà soát và cập nhật danh sách cho tất cả tài sản thuộc hệ thống thông tin định kỳ tối thiểu 01 lần/ năm.

4.2.2 Yêu cầu cụ thể

4.2.2.1 Thiết lập và duy trì hệ thống quản lý danh mục tài sản phần cứng

a) Lập danh sách, theo dõi, cập nhật trạng thái của tất cả tài sản phần cứng có khả năng lưu trữ hoặc xử lý dữ liệu, bao gồm: thiết bị của người dùng cuối, thiết bị di động, thiết bị lưu trữ ngoài, thiết bị văn phòng, thiết bị mạng, thiết bị OT/IoT và máy chủ trong môi trường vật lý, ảo hóa, truy cập từ xa và điện toán đám mây.

b) Danh sách tài sản phần cứng phải bao gồm tối thiểu các thông tin cơ bản sau: tên tài sản, địa chỉ mạng IP (đối với thiết bị đặt địa chỉ IP tĩnh), địa chỉ phần cứng MAC/ mã nhận diện serial, thời gian ngừng hỗ trợ kỹ thuật của hãng (nếu có), vị trí lắp đặt địa lý, vị trí lắp đặt trong hệ thống mạng, mục đích sử dụng, tình trạng sử dụng. Tài sản vật lý phải được giao, gán trách nhiệm cho cá nhân hoặc bộ phận quản lý, sử dụng.

c) Các thiết bị di động do tổ chức quản lý hoặc được tổ chức cho phép kết nối vào hệ thống thông tin phải được đăng ký để kiểm soát. Quy định trách nhiệm của cá nhân trong tổ chức khi sử dụng thiết bị di động để phục vụ công việc.

4.2.2.2 Xử lý các tài sản phần cứng chưa được quản lý

a) Có quy trình phát hiện và xử lý các tài sản phần cứng không có trong danh sách quản lý, đang kết nối trái phép vào hệ thống thông tin định kỳ tối thiểu 01 lần/ năm.

b) Có thể lựa chọn loại bỏ, từ chối kết nối hoặc cách ly tài sản trái phép.

4.2.2.3 Xử lý các tài sản phần cứng khi chuyển giao

Có phương án xóa sạch thông tin, dữ liệu trên tài sản phần cứng khi chuyển giao hoặc thay đổi mục đích sử dụng.

4.3 Quản lý tài sản phần mềm

4.3.1 Khái quát

a) Lập danh sách, theo dõi, cập nhật trạng thái của tất cả tài sản phần mềm thuộc hệ thống thông tin của cơ quan, tổ chức, đảm bảo chỉ những phần mềm đã phê duyệt mới được phép cài đặt và sử dụng.

b) Thực hiện kiểm kê, rà soát và cập nhật danh sách cho tất cả tài sản phần mềm định kỳ tối thiểu 01 lần/ năm.

4.3.2 Yêu cầu cụ thể

4.3.2.1 Thiết lập và duy trì hệ thống quản lý danh mục tài sản phần mềm

a) Lập danh sách, theo dõi, cập nhật trạng thái của tất cả tài sản phần mềm hiện đang được cài đặt trên các tài sản phần cứng thuộc hệ thống thông tin của cơ quan, tổ chức.

b) Danh sách tài sản phần mềm phải bao gồm tối thiểu các thông tin cơ bản sau: tên tài sản, mục đích sử dụng, thời gian ngừng hỗ trợ kỹ thuật (nếu có), phạm vi sử dụng, chủ thể quản lý, thông tin về bản quyền, phiên bản, hệ thống thông tin thành phần (nếu có). Tài sản phần mềm phải được gắn trách nhiệm cho cá nhân hoặc bộ phận quản lý, sử dụng.

4.3.2.2 Xử lý các tài sản phần mềm trái phép

a) Có quy trình phát hiện và xử lý các phần mềm trái phép định kỳ tối thiểu 01 lần/ năm.

b) Những phần mềm trái phép nhưng vẫn cần thiết đối với hoạt động của cơ quan, tổ chức phải được đưa vào danh sách ngoại lệ để quản lý. Danh sách ngoại lệ này phải thể hiện chi tiết các biện pháp kiểm soát giảm thiểu nguy cơ an ninh mạng ảnh hưởng đến hệ thống.

c) Những phần mềm trái phép không nằm trong danh sách ngoại lệ phải có kế hoạch để xóa/ gỡ bỏ hoàn toàn khỏi các tài sản phần cứng của cơ quan, tổ chức trong thời gian sớm nhất.

4.3.2.3 Phát triển phần mềm thuê khoán

a) Có biên bản, hợp đồng và cam kết bảo mật đối với bên thuê khoán các nội dung liên quan đến phát triển phần mềm thuê khoán.

b) Yêu cầu nhà phát triển cung cấp mã nguồn phần mềm. Trong trường hợp không thể cung cấp mã nguồn phần mềm, chủ quản hệ thống phải yêu cầu các bên thuê khoán cung cấp chứng chỉ đánh giá an toàn độc lập hoặc thực hiện các biện pháp kiểm thử xâm nhập, giám sát rủi ro thay thế và ký cam kết chịu trách nhiệm pháp lý về tính an toàn của phần mềm.

4.4 Quản lý tài sản thông tin

4.4.1 Khái quát

Thực hiện quản lý tài sản thông tin và triển khai các biện pháp kiểm soát để phát hiện, phân loại, xử lý, lưu trữ và loại bỏ tài sản thông tin một cách an toàn.

4.4.2 Yêu cầu cụ thể

4.4.2.1 Thiết lập và duy trì quy định quản lý tài sản thông tin

a) Có quy định quản lý tài sản thông tin. Trong quy định, xác định danh sách tài sản thông tin, mức độ nhạy cảm, chủ sở hữu, các bước xử lý, thời gian lưu trữ và các yêu cầu khi tiêu hủy/xóa bỏ dựa trên các tiêu chuẩn về mức độ bảo mật của tài sản thông tin.

b) Mức độ nhạy cảm của tài sản thông tin có thể được quy định như sau:

- Mức 1: Công khai. Tài sản thông tin công khai không yêu cầu về bảo mật.

- Mức 2: Nội bộ. Tài sản thông tin nội bộ yêu cầu chỉ những người trong tổ chức mới có quyền truy cập.

- Mức 3: Hạn chế truy cập. Tài sản thông tin bị hạn chế yêu cầu quyền truy cập, chỉ những người dùng được cấp quyền mới có thể truy cập vào dữ liệu. Việc tiết lộ tài sản thông tin bị hạn chế truy cập có khả năng ảnh hưởng đến hoạt động của các cơ quan, tổ chức.

c) Có quy trình yêu cầu truy cập, thêm mới, sửa, xóa dữ liệu để kiểm soát truy cập dữ liệu.

d) Kiểm tra cấp độ phân quyền dữ liệu định kỳ tối thiểu 01 lần/ năm.

e) Đánh giá và cập nhật quy trình quản lý tài sản thông tin định kỳ tối thiểu 01 lần/ năm hoặc khi xảy ra các thay đổi trong tổ chức ảnh hưởng đến quy trình.

4.4.2.2 Thiết lập và duy trì bản danh sách tài sản thông tin

a) Lập danh sách các tài sản thông tin dựa trên quy trình quản lý tài sản thông tin.

b) Đánh giá và cập nhật danh sách tài sản thông tin tối thiểu 01 lần/ năm hoặc khi xảy ra thay đổi trong tổ chức ảnh hưởng đến danh sách.

4.4.2.3 Xây dựng danh sách kiểm soát truy cập tài sản thông tin

Xây dựng danh sách quyền truy cập của các tài khoản, người dùng đối với từng loại tài sản thông tin.

4.4.2.4 Mã hóa dữ liệu

Mã hóa thông tin xác thực, dữ liệu (không phải là thông tin, dữ liệu công khai) được lưu trữ trong các tài sản phần cứng và phần mềm của cơ quan, tổ chức, không áp dụng cứng đối với hệ thống/dịch vụ có yêu cầu sử dụng, truy xuất lớn nếu đã có biện pháp kiểm soát rủi ro tương đương.

4.5 Cấu hình an toàn cho phần cứng và phần mềm

4.5.1 Khái quát

Thiết lập và duy trì cấu hình an toàn cho phần cứng (như thiết bị người dùng cuối bao gồm máy tính, thiết bị di động và cầm tay, thiết bị mạng, thiết bị OT/IoT, máy chủ...) và phần mềm (như hệ điều hành, ứng dụng…).

4.5.2 Yêu cầu cụ thể

4.5.2.1 Thiết lập và duy trì quy định, quy trình cấu hình an toàn cho tài sản phần cứng và phần mềm

a) Có quy định, quy trình cấu hình an toàn cho các tài sản phần cứng và phần mềm của cơ quan, tổ chức.

b) Có các tài liệu cấu hình tiêu chuẩn, tài liệu cấu hình tăng cường bảo mật cho các tài sản phần cứng và phần mềm của cơ quan, tổ chức. Đảm bảo sử dụng giao thức kết nối an toàn, thiết lập tường lửa cho máy chủ/ máy trạm và có phương án chống đăng nhập tự động đối với các tài sản xử lý và lưu trữ dữ liệu quan trọng.

c) Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ mà phần cứng, phần mềm không sử dụng.

d) Đánh giá và cập nhật quy định, quy trình quản lý cấu hình an toàn và các tài liệu liên quan tối thiểu 01 lần/ năm hoặc khi có thay đổi xảy ra trong tổ chức ảnh hưởng đến tài liệu.

4.5.2.2 Cấu hình tự động khóa phiên làm việc trên các tài sản phần cứng và phần mềm

a) Dựa trên yêu cầu sử dụng, kết quả đánh giá rủi ro, thực hiện cấu hình tự động khóa phiên làm việc trên các tài sản phần cứng và phần mềm. Có thể thực hiện cấu hình như sau:

- Tự động khóa phiên làm việc trên các tài sản sau một khoảng thời gian không sử dụng:

+ Đối với máy tính người dùng: không quá 15 phút.

+ Đối với các phiên quản trị phần mềm, máy chủ, thiết bị mạng, thiết bị IoT: không quá 05 phút.

+ Đối với thiết bị di động: không quá 05 phút.

+ Đối với các phần mềm nghiệp vụ xử lý dữ liệu quan trọng: không quá 15 phút.

- Tự động khóa thiết bị di động sau một số lần đăng nhập thất bại:

+ Đối với máy tính xách tay: tối đa 10 lần.

+ Đối với điện thoại: tối đa 10 lần.

+ Đối với các phần mềm nghiệp vụ lưu trữ và xử lý dữ liệu quan trọng: tối đa 05 lần.

+ Giới hạn thời gian mở khóa thiết bị sau khi bị khóa: tối thiểu 12 giờ, tối đa 30 ngày.

b) Có cơ chế mở khóa khẩn cấp dành cho quản trị viên/tài khoản đặc quyền.

4.6 Quản lý tài khoản và quyền truy cập tài khoản của người dùng

4.6.1 Khái quát

a) Có quy trình, công cụ để phân quyền và quản lý quyền truy cập của tài khoản người dùng bao gồm: tài khoản quản trị, tài khoản tác nghiệp (tài khoản của người dùng cuối tác nghiệp), tài khoản kỹ thuật (tài khoản dùng để kết nối giữa các hệ thống kỹ thuật), tài khoản dịch vụ (tài khoản cấp cho người thụ hưởng dịch vụ) trên các tài sản phần cứng và phần mềm.

b) Có quy trình tạo, gán, quản lý, thu hồi đặc quyền và quyền truy cập đối với các tài khoản người dùng cho tài sản phần cứng và phần mềm. Quyền truy cập của tài khoản quản trị, tài khoản tác nghiệp, tài khoản kỹ thuật, tài khoản dịch vụ phải nhất quán dựa trên vai trò và các yêu cầu cụ thể, đảm bảo người dùng chỉ có quyền truy cập vào dữ liệu, tài sản phù hợp.

c) Ghi nhật ký và giám sát tài khoản người dùng.

4.6.2 Yêu cầu cụ thể

4.6.2.1 Thiết lập và duy trì hệ thống quản lý tài khoản

a) Lập danh sách, theo dõi và cập nhật tất cả các tài khoản trên các tài sản phần cứng và phần mềm của tổ chức.

b) Danh sách tài khoản phải bao gồm tối thiểu các loại tài khoản sau: tài khoản quản trị, tài khoản tác nghiệp và tài khoản kỹ thuật.

c) Danh sách tài khoản phải bao gồm các thông tin tối thiểu: loại tài khoản, tên tài khoản, trạng thái tài khoản, tên tài sản/ hệ thống thông tin tương ứng, tên người quản lý, phòng ban, ngày kích hoạt tài khoản, ngày vô hiệu hóa tài khoản (nếu có). Đảm bảo tất cả tài khoản đang hoạt động là hợp lệ.

d) Danh sách tài khoản phải được rà soát định kỳ tối thiểu 01 lần/ năm.

4.6.2.2 Xây dựng và tuân thủ quy định sử dụng mật khẩu

a) Thiết lập cấu hình mật khẩu trên tài sản phần cứng, phần mềm để đảm bảo an toàn mật khẩu người sử dụng, bao gồm các yêu cầu sau:

- Yêu cầu thay đổi mật khẩu mặc định.

- Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự.

- Thiết lập thời gian yêu cầu thay đổi mật khẩu.

- Thiết lập thời gian mật khẩu hợp lệ.

b) Dựa trên yêu cầu sử dụng, kết quả đánh giá rủi ro, triển khai quy định sử dụng mật khẩu an toàn trong tổ chức. Có thể thực hiện cấu hình như sau:

- Sử dụng mật khẩu duy nhất cho mỗi tài sản hoặc sử dụng giải pháp xác thực và quản lý tập trung.

- Yêu cầu thay đổi mật khẩu trong lần đăng nhập đầu tiên.

- Đối với các hệ thống sử dụng xác thực MFA, quy định mật khẩu có tối thiểu 08 ký tự.

- Đối với các hệ thống không sử dụng xác thực MFA, quy định mật khẩu có tối thiểu 14 ký tự, bao gồm ký tự viết thường, ký tự viết hoa, ký tự đặc biệt, chữ số.

- Đối với tài khoản quản trị cần thay đổi mật khẩu định kỳ tối thiểu 01 lần/02 tháng.

4.6.2.3 Xây dựng và tuân thủ quy định quản lý tài khoản

Có quy định quản lý tài khoản trong tổ chức đáp ứng các yêu cầu sau:

- Thay đổi hoặc vô hiệu hóa tài khoản mặc định trên phần mềm, thiết bị (như tài khoản root, administrator, tài khoản cấu hình sẵn của nhà cung cấp dịch vụ).

- Quản lý tách biệt giữa các loại tài khoản: tài khoản quản trị, tài khoản tác nghiệp, tài khoản kỹ thuật, tài khoản dịch vụ.

- Mỗi tài khoản truy cập hệ thống phải được gán cho một người sử dụng duy nhất; trường hợp chia sẻ tài khoản dùng chung phải được phê duyệt bởi cấp có thẩm quyền và làm rõ trách nhiệm cá nhân tại mỗi thời điểm sử dụng.

- Xóa hoặc vô hiệu hóa các tài khoản không hoạt động sau 45 ngày hoặc ngay khi có thay đổi về nhân sự quản lý, sử dụng, khai thác tài khoản.

- Định kỳ rà soát và cập nhật quy định quản lý tài khoản và các tài liệu liên quan tối thiểu 01 lần/ năm hoặc khi có thay đổi trong tổ chức có ảnh hưởng đến quy định.

4.6.2.4 Xây dựng và tuân thủ quy định quản lý truy cập

Có quy định về quản lý truy cập đáp ứng các yêu cầu sau:

- Nguyên tắc cấp quyền tối thiểu và phân tách nhiệm vụ đối với mọi loại tài khoản.

- Tài liệu hóa các quyền truy cập cần thiết tương ứng với các chức danh, bộ phận trong cơ quan, tổ chức.

- Yêu cầu xác thực MFA đối với truy cập của người dùng từ bên ngoài tổ chức, từ đối tác/ bên thứ ba, từ Internet và truy cập vào tài khoản có quyền quản trị hệ thống.

- Định kỳ rà soát và cập nhật quy định quản lý truy cập và các tài liệu liên quan tối thiểu 01 lần/ năm hoặc khi có thay đổi trong tổ chức có ảnh hưởng đến quy định.

4.7 Quản lý lỗ hổng bảo mật

4.7.1 Khái quát

a) Xây dựng, phát triển kế hoạch đánh giá và theo dõi các lỗ hổng bảo mật thường xuyên để khắc phục và giảm thiểu nguy cơ bị tấn công mạng.

b) Theo dõi, cập nhật thông tin về các mối đe dọa, lỗ hổng bảo mật mới từ nhiều nguồn.

4.7.2 Yêu cầu cụ thể

4.7.2.1 Có quy trình quản lý lỗ hổng bảo mật

a) Có quy trình quản lý lỗ hổng bảo mật cho các tài sản công nghệ thông tin của tổ chức. Các nội dung tối thiểu bao gồm:

- Phát hiện lỗ hổng bảo mật: Xây dựng và triển khai giải pháp để rà quét lỗ hổng bảo mật cho các tài sản phần cứng và phần mềm của cơ quan, tổ chức.

- Đánh giá mức độ nghiêm trọng của lỗ hổng: Triển khai đánh giá mức độ nghiêm trọng của lỗ hổng, từ đó xác định mức độ ưu tiên của việc khắc phục lỗ hổng.

- Chia sẻ thông tin lỗ hổng: Có cơ chế để chia sẻ thông tin, tiếp nhận và phản hồi báo cáo lỗ hổng bảo mật từ bên liên quan hoặc các nguồn công khai khác.

- Triển khai các biện pháp khắc phục: Có phương án, biện pháp kiểm soát rủi ro, kế hoạch khắc phục cho các lỗ hổng đã phát hiện theo thứ tự ưu tiên và đánh giá lại hệ thống để đảm bảo lỗ hổng đã được khắc phục hoàn toàn.

b) Rà soát, cập nhật quy trình và rà quét lỗ hổng bảo mật tối thiểu 01 lần/ năm hoặc khi xảy ra thay đổi trong tổ chức ảnh hưởng đến quy trình này.

4.7.2.2 Có quy trình quản lý bản vá

Có quy trình quản lý bản vá. Các nội dung tối thiểu bao gồm:

- Có phương án triển khai bản vá cho toàn bộ tài sản phần cứng và phần mềm thuộc hệ thống thông tin.

- Đánh giá tác động, tiến hành kiểm thử và xây dựng phương án phục hồi trước khi triển khai bản vá trên các hệ thống thông tin có xử lý hoặc lưu trữ dữ liệu quan trọng.

- Thực hiện kiểm tra và cập nhật bản vá hệ điều hành, ứng dụng cho toàn bộ máy tính, thiết bị di động cấp cho người dùng tối thiểu 01 lần/ tháng (nếu có).

- Giám sát và duy trì hệ thống để đảm bảo phát hiện kịp thời các lỗ hổng mới xuất hiện và cập nhật bản vá.

4.8 Quản lý nhật ký an ninh mạng

4.8.1 Khái quát

Thực hiện thu thập, phân tích, giám sát và lưu trữ nhật ký an ninh mạng để phát hiện sớm và ứng phó sự cố tấn công mạng.

4.8.2 Yêu cầu cụ thể

4.8.2.1 Thiết lập quy trình quản lý nhật ký an ninh mạng

a) Có quy định quản lý nhật ký an ninh mạng, trong đó bao gồm:

- Quy định về cách thức ghi nhật ký.

- Quy định về việc thu thập, kiểm tra, lưu trữ nhật ký.

- Quy định các loại nhật ký được thu thập. Thu thập tối thiểu các loại nhật ký sau: nhật ký truy cập hệ thống, nhật ký ứng dụng, nhật ký cảnh báo của các thiết bị bảo mật.

- Nhật ký truy cập hệ thống tối thiểu bao gồm: địa chỉ nguồn (IP/ tên máy, tên miền), địa chỉ đích (IP/ tên máy, tên miền), tài khoản đích (tên người dùng/ mã định danh), thời điểm xảy ra, thông tin hành vi.

- Nhật ký cảnh báo tối thiểu bao gồm: tên cảnh báo, thiết bị, mức độ, địa chỉ nguồn, loại cảnh báo, thời điểm xảy ra.

- Sử dụng máy chủ thời gian để đồng bộ thời gian giữa các thiết bị mạng, thiết bị đầu cuối và các thành phần khác trong hệ thống tham gia giám sát.

- Đảm bảo duy trì không gian lưu trữ nhật ký tối thiểu 01 tháng.

- Định kỳ thực hiện rà soát nhật ký an ninh mạng tối thiểu 01 lần/ năm.

b) Kiểm tra và cập nhật tối thiểu 01 lần/ năm hoặc khi có thay đổi ảnh hưởng đến quy trình này.

4.9 Bảo vệ cho trình duyệt web, dịch vụ thư điện tử

4.9.1 Khái quát

Tăng cường bảo vệ và phát hiện các mối đe dọa từ dịch vụ thư điện tử, trình duyệt web thuộc hệ thống thông tin.

4.9.2 Yêu cầu cụ thể

4.9.2.1 Quản lý trình duyệt web và dịch vụ thư điện tử

a) Có danh sách các trình duyệt web và dịch vụ thư điện tử được phép sử dụng trong cơ quan, tổ chức.

b) Đảm bảo danh sách các trình duyệt web và dịch vụ thư điện tử trên đang trong thời gian hỗ trợ của nhà cung cấp.

c) Đảm bảo phiên bản trình duyệt web và dịch vụ thư điện tử được rà soát, cập nhật bản vá lỗ hổng bảo mật thường xuyên hoặc có biện pháp kiểm soát rủi ro tương đương.

4.9.2.2 Sử dụng dịch vụ lọc tên miền

Triển khai sử dụng dịch vụ lọc tên miền trong cơ quan, tổ chức để ngăn chặn các tên miền giả mạo và độc hại.

4.10 Phòng chống phần mềm độc hại

4.10.1 Khái quát

a) Có quy định để quản lý, phòng chống, khắc phục việc cài đặt, lây lan, thực thi các phần mềm và đoạn mã độc hại trong cơ quan, tổ chức.

b) Triển khai giải pháp phòng chống mã độc cho tất cả tài sản và các điểm kết nối giữa những hệ thống thông tin (bao gồm cả kết nối nội bộ và kết nối ra bên ngoài tổ chức). Giải pháp phòng chống mã độc phải phù hợp và tương thích với hệ thống thông tin của cơ quan, tổ chức, đồng thời có khả năng tự động dò quét, ngăn chặn khi phát hiện mã độc, cập nhật kịp thời các mẫu nhận diện mã độc mới và tích hợp với quy trình quản lý lỗ hổng, ứng phó sự cố.

4.10.2 Yêu cầu cụ thể

4.10.2.1 Triển khai và duy trì phần mềm, giải pháp phòng chống mã độc

a) Triển khai và duy trì phần mềm, giải pháp phòng, chống mã độc hoặc phương án tương đương trên máy chủ, máy tính người dùng.

b) Sử dụng giải pháp phòng, chống mã độc, bao gồm ít nhất các tính năng cơ bản như bảo vệ thời gian thực, tự động cập nhật các mẫu nhận diện mã độc mới.

4.10.2.2 Thực hiện phòng, chống mã độc đối với các thiết bị lưu trữ ngoài

Triển khai rà quét mã độc và vô hiệu hóa tính năng tự động thực thi (autorun, autoplay…) đối với các phương tiện lưu trữ di động như ổ cứng, thẻ nhớ, USB…

4.11 Sao lưu và khôi phục dữ liệu

4.11.1 Khái quát

Triển khai và duy trì phương án sao lưu, khôi phục dữ liệu, đảm bảo khôi phục các tài sản về trạng thái tin cậy trước khi có sự cố.

4.11.2 Yêu cầu cụ thể

4.11.2.1 Xây dựng và tuân thủ quy định sao lưu, khôi phục dữ liệu

a) Có quy định sao lưu và khôi phục dữ liệu. Các nội dung tối thiểu bao gồm:

- Định nghĩa các loại dữ liệu cần được sao lưu và khôi phục cơ bản sau: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu, dữ liệu, thông tin nghiệp vụ.

- Xác định tần suất sao lưu và khôi phục tương ứng với từng loại dữ liệu đã định nghĩa.

- Xác định phương pháp sao lưu và khôi phục tương ứng với từng loại dữ liệu đã định nghĩa.

- Quản lý vùng lưu trữ dữ liệu sao lưu, đảm bảo tính toàn vẹn của dữ liệu và khôi phục dữ liệu một cách nhanh, hiệu quả.

- Định kỳ thực hiện khôi phục dữ liệu đã sao lưu dựa trên mức độ nhạy cảm và tầm quan trọng của dữ liệu nhằm kiểm tra khả năng khôi phục của bản sao lưu.

b) Rà soát và cập nhật quy định tối thiểu 01 lần/ năm hoặc khi xảy ra thay đổi trong tổ chức ảnh hưởng đến quy định.

4.11.2.2 Thực hiện sao lưu dữ liệu tự động

Xác định danh sách dữ liệu cần sao lưu và phân loại tần suất sao lưu theo thời gian (ngày/tuần/tháng/năm…) đối với từng loại dữ liệu.

4.11.2.3 Bảo vệ bản sao lưu dữ liệu

Thực hiện bảo vệ bản sao lưu dữ liệu đảm bảo tính toàn vẹn, tính sẵn sàng và khả năng khôi phục của dữ liệu.

4.11.2.4 Thiết lập và duy trì hạ tầng lưu trữ tách biệt cho bản sao lưu dữ liệu

Các bản sao lưu dữ liệu cần phải được định danh, quản lý phiên bản và lưu trữ ở những hạ tầng tách biệt với môi trường vận hành.

4.12 Quản lý hạ tầng mạng

4.12.1 Khái quát

Có phương án thiết lập, thực thi và quản lý thiết bị mạng để phòng ngừa tin tặc khai thác lỗ hổng dịch vụ mạng và các điểm truy cập dễ bị tấn công.

4.12.2 Yêu cầu cụ thể

4.12.2.1 Thiết lập, duy trì các sơ đồ kiến trúc hệ thống mạng và kiến trúc mạng an toàn

a) Thiết lập và duy trì sơ đồ kiến trúc mạng và các hồ sơ khác về hệ thống mạng.

b) Triển khai và duy trì một kiến trúc hệ thống mạng an toàn, đảm bảo thực hiện tối thiểu 03 nguyên tắc: phân vùng mạng, đặc quyền ít nhất và tính sẵn sàng.

c) Tài liệu hóa sơ đồ kiến trúc hệ thống mạng tối thiểu bao gồm:

- Tổng quan kiến trúc hệ thống mạng.

- Sơ đồ cấp chi tiết của hệ thống mạng.

- Ghi chú các tài liệu đặc tả kỹ thuật, tài liệu thống kê,...

- Tài liệu mô tả phương án đảm bảo an ninh mạng.

d) Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống.

e) Xem xét và cập nhật sơ đồ mạng 01 lần/ năm hoặc mỗi khi có thay đổi ảnh hưởng đến sơ đồ hệ thống.

4.12.2.2 Quản lý an toàn cơ sở hạ tầng mạng

a) Thực hiện quản lý an toàn cơ sở hạ tầng mạng, đảm bảo tối thiểu:

- Có phương án dự phòng cho các thiết bị mạng chính.

- Sử dụng giải pháp tường lửa có tích hợp chức năng phòng, chống xâm nhập hoặc có phương án tương đương phục vụ kiểm soát truy cập và phòng, chống xâm nhập giữa các vùng mạng.

- Sử dụng giải pháp WAF hoặc có phương án tương đương phục vụ phòng chống tấn công ứng dụng web (nếu có).

- Định kỳ cập nhật cơ sở dữ liệu phát hiện tấn công mạng cho các giải pháp đảm bảo an ninh mạng trong hệ thống thông tin.

- Thực hiện quản lý thay đổi.

- Kiểm tra hiệu năng (RAM, CPU...), đảm bảo hoạt động bình thường của hệ thống.

b) Chia tách thành các vùng mạng khác nhau theo đối tượng sử dụng, mục đích sử dụng, tối thiểu:

- Vùng mạng riêng cho máy chủ của hệ thống thông tin.

- Vùng mạng trung gian (DMZ) để cung cấp dịch vụ.

- Vùng mạng riêng để cung cấp dịch vụ mạng không dây (nếu có).

- Vùng mạng nội bộ.

- Vùng mạng biên.

4.12.2.3 Kiểm thử và nghiệm thu hệ thống

a) Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống.

b) Thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng.

c) Có nhân sự chịu trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống.

4.12.2.4 Kiểm soát truy cập

a) Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn (nếu hỗ trợ) khi truy cập thông tin nội bộ hoặc thực hiện quản trị từ xa đối với tài sản phần cứng và phần mềm.

b) Kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả truy cập tới các tài sản phần cứng và phần mềm mà hệ thống không cung cấp hoặc không cho phép truy cập.

c) Giới hạn các dải địa chỉ mạng hoặc thiết bị cụ thể được phép kết nối để thực hiện quản trị từ xa đối với tài sản phần cứng và phần mềm.

d) Thiết lập giới hạn thời gian chờ (timeout) để tự động đóng các phiên kết nối khi không nhận được yêu cầu từ người dùng trong một khoảng thời gian quy định.

4.12.2.5 Xây dựng và áp dụng chính sách quản lý truy cập từ xa

Có chính sách quản lý truy cập từ xa đáp ứng các yêu cầu sau:

- Sử dụng mạng riêng ảo VPN hoặc phương án tương đương và yêu cầu xác thực cho việc truy cập từ xa vào hệ thống đối với người dùng quản trị, người dùng tác nghiệp hệ thống.

- Yêu cầu người dùng xác thực để kết nối truy cập từ xa và xác thực bổ sung trước khi truy cập vào hệ thống.

- Các thiết bị được phép truy cập từ xa phải đảm bảo các yêu cầu về bảo mật: cài đặt phần mềm phòng chống mã độc, cấu hình bảo mật theo chính sách an ninh, an toàn đã ban hành của tổ chức.

- Cấu hình thiết bị (nếu hỗ trợ) chỉ cho phép hạn chế các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa.

4.13 Nhân sự vận hành, quản trị hệ thống, bảo vệ an ninh mạng

4.13.1 Khái quát

a) Có cơ chế hoạt động độc lập về chuyên môn giữa các bộ phận vận hành, quản trị, bảo vệ an ninh mạng.

b) Thiết lập và duy trì chương trình đào tạo nâng cao nhận thức an ninh mạng và kỹ năng an ninh mạng.

4.13.2 Yêu cầu cụ thể

4.13.2.1 Có bộ phận phụ trách về vận hành, quản trị hệ thống và bảo vệ an ninh mạng

a) Có nhân sự phụ trách vận hành, quản trị hệ thống và bảo vệ an ninh mạng.

b) Nhân sự phụ trách về vận hành, quản trị hệ thống và bảo vệ an ninh mạng phải có trình độ chuyên môn về an ninh mạng, công nghệ thông tin; có cam kết bảo mật thông tin trong quá trình làm việc và sau khi nghỉ việc.

4.13.2.2 Thiết lập và duy trì chương trình đào tạo tổng quan để nâng cao nhận thức an ninh mạng cho cán bộ, nhân viên

a) Có chương trình nâng cao nhận thức an ninh mạng cho toàn bộ cán bộ, nhân viên có sử dụng hệ thống thông tin.

b) Tiến hành đào tạo tối thiểu 01 lần/ năm.

c) Cán bộ chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của tổ chức.

d) Có quy trình và thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.

4.14 Quản lý nhà cung cấp sản phẩm, dịch vụ

4.14.1 Khái quát

Có quy trình để đánh giá nhà cung cấp sản phẩm, dịch vụ an ninh mạng, lưu trữ, xử lý dữ liệu nhạy cảm hoặc chịu trách nhiệm về các quy trình, nền tảng quan trọng của hệ thống.

4.14.2 Yêu cầu cụ thể

Có phương án thiết lập và duy trì bản kiểm kê các nhà cung cấp sản phẩm, dịch vụ. Tối thiểu bao gồm:

- Lập danh sách, theo dõi, cập nhật trạng thái các nhà cung cấp sản phẩm, dịch vụ.

- Thực hiện phân loại các nhà cung cấp dịch vụ trong danh sách quản lý.

- Có văn bản xác định rõ phạm vi trách nhiệm của nhà cung cấp và tổ chức.

- Xem xét và cập nhật danh sách tối thiểu 01 lần/ năm hoặc khi xảy ra thay đổi ảnh hưởng đến danh sách này.

4.15 Quản trị ứng phó sự cố an ninh mạng

4.15.1 Khái quát

Có kế hoạch, chương trình để phát triển và duy trì khả năng ứng phó sự cố bao gồm chính sách, kế hoạch, thủ tục, vai trò, đào tạo, kênh liên lạc. Chính sách, quy trình xử lý sự cố an ninh mạng bao gồm tối thiểu các nội dung:

- Phân nhóm sự cố an ninh mạng.

- Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an ninh mạng.

- Kế hoạch ứng phó sự cố an ninh mạng.

- Giám sát, phát hiện và cảnh báo sự cố an ninh mạng.

- Quy trình ứng cứu sự cố an ninh mạng thông thường.

- Quy trình ứng cứu sự cố an ninh mạng nghiêm trọng.

- Cơ chế phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an ninh mạng.

4.15.2 Yêu cầu cụ thể

4.15.2.1 Thành lập lực lượng ứng phó sự cố an ninh mạng

a) Chỉ định một người chủ chốt và ít nhất một người dự phòng để quản lý quy trình ứng phó sự cố an ninh mạng.

b) Thiết lập và duy trì đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý nhà nước về an ninh mạng, cơ quan điều hành Liên minh ứng phó, khắc phục sự cố an ninh mạng quốc gia.

c) Thiết lập và duy trì đầu mối liên lạc để báo cáo sự cố. Xác minh thông tin liên hệ của các cơ quan, tổ chức hỗ trợ điều phối ứng phó sự cố hàng năm để đảm bảo thông tin được cập nhật.

d) Phân công vị trí, vai trò và trách nhiệm chính của từng thành viên trong lực lượng tham gia ứng phó sự cố.

e) Quy định về trách nhiệm phối hợp với lực lượng ứng phó sự cố an ninh mạng của các phòng ban có liên quan.

4.15.2.2 Thiết lập và duy trì quy trình nội bộ để báo cáo sự cố an ninh mạng

a) Có quy trình nội bộ để báo cáo sự cố an ninh mạng.

b) Thực hiện phân nhóm sự cố an ninh mạng.

c) Đánh giá và cập nhật quy trình tối thiểu 01 lần/ năm hoặc khi xảy ra các thay đổi ảnh hưởng đến quy trình.

4.15.2.3 Thiết lập và duy trì quy trình ứng phó sự cố an ninh mạng

a) Có quy trình ứng phó sự cố, đảm bảo có cơ chế phối hợp với các cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ khắc phục sự cố an ninh mạng.

b) Đánh giá và cập nhật quy trình tối thiểu 01 lần/ năm hoặc khi xảy ra các thay đổi ảnh hưởng đến quy trình.

5 Yêu cầu cơ bản đối với hệ thống thông tin cấp độ 3

5.1 Quản lý rủi ro an ninh mạng

5.1.1 Khái quát

Thực hiện xác định, đánh giá, xử lý rủi ro an ninh mạng và lên kế hoạch ứng phó khi rủi ro xảy ra.

5.1.2 Yêu cầu cụ thể

5.1.2.1 Thiết lập và duy trì quy định, quy trình quản lý rủi ro an ninh mạng

a) Có quy định, quy trình quản lý rủi ro an ninh mạng. Trong đó, yêu cầu thực hiện quản lý rủi ro an ninh mạng bao gồm tối thiểu các bước: xác định, phân tích, đánh giá và xử lý rủi ro an ninh mạng.

b) Đánh giá và cập nhật quy định, quy trình quản lý rủi ro an ninh mạng và các tài liệu liên quan tối thiểu 01 lần/ năm hoặc khi có thay đổi xảy ra trong tổ chức ảnh hưởng đến các văn bản đã ban hành có liên quan.

5.1.2.2 Xác định rủi ro an ninh mạng

a) Thực hiện xác định rủi ro an ninh mạng trong tổ chức (có thể dựa trên việc quản lý tài sản, quản lý lỗ hổng, quản lý hạ tầng mạng, quản lý nhận thức an ninh mạng, quản lý tài khoản và quyền truy cập…).

b) Xác định rủi ro an ninh mạng đến từ các bên thứ ba, nhà cung cấp.

c) Thực hiện xác định rủi ro an ninh mạng định kỳ tối thiểu 01 lần/ năm hoặc khi có thay đổi liên quan đến hệ thống thông tin (thay đổi hệ thống, lỗ hổng bảo mật mới, các sự kiện an ninh mạng...).

5.1.2.3 Đánh giá rủi ro an ninh mạng

a) Thực hiện phân tích, đánh giá rủi ro an ninh mạng để xác định mức độ ảnh hưởng, tác động của rủi ro đến tổ chức, từ đó đưa ra quyết định chấp nhận hoặc thực hiện các biện pháp giảm thiểu rủi ro.

b) Thực hiện phân tích và đánh giá rủi ro an ninh mạng ngay sau khi xác định rủi ro; phân tích, đánh giá lại khi có sự thay đổi về hệ thống, các sự kiện an ninh mạng hoặc những thay đổi trong tổ chức liên quan đến rủi ro đã xác định.

5.1.2.4 Xử lý rủi ro an ninh mạng

a) Thực hiện các biện pháp xử lý rủi ro an ninh mạng và xây dựng phương án ứng phó khi rủi ro còn lại (sau khi đã xử lý) xảy ra.

b) Định kỳ tối thiểu 01 lần/ năm đánh giá và cải thiện hiệu quả của các biện pháp kiểm soát được sử dụng để giảm thiểu rủi ro.

5.1.2.5 Giám sát rủi ro an ninh mạng

Giám sát và cập nhật những thay đổi liên quan đến rủi ro đã được xác định, tối thiểu bao gồm: khả năng xảy ra, mức độ ảnh hưởng, mức độ rủi ro, tài sản bị ảnh hưởng, biện pháp kiểm soát đã áp dụng.

5.1.2.6 Truyền thông rủi ro an ninh mạng

Thông báo kịp thời cho các bên liên quan về thay đổi quan trọng liên quan đến rủi ro.

5.2 Quản lý tài sản phần cứng

5.2.1 Khái quát

a) Lập danh sách, theo dõi, cập nhật trạng thái của tất cả tài sản phần cứng thuộc hệ thống thông tin và các tài sản không thuộc quyền kiểm soát của tổ chức nhưng có kết nối vào hệ thống thông tin; xác định danh sách tài sản cần được giám sát, bảo vệ.

b) Xác định các tài sản vô chủ, tài sản trái phép để loại bỏ hoặc đưa ra phương án quản lý.

c) Thực hiện kiểm kê, rà soát và cập nhật danh sách cho tất cả tài sản thuộc hệ thống thông tin định kỳ tối thiểu 01 lần/ năm.

5.2.2 Yêu cầu cụ thể

5.2.2.1 Thiết lập và duy trì hệ thống quản lý danh mục tài sản phần cứng

a) Lập danh sách, theo dõi, cập nhật trạng thái của tất cả tài sản phần cứng có khả năng lưu trữ hoặc xử lý dữ liệu, bao gồm: thiết bị của người dùng cuối, thiết bị di động, thiết bị lưu trữ ngoài, thiết bị văn phòng, thiết bị mạng, thiết bị OT/IoT và máy chủ trong môi trường vật lý, ảo hóa, truy cập từ xa và điện toán đám mây.

b) Danh sách tài sản phần cứng phải bao gồm tối thiểu các thông tin cơ bản sau: tên tài sản, địa chỉ mạng IP (đối với thiết bị đặt địa chỉ IP tĩnh), địa chỉ phần cứng MAC/ mã nhận diện serial, thời gian ngừng hỗ trợ kỹ thuật của hãng (nếu có), vị trí lắp đặt địa lý, vị trí lắp đặt trong hệ thống mạng, mục đích sử dụng, tình trạng sử dụng. Tài sản vật lý phải được giao, gán trách nhiệm cho cá nhân hoặc bộ phận quản lý, sử dụng.

c) Các thiết bị di động do tổ chức quản lý hoặc được tổ chức cho phép kết nối vào hệ thống thông tin phải được đăng ký để kiểm soát. Quy định trách nhiệm của cá nhân trong tổ chức khi sử dụng thiết bị di động để phục vụ công việc.

5.2.2.2 Xử lý các tài sản phần cứng chưa được quản lý

a) Có quy trình phát hiện và xử lý các tài sản phần cứng không có trong danh sách quản lý, đang kết nối trái phép vào hệ thống thông tin định kỳ tối thiểu 01 lần/ 06 tháng.

b) Có thể lựa chọn loại bỏ, từ chối kết nối hoặc cách ly tài sản trái phép.

5.2.2.3 Xử lý các tài sản phần cứng khi chuyển giao

Có phương án xóa sạch thông tin, dữ liệu trên tài sản phần cứng khi chuyển giao hoặc thay đổi mục đích sử dụng.

5.2.2.4 Sử dụng DHCP Logging để cập nhật bản kiểm kê tài sản công nghệ thông tin

a) Sử dụng tính năng ghi nhật ký DHCP trên tất cả các máy chủ DHCP hoặc công cụ quản lý địa chỉ mạng IP (nếu có).

b) Tiến hành rà soát nhật ký để cập nhật danh sách tài sản công nghệ thông tin định kỳ tối thiểu 01 lần/ 06 tháng.

5.3 Quản lý tài sản phần mềm

5.3.1 Khái quát

a) Lập danh sách, theo dõi, cập nhật trạng thái của tất cả tài sản phần mềm thuộc hệ thống thông tin của cơ quan, tổ chức, đảm bảo chỉ những phần mềm đã phê duyệt mới được phép cài đặt và sử dụng.

b) Thực hiện kiểm kê, rà soát và cập nhật danh sách cho tất cả tài sản phần mềm định kỳ tối thiểu 01 lần/ năm.

5.3.2 Yêu cầu cụ thể

5.3.2.1 Thiết lập và duy trì hệ thống quản lý danh mục tài sản phần mềm

a) Lập danh sách, theo dõi, cập nhật trạng thái của tất cả tài sản phần mềm hiện đang được cài đặt trên các tài sản phần cứng thuộc hệ thống thông tin của cơ quan, tổ chức.

b) Danh sách tài sản phần mềm phải bao gồm tối thiểu các thông tin cơ bản sau: tên tài sản, mục đích sử dụng, thời gian ngừng hỗ trợ kỹ thuật (nếu có), phạm vi sử dụng, chủ thể quản lý, thông tin về bản quyền, phiên bản, hệ thống thông tin thành phần (nếu có). Tài sản phần mềm phải được gắn trách nhiệm cho cá nhân hoặc bộ phận quản lý, sử dụng.

5.3.2.2 Thiết lập và duy trì danh sách các tài sản phần mềm được phép sử dụng

a) Lập danh sách, theo dõi, cập nhật danh sách các phần mềm được phép sử dụng trong hệ thống thông tin của cơ quan, tổ chức.

b) Danh sách phần mềm được phép sử dụng phải bao gồm cả các phần mềm được cung cấp bởi nhà cung cấp dịch vụ, các môi trường thực thi cần cài đặt cho ứng dụng.

c) Có quy định kiểm soát việc cài đặt và sử dụng các phần mềm đã được cấp phép, đảm bảo giới hạn đặc quyền tối thiểu các quyền quản trị trên các tài sản CNTT; ngăn chặn các tác vụ thực thi, vô hiệu hóa, cài đặt và gỡ bỏ phần mềm, thư viện, đoạn mã lệnh trái phép trên hệ thống; có phương án kỹ thuật để theo dõi hoạt động cài đặt chương trình phần mềm trên các tài sản CNTT.

d) Định kỳ đánh giá và cập nhật danh sách phần mềm được phép sử dụng tối thiểu 01 lần/ năm hoặc khi xảy ra các thay đổi trong tổ chức ảnh hưởng đến danh sách.

5.3.2.3 Xử lý các tài sản phần mềm trái phép

a) Có quy trình phát hiện và xử lý các phần mềm trái phép định kỳ tối thiểu 01 lần/ năm.

b) Những phần mềm trái phép nhưng vẫn cần thiết đối với hoạt động của cơ quan, tổ chức phải được đưa vào danh sách ngoại lệ để quản lý. Danh sách ngoại lệ này phải thể hiện chi tiết các biện pháp kiểm soát giảm thiểu nguy cơ an ninh mạng ảnh hưởng đến hệ thống.

c) Những phần mềm trái phép không nằm trong danh sách ngoại lệ phải có kế hoạch để xóa/ gỡ bỏ hoàn toàn khỏi các tài sản phần cứng của cơ quan, tổ chức trong thời gian sớm nhất.

5.4 Quản lý tài sản thông tin

5.4.1 Khái quát

Thực hiện quản lý tài sản thông tin và triển khai các biện pháp kiểm soát để phát hiện, phân loại, xử lý, lưu trữ và loại bỏ tài sản thông tin một cách an toàn.

5.4.2 Yêu cầu cụ thể

5.4.2.1 Thiết lập và duy trì quy định quản lý tài sản thông tin

a) Có quy định quản lý tài sản thông tin. Trong quy định, xác định danh sách tài sản thông tin, mức độ nhạy cảm, chủ sở hữu, các bước xử lý, thời gian lưu trữ và các yêu cầu khi tiêu hủy/xóa bỏ dựa trên các tiêu chuẩn về mức độ bảo mật của tài sản thông tin.

b) Mức độ nhạy cảm của tài sản thông tin có thể được quy định như sau:

- Mức 1: Công khai. Tài sản thông tin công khai không yêu cầu về bảo mật.

- Mức 2: Nội bộ. Tài sản thông tin nội bộ yêu cầu chỉ những người trong tổ chức mới có quyền truy cập.

- Mức 3: Hạn chế truy cập. Tài sản thông tin bị hạn chế yêu cầu quyền truy cập, chỉ những người dùng được cấp quyền mới có thể truy cập vào dữ liệu. Việc tiết lộ tài sản thông tin bị hạn chế truy cập có khả năng ảnh hưởng đến hoạt động của các cơ quan, tổ chức.

- Mức 4: Bí mật nhà nước. Thông tin có nội dung quan trọng, do cơ quan, tổ chức có thẩm quyền xác định; chưa công khai, nếu bị lộ, bị mất có thể gây nguy hại đến lợi ích quốc gia, dân tộc.

c) Có quy trình yêu cầu truy cập, thêm mới, sửa, xóa dữ liệu để kiểm soát truy cập dữ liệu.

d) Kiểm tra cấp độ phân quyền dữ liệu định kỳ tối thiểu 01 lần/ 06 tháng.

e) Đánh giá và cập nhật quy trình quản lý tài sản thông tin định kỳ tối thiểu 01 lần/ năm hoặc khi xảy ra các thay đổi trong tổ chức ảnh hưởng đến quy trình.

5.4.2.2 Thiết lập và duy trì bản danh sách tài sản thông tin

a) Lập danh sách các tài sản thông tin dựa trên quy trình quản lý tài sản thông tin.

b) Đánh giá và cập nhật danh sách tài sản thông tin tối thiểu 01 lần/ năm hoặc khi xảy ra thay đổi trong tổ chức ảnh hưởng đến danh sách.

5.4.2.3 Xây dựng danh sách kiểm soát truy cập tài sản thông tin

Xây dựng danh sách quyền truy cập của các tài khoản, người dùng đối với từng loại tài sản thông tin.

5.4.2.4 Mã hóa dữ liệu quan trọng

a) Mã hóa hoặc sử dụng biện pháp kiểm soát rủi ro tương đương để bảo mật thông tin xác thực, dữ liệu có độ nhạy cảm cao, dữ liệu quan trọng được lưu trữ trong các tài sản phần cứng và phần mềm của tổ chức.

b) Mã hóa hoặc sử dụng biện pháp kiểm soát rủi ro tương đương để bảo vệ thông tin xác thực, dữ liệu quan trọng trong quá trình truyền gửi.

c) Thực hiện bảo vệ và quản lý vòng đời mã khóa sử dụng để mã hóa dữ liệu.

5.4.2.5 Nguyên vẹn dữ liệu

Có phương án quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn.

5.4.2.6 Tài liệu hóa luồng dữ liệu

a) Có tài liệu mô tả các luồng dữ liệu quan trọng trong hệ thống thông tin.

b) Xây dựng và tuân thủ quy định quản lý phiên bản tài liệu tại tổ chức.

c) Đánh giá và cập nhật định kỳ tối thiểu 01 lần/ năm hoặc khi có thay đổi trong tổ chức ảnh hưởng đến tài liệu.

5.4.2.7 Tách biệt quá trình xử lý và lưu trữ dữ liệu quan trọng

a) Có quy định về việc xử lý dữ liệu quan trọng.

b) Tách biệt tài sản/môi trường xử lý, lưu trữ dữ liệu có độ nhạy cảm cao, dữ liệu quan trọng với dữ liệu có độ nhạy cảm thấp (về mặt logic hoặc vật lý) hoặc có phương án kiểm soát rủi ro tương đương đảm bảo an ninh dữ liệu. Không sử dụng các tài sản/ môi trường dành cho dữ liệu nhạy cảm thấp để lưu trữ và xử lý dữ liệu có mức độ nhạy cảm cao.

5.4.2.8 Sử dụng chữ ký số khi trao đổi thông tin số, dữ liệu số quan trọng

Sử dụng chữ ký số khi trao đổi dữ liệu có độ nhạy cảm cao, dữ liệu quan trọng.

5.5 Cấu hình an toàn cho phần cứng và phần mềm

5.5.1 Khái quát

Thiết lập và duy trì cấu hình an toàn cho phần cứng (như thiết bị người dùng cuối bao gồm máy tính, thiết bị di động và cầm tay, thiết bị mạng, thiết bị OT/IoT, máy chủ...) và phần mềm (như hệ điều hành, ứng dụng…).

5.5.2 Yêu cầu cụ thể

5.5.2.1 Thiết lập và duy trì quy định, quy trình cấu hình an toàn cho tài sản phần cứng và phần mềm

a) Có quy định, quy trình cấu hình an toàn cho các tài sản phần cứng và phần mềm của cơ quan, tổ chức.

b) Có các tài liệu cấu hình tiêu chuẩn, tài liệu cấu hình tăng cường bảo mật cho các tài sản phần cứng và phần mềm của cơ quan, tổ chức. Đảm bảo sử dụng giao thức kết nối an toàn, thiết lập tường lửa cho máy chủ/ máy trạm và có phương án chống đăng nhập tự động đối với các tài sản xử lý và lưu trữ dữ liệu quan trọng.

c) Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ mà phần cứng, phần mềm không sử dụng.

d) Cấu hình tối ưu và tăng cường bảo mật cho tài sản phần cứng trước khi đưa vào vận hành, khai thác.

e) Đánh giá và cập nhật quy định, quy trình quản lý cấu hình an toàn và các tài liệu liên quan tối thiểu 01 lần/ năm hoặc khi có thay đổi xảy ra trong tổ chức ảnh hưởng đến tài liệu.

5.5.2.2 Cấu hình tự động khóa phiên làm việc trên các tài sản phần cứng và phần mềm

a) Dựa trên yêu cầu sử dụng, kết quả đánh giá rủi ro, thực hiện cấu hình tự động khóa phiên làm việc trên các tài sản phần cứng và phần mềm. Có thể thực hiện cấu hình như sau:

- Tự động khóa phiên làm việc trên các tài sản sau một khoảng thời gian không sử dụng:

+ Đối với máy tính người dùng: không quá 15 phút.

+ Đối với các phiên quản trị phần mềm, máy chủ, thiết bị mạng, thiết bị IoT: không quá 05 phút.

+ Đối với thiết bị di động: không quá 05 phút.

+ Đối với các phần mềm nghiệp vụ xử lý dữ liệu quan trọng: không quá 15 phút.

- Tự động khóa thiết bị di động sau một số lần đăng nhập thất bại:

+ Đối với máy tính xách tay: tối đa 10 lần.

+ Đối với điện thoại: tối đa 10 lần.

+ Đối với các phần mềm nghiệp vụ lưu trữ và xử lý dữ liệu quan trọng: tối đa 05 lần.

+ Giới hạn thời gian mở khóa thiết bị sau khi bị khóa: tối thiểu 12 giờ, tối đa 30 ngày.

b) Có cơ chế mở khóa khẩn cấp dành cho quản trị viên/tài khoản đặc quyền.

5.6 Quản lý tài khoản và quyền truy cập tài khoản của người dùng

5.6.1 Khái quát

a) Có quy trình, công cụ để phân quyền và quản lý quyền truy cập của tài khoản người dùng bao gồm: tài khoản quản trị, tài khoản tác nghiệp (tài khoản của người dùng cuối tác nghiệp), tài khoản kỹ thuật (tài khoản dùng để kết nối giữa các hệ thống kỹ thuật), tài khoản dịch vụ (tài khoản cấp cho người thụ hưởng dịch vụ) trên các tài sản phần cứng và phần mềm.

b) Có quy trình tạo, gán, quản lý, thu hồi đặc quyền và quyền truy cập đối với các tài khoản người dùng cho tài sản phần cứng và phần mềm. Quyền truy cập của tài khoản quản trị, tài khoản tác nghiệp, tài khoản kỹ thuật, tài khoản dịch vụ phải nhất quán dựa trên vai trò và các yêu cầu cụ thể, đảm bảo người dùng chỉ có quyền truy cập vào dữ liệu, tài sản phù hợp.

c) Ghi nhật ký và giám sát tài khoản người dùng.

5.6.2 Yêu cầu cụ thể

5.6.2.1 Thiết lập và duy trì hệ thống quản lý tài khoản

a) Lập danh sách, theo dõi và cập nhật tất cả các tài khoản trên các tài sản phần cứng và phần mềm của tổ chức.

b) Danh sách tài khoản phải bao gồm tối thiểu các loại tài khoản sau: tài khoản quản trị, tài khoản tác nghiệp và tài khoản kỹ thuật.

c) Danh sách tài khoản phải bao gồm các thông tin tối thiểu: loại tài khoản, tên tài khoản, trạng thái tài khoản, tên tài sản/ hệ thống thông tin tương ứng, tên người quản lý, phòng ban, ngày kích hoạt tài khoản, ngày vô hiệu hóa tài khoản (nếu có). Đảm bảo tất cả tài khoản đang hoạt động là hợp lệ.

d) Danh sách tài khoản phải được rà soát định kỳ tối thiểu 01 lần/ 06 tháng.

5.6.2.2 Xây dựng và tuân thủ quy định sử dụng mật khẩu

a) Thiết lập cấu hình mật khẩu trên tài sản phần cứng, phần mềm để đảm bảo an toàn mật khẩu người sử dụng, bao gồm các yêu cầu sau:

- Yêu cầu thay đổi mật khẩu mặc định.

- Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự.

- Thiết lập thời gian yêu cầu thay đổi mật khẩu.

- Thiết lập thời gian mật khẩu hợp lệ.

b) Dựa trên yêu cầu sử dụng, kết quả đánh giá rủi ro, triển khai quy định sử dụng mật khẩu an toàn trong tổ chức. Có thể thực hiện cấu hình như sau:

- Sử dụng mật khẩu duy nhất cho mỗi tài sản hoặc sử dụng giải pháp xác thực và quản lý tập trung.

- Yêu cầu thay đổi mật khẩu trong lần đăng nhập đầu tiên.

- Đối với các hệ thống sử dụng xác thực MFA, quy định mật khẩu có tối thiểu 08 ký tự.

- Đối với các hệ thống không sử dụng xác thực MFA, quy định mật khẩu có tối thiểu 14 ký tự, bao gồm ký tự viết thường, ký tự viết hoa, ký tự đặc biệt, chữ số.

- Đối với tài khoản quản trị cần triển khai xác thực MFA, thay đổi mật khẩu định kỳ tối thiểu 01 lần/02 tháng và mật khẩu mới không được trùng với 10 mật khẩu trước đó.

5.6.2.3 Xây dựng và tuân thủ quy định quản lý tài khoản

Có quy định quản lý tài khoản trong tổ chức đáp ứng các yêu cầu sau:

- Quản lý tài khoản tập trung.

- Thay đổi hoặc vô hiệu hóa tài khoản mặc định trên phần mềm, thiết bị (như tài khoản root, administrator, tài khoản cấu hình sẵn của nhà cung cấp dịch vụ).

- Quản lý tách biệt giữa các loại tài khoản: tài khoản quản trị, tài khoản tác nghiệp, tài khoản kỹ thuật, tài khoản dịch vụ.

- Mỗi tài khoản truy cập hệ thống phải được gán cho một người sử dụng duy nhất; trường hợp chia sẻ tài khoản dùng chung phải được phê duyệt bởi cấp có thẩm quyền và làm rõ trách nhiệm cá nhân tại mỗi thời điểm sử dụng.

- Xóa hoặc vô hiệu hóa các tài khoản không hoạt động sau 45 ngày hoặc ngay khi có thay đổi về nhân sự quản lý, sử dụng, khai thác tài khoản.

- Định kỳ rà soát và cập nhật quy định quản lý tài khoản và các tài liệu liên quan tối thiểu 01 lần/ năm hoặc khi có thay đổi trong tổ chức có ảnh hưởng đến quy định.

5.6.2.4 Xây dựng và tuân thủ quy định quản lý truy cập

Có quy định về quản lý truy cập đáp ứng các yêu cầu sau:

- Nguyên tắc cấp quyền tối thiểu và phân tách nhiệm vụ đối với mọi loại tài khoản.

- Tài liệu hóa các quyền truy cập cần thiết tương ứng với các chức danh, bộ phận trong cơ quan, tổ chức.

- Yêu cầu xác thực MFA đối với truy cập của người dùng từ bên ngoài tổ chức, từ đối tác/ bên thứ ba, từ Internet và truy cập vào tài khoản có quyền quản trị hệ thống.

- Định kỳ rà soát và cập nhật quy định quản lý truy cập và các tài liệu liên quan tối thiểu 01 lần/ năm hoặc khi có thay đổi trong tổ chức có ảnh hưởng đến quy định.

5.7 Quản lý lỗ hổng bảo mật

5.7.1 Khái quát

a) Xây dựng, phát triển kế hoạch đánh giá và theo dõi các lỗ hổng bảo mật thường xuyên để khắc phục và giảm thiểu nguy cơ bị tấn công mạng.

b) Theo dõi, cập nhật thông tin về các mối đe dọa, lỗ hổng bảo mật mới từ nhiều nguồn.

5.7.2 Yêu cầu cụ thể

5.7.2.1 Có quy trình quản lý lỗ hổng bảo mật

a) Có quy trình quản lý lỗ hổng bảo mật cho các tài sản công nghệ thông tin của tổ chức. Các nội dung tối thiểu bao gồm:

- Phát hiện lỗ hổng bảo mật: Xây dựng và triển khai giải pháp để rà quét lỗ hổng bảo mật cho các tài sản phần cứng và phần mềm của cơ quan, tổ chức.

- Đánh giá mức độ nghiêm trọng của lỗ hổng: Triển khai đánh giá mức độ nghiêm trọng của lỗ hổng, từ đó xác định mức độ ưu tiên của việc khắc phục lỗ hổng.

- Chia sẻ thông tin lỗ hổng: Có cơ chế để chia sẻ thông tin, tiếp nhận và phản hồi báo cáo lỗ hổng bảo mật từ bên liên quan hoặc các nguồn công khai khác.

- Triển khai các biện pháp khắc phục: Có phương án, biện pháp kiểm soát rủi ro, kế hoạch khắc phục cho các lỗ hổng đã phát hiện theo thứ tự ưu tiên và đánh giá lại hệ thống để đảm bảo lỗ hổng đã được khắc phục hoàn toàn.

b) Rà soát, cập nhật quy trình và rà quét lỗ hổng bảo mật tối thiểu 01 lần/ 06 tháng hoặc khi xảy ra thay đổi trong tổ chức ảnh hưởng đến quy trình này.

5.7.2.2 Có quy trình quản lý bản vá

Có quy trình quản lý bản vá. Các nội dung tối thiểu bao gồm:

- Xây dựng và triển khai máy chủ quản lý bản vá tập trung cho toàn bộ tài sản phần cứng và phần mềm thuộc hệ thống thông tin.

- Đánh giá tác động, tiến hành kiểm thử và xây dựng phương án phục hồi trước khi triển khai bản vá trên các hệ thống thông tin có xử lý hoặc lưu trữ dữ liệu quan trọng.

- Thực hiện kiểm tra và cập nhật bản vá hệ điều hành, ứng dụng cho toàn bộ máy tính, thiết bị di động cấp cho người dùng tối thiểu 01 lần/ tháng (nếu có).

- Giám sát và duy trì hệ thống để đảm bảo phát hiện kịp thời các lỗ hổng mới xuất hiện và cập nhật bản vá.

5.8 Quản lý nhật ký an ninh mạng

5.8.1 Khái quát

Thực hiện thu thập, phân tích, giám sát và lưu trữ nhật ký an ninh mạng để phát hiện sớm và ứng phó sự cố tấn công mạng.

5.8.2 Yêu cầu cụ thể

5.8.2.1 Thiết lập quy trình quản lý nhật ký an ninh mạng

a) Có quy định quản lý nhật ký an ninh mạng, trong đó bao gồm:

- Quy định về cách thức ghi nhật ký.

- Quy định về việc thu thập, kiểm tra, lưu trữ nhật ký.

- Quy định các loại nhật ký được thu thập. Thu thập tối thiểu các loại nhật ký sau: nhật ký truy cập hệ thống, nhật ký tiến trình hoạt động, nhật ký ứng dụng, nhật ký cảnh báo của các thiết bị bảo mật.

- Nhật ký truy cập hệ thống tối thiểu bao gồm: địa chỉ nguồn (IP/ tên máy, tên miền, MAC), địa chỉ đích (IP/ tên máy, tên miền, MAC), tài khoản đích (tên người dùng/ mã định danh), thời điểm xảy ra, thông tin hành vi.

- Nhật ký tiến trình hoạt động tối thiểu bao gồm: thông tin thiết bị (IP/ tên thiết bị, tên miền, MAC), thông tin tiến trình (tên, mã định danh, tiến trình cha, lệnh khởi tạo), tài khoản đích (tên người dùng/ mã định danh), thời điểm xảy ra.

- Nhật ký cảnh báo tối thiểu bao gồm: tên cảnh báo, thiết bị, mức độ, địa chỉ nguồn, loại cảnh báo, thời điểm xảy ra.

- Sử dụng máy chủ thời gian để đồng bộ thời gian giữa các thiết bị mạng, thiết bị đầu cuối và các thành phần khác trong hệ thống tham gia giám sát.

- Sử dụng giải pháp SIEM hoặc có sản phẩm, phương án tương đương phục vụ quản lý và phân tích sự kiện an ninh mạng tập trung.

- Lưu trữ và quản lý tập trung nhật ký hệ thống thu thập được từ các thiết bị hệ thống.

- Đảm bảo duy trì không gian lưu trữ nhật ký tối thiểu 03 tháng. Triển khai hệ thống theo dõi tránh tình trạng đầy không gian lưu trữ, dẫn tới thất thoát dữ liệu.

- Định kỳ thực hiện rà soát nhật ký an ninh mạng tối thiểu 01 lần/ 06 tháng.

b) Kiểm tra và cập nhật tối thiểu 01 lần/ năm hoặc khi có thay đổi ảnh hưởng đến quy trình này.

5.9 Bảo vệ cho trình duyệt web, dịch vụ thư điện tử

5.9.1 Khái quát

Tăng cường bảo vệ và phát hiện các mối đe dọa từ dịch vụ thư điện tử, trình duyệt web thuộc hệ thống thông tin.

5.9.2 Yêu cầu cụ thể

5.9.2.1 Quản lý trình duyệt web và dịch vụ thư điện tử

a) Có danh sách các trình duyệt web và dịch vụ thư điện tử được phép sử dụng trong cơ quan, tổ chức.

b) Đảm bảo danh sách các trình duyệt web và dịch vụ thư điện tử trên đang trong thời gian hỗ trợ của nhà cung cấp.

c) Sử dụng giải pháp đảm bảo an ninh mạng cho hệ thống thư điện tử hoặc có phương án tương đương.

d) Đảm bảo phiên bản trình duyệt web và dịch vụ thư điện tử được rà soát, cập nhật bản vá lỗ hổng bảo mật thường xuyên hoặc có biện pháp kiểm soát rủi ro tương đương.

5.9.2.2 Sử dụng dịch vụ lọc tên miền

Triển khai sử dụng dịch vụ lọc tên miền trong cơ quan, tổ chức để ngăn chặn các tên miền giả mạo và độc hại.

5.10 Phòng chống phần mềm độc hại

5.10.1 Khái quát

a) Có quy định để quản lý, phòng chống, khắc phục việc cài đặt, lây lan, thực thi các phần mềm và đoạn mã độc hại trong cơ quan, tổ chức.

b) Triển khai giải pháp phòng chống mã độc cho tất cả tài sản và các điểm kết nối giữa những hệ thống thông tin (bao gồm cả kết nối nội bộ và kết nối ra bên ngoài tổ chức). Giải pháp phòng chống mã độc phải phù hợp và tương thích với hệ thống thông tin của cơ quan, tổ chức, đồng thời có khả năng tự động dò quét, ngăn chặn khi phát hiện mã độc, cập nhật kịp thời các mẫu nhận diện mã độc mới và tích hợp với quy trình quản lý lỗ hổng, ứng phó sự cố.

5.10.2 Yêu cầu cụ thể

5.10.2.1 Triển khai và duy trì phần mềm, giải pháp phòng chống mã độc

a) Triển khai và duy trì phần mềm, giải pháp phòng, chống mã độc hoặc phương án tương đương trên máy chủ, máy tính người dùng.

b) Sử dụng giải pháp phòng, chống mã độc, bao gồm ít nhất các tính năng cơ bản như bảo vệ thời gian thực, tự động cập nhật các mẫu nhận diện mã độc mới.

5.10.2.2 Thực hiện phòng, chống mã độc đối với các thiết bị lưu trữ ngoài

Triển khai rà quét mã độc và vô hiệu hóa tính năng tự động thực thi (autorun, autoplay…) đối với các phương tiện lưu trữ di động như ổ cứng, thẻ nhớ, USB…

5.10.2.3 Kích hoạt tính năng phòng chống khai thác lỗ hổng

Kích hoạt tính năng phòng chống khai thác lỗ hổng trên các tài sản phần cứng và phần mềm (nếu có).

5.10.2.4 Xây dựng và triển khai giải pháp phòng chống mã độc theo hành vi

a) Triển khai giải pháp EDR hoặc phương án tương đương có khả năng phát hiện mã độc, mối nguy dựa trên hành vi trên máy chủ, máy tính người dùng.

b) Kết nối về SIEM để thực hiện giám sát theo thời gian thực và đưa ra cảnh báo.

5.11 Sao lưu và khôi phục dữ liệu

5.11.1 Khái quát

Triển khai và duy trì phương án sao lưu, khôi phục dữ liệu, đảm bảo khôi phục các tài sản về trạng thái tin cậy trước khi có sự cố.

5.11.2 Yêu cầu cụ thể

5.11.2.1 Xây dựng và tuân thủ quy định sao lưu, khôi phục dữ liệu

a) Có quy định sao lưu và khôi phục dữ liệu. Các nội dung tối thiểu bao gồm:

- Định nghĩa các loại dữ liệu cần được sao lưu và khôi phục cơ bản sau: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu, dữ liệu, thông tin nghiệp vụ.

- Xác định tần suất sao lưu và khôi phục tương ứng với từng loại dữ liệu đã định nghĩa.

- Xác định phương pháp sao lưu và khôi phục tương ứng với từng loại dữ liệu đã định nghĩa.

- Quản lý vùng lưu trữ dữ liệu sao lưu, đảm bảo tính toàn vẹn của dữ liệu và khôi phục dữ liệu một cách nhanh, hiệu quả.

- Định kỳ thực hiện khôi phục dữ liệu đã sao lưu dựa trên mức độ nhạy cảm và tầm quan trọng của dữ liệu nhằm kiểm tra khả năng khôi phục của bản sao lưu.

b) Sử dụng giải pháp quản lý lưu trữ tập trung hoặc có phương án sao lưu dự phòng tập trung đảm bảo tính sẵn sàng, cho phép khôi phục dữ liệu khi một thành phần trong hệ thống xảy ra sự cố.

c) Rà soát và cập nhật quy định tối thiểu 01 lần/ năm hoặc khi xảy ra thay đổi trong tổ chức ảnh hưởng đến quy định.

5.11.2.2 Thực hiện sao lưu dữ liệu tự động

a) Xác định danh sách dữ liệu cần sao lưu và phân loại tần suất sao lưu theo thời gian (ngày/tuần/tháng/năm…) đối với từng loại dữ liệu.

b) Triển khai các giải pháp hoặc có biện pháp tương đương đảm bảo sao lưu dữ liệu tự động.

5.11.2.3 Bảo vệ bản sao lưu dữ liệu

a) Áp dụng quy tắc sao lưu 3-2-1 hoặc có biện pháp tương đương bảo vệ bản sao lưu dữ liệu đảm bảo tính toàn vẹn, tính sẵn sàng và khả năng khôi phục của dữ liệu.

b) Thực hiện mã hóa đối với những dữ liệu quan trọng.

5.11.2.4 Thiết lập và duy trì hạ tầng lưu trữ tách biệt cho bản sao lưu dữ liệu

Các bản sao lưu dữ liệu cần phải được định danh, quản lý phiên bản và lưu trữ ở những hạ tầng tách biệt với môi trường vận hành.

5.12 Quản lý hạ tầng mạng

5.12.1 Khái quát

Có phương án thiết lập, thực thi và quản lý thiết bị mạng để phòng ngừa tin tặc khai thác lỗ hổng dịch vụ mạng và các điểm truy cập dễ bị tấn công.

5.12.2 Yêu cầu cụ thể

5.12.2.1 Thiết lập, duy trì các sơ đồ kiến trúc hệ thống mạng và kiến trúc mạng an toàn

a) Thiết lập và duy trì sơ đồ kiến trúc mạng và các hồ sơ khác về hệ thống mạng.

b) Triển khai và duy trì một kiến trúc hệ thống mạng an toàn, đảm bảo thực hiện tối thiểu 03 nguyên tắc: phân vùng mạng, đặc quyền ít nhất và tính sẵn sàng.

c) Tài liệu hóa sơ đồ kiến trúc hệ thống mạng tối thiểu bao gồm:

- Tổng quan kiến trúc hệ thống mạng.

- Sơ đồ cấp chi tiết của hệ thống mạng.

- Ghi chú các tài liệu đặc tả kỹ thuật, tài liệu thống kê,...

- Tài liệu mô tả phương án đảm bảo an ninh mạng.

d) Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống.

e) Xem xét và cập nhật sơ đồ mạng 01 lần/ năm hoặc mỗi khi có thay đổi ảnh hưởng đến sơ đồ hệ thống.

5.12.2.2 Quản lý an toàn cơ sở hạ tầng mạng

a) Thực hiện quản lý an toàn cơ sở hạ tầng mạng, đảm bảo tối thiểu:

- Có phương án cân bằng tải và dự phòng nóng cho các thiết bị mạng chính.

- Có phương án phòng, chống thất thoát dữ liệu.

- Có phương án bảo đảm an toàn cho mạng không dây (nếu có).

- Có phương án dự phòng kết nối mạng cho các máy chủ cung cấp dịch vụ.

- Sử dụng giải pháp tường lửa có tích hợp chức năng phòng, chống xâm nhập hoặc có phương án tương đương phục vụ kiểm soát truy cập, phòng, chống xâm nhập giữa các vùng mạng.

- Sử dụng giải pháp tường lửa tích hợp chức năng phòng, chống mã độc trên môi trường mạng hoặc có phương án tương đương.

- Sử dụng giải pháp DBF hoặc có phương án tương đương đối với hệ thống cơ sở dữ liệu tập trung.

- Sử dụng giải pháp quản lý truy cập lớp mạng hoặc có phương án tương đương kiểm soát truy cập lớp mạng, kiểm soát truy cập thiết bị đầu cuối, máy tính người dùng kết nối vào mạng.

- Có phương án giám sát hệ thống thông tin tập trung.

- Sử dụng giải pháp WAF hoặc có phương án tương đương phục vụ phòng chống tấn công ứng dụng web (nếu có).

- Sử dụng dịch vụ của doanh nghiệp hoặc sản phẩm phòng, chống tấn công từ chối dịch vụ hoặc có phương án tương đương phòng, chống tấn công từ chối dịch vụ.

- Định kỳ cập nhật cơ sở dữ liệu phát hiện tấn công mạng cho các giải pháp đảm bảo an ninh mạng trong hệ thống thông tin.

- Thực hiện quản lý thay đổi.

- Kiểm tra hiệu năng (RAM, CPU...), đảm bảo hoạt động bình thường của hệ thống.

b) Chia tách thành các vùng mạng khác nhau theo đối tượng sử dụng, mục đích sử dụng, tối thiểu:

- Vùng mạng nội bộ.

- Vùng mạng biên.

- Vùng mạng máy chủ nội bộ.

- Vùng mạng trung gian (DMZ) để cung cấp dịch vụ.

- Vùng mạng máy chủ cơ sở dữ liệu.

- Vùng mạng riêng để cung cấp dịch vụ mạng không dây (nếu có).

- Vùng quản trị.

5.12.2.3 Kiểm thử và nghiệm thu hệ thống

a) Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống.

b) Thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng.

c) Có bộ phận chịu trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống.

d) Có đơn vị độc lập (bên thứ ba) hoặc bộ phận độc lập thuộc cơ quan, tổ chức thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống.

e) Có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng.

5.12.2.4 Kiểm soát truy cập

a) Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập thông tin nội bộ hoặc thực hiện quản trị từ xa đối với tài sản phần cứng và phần mềm.

b) Cấu hình chức năng xác thực trên các thiết bị hệ thống để xác thực người dùng khi quản trị thiết bị trực tiếp hoặc từ xa.

c) Thiết lập giới hạn thời gian chờ (timeout) để tự động đóng các phiên kết nối khi không nhận được yêu cầu từ người dùng trong một khoảng thời gian quy định.

d) Kiểm soát truy cập từ bên ngoài vào hệ thống và từ bên trong hệ thống ra ngoài theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả truy cập tới các tài sản phần cứng và phần mềm mà hệ thống không cung cấp hoặc không cho phép truy cập.

e) Giới hạn số lượng kết nối đồng thời từ một địa chỉ nguồn và tổng số lượng kết nối đồng thời cho từng ứng dụng, dịch vụ được hệ thống cung cấp theo năng lực thực tế của hệ thống, không áp dụng cứng đối với hệ thống/dịch vụ có yêu cầu kết nối lớn nếu đã có biện pháp kiểm soát rủi ro tương đương.

f) Có phương án kiểm soát truy cập của người dùng vào các dịch vụ, các máy chủ nội bộ theo chính sách.

5.12.2.5 Xây dựng và áp dụng chính sách quản lý truy cập từ xa

Có chính sách quản lý truy cập từ xa đáp ứng các yêu cầu sau:

- Sử dụng mạng riêng ảo VPN hoặc phương án tương đương và yêu cầu xác thực cho việc truy cập từ xa vào hệ thống đối với người dùng quản trị, người dùng tác nghiệp hệ thống.

- Yêu cầu người dùng xác thực để kết nối truy cập từ xa và xác thực bổ sung trước khi truy cập vào hệ thống.

- Giới hạn các dải địa chỉ mạng hoặc thiết bị cụ thể (nếu hỗ trợ) được phép kết nối để thực hiện quản trị từ xa đối với tài sản phần cứng và phần mềm.

5.13 Giám sát và phòng thủ an ninh mạng

5.13.1 Khái quát

Xây dựng, vận hành các quy trình và công cụ để thiết lập, duy trì giám sát mạng toàn diện và bảo vệ hệ thống mạng khỏi các mối đe dọa.

5.13.2 Yêu cầu cụ thể

5.13.2.1 Thực hiện giám sát và quản lý tập trung các cảnh báo và sự kiện an ninh mạng

a) Triển khai giám sát an ninh mạng đối với tối thiểu các đối tượng: thiết bị hệ thống, máy chủ, ứng dụng, dịch vụ và các thành phần khác trong hệ thống (nếu có).

b) Triển khai SIEM để liên kết các sự kiện liên quan, phân tích theo hướng dẫn, yêu cầu và quy định của cơ quan, tổ chức có thẩm quyền.

5.13.2.2 Thiết lập và sử dụng tính năng về tường lửa, cảnh báo phát hiện và ngăn chặn xâm nhập của hệ điều hành và hệ thống

Thiết lập và sử dụng tính năng về tường lửa, cảnh báo phát hiện, ngăn chặn xâm nhập của hệ điều hành và hệ thống (nếu có).

5.13.2.3 Thiết lập cấu hình kiểm soát truy cập các cổng kết nối mạng

a) Thiết lập cấu hình trên các thiết bị mạng để kiểm soát truy cập các cổng kết nối mạng nếu thiết bị hỗ trợ.

b) Thay đổi, tách biệt cổng quản trị ứng dụng với cổng cung cấp dịch vụ ứng dụng.

5.13.2.4 Thu thập thông tin dữ liệu mạng

Thu thập nhật ký luồng dữ liệu mạng và/ hoặc dữ liệu lưu lượng từ các thiết bị mạng để rà soát và đưa ra các cảnh báo.

5.13.2.5 Điều chỉnh các ngưỡng cảnh báo sự kiện an ninh mạng

Điều chỉnh ngưỡng cảnh báo sự kiện an ninh mạng tối thiểu 01 lần/ 06 tháng.

5.14 Nhân sự vận hành, quản trị hệ thống, bảo vệ an ninh mạng

5.14.1 Khái quát

a) Có cơ chế hoạt động độc lập về chuyên môn giữa các bộ phận vận hành, quản trị, bảo vệ an ninh mạng.

b) Thiết lập và duy trì chương trình đào tạo nâng cao nhận thức an ninh mạng và kỹ năng an ninh mạng.

5.14.2 Yêu cầu cụ thể

5.14.2.1 Có bộ phận phụ trách về vận hành, quản trị hệ thống và bảo vệ an ninh mạng

a) Thành lập các bộ phận riêng biệt vận hành, quản trị hệ thống và bảo vệ an ninh mạng.

b) Có cơ chế hoạt động độc lập về chuyên môn giữa các bộ phận vận hành, quản trị hệ thống và bảo vệ an ninh mạng.

c) Nhân sự phụ trách về vận hành, quản trị hệ thống và bảo vệ an ninh mạng phải có trình độ chuyên môn về an ninh mạng, công nghệ thông tin; có cam kết bảo mật thông tin trong quá trình làm việc và sau khi nghỉ việc.

5.14.2.2 Thiết lập và duy trì quy định sử dụng hệ thống thông tin, triển khai chương trình đào tạo tổng quan để nâng cao nhận thức an ninh mạng cho cán bộ, nhân viên

a) Có chương trình nâng cao nhận thức an ninh mạng cho toàn bộ cán bộ, nhân viên có sử dụng hệ thống thông tin.

b) Cán bộ chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của tổ chức.

c) Có quy trình và thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.

d) Tiến hành đào tạo tối thiểu 01 lần/ năm.

5.15 Quản lý nhà cung cấp sản phẩm, dịch vụ

5.15.1 Khái quát

Có quy trình để đánh giá nhà cung cấp sản phẩm, dịch vụ an ninh mạng, lưu trữ, xử lý dữ liệu nhạy cảm hoặc chịu trách nhiệm về các quy trình, nền tảng quan trọng của hệ thống.

5.15.2 Yêu cầu cụ thể

Có phương án thiết lập và duy trì bản kiểm kê các nhà cung cấp sản phẩm, dịch vụ. Tối thiểu bao gồm:

- Lập danh sách, theo dõi, cập nhật trạng thái các nhà cung cấp sản phẩm, dịch vụ.

- Thực hiện phân loại các nhà cung cấp dịch vụ trong danh sách quản lý.

- Có văn bản xác định rõ phạm vi trách nhiệm của nhà cung cấp và tổ chức.

- Xem xét và cập nhật danh sách tối thiểu 01 lần/ năm hoặc khi xảy ra thay đổi ảnh hưởng đến danh sách này.

5.16 Quản trị ứng phó sự cố an ninh mạng

5.16.1 Khái quát

Có kế hoạch, chương trình để phát triển và duy trì khả năng ứng phó sự cố bao gồm chính sách, kế hoạch, thủ tục, vai trò, đào tạo, kênh liên lạc. Chính sách, quy trình xử lý sự cố an ninh mạng bao gồm tối thiểu các nội dung:

- Phân nhóm sự cố an ninh mạng.

- Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an ninh mạng.

- Kế hoạch ứng phó sự cố an ninh mạng.

- Giám sát, phát hiện và cảnh báo sự cố an ninh mạng.

- Quy trình ứng cứu sự cố an ninh mạng thông thường.

- Quy trình ứng cứu sự cố an ninh mạng nghiêm trọng.

- Cơ chế phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an ninh mạng.

- Định kỳ tổ chức diễn tập phương án xử lý sự cố an ninh mạng.

5.16.2 Yêu cầu cụ thể

5.16.2.1 Thành lập lực lượng ứng phó sự cố an ninh mạng

a) Chỉ định một người chủ chốt và ít nhất một người dự phòng để quản lý quy trình ứng phó sự cố an ninh mạng.

b) Thiết lập và duy trì đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý nhà nước về an ninh mạng, cơ quan điều hành Liên minh ứng phó, khắc phục sự cố an ninh mạng quốc gia.

c) Thiết lập và duy trì đầu mối liên lạc để báo cáo sự cố. Xác minh thông tin liên hệ của các cơ quan, tổ chức hỗ trợ điều phối ứng phó sự cố hàng năm để đảm bảo thông tin được cập nhật.

d) Phân công vị trí, vai trò và trách nhiệm chính của từng thành viên trong lực lượng tham gia ứng phó sự cố.

e) Quy định về trách nhiệm phối hợp với lực lượng ứng phó sự cố an ninh mạng của các phòng ban có liên quan.

5.16.2.2 Thiết lập và duy trì quy trình nội bộ để báo cáo sự cố an ninh mạng

a) Có quy trình nội bộ để báo cáo sự cố an ninh mạng.

b) Thực hiện phân nhóm sự cố an ninh mạng.

c) Đánh giá và cập nhật quy trình tối thiểu 01 lần/ năm hoặc khi xảy ra các thay đổi ảnh hưởng đến quy trình.

5.16.2.3 Thiết lập và duy trì quy trình ứng phó sự cố an ninh mạng

a) Có quy trình ứng phó sự cố, đảm bảo có cơ chế phối hợp với các cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ khắc phục sự cố an ninh mạng.

b) Đánh giá và cập nhật quy trình tối thiểu 01 lần/ năm hoặc khi xảy ra các thay đổi ảnh hưởng đến quy trình.

5.17 Phát triển ứng dụng an toàn

5.17.1 Khái quát

Quản lý vòng đời bảo mật của các phần mềm ứng dụng để phòng ngừa, phát hiện và xử lý các điểm yếu, lỗ hổng bảo mật.

5.17.2 Yêu cầu cụ thể

5.17.2.1 Thiết lập và duy trì quy trình phát triển ứng dụng an toàn

a) Có quy trình phát triển ứng dụng an toàn.

b) Đánh giá và cập nhật quy trình tối thiểu 01 lần/ năm hoặc khi xảy ra các thay đổi có thể ảnh hưởng đến quy trình.

c) Đối với các phần mềm phát triển thuê khoán, yêu cầu:

- Có biên bản, hợp đồng và cam kết bảo mật đối với bên thuê khoán các nội dung liên quan đến phát triển phần mềm thuê khoán.

- Yêu cầu nhà phát triển cung cấp mã nguồn phần mềm. Trong trường hợp không thể cung cấp mã nguồn phần mềm, chủ quản hệ thống phải yêu cầu các bên thuê khoán cung cấp chứng chỉ đánh giá an toàn độc lập hoặc thực hiện các biện pháp kiểm thử xâm nhập, giám sát rủi ro thay thế và ký cam kết chịu trách nhiệm pháp lý về tính an toàn của phần mềm.

5.17.2.2 Thiết lập và duy trì quy trình tiếp nhận và xử lý lỗ hổng bảo mật phần mềm

a) Có quy trình tiếp nhận và xử lý báo cáo về lỗ hổng bảo mật phần mềm, bao gồm cả việc cung cấp phương tiện để các cá nhân, tổ chức bên ngoài báo cáo.

b) Đánh giá và cập nhật quy trình tối thiểu 01 lần/ năm hoặc khi xảy ra các thay đổi có thể ảnh hưởng đến quy trình.

5.17.2.3 Kết hợp các nguyên tắc bảo mật trong kiến trúc ứng dụng

Kết hợp các nguyên tắc bảo mật trong quá trình xây dựng kiến trúc ứng dụng. Trong đó bao gồm nhưng không giới hạn các yêu cầu:

- Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý.

- Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu ra trước khi gửi về máy yêu cầu.

- Có phương án bảo vệ ứng dụng chống lại những dạng tấn công phổ biến.

- Có chức năng kiểm soát lỗi, thông báo lỗi từ ứng dụng.

- Không lưu trữ thông tin xác thực, thông tin bí mật trên mã nguồn ứng dụng.

5.17.2.4 Tiến hành kiểm tra an ninh, an toàn các ứng dụng

Kiểm tra và khắc phục các lỗ hổng bảo mật của ứng dụng, lỗ hổng trong mã nguồn, các thư viện, thành phần mở rộng của bên thứ ba mà ứng dụng sử dụng trước khi đưa vào vận hành chính thức.

5.18 Quản lý kiểm tra an ninh mạng

5.18.1 Khái quát

Xác định tính hiệu quả trong năng lực phòng vệ và khả năng phục hồi của các tài sản thông qua việc đánh giá khả năng khai thác các điểm yếu trong quy trình kiểm soát về con người, quy trình, công nghệ; mô phỏng lại các mục tiêu và hành động tấn công; khắc phục các tồn tại phát hiện được qua kết quả kiểm thử xâm nhập.

5.18.2 Yêu cầu cụ thể

5.18.2.1 Thiết lập và duy trì một chương trình kiểm thử xâm nhập

a) Có chương trình kiểm thử xâm nhập phù hợp với quy mô, mức độ phức tạp và trạng thái của tổ chức.

b) Chương trình kiểm thử xâm nhập cần đáp ứng một số nội dung sau:

- Về yêu cầu: hoạt động kiểm thử xâm nhập phải được phê duyệt về phạm vi, thời gian, phương pháp, đầu mối phối hợp, phương án đảm bảo an ninh mạng và phương án xử lý dữ liệu thu được; đối với hệ thống đang vận hành, phải chọn thời điểm và cách thức kiểm thử phù hợp để không làm gián đoạn dịch vụ, ưu tiên thực hiện trên môi trường phát triển hoặc trong thời gian đã được phê duyệt.

- Về phạm vi tiến hành: kiểm tra một phần hoặc toàn bộ hạ tầng công nghệ thông tin của tổ chức.

- Về tần suất: hàng quý, nửa năm, một năm hoặc đột xuất.

- Về các giới hạn: xác định các hành vi tấn công bị cấm (tấn công vật lý, tấn công lừa đảo, tấn công phi kỹ thuật…).

- Về cách phản ứng của tổ chức: có thực hiện việc ngăn chặn hay không, cơ chế kiểm soát thông tin (về cuộc kiểm thử) trong nội bộ.

5.18.2.2 Khắc phục các tồn tại phát hiện được qua việc kiểm thử xâm nhập

Khắc phục các tồn tại phát hiện được qua kiểm thử xâm nhập dựa trên chính sách của tổ chức về phạm vi và mức độ ưu tiên khắc phục.

5.18.2.3 Rà soát các biện pháp bảo mật

Kiểm tra, đánh giá hiệu quả các biện pháp bảo mật sau mỗi lần thực hiện kiểm thử xâm nhập.

6 Yêu cầu cơ bản đối với hệ thống thông tin cấp độ 4

6.1 Quản lý rủi ro an ninh mạng

6.1.1 Khái quát

Thực hiện xác định, đánh giá, xử lý rủi ro an ninh mạng và lên kế hoạch ứng phó khi rủi ro xảy ra.

6.1.2 Yêu cầu cụ thể

6.1.2.1 Thiết lập và duy trì quy định, quy trình quản lý rủi ro an ninh mạng

a) Có quy định, quy trình quản lý rủi ro an ninh mạng. Trong đó, yêu cầu thực hiện quản lý rủi ro an ninh mạng bao gồm tối thiểu các bước: xác định, phân tích, đánh giá và xử lý rủi ro an ninh mạng.

b) Đánh giá và cập nhật quy định, quy trình quản lý rủi ro an ninh mạng và các tài liệu liên quan tối thiểu 01 lần/ năm hoặc khi có thay đổi xảy ra trong tổ chức ảnh hưởng đến các văn bản đã ban hành có liên quan.

6.1.2.2 Xác định rủi ro an ninh mạng

a) Thực hiện xác định rủi ro an ninh mạng trong tổ chức (có thể dựa trên việc quản lý tài sản, quản lý lỗ hổng, quản lý hạ tầng mạng, quản lý nhận thức an ninh mạng, quản lý tài khoản và quyền truy cập…).

b) Xác định rủi ro an ninh mạng đến từ các bên thứ ba, nhà cung cấp.

c) Thực hiện xác định rủi ro an ninh mạng định kỳ tối thiểu 01 lần/ 06 tháng hoặc khi có thay đổi liên quan đến hệ thống thông tin (thay đổi hệ thống, lỗ hổng bảo mật mới, các sự kiện an ninh mạng...).

6.1.2.3 Đánh giá rủi ro an ninh mạng

a) Thực hiện phân tích, đánh giá rủi ro an ninh mạng để xác định mức độ ảnh hưởng, tác động của rủi ro đến tổ chức, từ đó đưa ra quyết định chấp nhận hoặc thực hiện các biện pháp giảm thiểu rủi ro.

b) Thực hiện phân tích và đánh giá rủi ro an ninh mạng ngay sau khi xác định rủi ro; phân tích, đánh giá lại khi có sự thay đổi về hệ thống, các sự kiện an ninh mạng hoặc những thay đổi trong tổ chức liên quan đến rủi ro đã xác định.

6.1.2.4 Xử lý rủi ro an ninh mạng

a) Thực hiện các biện pháp xử lý rủi ro an ninh mạng và xây dựng phương án ứng phó khi rủi ro còn lại (sau khi đã xử lý) xảy ra.

b) Định kỳ tối thiểu 01 lần/ 06 tháng đánh giá và cải thiện hiệu quả của các biện pháp kiểm soát được sử dụng để giảm thiểu rủi ro.

6.1.2.5 Giám sát rủi ro an ninh mạng

Giám sát và cập nhật những thay đổi liên quan đến rủi ro đã được xác định, tối thiểu bao gồm: khả năng xảy ra, mức độ ảnh hưởng, mức độ rủi ro, tài sản bị ảnh hưởng, biện pháp kiểm soát đã áp dụng.

6.1.2.6 Truyền thông rủi ro an ninh mạng

a) Chia sẻ kết quả đánh giá rủi ro cho các bên liên quan.

b) Thông báo kịp thời cho các bên liên quan về thay đổi quan trọng liên quan đến rủi ro.

6.2 Quản lý tài sản phần cứng

6.2.1 Khái quát

a) Lập danh sách, theo dõi, cập nhật trạng thái của tất cả tài sản phần cứng thuộc hệ thống thông tin và các tài sản không thuộc quyền kiểm soát của tổ chức nhưng có kết nối vào hệ thống thông tin; xác định danh sách tài sản cần được giám sát, bảo vệ.

b) Xác định các tài sản vô chủ, tài sản trái phép để loại bỏ hoặc đưa ra phương án quản lý.

c) Thực hiện kiểm kê, rà soát và cập nhật danh sách cho tất cả tài sản thuộc hệ thống thông tin định kỳ tối thiểu 01 lần/ năm.

6.2.2 Yêu cầu cụ thể

6.2.2.1 Thiết lập và duy trì hệ thống quản lý danh mục tài sản phần cứng

a) Lập danh sách, theo dõi, cập nhật trạng thái của tất cả tài sản phần cứng có khả năng lưu trữ hoặc xử lý dữ liệu, bao gồm: thiết bị của người dùng cuối, thiết bị di động, thiết bị lưu trữ ngoài, thiết bị văn phòng, thiết bị mạng, thiết bị OT/IoT và máy chủ trong môi trường vật lý, ảo hóa, truy cập từ xa và điện toán đám mây.

b) Căn cứ vào điều kiện thực tế, tổ chức thực hiện kiểm tra an ninh tất cả tài sản vật lý đưa vào sử dụng.

c) Danh sách tài sản phần cứng phải bao gồm tối thiểu các thông tin cơ bản sau: tên tài sản, địa chỉ mạng IP (đối với thiết bị đặt địa chỉ IP tĩnh), địa chỉ phần cứng MAC/ mã nhận diện serial, thời gian ngừng hỗ trợ kỹ thuật của hãng (nếu có), vị trí lắp đặt địa lý, vị trí lắp đặt trong hệ thống mạng, mục đích sử dụng, tình trạng sử dụng. Tài sản vật lý phải được giao, gán trách nhiệm cho cá nhân hoặc bộ phận quản lý, sử dụng.

d) Các thiết bị di động do tổ chức quản lý hoặc được tổ chức cho phép kết nối vào hệ thống thông tin phải được đăng ký để kiểm soát. Quy định trách nhiệm của cá nhân trong tổ chức khi sử dụng thiết bị di động để phục vụ công việc.

6.2.2.2 Xử lý các tài sản phần cứng chưa được quản lý

a) Có quy trình phát hiện và xử lý các tài sản phần cứng không có trong danh sách quản lý, đang kết nối trái phép vào hệ thống thông tin định kỳ tối thiểu 01 lần/ quý.

b) Có thể lựa chọn loại bỏ, từ chối kết nối hoặc cách ly tài sản trái phép.

6.2.2.3 Rà soát các tài sản kết nối vào hệ thống thông tin

a) Có quy định rà quét để phát hiện tài sản kết nối vào hệ thống thông tin định kỳ tối thiểu 01 lần/ quý.

b) Thực hiện cập nhật danh sách tài sản dựa trên kết quả rà quét.

6.2.2.4 Sử dụng DHCP Logging để cập nhật bản kiểm kê tài sản công nghệ thông tin

a) Sử dụng tính năng ghi nhật ký DHCP trên tất cả các máy chủ DHCP hoặc công cụ quản lý địa chỉ mạng IP (nếu có).

b) Tiến hành rà soát nhật ký để cập nhật danh sách tài sản công nghệ thông tin định kỳ tối thiểu 01 lần/ quý.

6.2.2.5 Quản lý tài sản thanh lý/ hư hỏng

a) Có quy trình thanh lý/ tiêu hủy tài sản CNTT.

b) Có biện pháp chuyên dụng để xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng.

6.3 Quản lý tài sản phần mềm

6.3.1 Khái quát

a) Lập danh sách, theo dõi, cập nhật trạng thái của tất cả tài sản phần mềm thuộc hệ thống thông tin của cơ quan, tổ chức, đảm bảo chỉ những phần mềm đã phê duyệt mới được phép cài đặt và sử dụng.

b) Thực hiện kiểm kê, rà soát và cập nhật danh sách cho tất cả tài sản phần mềm định kỳ tối thiểu 01 lần/ năm.

6.3.2 Yêu cầu cụ thể

6.3.2.1 Thiết lập và duy trì hệ thống quản lý danh mục tài sản phần mềm

a) Lập danh sách, theo dõi, cập nhật trạng thái của tất cả tài sản phần mềm hiện đang được cài đặt trên các tài sản phần cứng thuộc hệ thống thông tin của cơ quan, tổ chức.

b) Danh sách tài sản phần mềm phải bao gồm tối thiểu các thông tin cơ bản sau: tên tài sản, mục đích sử dụng, thời gian ngừng hỗ trợ kỹ thuật (nếu có), phạm vi sử dụng, chủ thể quản lý, thông tin về bản quyền, phiên bản, hệ thống thông tin thành phần (nếu có). Tài sản phần mềm phải được gắn trách nhiệm cho cá nhân hoặc bộ phận quản lý, sử dụng.

6.3.2.2 Thiết lập và duy trì danh sách các tài sản phần mềm được phép sử dụng

a) Lập danh sách, theo dõi, cập nhật danh sách các phần mềm được phép sử dụng trong hệ thống thông tin của cơ quan, tổ chức.

b) Danh sách phần mềm được phép sử dụng phải bao gồm cả các phần mềm được cung cấp bởi nhà cung cấp dịch vụ, các môi trường thực thi cần cài đặt cho ứng dụng.

c) Có quy định kiểm soát việc cài đặt và sử dụng các phần mềm đã được cấp phép, đảm bảo giới hạn đặc quyền tối thiểu các quyền quản trị trên các tài sản CNTT; ngăn chặn các tác vụ thực thi, vô hiệu hóa, cài

đặt và gỡ bỏ phần mềm, thư viện, đoạn mã lệnh trái phép trên hệ thống; có phương án kỹ thuật để theo dõi hoạt động cài đặt chương trình phần mềm trên các tài sản CNTT.

d) Định kỳ đánh giá và cập nhật danh sách phần mềm được phép sử dụng tối thiểu 01 lần/ năm hoặc khi xảy ra các thay đổi trong tổ chức ảnh hưởng đến danh sách.

6.3.2.3 Đảm bảo toàn bộ các tài sản phần mềm được phép sử dụng đang trong thời gian hỗ trợ của nhà cung cấp

Thực hiện định kỳ rà soát danh sách tài sản phần mềm được phép sử dụng và danh sách tài sản phần mềm cài đặt trên các tài sản phần cứng để đảm bảo tất cả tài sản phần mềm đang trong thời gian hỗ trợ của nhà cung cấp, tối thiểu 01 lần/ năm.

6.3.2.4 Xử lý các tài sản phần mềm trái phép

a) Có quy trình phát hiện và xử lý các phần mềm trái phép định kỳ tối thiểu 01 lần/ 06 tháng.

b) Những phần mềm trái phép nhưng vẫn cần thiết đối với hoạt động của cơ quan, tổ chức phải được đưa vào danh sách ngoại lệ để quản lý. Danh sách ngoại lệ này phải thể hiện chi tiết các biện pháp kiểm soát giảm thiểu nguy cơ an ninh mạng ảnh hưởng đến hệ thống.

c) Những phần mềm trái phép không nằm trong danh sách ngoại lệ phải có kế hoạch để xóa/ gỡ bỏ hoàn toàn khỏi các tài sản phần cứng của cơ quan, tổ chức trong thời gian sớm nhất.

6.4 Quản lý tài sản thông tin

6.4.1 Khái quát

Thực hiện quản lý tài sản thông tin và triển khai các biện pháp kiểm soát để phát hiện, phân loại, xử lý, lưu trữ, loại bỏ tài sản thông tin một cách an toàn.

6.4.2 Yêu cầu cụ thể

6.4.2.1 Thiết lập và duy trì quy định quản lý tài sản thông tin

a) Có quy định quản lý tài sản thông tin. Trong quy định, xác định danh sách tài sản thông tin, mức độ nhạy cảm, chủ sở hữu, các bước xử lý, thời gian lưu trữ và các yêu cầu khi tiêu hủy/xóa bỏ dựa trên các tiêu chuẩn về mức độ bảo mật của tài sản thông tin.

b) Mức độ nhạy cảm của tài sản thông tin có thể được quy định như sau:

- Mức 1: Công khai. Tài sản thông tin công khai không yêu cầu về bảo mật.

- Mức 2: Nội bộ. Tài sản thông tin nội bộ yêu cầu chỉ những người trong tổ chức mới có quyền truy cập.

- Mức 3: Hạn chế truy cập. Tài sản thông tin bị hạn chế yêu cầu quyền truy cập, chỉ những người dùng được cấp quyền mới có thể truy cập vào dữ liệu. Việc tiết lộ tài sản thông tin bị hạn chế truy cập có khả năng ảnh hưởng đến hoạt động của cơ quan, tổ chức.

- Mức 4: Bí mật nhà nước. Thông tin có nội dung quan trọng, do cơ quan, tổ chức có thẩm quyền xác định; chưa công khai, nếu bị lộ, bị mất có thể gây nguy hại đến lợi ích quốc gia, dân tộc.

c) Có quy trình yêu cầu truy cập, thêm mới, sửa, xóa dữ liệu để kiểm soát truy cập dữ liệu.

d) Kiểm tra cấp độ phân quyền dữ liệu định kỳ tối thiểu 01 lần/ quý.

e) Đánh giá và cập nhật quy trình quản lý tài sản thông tin định kỳ tối thiểu 01 lần/ năm hoặc khi xảy ra các thay đổi trong tổ chức ảnh hưởng đến quy trình.

6.4.2.2 Thiết lập và duy trì bản danh sách tài sản thông tin

a) Lập danh sách các tài sản thông tin dựa trên quy trình quản lý tài sản thông tin.

b) Đánh giá và cập nhật danh sách tài sản thông tin tối thiểu 01 lần/ năm hoặc khi xảy ra thay đổi trong tổ chức ảnh hưởng đến danh sách.

6.4.2.3 Xây dựng danh sách kiểm soát truy cập tài sản thông tin

Xây dựng danh sách quyền truy cập của các tài khoản, người dùng đối với từng loại tài sản thông tin.

6.4.2.4 Mã hóa dữ liệu quan trọng

a) Mã hóa hoặc sử dụng biện pháp kiểm soát rủi ro tương đương để bảo mật thông tin xác thực, dữ liệu có độ nhạy cảm cao, dữ liệu quan trọng được lưu trữ trong các tài sản phần cứng và phần mềm của tổ chức.

b) Mã hóa hoặc sử dụng biện pháp kiểm soát rủi ro tương đương để bảo vệ thông tin xác thực, dữ liệu có độ nhạy cảm cao, dữ liệu quan trọng trong quá trình truyền gửi.

c) Sử dụng kết hợp các kết nối mạng an toàn, các biện pháp mã hóa hoặc biện pháp kiểm soát rủi ro tương đương để bảo đảm dữ liệu quan trọng được mã hóa tối thiểu 02 lần khi truyền qua môi trường mạng.

d) Có phương án chuyên dụng để quản lý và bảo vệ dữ liệu mã hóa và khóa giải mã.

e) Sử dụng các phương pháp mã hóa mạnh (chưa được các tổ chức quốc tế công bố điểm yếu) để mã hóa dữ liệu.

6.4.2.5 Nguyên vẹn dữ liệu

a) Có phương án quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn.

b) Có phương án giám sát, cảnh báo khi có thay đổi thông tin, dữ liệu lưu trên hệ thống lưu trữ/phương tiện lưu trữ.

c) Có phương án khôi phục tính nguyên vẹn của dữ liệu.

6.4.2.6 Tài liệu hóa luồng dữ liệu

a) Có tài liệu mô tả các luồng dữ liệu trong hệ thống thông tin.

b) Xây dựng và tuân thủ quy định quản lý phiên bản tài liệu tại tổ chức.

c) Đánh giá và cập nhật định kỳ tối thiểu 01 lần/ năm hoặc khi có thay đổi trong tổ chức ảnh hưởng đến tài liệu.

6.4.2.7 Tách biệt quá trình xử lý và lưu trữ dữ liệu theo mức độ nhạy cảm

a) Có quy định về việc xử lý dữ liệu nhạy cảm.

b) Tách biệt tài sản/môi trường xử lý, lưu trữ dữ liệu có độ nhạy cảm cao, dữ liệu quan trọng với dữ liệu có độ nhạy cảm thấp (về mặt logic hoặc vật lý) hoặc có phương án kiểm soát rủi ro tương đương đảm bảo an ninh dữ liệu. Không sử dụng các tài sản/ môi trường dành cho dữ liệu nhạy cảm thấp để lưu trữ và xử lý dữ liệu quan trọng, dữ liệu có mức độ nhạy cảm cao.

c) Sử dụng kênh vật lý riêng hoặc có phương án kiểm soát rủi ro tương đương để bảo mật dữ liệu quan trọng, dữ liệu có độ nhạy cảm cao khi truyền đưa, trao đổi qua môi trường mạng.

6.4.2.8 Triển khai giải pháp phòng chống thất thoát dữ liệu

Xây dựng và triển khai giải pháp chống thất thoát dữ liệu đối với dữ liệu có độ nhạy cảm cao, dữ liệu quan trọng được lưu trữ, xử lý trong hệ thống thông tin.

6.4.2.9 Lưu trữ nhật ký truy cập dữ liệu quan trọng

a) Ghi lại nhật ký hành vi đối dữ liệu có độ nhạy cảm cao, dữ liệu quan trọng.

b) Rà soát nhật ký thường xuyên, định kỳ tối thiểu 01 lần/ quý để phát hiện sớm những hành vi truy cập trái phép.

6.4.2.10 Sử dụng chữ ký số khi trao đổi thông tin số, dữ liệu số quan trọng

a) Sử dụng chữ ký số khi trao đổi dữ liệu có độ nhạy cảm cao, dữ liệu quan trọng.

b) Chữ ký số được cung cấp bởi cơ quan có thẩm quyền hoặc đơn vị cung cấp dịch vụ chữ ký số được cấp phép.

c) Có phương án bảo đảm an ninh mạng trong việc quản lý và sử dụng chữ ký số.

6.5 Cấu hình an toàn cho phần cứng và phần mềm

6.5.1 Khái quát

Thiết lập và duy trì cấu hình an toàn cho phần cứng (như thiết bị người dùng cuối bao gồm máy tính, thiết bị di động và cầm tay, thiết bị mạng, thiết bị OT/IoT, máy chủ...) và phần mềm (như hệ điều hành, ứng dụng…).

6.5.2 Yêu cầu cụ thể

6.5.2.1 Thiết lập và duy trì quy định, quy trình cấu hình an toàn cho tài sản phần cứng và phần mềm

a) Có quy định, quy trình cấu hình an toàn cho các tài sản phần cứng và phần mềm của cơ quan, tổ chức.

b) Có các tài liệu cấu hình tiêu chuẩn, tài liệu cấu hình tăng cường bảo mật cho tài sản phần cứng và phần mềm của cơ quan, tổ chức. Đảm bảo sử dụng giao thức kết nối an toàn, thiết lập tường lửa cho máy chủ/ máy trạm và có phương án chống đăng nhập tự động đối với các tài sản xử lý và lưu trữ dữ liệu quan trọng.

c) Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ mà phần cứng, phần mềm không sử dụng.

d) Cấu hình tối ưu và tăng cường bảo mật cho tài sản phần cứng trước khi đưa vào vận hành, khai thác.

e) Đánh giá và cập nhật quy trình quản lý cấu hình an toàn, các tài liệu liên quan tối thiểu 01 lần/ năm hoặc khi có thay đổi xảy ra trong tổ chức ảnh hưởng đến tài liệu.

6.5.2.2 Cấu hình tự động khóa phiên làm việc trên các tài sản phần cứng và phần mềm

a) Dựa trên yêu cầu sử dụng, kết quả đánh giá rủi ro, thực hiện cấu hình tự động khóa phiên làm việc trên các tài sản phần cứng và phần mềm. Có thể thực hiện cấu hình như sau:

- Tự động khóa phiên làm việc trên các tài sản sau một khoảng thời gian không sử dụng:

+ Đối với máy tính người dùng: không quá 15 phút.

+ Đối với các phiên quản trị phần mềm, máy chủ, thiết bị mạng, thiết bị IoT: không quá 05 phút.

+ Đối với thiết bị di động: không quá 05 phút.

+ Đối với các phần mềm nghiệp vụ xử lý dữ liệu quan trọng: không quá 15 phút.

- Tự động khóa thiết bị di động sau một số lần đăng nhập thất bại:

+ Đối với máy tính xách tay: tối đa 10 lần.

+ Đối với điện thoại: tối đa 10 lần.

+ Đối với các phần mềm nghiệp vụ lưu trữ và xử lý dữ liệu quan trọng: tối đa 05 lần.

+ Giới hạn thời gian mở khóa thiết bị sau khi bị khóa: tối thiểu 12 giờ, tối đa 30 ngày.

b) Có cơ chế mở khóa khẩn cấp dành cho quản trị viên/tài khoản đặc quyền.

6.5.2.3 Gỡ bỏ hoặc vô hiệu hóa các tính năng, dịch vụ không cần thiết trên các tài sản phần cứng và phần mềm

Có quy định gỡ bỏ hoặc vô hiệu hóa các tính năng, dịch vụ không cần thiết trên các tài sản phần cứng và phần mềm.

6.5.2.4 Cấu hình máy chủ DNS tin cậy

Thiết lập các cấu hình máy chủ DNS tin cậy trên các tài sản phần cứng nếu có.

6.5.2.5 Thiết lập khả năng xóa sạch dữ liệu từ xa trên thiết bị di động cấp cho người dùng

Xây dựng và triển khai giải pháp xóa sạch dữ liệu từ xa trên thiết bị di động cấp cho người dùng.

6.5.2.6 Phân tách các không gian làm việc riêng biệt trên các thiết bị di động cấp cho người dùng

Có quy định tách biệt các không gian làm việc riêng biệt trên thiết bị di động cấp cho người dùng.

6.6 Quản lý tài khoản và quyền truy cập tài khoản của người dùng

6.6.1 Khái quát

a) Có quy trình, công cụ để phân quyền và quản lý quyền truy cập của tài khoản người dùng bao gồm: tài khoản quản trị, tài khoản tác nghiệp (tài khoản của người dùng cuối tác nghiệp), tài khoản kỹ thuật (tài khoản dùng để kết nối giữa các hệ thống kỹ thuật), tài khoản dịch vụ (tài khoản cấp cho người thụ hưởng dịch vụ) trên các tài sản phần cứng và phần mềm.

b) Có quy trình tạo, gán, quản lý, thu hồi đặc quyền và quyền truy cập đối với các tài khoản người dùng cho tài sản phần cứng và phần mềm. Quyền truy cập của tài khoản quản trị, tài khoản tác nghiệp, tài khoản kỹ thuật, tài khoản dịch vụ phải nhất quán dựa trên vai trò và các yêu cầu cụ thể, đảm bảo người dùng chỉ có quyền truy cập vào dữ liệu, tài sản phù hợp.

c) Ghi nhật ký và giám sát tài khoản người dùng.

6.6.2 Yêu cầu cụ thể

6.6.2.1 Thiết lập và duy trì hệ thống quản lý tài khoản

a) Lập danh sách, theo dõi và cập nhật tất cả tài khoản trên các tài sản phần cứng và phần mềm của tổ chức.

b) Danh sách tài khoản phải bao gồm tối thiểu các loại tài khoản sau: tài khoản quản trị, tài khoản tác nghiệp và tài khoản kỹ thuật.

c) Danh sách tài khoản phải bao gồm các thông tin tối thiểu: loại tài khoản, tên tài khoản, trạng thái tài khoản, tên tài sản/ hệ thống thông tin tương ứng, tên người quản lý, phòng ban, ngày kích hoạt tài khoản, ngày vô hiệu hóa tài khoản (nếu có). Đảm bảo tất cả tài khoản đang hoạt động là hợp lệ.

d) Danh sách tài khoản phải được rà soát định kỳ 01 lần/ quý.

6.6.2.2 Xây dựng và tuân thủ quy định sử dụng mật khẩu

a) Thiết lập cấu hình mật khẩu trên tài sản phần cứng, phần mềm để đảm bảo an toàn mật khẩu người sử dụng, bao gồm các yêu cầu sau:

- Yêu cầu thay đổi mật khẩu mặc định.

- Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự.

- Thiết lập thời gian yêu cầu thay đổi mật khẩu.

- Thiết lập thời gian mật khẩu hợp lệ.

b) Dựa trên yêu cầu sử dụng, kết quả đánh giá rủi ro, triển khai quy định sử dụng mật khẩu an toàn trong tổ chức. Có thể thực hiện cấu hình như sau:

- Sử dụng mật khẩu duy nhất cho mỗi tài sản hoặc sử dụng giải pháp xác thực và quản lý tập trung.

- Yêu cầu thay đổi mật khẩu trong lần đăng nhập đầu tiên.

- Đối với các hệ thống sử dụng xác thực MFA, quy định mật khẩu có tối thiểu 08 ký tự.

- Đối với các hệ thống không sử dụng xác thực MFA, quy định mật khẩu có tối thiểu 14 ký tự, bao gồm ký tự viết thường, ký tự viết hoa, ký tự đặc biệt, chữ số.

- Đối với tài khoản quản trị cần triển khai xác thực MFA, thay đổi mật khẩu định kỳ 01 lần/02 tháng và mật khẩu mới không được trùng với 10 mật khẩu trước đó.

6.6.2.3 Xây dựng và tuân thủ quy định quản lý tài khoản

Có quy định quản lý tài khoản trong tổ chức đáp ứng các yêu cầu sau:

- Sử dụng giải pháp quản lý tài khoản đặc quyền hoặc có phương án tương đương phục quản lý tài khoản đặc quyền.

- Quản lý tài khoản tập trung.

- Thay đổi hoặc vô hiệu hóa tài khoản mặc định trên phần mềm, thiết bị (như tài khoản root, administrator, tài khoản cấu hình sẵn của nhà cung cấp dịch vụ).

- Quản lý tách biệt giữa các loại tài khoản: tài khoản quản trị, tài khoản tác nghiệp, tài khoản kỹ thuật, tài khoản dịch vụ.

- Mỗi tài khoản truy cập hệ thống phải được gán cho một người sử dụng duy nhất; trường hợp chia sẻ tài khoản dùng chung phải được phê duyệt bởi cấp có thẩm quyền và làm rõ trách nhiệm cá nhân tại mỗi thời điểm sử dụng.

- Quy định về quản lý thiết bị lưu khóa bí mật và khóa bí mật.

- Xóa hoặc vô hiệu hóa các tài khoản không hoạt động sau 45 ngày hoặc ngay khi có thay đổi về nhân sự quản lý, sử dụng, khai thác tài khoản.

- Định kỳ rà soát và cập nhật quy định quản lý tài khoản và các tài liệu liên quan tối thiểu 01 lần/ năm hoặc khi có thay đổi trong tổ chức có ảnh hưởng đến quy định.

6.6.2.4 Xây dựng và tuân thủ quy định quản lý truy cập

Có quy định về quản lý truy cập đáp ứng các yêu cầu sau:

- Nguyên tắc cấp quyền tối thiểu và phân tách nhiệm vụ đối với mọi loại tài khoản.

- Tài liệu hóa các quyền truy cập cần thiết tương ứng với các chức danh, bộ phận trong cơ quan, tổ chức.

- Yêu cầu xác thực MFA đối với truy cập của người dùng từ bên ngoài tổ chức, từ đối tác/ bên thứ ba, từ Internet và truy cập vào tài khoản có quyền quản trị hệ thống.

- Định kỳ rà soát và cập nhật quy định quản lý truy cập và các tài liệu liên quan tối thiểu 01 lần/ năm hoặc khi có thay đổi trong tổ chức có ảnh hưởng đến quy định.

6.6.2.5 Xây dựng và tuân thủ quy trình cấp mới, thay đổi và thu hồi quyền truy cập

a) Có quy trình cấp mới, thay đổi và thu hồi quyền truy cập vào các tài sản CNTT của cơ quan, tổ chức.

b) Định kỳ rà soát quy trình và công tác thực hiện cấp quyền truy cập vào các tài sản CNTT của cơ quan, tổ chức tối thiểu 01 lần/ năm hoặc khi có thay đổi trong tổ chức có ảnh hưởng đến quy trình.

6.7 Quản lý lỗ hổng bảo mật

6.7.1 Khái quát

a) Xây dựng, phát triển kế hoạch đánh giá, theo dõi các lỗ hổng bảo mật thường xuyên để khắc phục và giảm thiểu nguy cơ bị tấn công mạng.

b) Theo dõi, cập nhật thông tin về các mối đe dọa, lỗ hổng bảo mật mới từ nhiều nguồn.

6.7.2 Yêu cầu cụ thể

6.7.2.1 Có quy trình quản lý lỗ hổng bảo mật

a) Có quy trình quản lý lỗ hổng bảo mật cho tài sản công nghệ thông tin của tổ chức. Các nội dung tối thiểu bao gồm:

- Phát hiện lỗ hổng bảo mật: Xây dựng và triển khai các giải pháp để rà quét lỗ hổng bảo mật cho các tài sản phần cứng và phần mềm của cơ quan, tổ chức. Định kỳ thực hiện rà soát tổng thể hệ thống tối thiểu 01 lần/ 06 tháng và rà soát đối với các tài sản quan trọng tối thiểu 01 lần/ quý.

- Đánh giá mức độ nghiêm trọng của lỗ hổng: Thực hiện đánh giá mức độ nghiêm trọng của lỗ hổng, từ đó xác định mức độ ưu tiên của việc khắc phục lỗ hổng.

- Chia sẻ thông tin lỗ hổng: Có cơ chế để chia sẻ thông tin, tiếp nhận và phản hồi báo cáo lỗ hổng bảo mật từ bên liên quan hoặc các nguồn công khai khác.

- Triển khai các biện pháp khắc phục: Có phương án, biện pháp kiểm soát rủi ro, kế hoạch khắc phục cho các lỗ hổng đã phát hiện theo thứ tự ưu tiên và đánh giá lại hệ thống để đảm bảo lỗ hổng đã được khắc phục hoàn toàn.

b) Rà soát, cập nhật quy trình và rà quét lỗ hổng bảo mật tối thiểu 01 lần/ 06 tháng hoặc khi xảy ra thay đổi trong tổ chức ảnh hưởng đến quy trình này.

6.7.2.2 Có quy trình quản lý bản vá

Có quy trình quản lý bản vá. Các nội dung tối thiểu bao gồm:

- Xây dựng và triển khai máy chủ quản lý bản vá tập trung cho toàn bộ tài sản phần cứng và phần mềm thuộc hệ thống thông tin.

- Đánh giá tác động, tiến hành kiểm thử và xây dựng phương án phục hồi trước khi triển khai bản vá trên các hệ thống thông tin có xử lý hoặc lưu trữ dữ liệu quan trọng.

- Thực hiện kiểm tra và cập nhật bản vá hệ điều hành, ứng dụng cho toàn bộ máy tính, thiết bị di động cấp cho người dùng tối thiểu 01 lần/ tháng (nếu có).

- Giám sát và duy trì hệ thống để đảm bảo phát hiện kịp thời các lỗ hổng mới xuất hiện và cập nhật bản vá.

6.8 Quản lý nhật ký an ninh mạng

6.8.1 Khái quát

Thực hiện thu thập, phân tích, giám sát và lưu trữ nhật ký an ninh mạng để phát hiện sớm và ứng phó sự cố tấn công mạng.

6.8.2 Yêu cầu cụ thể

6.8.2.1 Thiết lập quy trình quản lý nhật ký an ninh mạng

a) Có quy định quản lý nhật ký an ninh mạng, trong đó bao gồm:

- Quy định về cách thức ghi nhật ký.

- Quy định về việc thu thập, kiểm tra, lưu trữ nhật ký.

- Quy định các loại nhật ký được thu thập. Thu thập tối thiểu các loại nhật ký sau: nhật ký truy cập hệ thống, nhật ký tiến trình hoạt động, nhật ký ứng dụng, nhật ký truy cập dữ liệu, nhật ký cảnh báo của các thiết bị bảo mật.

- Nhật ký truy cập hệ thống tối thiểu bao gồm: địa chỉ nguồn (IP/ tên máy, tên miền, MAC), địa chỉ đích (IP/ tên máy, tên miền, MAC), tài khoản đích (tên người dùng/ mã định danh), thời điểm xảy ra, thông tin hành vi.

- Nhật ký tiến trình hoạt động tối thiểu bao gồm: thông tin thiết bị (IP/ tên thiết bị, tên miền, MAC), thông tin tiến trình (tên, mã định danh, tiến trình cha, lệnh khởi tạo), tài khoản đích (tên người dùng/ mã định danh), thời điểm xảy ra.

- Nhật ký truy cập dữ liệu tối thiểu bao gồm: địa chỉ nguồn (IP/ tên máy, tên miền, MAC), địa chỉ đích (IP/ tên máy, tên miền, MAC), thông tin hành động (đọc, thêm, sửa, xóa, sao chép), tài khoản đích (tên người dùng/ mã định danh), thời điểm xảy ra.

- Nhật ký cảnh báo tối thiểu bao gồm: tên cảnh báo, thiết bị, mức độ, địa chỉ nguồn, loại cảnh báo, thời điểm xảy ra.

- Nhật ký ứng dụng tối thiểu bao gồm: thông tin truy cập ứng dụng, thông tin đăng nhập khi quản trị ứng dụng, thông tin các lỗi phát sinh trong quá trình hoạt động, thông tin thay đổi cấu hình ứng dụng.

- Đảm bảo việc thu thập nhật ký được áp dụng trên toàn bộ tài sản CNTT.

- Sử dụng máy chủ thời gian để đồng bộ thời gian giữa các thiết bị mạng, thiết bị đầu cuối và các thành phần khác trong hệ thống tham gia giám sát.

- Sử dụng giải pháp SIEM hoặc có phương án tương đương phục vụ quản lý và phân tích sự kiện an ninh mạng tập trung.

- Đảm bảo duy trì không gian lưu trữ nhật ký tối thiểu 06 tháng. Triển khai hệ thống theo dõi tránh tình trạng đầy không gian lưu trữ, dẫn tới thất thoát dữ liệu.

- Kết nối và gửi nhật ký an ninh mạng từ đối tượng giám sát về hệ thống giám sát tập trung.

- Định kỳ thực hiện rà soát nhật ký an ninh mạng tối thiểu 01 lần/ tháng.

b) Kiểm tra và cập nhật tối thiểu 01 lần/ năm hoặc khi có thay đổi ảnh hưởng đến quy trình này.

6.8.2.2 Thu thập nhật ký an ninh mạng của nhà cung cấp dịch vụ

Thực hiện thu thập nhật ký an ninh mạng của các nhà cung cấp dịch vụ đối với các dịch vụ mà hệ thống kết nối, sử dụng.

6.8.2.3 Bảo vệ nhật ký an ninh mạng

a) Kiểm soát truy cập và ghi lại lịch sử tác động tới nhật ký an ninh mạng.

b) Đảm bảo nhật ký an ninh mạng không bị sửa đổi, xóa bỏ.

c) Lưu trữ dữ liệu nhật ký hệ thống trên hệ thống riêng biệt không cùng phân vùng mạng với hệ thống phát sinh dữ liệu nhật ký, mã hóa với những dữ liệu nhật ký quan trọng (nếu có).

6.9 Bảo vệ cho trình duyệt web, dịch vụ thư điện tử

6.9.1 Khái quát

Tăng cường bảo vệ và phát hiện các mối đe dọa từ dịch vụ thư điện tử, trình duyệt web thuộc hệ thống thông tin.

6.9.2 Yêu cầu cụ thể

6.9.2.1 Quản lý trình duyệt web và dịch vụ thư điện tử

a) Có danh sách các trình duyệt web và dịch vụ thư điện tử được phép sử dụng trong cơ quan, tổ chức.

b) Đảm bảo danh sách các trình duyệt web và dịch vụ thư điện tử trên đang trong thời gian hỗ trợ của nhà cung cấp.

c) Sử dụng giải pháp đảm bảo an ninh mạng cho hệ thống thư điện tử hoặc có phương án tương đương.

d) Đảm bảo phiên bản trình duyệt web và dịch vụ thư điện tử được rà soát, cập nhật bản vá lỗ hổng bảo mật thường xuyên hoặc có biện pháp kiểm soát rủi ro tương đương.

6.9.2.2 Sử dụng dịch vụ lọc tên miền

Triển khai sử dụng dịch vụ lọc tên miền trong cơ quan, tổ chức để ngăn chặn các tên miền giả mạo và độc hại.

6.9.2.3 Thực thi, cập nhật các bộ lọc URL và giới hạn số lượng kết nối đến các ứng dụng, dịch vụ

Triển khai và định kỳ cập nhật các bộ lọc URL để hạn chế tài sản kết nối với các trang web độc hại tiềm ẩn hoặc không được chấp thuận.

6.9.2.4 Kiểm soát việc sử dụng các tiện ích mở rộng trong trình duyệt web và dịch vụ thư điện tử

a) Xác định danh sách tiện ích mở rộng được phép sử dụng trong trình duyệt web, dịch vụ thư điện tử.

b) Kiểm soát việc cài đặt và sử dụng các tiện ích mở rộng trong trình duyệt web, dịch vụ thư điện tử.

c) Gỡ cài đặt hoặc vô hiệu hóa các tiện ích mở rộng không được cấp phép.

6.9.2.5 Triển khai giải pháp xác thực email

Triển khai giải pháp xác thực email thông qua DMARC để tăng cường bảo mật và ngăn chặn các cuộc tấn công lừa đảo, giả mạo đối với các tên miền của tổ chức.

6.9.2.6 Quản lý các loại tệp được phép đính kèm trong thư điện tử

a) Xác định danh sách các loại tệp được phép gửi qua hệ thống thư điện tử.

b) Ngăn chặn việc đính kèm những loại tệp không có trong danh sách cho phép và kiểm soát thư điện tử có chứa tệp đính kèm.

6.10 Phòng chống phần mềm độc hại

6.10.1 Khái quát

a) Có quy định để quản lý, phòng chống, khắc phục việc cài đặt, lây lan, thực thi các phần mềm và đoạn mã độc hại trong cơ quan, tổ chức.

b) Triển khai giải pháp phòng chống mã độc cho tất cả tài sản và các điểm kết nối giữa những hệ thống thông tin (bao gồm cả kết nối nội bộ và kết nối ra bên ngoài tổ chức). Giải pháp phòng chống mã độc phải phù hợp và tương thích với hệ thống thông tin của cơ quan, tổ chức, đồng thời có khả năng tự động dò quét, ngăn chặn khi phát hiện mã độc, cập nhật kịp thời các mẫu nhận diện mã độc mới, tích hợp với quy trình quản lý lỗ hổng, ứng phó sự cố.

6.10.2 Yêu cầu cụ thể

6.10.2.1 Triển khai và duy trì phần mềm, giải pháp phòng chống mã độc

a) Triển khai và duy trì phần mềm, giải pháp phòng, chống mã độc hoặc phương án tương đương trên máy chủ, máy tính người dùng.

b) Sử dụng giải pháp phòng, chống mã độc, bao gồm ít nhất các tính năng cơ bản như bảo vệ thời gian thực, phát hiện mã độc dựa trên hành vi, tự động cập nhật các mẫu nhận diện mã độc mới.

6.10.2.2 Thực hiện phòng, chống mã độc đối với các thiết bị lưu trữ ngoài

a) Triển khai rà quét mã độc và vô hiệu hóa tính năng tự động thực thi đối với các phương tiện lưu trữ di động như ổ cứng, thẻ nhớ, USB…

6.10.2.3 Quản lý tập trung các phần mềm phòng, chống mã độc

Quản lý tập trung (cập nhật, cảnh báo và quản lý) các phần mềm phòng chống mã độc cài đặt trên máy chủ và các máy tính người sử dụng trong hệ thống.

6.10.2.4 Kích hoạt tính năng phòng chống khai thác lỗ hổng

Kích hoạt tính năng phòng chống khai thác lỗ hổng trên các tài sản phần cứng và phần mềm (nếu có).

6.10.2.5 Xây dựng và triển khai giải pháp phòng chống mã độc theo hành vi

a) Triển khai giải pháp EDR hoặc phương án tương đương có khả năng phát hiện mã độc, mối nguy dựa trên hành vi trên máy chủ, máy tính người dùng.

b) Kết nối về SIEM để thực hiện giám sát theo thời gian thực và đưa ra cảnh báo.

6.11 Sao lưu và khôi phục dữ liệu

6.11.1 Khái quát

Triển khai và duy trì phương án sao lưu, khôi phục dữ liệu, đảm bảo khôi phục các tài sản về trạng thái tin cậy trước khi có sự cố.

6.11.2 Yêu cầu cụ thể

6.11.2.1 Xây dựng và tuân thủ quy định sao lưu, khôi phục dữ liệu

a) Có quy định sao lưu và khôi phục dữ liệu. Các nội dung tối thiểu bao gồm:

- Định nghĩa các loại dữ liệu cần được sao lưu và khôi phục.

- Thực hiện sao lưu dự phòng tối thiểu các thông tin, dữ liệu sau: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

- Xác định tần suất sao lưu và khôi phục tương ứng với từng loại dữ liệu đã định nghĩa.

- Xác định phương pháp sao lưu và khôi phục tương ứng với từng loại dữ liệu đã định nghĩa.

- Quản lý vùng lưu trữ dữ liệu sao lưu, đảm bảo tính toàn vẹn của dữ liệu và khôi phục dữ liệu một cách nhanh, hiệu quả.

- Định kỳ thực hiện khôi phục dữ liệu đã sao lưu dựa trên mức độ nhạy cảm và tầm quan trọng của dữ liệu nhằm kiểm tra khả năng khôi phục của bản sao lưu.

b) Sử dụng giải pháp quản lý lưu trữ tập trung hoặc có phương án sao lưu dự phòng tập trung đảm bảo tính sẵn sàng cao, cho phép khôi phục dữ liệu nóng khi một thành phần trong hệ thống xảy ra sự cố.

c) Rà soát và cập nhật quy định tối thiểu 01 lần/ năm hoặc khi xảy ra thay đổi trong tổ chức ảnh hưởng đến quy định.

6.11.2.2 Thực hiện sao lưu dữ liệu tự động

a) Xác định danh sách dữ liệu cần sao lưu và phân loại tần suất sao lưu theo thời gian (ngày/tuần/tháng/năm…) đối với từng loại dữ liệu.

b) Triển khai các giải pháp hoặc có biện pháp tương đương đảm bảo sao lưu dữ liệu tự động.

6.11.2.3 Bảo vệ bản sao lưu dữ liệu

a) Áp dụng quy tắc sao lưu 3-2-1 hoặc có biện pháp tương đương bảo vệ bản sao lưu dữ liệu đảm bảo tính toàn vẹn, tính sẵn sàng và khả năng khôi phục của dữ liệu.

b) Thực hiện mã hóa đối với dữ liệu nhạy cảm cao, dữ liệu quan trọng.

6.11.2.4 Thiết lập và duy trì hạ tầng lưu trữ tách biệt cho bản sao lưu dữ liệu

Các bản sao lưu dữ liệu cần phải được định danh, quản lý phiên bản và lưu trữ ở những hạ tầng độc lập, tách biệt với môi trường vận hành.

6.11.2.5 Kiểm tra khả năng khôi phục dữ liệu

Có phương án khôi phục tính nguyên vẹn của dữ liệu. Kiểm tra khả năng khôi phục bản sao lưu dữ liệu tối thiểu 01 lần/ 06 tháng.

6.12 Quản lý hạ tầng mạng

6.12.1 Khái quát

Có phương án thiết lập, thực thi và quản lý thiết bị mạng để phòng ngừa tin tặc khai thác lỗ hổng dịch vụ mạng và các điểm truy cập dễ bị tấn công.

6.12.2 Yêu cầu cụ thể

6.12.2.1 Thiết lập, duy trì các sơ đồ kiến trúc hệ thống mạng và kiến trúc mạng an toàn

a) Thiết lập và duy trì sơ đồ kiến trúc mạng và các hồ sơ khác về hệ thống mạng. Có bộ phận chuyên môn, tổ chức chuyên gia đánh giá hồ sơ thiết kế hệ thống thông tin, các biện pháp đảm bảo an ninh mạng trước khi triển khai thực hiện.

b) Thiết kế kiến trúc hệ thống mạng theo nguyên tắc lấy tài nguyên/dữ liệu làm trung tâm bảo vệ, áp dụng phân đoạn vi mô hoặc có phương án tương đương để cách ly các máy chủ, ứng dụng quan trọng.

c) Triển khai và duy trì một kiến trúc hệ thống mạng an toàn, đảm bảo thực hiện tối thiểu 03 nguyên tắc: phân vùng mạng, đặc quyền ít nhất và tính sẵn sàng.

d) Triển khai kết nối mạng an toàn, bảo đảm an toàn trong quá trình khởi tạo kết nối kênh truyền và trao đổi thông tin qua kênh truyền.

e) Tài liệu hóa sơ đồ kiến trúc hệ thống mạng tối thiểu bao gồm:

- Tổng quan kiến trúc hệ thống mạng.

- Sơ đồ cấp chi tiết của hệ thống mạng.

- Ghi chú các tài liệu đặc tả kỹ thuật, tài liệu thống kê,...

- Tài liệu mô tả phương án đảm bảo an ninh mạng.

f) Xây dựng phương án và thực hiện quản lý và bảo vệ tài liệu, hồ sơ thiết kế.

g) Xem xét và cập nhật sơ đồ mạng 01 lần/ 06 tháng hoặc mỗi khi có thay đổi ảnh hưởng đến sơ đồ hệ thống.

6.12.2.2 Quản lý an toàn cơ sở hạ tầng mạng

a) Thực hiện quản lý an toàn cơ sở hạ tầng mạng, đảm bảo tối thiểu:

- Có phương án dự phòng kết nối mạng cho các máy chủ cung cấp dịch vụ.

- Có phương án cân bằng tải và dự phòng nóng cho các thiết bị mạng chính. Đối với các hệ thống buộc phải có kết nối mạng Internet, xây dựng và triển khai phương án duy trì ít nhất 02 hướng kết nối mạng Internet quốc tế từ các nhà cung cấp dịch vụ trong nước có hạ tầng khác nhau.

- Sử dụng giải pháp tường lửa có tích hợp chức năng phòng, chống xâm nhập hoặc có phương án tương đương phục vụ kiểm soát truy cập, phòng, chống xâm nhập giữa các vùng mạng.

- Sử dụng giải pháp tường lửa tích hợp chức năng phòng, chống mã độc trên môi trường mạng hoặc có phương án tương đương phục vụ phòng, chống mã độc trên môi trường mạng.

- Sử dụng giải pháp DBF hoặc có phương án tương đương bảo đảm an ninh mạng đối với hệ thống cơ sở dữ liệu tập trung.

- Sử dụng giải pháp quản lý truy cập lớp mạng hoặc có phương án tương đương kiểm soát truy cập lớp mạng, kiểm soát truy cập thiết bị đầu cuối, máy tính người dùng kết nối vào mạng.

- Sử dụng giải pháp giám sát hệ thống thông tin tập trung hoặc có phương án tương đương phục vụ giám sát hệ thống thông tin tập trung.

- Sử dụng giải pháp WAF hoặc có phương án tương đương phục vụ phòng chống tấn công ứng dụng web (nếu có).

- Sử dụng dịch vụ của doanh nghiệp hoặc giải pháp phòng, chống tấn công từ chối dịch vụ hoặc có phương án tương đương phòng, chống tấn công từ chối dịch vụ.

- Sử dụng Datadiode, USG, BSG hoặc có phương án kiểm soát rủi ro tương đương để phân vùng, bảo mật, kiểm soát luồng dữ liệu cho vùng mạng lõi, vùng mạng OT với vùng mạng có mức độ tin cậy thấp hơn, bao gồm nhưng không giới hạn: vùng mạng có kết nối Internet, vùng mạng không dây công cộng/ dùng riêng và các mạng kết nối từ xa của bên thứ ba.

- Định kỳ cập nhật cơ sở dữ liệu phát hiện tấn công mạng cho các giải pháp đảm bảo an ninh mạng trong hệ thống thông tin.

- Thực hiện quản lý thay đổi, xây dựng và tuân thủ quy định về việc kết nối và gỡ bỏ hệ thống máy chủ, dịch vụ, thiết bị đầu cuối khỏi hệ thống.

- Kiểm tra hiệu năng (RAM, CPU...), đảm bảo hoạt động bình thường của hệ thống.

- Có phương án bảo đảm an toàn cho mạng không dây (nếu có).

b) Chia tách thành các vùng mạng khác nhau theo đối tượng sử dụng, mục đích sử dụng, tối thiểu:

- Vùng mạng nội bộ.

- Vùng mạng biên.

- Vùng mạng máy chủ nội bộ.

- Vùng mạng trung gian (DMZ) để cung cấp dịch vụ.

- Vùng mạng máy chủ cơ sở dữ liệu.

- Vùng mạng riêng để cung cấp dịch vụ mạng không dây (nếu có).

- Vùng mạng WAN (nếu có).

- Vùng quản trị thiết bị hệ thống.

- Vùng quản trị.

6.12.2.3 Sử dụng các giao thức truyền thông và quản trị mạng an toàn

Cấu hình hệ thống thông tin chỉ sử dụng các giao thức truyền thông và quản trị mạng an toàn (chưa được các tổ chức quốc tế công bố điểm yếu).

6.12.2.4 Kiểm soát truy cập

a) Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập thông tin nội bộ hoặc thực hiện quản trị từ xa đối với tài sản phần cứng và phần mềm.

b) Cấu hình chức năng xác thực trên các thiết bị hệ thống để xác thực người dùng khi quản trị thiết bị trực tiếp hoặc từ xa.

c) Kiểm soát truy cập từ bên ngoài vào hệ thống và từ bên trong hệ thống ra ngoài theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả truy cập tới các tài sản phần cứng và phần mềm mà hệ thống không cung cấp hoặc không cho phép truy cập.

d) Thiết lập giới hạn thời gian chờ (timeout) để tự động đóng các phiên kết nối khi không nhận được yêu cầu từ người dùng trong một khoảng thời gian quy định.

e) Giới hạn số lượng kết nối đồng thời từ một địa chỉ nguồn và tổng số lượng kết nối đồng thời cho từng ứng dụng, dịch vụ được hệ thống cung cấp theo năng lực thực tế của hệ thống, không áp dụng cứng đối với hệ thống/dịch vụ có yêu cầu kết nối lớn nếu đã có biện pháp kiểm soát rủi ro tương đương.

f) Có phương án kiểm soát truy cập của người dùng vào các dịch vụ, các máy chủ nội bộ theo chính sách.

g) Không cho phép hoặc giới hạn truy cập (theo chức năng của máy chủ) từ các máy chủ ra các mạng bên ngoài hệ thống.

6.12.2.5 Xây dựng và áp dụng chính sách quản lý truy cập từ xa

Có chính sách quản lý truy cập từ xa đáp ứng các yêu cầu sau:

- Sử dụng mạng riêng ảo VPN, ZTNA hoặc phương án tương đương và yêu cầu xác thực cho việc truy cập từ xa vào hệ thống đối với người dùng quản trị, người dùng tác nghiệp hệ thống.

- Yêu cầu người dùng xác thực MFA để kết nối truy cập từ xa và xác thực bổ sung trước khi truy cập vào hệ thống.

- Giới hạn các dải địa chỉ mạng hoặc thiết bị cụ thể được phép kết nối để thực hiện quản trị từ xa đối với tài sản phần cứng và phần mềm.

- Không cho phép quản trị, cấu hình thiết bị trực tiếp từ các mạng bên ngoài, trường hợp bắt buộc phải quản trị thiết bị từ xa phải thực hiện gián tiếp thông qua các máy quản trị trong hệ thống và sử dụng kết nối mạng an toàn.

- Các thiết bị được phép truy cập từ xa phải đảm bảo các yêu cầu về bảo mật: cài đặt phần mềm phòng chống mã độc, cấu hình bảo mật theo chính sách an ninh, an toàn đã ban hành của tổ chức.

6.12.2.6 Thiết lập và duy trì tài nguyên hệ thống dành riêng cho công tác quản trị

Thiết lập và duy trì các nguồn tài nguyên dành riêng cho công tác quản trị, tách biệt về mặt vật lý hoặc logic; được phân tách với mạng chính của hệ thống và không kết nối với Internet.

6.12.2.7 Kiểm thử và nghiệm thu hệ thống

a) Thực hiện thử nghiệm và nghiệm thu hệ thống trước khi bàn giao và đưa vào sử dụng.

b) Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống.

c) Có đơn vị độc lập hoặc bộ phận độc lập thuộc cơ quan, tổ chức thực hiện tư vấn, giám sát quá trình thử nghiệm và nghiệm thu hệ thống.

d) Thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng.

e) Có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng.

6.13 Giám sát và phòng thủ an ninh mạng

6.13.1 Khái quát

Xây dựng, vận hành các quy trình và công cụ để thiết lập, duy trì giám sát mạng toàn diện và bảo vệ hệ thống mạng khỏi các mối đe dọa.

6.13.2 Yêu cầu cụ thể

6.13.2.1 Thực hiện giám sát và quản lý tập trung các cảnh báo và sự kiện an ninh mạng

a) Triển khai giám sát an ninh mạng đối với tối thiểu các đối tượng: thiết bị hệ thống, máy chủ, ứng dụng, dịch vụ và các thành phần khác trong hệ thống (nếu có).

b) Triển khai SIEM để liên kết các sự kiện liên quan, phân tích theo hướng dẫn, yêu cầu và quy định của cơ quan, tổ chức có thẩm quyền.

c) Bố trí nguồn lực và tổ chức giám sát an ninh mạng 24/7.

6.13.2.2 Thiết lập và sử dụng tính năng về tường lửa, cảnh báo phát hiện và ngăn chặn xâm nhập của hệ điều hành và hệ thống

Thiết lập và sử dụng tính năng về tường lửa, cảnh báo phát hiện, ngăn chặn xâm nhập của hệ điều hành và hệ thống (nếu có).

6.13.2.3 Thiết lập cấu hình kiểm soát truy cập các cổng kết nối mạng

a) Thiết lập cấu hình trên các thiết bị mạng để kiểm soát truy cập các cổng kết nối mạng nếu thiết bị hỗ trợ.

b) Thay đổi, tách biệt cổng quản trị ứng dụng với cổng cung cấp dịch vụ ứng dụng.

6.13.2.4 Thu thập thông tin dữ liệu mạng

Thu thập nhật ký luồng dữ liệu mạng và/ hoặc dữ liệu lưu lượng từ các thiết bị mạng để rà soát và đưa ra các cảnh báo.

6.13.2.5 Điều chỉnh các ngưỡng cảnh báo sự kiện an ninh mạng

Điều chỉnh ngưỡng cảnh báo sự kiện an ninh mạng tối thiểu 01 lần/ quý.

6.14 Nhân sự vận hành, quản trị hệ thống, bảo vệ an ninh mạng

6.14.1 Khái quát

a) Có cơ chế hoạt động độc lập về chuyên môn giữa các bộ phận vận hành, quản trị, bảo vệ an ninh mạng.

b) Có chương trình đào tạo nâng cao nhận thức an ninh mạng và kỹ năng an ninh mạng.

c) Có trình độ chuyên môn phù hợp với các bộ phận vận hành, quản trị, bảo vệ an ninh mạng.

6.14.2 Yêu cầu cụ thể

6.14.2.1 Có bộ phận phụ trách về vận hành, quản trị hệ thống và bảo vệ an ninh mạng

a) Có các bộ phận riêng biệt vận hành, quản trị hệ thống và bảo vệ an ninh mạng.

b) Có cơ chế hoạt động độc lập về chuyên môn giữa các bộ phận vận hành, quản trị hệ thống và bảo vệ an ninh mạng.

6.14.2.2 Thiết lập và duy trì chương trình đào tạo tổng quan để nâng cao nhận thức an ninh mạng cho cán bộ, nhân viên

a) Có chương trình nâng cao nhận thức an ninh mạng cho toàn bộ cán bộ, nhân viên có sử dụng hệ thống thông tin.

b) Cán bộ chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của tổ chức.

c) Có quy trình và thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.

d) Có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc.

e) Tiến hành đào tạo tối thiểu 01 lần/ năm.

6.14.2.3 Thực hiện đào tạo kiến thức an ninh mạng theo từng vị trí, vai trò cụ thể

a) Thực hiện đào tạo kiến thức chuyên môn an ninh mạng theo từng vị trí, vai trò cụ thể. Đào tạo nhận thức về quy định pháp luật liên quan, trách nhiệm pháp lý cho các cá nhân tham gia bảo vệ an ninh mạng.

b) Tiến hành đào tạo tối thiểu 01 lần/ năm hoặc khi có thay đổi về các nhân sự liên quan trong tổ chức.

6.15 Quản lý nhà cung cấp sản phẩm, dịch vụ

6.15.1 Khái quát

Có quy trình để đánh giá nhà cung cấp sản phẩm, dịch vụ an ninh mạng, lưu trữ, xử lý dữ liệu nhạy cảm hoặc chịu trách nhiệm về các quy trình, nền tảng quan trọng của hệ thống.

6.15.2 Yêu cầu cụ thể

6.15.2.1 Thiết lập và duy trì bản kiểm kê các nhà cung cấp sản phẩm, dịch vụ

Có phương án thiết lập và duy trì bản kiểm kê các nhà cung cấp sản phẩm, dịch vụ. Tối thiểu bao gồm:

- Lập danh sách, theo dõi, cập nhật trạng thái các nhà cung cấp sản phẩm, dịch vụ.

- Thực hiện phân loại các nhà cung cấp dịch vụ trong danh sách quản lý.

- Các nhà cung cấp sản phẩm, dịch vụ an ninh mạng phải đủ điều kiện kinh doanh sản phẩm, dịch vụ an ninh mạng.

- Có văn bản xác định rõ phạm vi trách nhiệm của nhà cung cấp và tổ chức.

- Xem xét và cập nhật danh sách tối thiểu 01 lần/ năm hoặc khi xảy ra thay đổi ảnh hưởng đến danh sách này.

6.15.2.2 Thiết lập và duy trì quy định quản lý nhà cung cấp dịch vụ

a) Có quy định quản lý các nhà cung cấp dịch vụ.

b) Đánh giá và cập nhật quy định tối thiểu 01 lần/ năm hoặc khi xảy ra thay đổi ảnh hưởng đến quy định này.

6.15.2.3 Đảm bảo các hợp đồng cung cấp dịch vụ có kèm theo các yêu cầu bảo mật

a) Đảm bảo các hợp đồng với nhà cung cấp dịch vụ an ninh mạng bao gồm đầy đủ yêu cầu về bảo mật.

b) Đánh giá và cập nhật hợp đồng của nhà cung cấp dịch vụ khi gia hạn để đảm bảo đầy đủ các yêu cầu bảo mật.

6.15.2.4 Thực hiện theo dõi các nhà cung cấp dịch vụ

Giám sát các nhà cung cấp dịch vụ thực hiện quy định quản lý cung cấp dịch vụ của tổ chức.

6.15.2.5 Rà soát vấn đề bảo mật khi kết thúc hợp đồng với các nhà cung cấp dịch vụ

Rà soát vấn đề bảo mật khi kết thúc hợp đồng với các nhà cung cấp dịch vụ.

6.16 Phát triển ứng dụng an toàn

6.16.1 Khái quát

Quản lý vòng đời bảo mật của các phần mềm ứng dụng để phòng ngừa, phát hiện và xử lý các điểm yếu, lỗ hổng bảo mật.

6.16.2 Yêu cầu cụ thể

6.16.2.1 Thiết lập và duy trì quy trình phát triển ứng dụng an toàn

a) Có quy trình phát triển ứng dụng an toàn.

b) Đánh giá và cập nhật quy trình tối thiểu 01 lần/ năm hoặc khi xảy ra các thay đổi có thể ảnh hưởng đến quy trình.

c) Đối với các phần mềm phát triển thuê khoán, yêu cầu:

- Có biên bản, hợp đồng và cam kết bảo mật đối với bên thuê khoán các nội dung liên quan đến phát triển phần mềm thuê khoán.

- Yêu cầu nhà phát triển cung cấp mã nguồn phần mềm. Trong trường hợp không thể cung cấp mã nguồn phần mềm, chủ quản hệ thống phải yêu cầu các bên thuê khoán cung cấp chứng chỉ đánh giá an toàn độc lập hoặc thực hiện các biện pháp kiểm thử xâm nhập, giám sát rủi ro thay thế và ký cam kết chịu trách nhiệm pháp lý về tính an toàn của phần mềm.

- Kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng.

- Kiểm tra, đánh giá an ninh mạng của phần mềm trước khi đưa vào sử dụng.

- Khi thay đổi mã nguồn, kiến trúc phần mềm thực hiện kiểm tra, đánh giá an ninh mạng cho phần mềm.

- Có cam kết của bên phát triển về bảo đảm tính bí mật và bản quyền của phần mềm phát triển.

6.16.2.2 Thiết lập và duy trì quy trình tiếp nhận và xử lý lỗ hổng bảo mật phần mềm

a) Có quy trình tiếp nhận và xử lý báo cáo về lỗ hổng bảo mật phần mềm, bao gồm cả việc cung cấp phương tiện để các cá nhân, tổ chức bên ngoài báo cáo.

b) Đánh giá và cập nhật quy trình tối thiểu 01 lần/ năm hoặc khi xảy ra các thay đổi có thể ảnh hưởng đến quy trình.

6.16.2.3 Thực hiện phân tích nguyên nhân cốt lõi của lỗ hổng bảo mật

Thực hiện phân tích nguyên nhân cốt lõi của các lỗ hổng bảo mật.

6.16.2.4 Thiết lập, quản lý các cấu thành phần mềm của bên thứ ba

a) Thiết lập và quản lý một danh sách cập nhật các thành phần của bên thứ ba được sử dụng trong quá trình phát triển (thư viện, mô-đun…) và các thành phần dự kiến sẽ sử dụng trong tương lai để phát triển phần mềm.

b) Danh sách bao gồm các rủi ro an ninh mạng mà mỗi thành phần bên thứ ba có thể gây ra.

c) Đánh giá và cập nhật danh sách tối thiểu 01 lần/ quý.

6.16.2.5 Tách biệt môi trường cho các hoạt động phát triển, kiểm thử và vận hành

Duy trì việc tách biệt môi trường vận hành chính thức, môi trường kiểm thử và môi trường phát triển. Trong đó yêu cầu không lưu trữ thông tin xác thực, thông tin bí mật trên mã nguồn ứng dụng.

6.16.2.6 Đào tạo về bảo mật và lập trình an toàn

a) Đảm bảo tất cả nhân viên phát triển phần mềm được đào tạo về trách nhiệm và phương thức phát triển phần mềm an toàn đối với từng môi trường/giải pháp cụ thể.

b) Thực hiện đào tạo tối thiểu 01 lần/ năm.

6.16.2.7 Kết hợp các nguyên tắc bảo mật trong kiến trúc ứng dụng

Kết hợp các nguyên tắc bảo mật trong quá trình xây dựng kiến trúc ứng dụng. Trong đó bao gồm nhưng không giới hạn các yêu cầu:

- Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý.

- Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu ra trước khi gửi về máy yêu cầu.

- Có phương án bảo vệ ứng dụng chống lại những dạng tấn công phổ biến.

- Có chức năng kiểm soát lỗi, thông báo lỗi từ ứng dụng.

- Không lưu trữ thông tin xác thực, thông tin bí mật trên mã nguồn ứng dụng.

- Có chức năng tạo lập, duy trì và quản lý phiên làm việc an toàn.

6.16.2.8 Tận dụng các mô-đun hoặc dịch vụ đã được kiểm chứng cho các thành phần bảo mật ứng dụng

a) Tận dụng mô-đun hoặc dịch vụ đã được kiểm chứng cho các thành phần bảo mật của ứng dụng.

b) Chỉ sử dụng thuật toán mã hóa mạnh (chưa được các tổ chức quốc tế công bố điểm yếu), được chuẩn hóa và đánh giá rộng rãi.

c) Ghi nhật ký kiểm toán hành vi của người dùng trong sản phẩm.

6.16.2.9 Tiến hành kiểm tra an ninh, an toàn các ứng dụng

a) Kiểm tra các lỗ hổng bảo mật trong mã nguồn được phát triển, lỗ hổng trong các thư viện, thành phần mở rộng của bên thứ ba mà ứng dụng sử dụng.

b) Kiểm thử xâm nhập và khắc phục các lỗ hổng bảo mật trước khi đưa vào vận hành chính thức.

6.17 Quản trị ứng phó sự cố an ninh mạng

6.17.1 Khái quát

Có kế hoạch, chương trình để phát triển và duy trì khả năng ứng phó sự cố bao gồm chính sách, kế hoạch, thủ tục, vai trò, đào tạo, kênh liên lạc.

6.17.2 Yêu cầu cụ thể

6.17.2.1 Thành lập lực lượng ứng phó sự cố an ninh mạng

a) Chỉ định một người chủ chốt và ít nhất một người dự phòng để quản lý quy trình ứng phó sự cố an ninh mạng.

b) Thiết lập và duy trì đầu mối liên lạc để báo cáo sự cố. Xác minh thông tin liên hệ hàng năm để đảm bảo rằng thông tin được cập nhật.

c) Phân công vị trí, vai trò và trách nhiệm chính của từng thành viên trong lực lượng tham gia ứng phó sự cố.

d) Quy định về trách nhiệm phối hợp với lực lượng ứng phó sự cố an ninh mạng của các phòng ban có liên quan.

6.17.2.2 Thiết lập và duy trì quy trình nội bộ để báo cáo sự cố an ninh mạng

a) Có quy trình nội bộ để báo cáo sự cố an ninh mạng.

b) Thực hiện phân nhóm sự cố an ninh mạng.

c) Đánh giá và cập nhật quy trình tối thiểu 01 lần/ năm hoặc khi xảy ra các thay đổi ảnh hưởng đến quy trình.

6.17.2.3 Thiết lập và duy trì quy trình ứng phó sự cố an ninh mạng

a) Có quy trình ứng phó sự cố, đảm bảo có cơ chế phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ khắc phục sự cố an ninh mạng.

b) Đánh giá và cập nhật quy trình tối thiểu 01 lần/ năm hoặc khi xảy ra các thay đổi ảnh hưởng đến quy trình.

6.17.2.4 Thiết lập cơ chế (kênh kỹ thuật) liên lạc trong quá trình xử lý sự cố

a) Thiết lập cơ chế chính và cơ chế phụ sử dụng để giao tiếp và báo cáo trong xử lý sự cố an ninh mạng.

b) Đánh giá và cập nhật cơ chế liên lạc tối thiểu 01 lần/ năm hoặc khi xảy ra các thay đổi ảnh hưởng đến cơ chế.

6.17.2.5 Thực hiện đánh giá sau sự cố an ninh mạng

Thực hiện đánh giá sau sự cố an ninh mạng.

6.17.2.6 Định kỳ diễn tập ứng phó sự cố an ninh mạng

Có kế hoạch và thực hiện diễn tập các kịch bản ứng phó sự cố định kỳ tối thiểu 01 lần/ năm.

6.17.2.7 Triển khai và duy trì các ngưỡng sự cố an ninh mạng

a) Thiết lập và duy trì các ngưỡng sự cố an ninh mạng.

b) Đánh giá và cập nhật ngưỡng tối thiểu 01 lần/ năm hoặc khi xảy ra các thay đổi ảnh hưởng đến ngưỡng.

6.18 Quản lý kiểm tra an ninh mạng

6.18.1 Khái quát

Xác định tính hiệu quả trong năng lực phòng vệ và khả năng phục hồi của các tài sản thông qua việc đánh giá khả năng khai thác các điểm yếu trong quy trình kiểm soát về con người, quy trình, công nghệ; mô phỏng lại các mục tiêu và hành động tấn công; khắc phục các tồn tại phát hiện được qua kết quả kiểm thử xâm nhập.

6.18.2 Yêu cầu cụ thể

6.18.2.1 Thiết lập và duy trì một chương trình kiểm thử xâm nhập

a) Có chương trình kiểm thử xâm nhập phù hợp với quy mô, mức độ phức tạp và trạng thái của tổ chức.

b) Chương trình kiểm thử xâm nhập cần đáp ứng một số nội dung sau:

- Về yêu cầu: hoạt động kiểm thử xâm nhập phải được phê duyệt về phạm vi, thời gian, phương pháp, đầu mối phối hợp, phương án đảm bảo an ninh mạng và phương án xử lý dữ liệu thu được; đối với hệ thống đang vận hành, phải chọn thời điểm và cách thức kiểm thử phù hợp để không làm gián đoạn dịch vụ, ưu tiên thực hiện trên môi trường phát triển hoặc trong thời gian đã được phê duyệt.

- Về phạm vi tiến hành: kiểm tra một phần hoặc toàn bộ hạ tầng công nghệ thông tin của tổ chức.

- Về tần suất: hàng quý, nửa năm, một năm hoặc đột xuất.

- Về các giới hạn: xác định các hành vi tấn công bị cấm (tấn công vật lý, tấn công lừa đảo, tấn công phi kỹ thuật…).

- Về cách phản ứng của tổ chức: có thực hiện việc ngăn chặn hay không, cơ chế kiểm soát thông tin (về cuộc kiểm thử) trong nội bộ.

6.18.2.2 Định kỳ thực hiện kiểm thử xâm nhập từ bên ngoài

a) Định kỳ thực hiện kiểm thử xâm nhập từ bên ngoài tối thiểu 01 lần/ năm.

b) Áp dụng với các ứng dụng, dịch vụ của tổ chức được công khai ra mạng Internet.

6.18.2.3 Khắc phục các tồn tại phát hiện được qua việc kiểm thử xâm nhập

Khắc phục các tồn tại phát hiện được qua kiểm thử xâm nhập dựa trên chính sách của tổ chức về phạm vi và mức độ ưu tiên khắc phục.

6.18.2.4 Rà soát các biện pháp bảo mật

Kiểm tra, đánh giá hiệu quả các biện pháp bảo mật sau mỗi lần thực hiện kiểm thử xâm nhập.

6.18.2.5 Định kỳ thực hiện kiểm thử xâm nhập từ bên trong

a) Định kỳ thực hiện kiểm thử xâm nhập từ bên trong tối thiểu 01 lần/ năm.

b) Áp dụng với các tài nguyên nội bộ trong hệ thống thông tin của tổ chức.

7 Yêu cầu cơ bản đối với hệ thống thông tin cấp độ 5

7.1 Quản lý rủi ro an ninh mạng

7.1.1 Khái quát

Thực hiện xác định, đánh giá, xử lý rủi ro an ninh mạng và lên kế hoạch ứng phó khi rủi ro xảy ra.

7.1.2 Yêu cầu cụ thể

7.1.2.1 Thiết lập và duy trì quy định, quy trình quản lý rủi ro an ninh mạng

a) Có quy định, quy trình quản lý rủi ro an ninh mạng. Trong đó, yêu cầu thực hiện quản lý rủi ro an ninh mạng bao gồm tối thiểu các bước: xác định, phân tích, đánh giá và xử lý rủi ro an ninh mạng.

b) Đánh giá và cập nhật quy định, quy trình quản lý rủi ro an ninh mạng và các tài liệu liên quan tối thiểu 01 lần/ 06 tháng hoặc khi có thay đổi xảy ra trong tổ chức ảnh hưởng đến các văn bản đã ban hành có liên quan.

7.1.2.2 Xác định rủi ro an ninh mạng

a) Thực hiện xác định rủi ro an ninh mạng trong tổ chức (có thể dựa trên việc quản lý tài sản, quản lý lỗ hổng, quản lý hạ tầng mạng, quản lý nhận thức an ninh mạng, quản lý tài khoản và quyền truy cập…).

b) Xác định rủi ro an ninh mạng đến từ các bên thứ ba, nhà cung cấp.

c) Thực hiện xác định rủi ro an ninh mạng định kỳ tối thiểu 01 lần/ 06 tháng hoặc khi có thay đổi liên quan đến hệ thống thông tin (thay đổi hệ thống, lỗ hổng bảo mật mới, các sự kiện an ninh mạng...).

7.1.2.3 Đánh giá rủi ro an ninh mạng

a) Thực hiện phân tích, đánh giá rủi ro an ninh mạng để xác định mức độ ảnh hưởng, tác động của rủi ro đến tổ chức, từ đó đưa ra quyết định chấp nhận hoặc thực hiện các biện pháp giảm thiểu rủi ro.

b) Thực hiện phân tích và đánh giá rủi ro an ninh mạng ngay sau khi xác định rủi ro; phân tích, đánh giá lại khi có sự thay đổi về hệ thống, các sự kiện an ninh mạng hoặc những thay đổi trong tổ chức liên quan đến rủi ro đã xác định.

7.1.2.4 Xử lý rủi ro an ninh mạng

a) Thực hiện các biện pháp xử lý rủi ro an ninh mạng và xây dựng phương án ứng phó khi rủi ro còn lại (sau khi đã xử lý) xảy ra.

b) Định kỳ tối thiểu 01 lần/ 06 tháng đánh giá và cải thiện hiệu quả của các biện pháp kiểm soát được sử dụng để giảm thiểu rủi ro.

7.1.2.5 Giám sát rủi ro an ninh mạng

Giám sát và cập nhật những thay đổi liên quan đến rủi ro đã được xác định, tối thiểu bao gồm: khả năng xảy ra, mức độ ảnh hưởng, mức độ rủi ro, tài sản bị ảnh hưởng, biện pháp kiểm soát đã áp dụng.

7.1.2.6 Truyền thông rủi ro an ninh mạng

a) Chia sẻ kết quả đánh giá rủi ro cho các bên liên quan.

b) Thông báo kịp thời cho các bên liên quan về thay đổi quan trọng liên quan đến rủi ro.

7.2 Quản lý tài sản phần cứng

7.2.1 Khái quát

a) Lập danh sách, theo dõi, cập nhật trạng thái của tất cả tài sản phần cứng thuộc hệ thống thông tin và các tài sản không thuộc quyền kiểm soát của tổ chức nhưng có kết nối vào hệ thống thông tin; xác định danh sách tài sản cần được giám sát, bảo vệ.

b) Xác định các tài sản vô chủ, tài sản trái phép để loại bỏ hoặc đưa ra phương án quản lý.

c) Thực hiện kiểm kê, rà soát và cập nhật danh sách cho tất cả tài sản thuộc hệ thống thông tin định kỳ tối thiểu 01 lần/ 06 tháng.

7.2.2 Yêu cầu cụ thể

7.2.2.1 Thiết lập và duy trì hệ thống quản lý danh mục tài sản phần cứng

a) Lập danh sách, theo dõi, cập nhật trạng thái của tất cả tài sản phần cứng có khả năng lưu trữ hoặc xử lý dữ liệu, bao gồm: thiết bị của người dùng cuối, thiết bị di động, thiết bị lưu trữ ngoài, thiết bị văn phòng, thiết bị mạng, thiết bị OT/IoT và máy chủ trong môi trường vật lý, ảo hóa, truy cập từ xa và điện toán đám mây.

b) Căn cứ vào điều kiện thực tế, tổ chức thực hiện kiểm tra an ninh tất cả tài sản vật lý đưa vào sử dụng.

c) Danh sách tài sản phần cứng phải bao gồm tối thiểu các thông tin cơ bản sau: tên tài sản, địa chỉ mạng IP (đối với thiết bị đặt địa chỉ IP tĩnh), địa chỉ phần cứng MAC/ mã nhận diện serial, thời gian ngừng hỗ trợ kỹ thuật của hãng (nếu có), vị trí lắp đặt địa lý, vị trí lắp đặt trong hệ thống mạng, mục đích sử dụng, tình trạng sử dụng. Tài sản vật lý phải được giao, gán trách nhiệm cho cá nhân hoặc bộ phận quản lý, sử dụng.

d) Các thiết bị di động do tổ chức quản lý hoặc được tổ chức cho phép kết nối vào hệ thống thông tin phải được đăng ký để kiểm soát. Quy định trách nhiệm của cá nhân trong tổ chức khi sử dụng thiết bị di động để phục vụ công việc.

7.2.2.2 Xử lý các tài sản phần cứng chưa được quản lý

a) Có quy trình phát hiện và xử lý các tài sản phần cứng không có trong danh sách quản lý, đang kết nối trái phép vào hệ thống thông tin định kỳ tối thiểu 01 lần/ tháng.

b) Có thể lựa chọn loại bỏ, từ chối kết nối hoặc cách ly tài sản trái phép.

7.2.2.3 Rà soát các tài sản kết nối vào hệ thống thông tin

a) Có quy định rà quét để phát hiện tài sản kết nối vào hệ thống thông tin định kỳ tối thiểu 01 lần/ tháng.

b) Thực hiện cập nhật danh sách tài sản dựa trên kết quả rà quét.

7.2.2.4 Sử dụng DHCP Logging để cập nhật bản kiểm kê tài sản công nghệ thông tin

a) Sử dụng tính năng ghi nhật ký DHCP trên tất cả các máy chủ DHCP hoặc công cụ quản lý địa chỉ mạng IP (nếu có).

b) Tiến hành rà soát nhật ký để cập nhật danh sách tài sản công nghệ thông tin định kỳ tối thiểu 01 lần/ tháng.

7.2.2.5 Quản lý tài sản thanh lý/ hư hỏng

a) Có quy trình thanh lý/ tiêu hủy tài sản CNTT.

b) Có biện pháp chuyên dụng để xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng.

c) Sao lưu dự phòng thông tin, dữ liệu trên máy chủ, bản dự phòng hệ điều hành máy chủ trước khi thực hiện xóa dữ liệu, hệ điều hành.

d) Có biện pháp kiểm tra, bảo đảm dữ liệu không thể khôi phục sau khi xóa.

7.3 Quản lý tài sản phần mềm

7.3.1 Khái quát

a) Lập danh sách, theo dõi, cập nhật trạng thái của tất cả tài sản phần mềm thuộc hệ thống thông tin của cơ quan, tổ chức, đảm bảo chỉ những phần mềm đã phê duyệt mới được phép cài đặt và sử dụng.

b) Thực hiện kiểm kê, rà soát và cập nhật danh sách cho tất cả tài sản phần mềm định kỳ tối thiểu 01 lần/ 06 tháng.

7.3.2 Yêu cầu cụ thể

7.3.2.1 Thiết lập và duy trì hệ thống quản lý danh mục tài sản phần mềm

a) Lập danh sách, theo dõi, cập nhật trạng thái của tất cả tài sản phần mềm hiện đang được cài đặt trên các tài sản phần cứng thuộc hệ thống thông tin của cơ quan, tổ chức.

b) Danh sách tài sản phần mềm phải bao gồm tối thiểu các thông tin cơ bản sau: tên tài sản, mục đích sử dụng, thời gian ngừng hỗ trợ kỹ thuật (nếu có), phạm vi sử dụng, chủ thể quản lý, thông tin về bản quyền, phiên bản, hệ thống thông tin thành phần (nếu có). Tài sản phần mềm phải được gắn trách nhiệm cho cá nhân hoặc bộ phận quản lý, sử dụng.

7.3.2.2 Thiết lập và duy trì danh sách các tài sản phần mềm được phép sử dụng

a) Lập danh sách, theo dõi, cập nhật danh sách các phần mềm được phép sử dụng trong hệ thống thông tin của cơ quan, tổ chức.

b) Danh sách phần mềm được phép sử dụng phải bao gồm cả các phần mềm được cung cấp bởi nhà cung cấp dịch vụ, các môi trường thực thi cần cài đặt cho ứng dụng.

c) Có quy định kiểm soát việc cài đặt và sử dụng các phần mềm đã được cấp phép, đảm bảo giới hạn đặc quyền tối thiểu các quyền quản trị trên các tài sản CNTT; ngăn chặn các tác vụ thực thi, vô hiệu hóa, cài đặt và gỡ bỏ phần mềm, thư viện, đoạn mã lệnh trái phép trên hệ thống; có phương án kỹ thuật để theo dõi hoạt động cài đặt chương trình phần mềm trên các tài sản CNTT.

d) Định kỳ đánh giá và cập nhật danh sách phần mềm được phép sử dụng tối thiểu 01 lần/ 06 tháng hoặc khi xảy ra các thay đổi trong tổ chức ảnh hưởng đến danh sách.

7.3.2.3 Đảm bảo toàn bộ các tài sản phần mềm được phép sử dụng đang trong thời gian hỗ trợ của nhà cung cấp

Thực hiện định kỳ rà soát danh sách tài sản phần mềm được phép sử dụng và danh sách tài sản phần mềm cài đặt trên các tài sản phần cứng để đảm bảo tất cả tài sản phần mềm đang trong thời gian hỗ trợ của nhà cung cấp, tối thiểu 01 lần/ 06 tháng.

7.3.2.4 Xử lý các tài sản phần mềm trái phép

a) Có quy trình phát hiện và xử lý các phần mềm trái phép định kỳ tối thiểu 01 lần/ tháng.

b) Những phần mềm trái phép nhưng vẫn cần thiết đối với hoạt động của cơ quan, tổ chức phải được đưa vào danh sách ngoại lệ để quản lý. Danh sách ngoại lệ này phải thể hiện chi tiết các biện pháp kiểm soát giảm thiểu nguy cơ an ninh mạng ảnh hưởng đến hệ thống.

c) Những phần mềm trái phép không nằm trong danh sách ngoại lệ phải có kế hoạch để xóa/ gỡ bỏ hoàn toàn khỏi các tài sản phần cứng của cơ quan, tổ chức trong thời gian sớm nhất.

7.4 Quản lý tài sản thông tin

7.4.1 Khái quát

Thực hiện quản lý tài sản thông tin và triển khai các biện pháp kiểm soát để phát hiện, phân loại, xử lý, lưu trữ, loại bỏ tài sản thông tin một cách an toàn.

7.4.2 Yêu cầu cụ thể

7.4.2.1 Thiết lập và duy trì quy định quản lý tài sản thông tin

a) Có quy định quản lý tài sản thông tin. Trong quy định, xác định danh sách tài sản thông tin, mức độ nhạy cảm, chủ sở hữu, các bước xử lý, thời gian lưu trữ và các yêu cầu khi tiêu hủy/xóa bỏ dựa trên các tiêu chuẩn về mức độ bảo mật của tài sản thông tin.

b) Mức độ nhạy cảm của tài sản thông tin có thể được quy định như sau:

- Mức 1: Công khai. Tài sản thông tin công khai không yêu cầu về bảo mật.

- Mức 2: Nội bộ. Tài sản thông tin nội bộ yêu cầu chỉ những người trong tổ chức mới có quyền truy cập.

- Mức 3: Hạn chế truy cập. Tài sản thông tin bị hạn chế yêu cầu quyền truy cập, chỉ những người dùng được cấp quyền mới có thể truy cập vào dữ liệu. Việc tiết lộ tài sản thông tin bị hạn chế truy cập có khả năng ảnh hưởng đến hoạt động của các cơ quan, tổ chức.

- Mức 4: Bí mật nhà nước. Thông tin có nội dung quan trọng, do cơ quan, tổ chức có thẩm quyền xác định; chưa công khai, nếu bị lộ, bị mất có thể gây nguy hại đến lợi ích quốc gia, dân tộc.

c) Có quy trình yêu cầu truy cập, thêm mới, sửa, xóa dữ liệu để kiểm soát truy cập dữ liệu.

d) Kiểm tra cấp độ phân quyền dữ liệu định kỳ tối thiểu 01 lần/ tháng.

e) Đánh giá và cập nhật quy trình quản lý tài sản thông tin định kỳ tối thiểu 01 lần/ 06 tháng hoặc khi xảy ra các thay đổi trong tổ chức ảnh hưởng đến quy trình.

7.4.2.2 Thiết lập và duy trì bản danh sách tài sản thông tin

a) Lập danh sách các tài sản thông tin dựa trên quy trình quản lý tài sản thông tin.

b) Đánh giá và cập nhật danh sách tài sản thông tin tối thiểu 01 lần/ 06 tháng hoặc khi xảy ra thay đổi trong tổ chức ảnh hưởng đến danh sách.

7.4.2.3 Xây dựng danh sách kiểm soát truy cập tài sản thông tin

Xây dựng danh sách quyền truy cập của các tài khoản, người dùng đối với từng loại tài sản thông tin.

7.4.2.4 Mã hóa dữ liệu quan trọng

a) Mã hóa hoặc sử dụng biện pháp kiểm soát rủi ro tương đương để bảo mật thông tin xác thực, dữ liệu có độ nhạy cảm cao, dữ liệu quan trọng được lưu trữ trong các tài sản phần cứng và phần mềm của tổ chức.

b) Mã hóa, ký số hoặc sử dụng biện pháp kiểm soát rủi ro tương đương để bảo vệ thông tin xác thực, dữ liệu có độ nhạy cảm cao, dữ liệu quan trọng trong quá trình truyền gửi.

c) Có phương án chuyên dụng để bảo vệ và quản lý vòng đời mã khóa sử dụng để mã hóa dữ liệu.

d) Sử dụng kết hợp các kết nối mạng an toàn, các biện pháp mã hóa hoặc biện pháp kiểm soát rủi ro tương đương để bảo đảm dữ liệu quan trọng được mã hóa tối thiểu 02 lần khi truyền qua môi trường mạng.

e) Sử dụng các phương pháp mã hóa mạnh (chưa được các tổ chức quốc tế công bố điểm yếu) để mã hóa dữ liệu.

f) Sử dụng thiết bị phần cứng chuyên dụng để phục vụ mã hóa và giải mã.

7.4.2.5 Nguyên vẹn dữ liệu

a) Có phương án quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn.

b) Có phương án giám sát, cảnh báo khi có thay đổi thông tin, dữ liệu lưu trên hệ thống lưu trữ/phương tiện lưu trữ.

c) Có phương án khôi phục tính nguyên vẹn của dữ liệu.

7.4.2.6 Tài liệu hóa luồng dữ liệu

a) Có tài liệu mô tả các luồng dữ liệu trong hệ thống thông tin.

b) Xây dựng và tuân thủ quy định quản lý phiên bản tài liệu tại tổ chức.

c) Đánh giá và cập nhật định kỳ tối thiểu 01 lần/ năm hoặc khi có thay đổi trong tổ chức ảnh hưởng đến tài liệu.

7.4.2.7 Tách biệt quá trình xử lý và lưu trữ dữ liệu theo mức độ nhạy cảm

a) Có quy định về việc xử lý dữ liệu nhạy cảm.

b) Tách biệt tài sản/môi trường xử lý, lưu trữ dữ liệu có độ nhạy cảm cao, dữ liệu quan trọng với dữ liệu có độ nhạy cảm thấp (về mặt logic hoặc vật lý) hoặc có phương án kiểm soát rủi ro tương đương đảm bảo an ninh dữ liệu. Không sử dụng các tài sản/ môi trường dành cho dữ liệu nhạy cảm thấp để lưu trữ và xử lý dữ liệu quan trọng, dữ liệu có mức độ nhạy cảm cao.

c) Sử dụng kênh vật lý riêng hoặc có phương án kiểm soát rủi ro tương đương để bảo mật dữ liệu quan trọng, dữ liệu có độ nhạy cảm cao khi truyền đưa, trao đổi qua môi trường mạng.

7.4.2.8 Triển khai giải pháp phòng chống thất thoát dữ liệu

Xây dựng và triển khai giải pháp chống thất thoát dữ liệu đối với dữ liệu có độ nhạy cảm cao, dữ liệu quan trọng được lưu trữ, xử lý trong hệ thống thông tin.

7.4.2.9 Lưu trữ nhật ký truy cập dữ liệu quan trọng

a) Ghi lại nhật ký hành vi đối dữ liệu có độ nhạy cảm cao, dữ liệu quan trọng.

b) Rà soát nhật ký thường xuyên, định kỳ tối thiểu 01 lần/ tháng để phát hiện sớm những hành vi truy cập trái phép.

7.4.2.10 Sử dụng chữ ký số khi trao đổi thông tin, dữ liệu số quan trọng

a) Sử dụng chữ ký số để ký số và xác thực, kiểm tra tính toàn vẹn khi trao đổi dữ liệu có độ nhạy cảm cao, dữ liệu quan trọng.

b) Chữ ký số được cung cấp bởi cơ quan có thẩm quyền hoặc đơn vị cung cấp dịch vụ chữ ký số được cấp phép.

c) Có phương án bảo đảm an ninh mạng trong việc quản lý và sử dụng chữ ký số.

d) Sử dụng thiết bị, phương tiện chuyên dụng để thực hiện ký và giải mã thông tin, dữ liệu khi gửi và nhận.

7.5 Cấu hình an toàn cho phần cứng và phần mềm

7.5.1 Khái quát

Thiết lập và duy trì cấu hình an toàn cho phần cứng (như thiết bị người dùng cuối bao gồm máy tính, thiết bị di động và cầm tay, thiết bị mạng, thiết bị OT/IoT, máy chủ...) và phần mềm (như hệ điều hành, ứng dụng…).

7.5.2 Yêu cầu cụ thể

7.5.2.1 Thiết lập và duy trì quy định, quy trình cấu hình an toàn cho tài sản phần cứng và phần mềm

a) Có quy định, quy trình cấu hình an toàn cho các tài sản phần cứng và phần mềm của cơ quan, tổ chức.

b) Có các tài liệu cấu hình tiêu chuẩn, tài liệu cấu hình bảo mật nâng cao cho tài sản phần cứng và phần mềm của cơ quan, tổ chức. Đảm bảo sử dụng giao thức kết nối an toàn, thiết lập tường lửa cho máy chủ/ máy trạm và có phương án chống đăng nhập tự động đối với các tài sản xử lý và lưu trữ dữ liệu quan trọng.

c) Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ mà phần cứng, phần mềm không sử dụng.

d) Cấu hình tối ưu và tăng cường bảo mật cho tài sản phần cứng trước khi đưa vào vận hành, khai thác.

e) Đánh giá và cập nhật quy trình quản lý cấu hình an toàn, các tài liệu liên quan tối thiểu 01 lần/ năm hoặc khi có thay đổi xảy ra trong tổ chức ảnh hưởng đến tài liệu.

7.5.2.2 Cấu hình tự động khóa phiên làm việc trên các tài sản phần cứng và phần mềm

a) Dựa trên yêu cầu sử dụng, kết quả đánh giá rủi ro, thực hiện cấu hình tự động khóa phiên làm việc trên các tài sản phần cứng và phần mềm. Có thể thực hiện cấu hình như sau:

- Tự động khóa phiên làm việc trên các tài sản sau một khoảng thời gian không sử dụng:

+ Đối với máy tính người dùng: không quá 15 phút.

+ Đối với các phiên quản trị phần mềm, máy chủ, thiết bị mạng, thiết bị IoT: không quá 05 phút.

+ Đối với thiết bị di động: không quá 05 phút.

+ Đối với các phần mềm nghiệp vụ xử lý dữ liệu quan trọng: không quá 15 phút.

- Tự động khóa thiết bị di động sau một số lần đăng nhập thất bại:

+ Đối với máy tính xách tay: tối đa 10 lần.

+ Đối với điện thoại: tối đa 10 lần.

+ Đối với các phần mềm nghiệp vụ lưu trữ và xử lý dữ liệu quan trọng: tối đa 05 lần.

+ Giới hạn thời gian mở khóa thiết bị sau khi bị khóa: tối thiểu 12 giờ, tối đa 30 ngày.

b) Có cơ chế mở khóa khẩn cấp dành cho quản trị viên/tài khoản đặc quyền.

7.5.2.3 Gỡ bỏ hoặc vô hiệu hóa các tính năng, dịch vụ không cần thiết trên các tài sản phần cứng và phần mềm

Có quy định gỡ bỏ hoặc vô hiệu hóa các tính năng, dịch vụ không cần thiết trên các tài sản phần cứng và phần mềm.

7.5.2.4 Cấu hình máy chủ DNS tin cậy

Thiết lập các cấu hình máy chủ DNS tin cậy trên các tài sản phần cứng nếu có.

7.5.2.5 Thiết lập khả năng xóa sạch dữ liệu từ xa trên thiết bị di động cấp cho người dùng

Xây dựng và triển khai giải pháp xóa sạch dữ liệu từ xa trên thiết bị di động cấp cho người dùng.

7.5.2.6 Phân tách các không gian làm việc riêng biệt trên các thiết bị di động cấp cho người dùng

a) Có quy định tách biệt các không gian làm việc riêng biệt trên thiết bị di động cấp cho người dùng.

b) Xây dựng giải pháp kỹ thuật cho phép quản lý thiết bị di động khi người dùng sử dụng hoặc kết nối tới các hệ thống của tổ chức.

7.6 Quản lý tài khoản và quyền truy cập tài khoản của người dùng

7.6.1 Khái quát

a) Có quy trình, công cụ để phân quyền và quản lý quyền truy cập của tài khoản người dùng bao gồm: tài khoản quản trị, tài khoản tác nghiệp (tài khoản của người dùng cuối tác nghiệp), tài khoản kỹ thuật (tài khoản dùng để kết nối giữa các hệ thống kỹ thuật), tài khoản dịch vụ (tài khoản cấp cho người thụ hưởng dịch vụ) trên các tài sản phần cứng và phần mềm.

b) Có quy trình tạo, gán, quản lý, thu hồi đặc quyền và quyền truy cập đối với các tài khoản người dùng cho tài sản phần cứng và phần mềm. Quyền truy cập của tài khoản quản trị, tài khoản tác nghiệp, tài khoản kỹ thuật, tài khoản dịch vụ phải nhất quán dựa trên vai trò và các yêu cầu cụ thể, đảm bảo người dùng chỉ có quyền truy cập vào dữ liệu, tài sản phù hợp.

c) Ghi nhật ký và giám sát tài khoản người dùng.

7.6.2 Yêu cầu cụ thể

7.6.2.1 Thiết lập và duy trì hệ thống quản lý tài khoản

a) Lập danh sách, theo dõi và cập nhật tất cả tài khoản trên các tài sản phần cứng và phần mềm của tổ chức.

b) Danh sách tài khoản phải bao gồm tối thiểu các loại tài khoản sau: tài khoản quản trị, tài khoản tác nghiệp và tài khoản kỹ thuật.

c) Danh sách tài khoản phải bao gồm các thông tin tối thiểu: loại tài khoản, tên tài khoản, trạng thái tài khoản, tên tài sản/ hệ thống thông tin tương ứng, tên người quản lý, phòng ban, ngày kích hoạt tài khoản, ngày vô hiệu hóa tài khoản (nếu có). Đảm bảo tất cả tài khoản đang hoạt động là hợp lệ.

d) Danh sách tài khoản phải được rà soát định kỳ tối thiểu 01 lần/ tháng.

7.6.2.2 Xây dựng và tuân thủ quy định sử dụng mật khẩu

a) Thiết lập cấu hình mật khẩu trên tài sản phần cứng, phần mềm để đảm bảo an toàn mật khẩu người sử dụng, bao gồm các yêu cầu sau:

- Yêu cầu thay đổi mật khẩu mặc định.

- Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự.

- Thiết lập thời gian yêu cầu thay đổi mật khẩu.

- Thiết lập thời gian mật khẩu hợp lệ.

b) Dựa trên yêu cầu sử dụng, kết quả đánh giá rủi ro, triển khai quy định sử dụng mật khẩu an toàn trong tổ chức. Có thể thực hiện cấu hình như sau:

- Sử dụng mật khẩu duy nhất cho mỗi tài sản hoặc sử dụng giải pháp xác thực và quản lý tập trung.

- Yêu cầu thay đổi mật khẩu trong lần đăng nhập đầu tiên.

- Đối với các hệ thống sử dụng xác thực MFA, quy định mật khẩu có tối thiểu 08 ký tự.

- Đối với các hệ thống không sử dụng xác thực MFA, quy định mật khẩu có tối thiểu 14 ký tự, bao gồm ký tự viết thường, ký tự viết hoa, ký tự đặc biệt, chữ số.

- Đối với tài khoản quản trị cần triển khai xác thực MFA, thay đổi mật khẩu định kỳ tối thiểu 01 lần/02 tháng và mật khẩu mới không được trùng với 10 mật khẩu trước đó.

7.6.2.3 Xây dựng và tuân thủ quy định quản lý tài khoản

Có quy định quản lý tài khoản trong tổ chức đáp ứng các yêu cầu sau:

- Sử dụng giải pháp quản lý tài khoản đặc quyền hoặc có phương án tương đương phục quản lý tài khoản đặc quyền.

- Quản lý tài khoản tập trung.

- Thay đổi hoặc vô hiệu hóa tài khoản mặc định trên phần mềm, thiết bị (như tài khoản root, administrator, tài khoản cấu hình sẵn của nhà cung cấp dịch vụ).

- Quản lý tách biệt giữa các loại tài khoản: tài khoản quản trị, tài khoản tác nghiệp, tài khoản kỹ thuật, tài khoản dịch vụ.

- Mỗi tài khoản truy cập hệ thống phải được gán cho một người sử dụng duy nhất; trường hợp chia sẻ tài khoản dùng chung phải được phê duyệt bởi cấp có thẩm quyền và làm rõ trách nhiệm cá nhân tại mỗi thời điểm sử dụng.

- Quy định về quản lý thiết bị lưu khóa bí mật và khóa bí mật.

- Xóa hoặc vô hiệu hóa các tài khoản không hoạt động sau 45 ngày hoặc ngay khi có thay đổi về nhân sự quản lý, sử dụng, khai thác tài khoản.

- Định kỳ rà soát và cập nhật quy định quản lý tài khoản và các tài liệu liên quan tối thiểu 01 lần/ năm hoặc khi có thay đổi trong tổ chức có ảnh hưởng đến quy định.

7.6.2.4 Xây dựng và tuân thủ quy định quản lý truy cập

Có quy định về quản lý truy cập đáp ứng các yêu cầu sau:

- Nguyên tắc cấp quyền tối thiểu và phân tách nhiệm vụ đối với mọi loại tài khoản.

- Tài liệu hóa các quyền truy cập cần thiết tương ứng với các chức danh, bộ phận trong cơ quan, tổ chức.

- Yêu cầu xác thực MFA đối với truy cập của người dùng từ bên ngoài tổ chức, từ đối tác/ bên thứ ba, từ Internet và truy cập vào tài khoản có quyền quản trị hệ thống.

- Định kỳ rà soát và cập nhật quy định quản lý truy cập và các tài liệu liên quan tối thiểu 01 lần/ năm hoặc khi có thay đổi trong tổ chức có ảnh hưởng đến quy định.

7.6.2.5 Xây dựng và tuân thủ quy trình cấp mới, thay đổi và thu hồi quyền truy cập

a) Có quy trình cấp mới, thay đổi và thu hồi quyền truy cập vào các tài sản CNTT của cơ quan, tổ chức.

b) Định kỳ rà soát quy trình và công tác thực hiện cấp quyền truy cập vào các tài sản CNTT của cơ quan, tổ chức tối thiểu 01 lần/ 06 tháng hoặc khi có thay đổi trong tổ chức có ảnh hưởng đến quy trình.

7.7 Quản lý lỗ hổng bảo mật

7.7.1 Khái quát

a) Xây dựng, phát triển kế hoạch đánh giá, theo dõi các lỗ hổng bảo mật thường xuyên để khắc phục và giảm thiểu nguy cơ bị tấn công mạng.

b) Theo dõi, cập nhật thông tin về các mối đe dọa, lỗ hổng bảo mật mới từ nhiều nguồn.

7.7.2 Yêu cầu cụ thể

7.7.2.1 Có quy trình quản lý lỗ hổng bảo mật

a) Có quy trình quản lý lỗ hổng bảo mật cho tài sản công nghệ thông tin của tổ chức. Các nội dung tối thiểu bao gồm:

- Phát hiện lỗ hổng bảo mật: Xây dựng và triển khai các giải pháp để rà quét lỗ hổng bảo mật cho các tài sản phần cứng và phần mềm của cơ quan, tổ chức. Định kỳ thực hiện rà soát tổng thể hệ thống tối thiểu 01 lần/ quý và rà soát đối với các tài sản quan trọng tối thiểu 01 lần/ tháng.

- Đánh giá mức độ nghiêm trọng của lỗ hổng: Thực hiện đánh giá mức độ nghiêm trọng của lỗ hổng, từ đó xác định mức độ ưu tiên của việc khắc phục lỗ hổng.

- Chia sẻ thông tin lỗ hổng: Có cơ chế để chia sẻ thông tin, tiếp nhận và phản hồi báo cáo lỗ hổng bảo mật từ bên liên quan hoặc các nguồn công khai khác.

- Triển khai các biện pháp khắc phục: Có phương án, biện pháp kiểm soát rủi ro, kế hoạch khắc phục cho các lỗ hổng đã phát hiện theo thứ tự ưu tiên và đánh giá lại hệ thống để đảm bảo lỗ hổng đã được khắc phục hoàn toàn.

b) Rà soát, cập nhật quy trình và rà quét lỗ hổng bảo mật tối thiểu 01 lần/ quý hoặc khi xảy ra thay đổi trong tổ chức ảnh hưởng đến quy trình này.

7.7.2.2 Có quy trình quản lý bản vá

Có quy trình quản lý bản vá. Các nội dung tối thiểu bao gồm:

- Xây dựng và triển khai máy chủ quản lý bản vá tập trung cho toàn bộ tài sản phần cứng và phần mềm thuộc hệ thống thông tin.

- Đánh giá tác động, tiến hành kiểm thử và xây dựng phương án phục hồi trước khi triển khai bản vá trên các hệ thống thông tin có xử lý hoặc lưu trữ dữ liệu quan trọng.

- Thực hiện kiểm tra và cập nhật bản vá hệ điều hành, ứng dụng cho toàn bộ máy tính, thiết bị di động cấp cho người dùng tối thiểu 01 lần/ tháng (nếu có).

- Giám sát và duy trì hệ thống để đảm bảo phát hiện kịp thời các lỗ hổng mới xuất hiện và cập nhật bản vá.

7.8 Quản lý nhật ký an ninh mạng

7.8.1 Khái quát

Thực hiện thu thập, phân tích, giám sát và lưu trữ nhật ký an ninh mạng để phát hiện sớm và ứng phó sự cố tấn công mạng.

7.8.2 Yêu cầu cụ thể

7.8.2.1 Có quy trình quản lý nhật ký an ninh mạng

a) Có quy định quản lý nhật ký an ninh mạng, trong đó bao gồm:

- Quy định về cách thức ghi nhật ký.

- Quy định về việc thu thập, kiểm tra, lưu trữ nhật ký.

- Quy định các loại nhật ký được thu thập. Thu thập tối thiểu các loại nhật ký sau: nhật ký truy cập hệ thống, nhật ký tiến trình hoạt động, nhật ký ứng dụng, nhật ký truy cập dữ liệu, nhật ký cảnh báo của các thiết bị bảo mật.

- Nhật ký truy cập hệ thống tối thiểu bao gồm: địa chỉ nguồn (IP/ tên máy, tên miền, MAC), địa chỉ đích (IP/ tên máy, tên miền, MAC), tài khoản đích (tên người dùng/ mã định danh), thời điểm xảy ra, thông tin hành vi.

- Nhật ký tiến trình hoạt động tối thiểu bao gồm: thông tin thiết bị (IP/ tên thiết bị, tên miền, MAC), thông tin tiến trình (tên, mã định danh, tiến trình cha, lệnh khởi tạo), tài khoản đích (tên người dùng/ mã định danh), thời điểm xảy ra.

- Nhật ký cảnh báo tối thiểu bao gồm: tên cảnh báo, thiết bị, mức độ, địa chỉ nguồn, loại cảnh báo, thời điểm xảy ra.

- Nhật ký ứng dụng tối thiểu bao gồm: thông tin truy cập ứng dụng, thông tin đăng nhập khi quản trị ứng dụng, thông tin các lỗi phát sinh trong quá trình hoạt động, thông tin thay đổi cấu hình ứng dụng.

- Nhật ký truy cập dữ liệu tối thiểu bao gồm: địa chỉ nguồn (IP/ tên máy, tên miền, MAC), địa chỉ đích (IP/ tên máy, tên miền, MAC), thông tin hành động (đọc, thêm, sửa, xóa, sao chép), tài khoản đích (tên người dùng/ mã định danh), thời điểm xảy ra.

- Đảm bảo việc thu thập nhật ký được áp dụng trên toàn bộ tài sản CNTT.

- Sử dụng máy chủ thời gian để đồng bộ thời gian giữa các thiết bị mạng, thiết bị đầu cuối và các thành phần khác trong hệ thống tham gia giám sát.

- Sử dụng giải pháp SIEM hoặc có phương án tương đương phục vụ quản lý và phân tích sự kiện an ninh mạng tập trung.

- Đảm bảo duy trì không gian lưu trữ nhật ký tối thiểu 12 tháng. Triển khai hệ thống theo dõi tránh tình trạng đầy không gian lưu trữ, dẫn tới thất thoát dữ liệu.

- Kết nối và gửi nhật ký an ninh mạng từ đối tượng giám sát về hệ thống giám sát tập trung.

- Định kỳ thực hiện rà soát nhật ký an ninh mạng tối thiểu 01 lần/ tháng.

b) Kiểm tra và cập nhật tối thiểu 01 lần/ năm hoặc khi có thay đổi ảnh hưởng đến quy trình này.

7.8.2.2 Thu thập nhật ký an ninh mạng của nhà cung cấp dịch vụ

Thực hiện thu thập nhật ký an ninh mạng của các nhà cung cấp dịch vụ đối với các dịch vụ mà tổ chức sử dụng.

7.8.2.3 Bảo vệ nhật ký an ninh mạng

a) Kiểm soát truy cập và ghi lại lịch sử tác động tới nhật ký an ninh mạng.

b) Đảm bảo nhật ký an ninh mạng không bị sửa đổi, xóa bỏ.

c) Lưu trữ dữ liệu nhật ký an ninh mạng trên hệ thống riêng biệt không cùng phân vùng mạng với hệ thống phát sinh dữ liệu nhật ký, mã hóa với những dữ liệu nhật ký quan trọng (nếu có).

7.9 Bảo vệ cho trình duyệt web, dịch vụ thư điện tử

7.9.1 Khái quát

Tăng cường bảo vệ và phát hiện các mối đe dọa từ dịch vụ thư điện tử, trình duyệt web thuộc hệ thống thông tin.

7.9.2 Yêu cầu cụ thể

7.9.2.1 Quản lý trình duyệt web và dịch vụ thư điện tử

a) Có danh sách các trình duyệt web và dịch vụ thư điện tử được phép sử dụng trong cơ quan, tổ chức.

b) Đảm bảo danh sách các trình duyệt web và dịch vụ thư điện tử trên đang trong thời gian hỗ trợ của nhà cung cấp.

c) Sử dụng giải pháp đảm bảo an ninh mạng cho hệ thống thư điện tử hoặc có phương án tương đương.

d) Đảm bảo phiên bản trình duyệt web và dịch vụ thư điện tử được rà soát, cập nhật bản vá lỗ hổng bảo mật thường xuyên hoặc có biện pháp kiểm soát rủi ro tương đương.

7.9.2.2 Sử dụng dịch vụ lọc tên miền

Triển khai sử dụng dịch vụ lọc tên miền trong cơ quan, tổ chức để ngăn chặn các tên miền giả mạo và độc hại.

7.9.2.3 Thực thi, cập nhật các bộ lọc URL và giới hạn số lượng kết nối đến các ứng dụng, dịch vụ

Triển khai và định kỳ cập nhật các bộ lọc URL để hạn chế tài sản kết nối với các trang web độc hại tiềm ẩn hoặc không được chấp thuận.

7.9.2.4 Kiểm soát việc sử dụng các tiện ích mở rộng trong trình duyệt web và dịch vụ thư điện tử

a) Xác định danh sách tiện ích mở rộng được phép sử dụng trong trình duyệt web, dịch vụ thư điện tử.

b) Kiểm soát việc cài đặt và sử dụng các tiện ích mở rộng trong trình duyệt web, dịch vụ thư điện tử.

c) Gỡ cài đặt hoặc vô hiệu hóa các tiện ích mở rộng không được cấp phép.

7.9.2.5 Triển khai giải pháp xác thực email

Triển khai giải pháp xác thực email thông qua DMARC để tăng cường bảo mật và ngăn chặn các cuộc tấn công lừa đảo, giả mạo đối với các tên miền của tổ chức.

7.9.2.6 Quản lý các loại tệp được phép đính kèm trong thư điện tử

a) Xác định danh sách các loại tệp được phép gửi qua hệ thống thư điện tử.

b) Ngăn chặn việc đính kèm những loại tệp không có trong danh sách cho phép và kiểm soát thư điện tử có chứa tệp đính kèm.

7.9.2.7 Triển khai và duy trì biện pháp bảo vệ mã độc đối với máy chủ thư điện tử

Xây dựng và triển khai các phương án bảo vệ mã độc đối với máy chủ thư điện tử.

7.10 Phòng chống phần mềm độc hại

7.10.1 Khái quát

a) Có quy định để quản lý, phòng chống, khắc phục việc cài đặt, lây lan, thực thi các phần mềm và đoạn mã độc hại trong cơ quan, tổ chức.

b) Triển khai giải pháp phòng chống mã độc cho tất cả tài sản và các điểm kết nối giữa những hệ thống thông tin (bao gồm cả kết nối nội bộ và kết nối ra bên ngoài tổ chức). Giải pháp phòng chống mã độc phải phù hợp và tương thích với hệ thống thông tin của cơ quan, tổ chức, đồng thời có khả năng tự động dò quét, ngăn chặn khi phát hiện mã độc, cập nhật kịp thời các mẫu nhận diện mã độc mới, tích hợp với quy trình quản lý lỗ hổng, ứng phó sự cố.

7.10.2 Yêu cầu cụ thể

7.10.2.1 Triển khai và duy trì phần mềm, giải pháp phòng chống mã độc

a) Triển khai và duy trì phần mềm, giải pháp phòng, chống mã độc hoặc phương án tương đương trên máy chủ, máy tính người dùng.

b) Sử dụng giải pháp phòng, chống mã độc, bao gồm ít nhất các tính năng cơ bản như bảo vệ thời gian thực, phát hiện mã độc dựa trên hành vi, tự động cập nhật các mẫu nhận diện mã độc mới.

7.10.2.2 Thực hiện phòng, chống mã độc đối với các thiết bị lưu trữ ngoài

Triển khai rà quét mã độc và vô hiệu hóa tính năng tự động thực thi đối với các phương tiện lưu trữ di động như ổ cứng, thẻ nhớ, USB…

7.10.2.3 Quản lý tập trung các phần mềm phòng, chống mã độc

Quản lý tập trung (cập nhật, cảnh báo và quản lý) các phần mềm phòng chống mã độc cài đặt trên máy chủ và các máy tính người sử dụng trong hệ thống.

7.10.2.4 Kích hoạt tính năng phòng chống khai thác lỗ hổng

Kích hoạt tính năng phòng chống khai thác lỗ hổng trên các tài sản phần cứng và phần mềm (nếu có).

7.10.2.5 Xây dựng và triển khai giải pháp phòng chống mã độc theo hành vi

a) Triển khai giải pháp EDR hoặc phương án tương đương có khả năng phát hiện mã độc, mối nguy dựa trên hành vi trên máy chủ, máy tính người dùng.

b) Kết nối về SIEM để thực hiện giám sát theo thời gian thực và đưa ra cảnh báo.

7.11 Sao lưu và khôi phục dữ liệu

7.11.1 Khái quát

Triển khai và duy trì phương án sao lưu, khôi phục dữ liệu, đảm bảo khôi phục các tài sản về trạng thái tin cậy trước khi có sự cố.

7.11.2 Yêu cầu cụ thể

7.11.2.1 Xây dựng và tuân thủ quy định sao lưu, khôi phục dữ liệu

a) Có quy định sao lưu và khôi phục dữ liệu. Các nội dung tối thiểu bao gồm:

- Định nghĩa các loại dữ liệu cần được sao lưu và khôi phục.

- Thực hiện sao lưu dự phòng tối thiểu các thông tin, dữ liệu sau: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

- Xác định tần suất sao lưu và khôi phục tương ứng với từng loại dữ liệu đã định nghĩa.

- Xác định phương pháp sao lưu và khôi phục tương ứng với từng loại dữ liệu đã định nghĩa.

- Quản lý vùng lưu trữ dữ liệu sao lưu, đảm bảo tính toàn vẹn của dữ liệu và khôi phục dữ liệu một cách nhanh, hiệu quả.

- Định kỳ thực hiện khôi phục dữ liệu đã sao lưu dựa trên mức độ nhạy cảm và tầm quan trọng của dữ liệu nhằm kiểm tra khả năng khôi phục của bản sao lưu.

b) Sử dụng giải pháp quản lý lưu trữ tập trung hoặc có phương án sao lưu dự phòng tập trung đảm bảo tính sẵn sàng cao, cho phép khôi phục dữ liệu nóng khi một thành phần trong hệ thống xảy ra sự cố.

c) Rà soát và cập nhật quy định tối thiểu 01 lần/ năm hoặc khi xảy ra thay đổi trong tổ chức ảnh hưởng đến quy định.

7.11.2.2 Thực hiện sao lưu dữ liệu tự động

a) Xác định danh sách dữ liệu cần sao lưu và phân loại tần suất sao lưu theo thời gian (ngày/tuần/tháng/năm…) đối với từng loại dữ liệu.

b) Triển khai các giải pháp hoặc có biện pháp tương đương đảm bảo sao lưu dữ liệu tự động.

7.11.2.3 Bảo vệ bản sao lưu dữ liệu

a) Áp dụng quy tắc sao lưu 3-2-1 hoặc có biện pháp tương đương bảo vệ bản sao lưu dữ liệu đảm bảo tính toàn vẹn, tính sẵn sàng và khả năng khôi phục của dữ liệu.

b) Thực hiện mã hóa đối với dữ liệu nhạy cảm cao, dữ liệu quan trọng.

7.11.2.4 Thiết lập và duy trì hạ tầng lưu trữ tách biệt cho bản sao lưu dữ liệu

a) Các bản sao lưu dữ liệu cần phải được định danh, quản lý phiên bản và lưu trữ ở những hạ tầng độc lập, tách biệt với môi trường vận hành.

b) Lưu trữ dự phòng các dữ liệu quan trọng, dữ liệu có độ nhạy cảm cao trên hệ thống/phương tiện lưu trữ dự phòng ở vị trí địa lý khác nhau; bảo đảm môi trường bảo quản và phương pháp quản lý giống như với hệ thống chính.

c) Duy trì ít nhất 02 kết nối mạng từ hệ thống sao lưu dự phòng chính với hệ thống sao lưu dự phòng phụ.

7.11.2.5 Kiểm tra khả năng khôi phục dữ liệu

Có phương án khôi phục tính nguyên vẹn của dữ liệu. Kiểm tra khả năng khôi phục bản sao lưu dữ liệu tối thiểu 01 lần/ quý.

7.12 Quản lý hạ tầng mạng

7.12.1 Khái quát

Có phương án thiết lập, thực thi và quản lý thiết bị mạng để phòng ngừa tin tặc khai thác lỗ hổng dịch vụ mạng và các điểm truy cập dễ bị tấn công.

7.12.2 Yêu cầu cụ thể

7.12.2.1 Thiết lập, duy trì các sơ đồ kiến trúc hệ thống mạng và kiến trúc mạng an toàn

a) Thiết lập và duy trì sơ đồ kiến trúc mạng và các hồ sơ khác về hệ thống mạng. Có bộ phận chuyên môn, tổ chức chuyên gia đánh giá hồ sơ thiết kế hệ thống thông tin, các biện pháp đảm bảo an ninh mạng trước khi triển khai thực hiện.

b) Thiết kế kiến trúc hệ thống mạng theo nguyên tắc Zero trust, lấy tài nguyên/dữ liệu làm trung tâm bảo vệ, áp dụng phân đoạn vi mô để cách ly các máy chủ, ứng dụng quan trọng.

c) Triển khai và duy trì một kiến trúc hệ thống mạng an toàn, đảm bảo thực hiện tối thiểu 03 nguyên tắc: phân vùng mạng, đặc quyền ít nhất và tính sẵn sàng.

d) Triển khai kết nối mạng an toàn, bảo đảm an toàn trong quá trình khởi tạo kết nối kênh truyền và trao đổi thông tin qua kênh truyền.

e) Tài liệu hóa sơ đồ kiến trúc hệ thống mạng tối thiểu bao gồm:

- Tổng quan kiến trúc hệ thống mạng.

- Sơ đồ cấp chi tiết của hệ thống mạng.

- Ghi chú các tài liệu đặc tả kỹ thuật, tài liệu thống kê,...

- Tài liệu mô tả phương án đảm bảo an ninh mạng.

f) Xây dựng phương án và thực hiện quản lý và bảo vệ tài liệu, hồ sơ thiết kế.

g) Xem xét và cập nhật sơ đồ mạng 01 lần/ quý hoặc mỗi khi có thay đổi ảnh hưởng đến sơ đồ hệ thống.

7.12.2.2 Quản lý an toàn cơ sở hạ tầng mạng

a) Thực hiện quản lý an toàn cơ sở hạ tầng mạng, đảm bảo tối thiểu:

- Có phương án dự phòng hệ thống ở vị trí địa lý khác nhau, cách nhau tối thiểu 30 km.

- Có phương án dự phòng cho kết nối mạng giữa các hệ thống chính và dự phòng.

- Có phương án dự phòng kết nối mạng cho các máy chủ cung cấp dịch vụ.

- Có phương án cân bằng tải và dự phòng nóng cho các thiết bị mạng chính. Đối với các hệ thống buộc phải có kết nối mạng Internet, xây dựng và triển khai phương án duy trì ít nhất 02 hướng kết nối mạng Internet quốc tế từ các nhà cung cấp dịch vụ trong nước có hạ tầng khác nhau.

- Sử dụng giải pháp tường lửa có tích hợp chức năng phòng, chống xâm nhập hoặc có phương án tương đương phục vụ kiểm soát truy cập, phòng, chống xâm nhập giữa các vùng mạng.

- Sử dụng giải pháp tường lửa tích hợp chức năng phòng, chống mã độc trên môi trường mạng hoặc có phương án tương đương phục vụ phòng, chống mã độc trên môi trường mạng.

- Sử dụng giải pháp DBF hoặc có phương án tương đương bảo đảm an ninh mạng đối với hệ thống cơ sở dữ liệu tập trung.

- Sử dụng giải pháp quản lý truy cập lớp mạng hoặc có phương án tương đương kiểm soát truy cập lớp mạng, kiểm soát truy cập thiết bị đầu cuối, máy tính người dùng kết nối vào mạng.

- Sử dụng giải pháp WAF hoặc có phương án tương đương phục vụ phòng chống tấn công ứng dụng web (nếu có).

- Sử dụng giải pháp giám sát hệ thống thông tin tập trung hoặc có phương án tương đương phục vụ giám sát hệ thống thông tin tập trung.

- Sử dụng dịch vụ của doanh nghiệp hoặc sản phẩm phòng, chống tấn công từ chối dịch vụ hoặc có phương án tương đương phòng, chống tấn công từ chối dịch vụ.

- Tách biệt, cô lập vật lý hoặc sử dụng Datadiode, USG, BSG hoặc có phương án kiểm soát rủi ro tương đương phân vùng, bảo mật, kiểm soát luồng dữ liệu cho vùng mạng lõi, vùng mạng OT với vùng mạng có mức độ tin cậy thấp hơn, bao gồm nhưng không giới hạn: vùng mạng có kết nối Internet, vùng mạng không dây công cộng/ dùng riêng và các mạng kết nối từ xa của bên thứ ba.

- Định kỳ cập nhật cơ sở dữ liệu phát hiện tấn công mạng cho các giải pháp đảm bảo an ninh mạng trong hệ thống thông tin.

- Thực hiện quản lý thay đổi, xây dựng và tuân thủ quy định về việc kết nối và gỡ bỏ hệ thống máy chủ, dịch vụ, thiết bị đầu cuối khỏi hệ thống.

- Kiểm tra hiệu năng (RAM, CPU...), đảm bảo hoạt động bình thường của hệ thống.

- Có phương án bảo đảm an toàn cho mạng không dây (nếu có).

b) Chia tách thành các vùng mạng khác nhau theo đối tượng sử dụng, mục đích sử dụng, tối thiểu:

- Vùng mạng nội bộ.

- Vùng mạng biên.

- Vùng mạng máy chủ nội bộ.

- Vùng mạng trung gian (DMZ) để cung cấp dịch vụ.

- Vùng mạng máy chủ cơ sở dữ liệu.

- Vùng mạng riêng để cung cấp dịch vụ mạng không dây (nếu có).

- Vùng mạng WAN (nếu có).

- Vùng quản trị thiết bị hệ thống.

- Vùng quản trị.

7.12.2.3 Quản lý xác thực, cấp quyền và kiểm toán truy cập hệ thống thông tin

Có giải pháp quản lý việc xác thực, cấp quyền và kiểm toán truy cập hệ thống thông tin.

7.12.2.4 Sử dụng các giao thức truyền thông và quản trị mạng an toàn

Cấu hình hệ thống thông tin chỉ sử dụng các giao thức truyền thông và quản trị mạng an toàn (chưa được các tổ chức quốc tế công bố điểm yếu).

7.12.2.5 Kiểm soát truy cập

a) Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập thông tin nội bộ hoặc thực hiện quản trị từ xa đối với tài sản phần cứng và phần mềm.

b) Cấu hình chức năng xác thực trên các thiết bị hệ thống để xác thực người dùng khi quản trị thiết bị trực tiếp hoặc từ xa.

c) Kiểm soát truy cập từ bên ngoài vào hệ thống và từ bên trong hệ thống ra ngoài theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả truy cập tới các tài sản phần cứng và phần mềm mà hệ thống không cung cấp hoặc không cho phép truy cập.

d) Thiết lập giới hạn thời gian chờ (timeout) để tự động đóng các phiên kết nối khi không nhận được yêu cầu từ người dùng trong một khoảng thời gian quy định.

e) Có phương án kiểm soát truy cập của người dùng vào các dịch vụ, các máy chủ nội bộ theo chính sách.

f) Có phương án ưu tiên, bảo đảm chất lượng dịch vụ (QoS).

g) Giới hạn số lượng kết nối đồng thời từ một địa chỉ nguồn và tổng số lượng kết nối đồng thời cho từng ứng dụng, dịch vụ được hệ thống cung cấp theo năng lực thực tế của hệ thống, không áp dụng cứng đối với hệ thống/dịch vụ có yêu cầu kết nối lớn nếu đã có biện pháp kiểm soát rủi ro tương đương.

h) Không cho phép hoặc giới hạn truy cập (theo chức năng của máy chủ) từ các máy chủ ra các mạng bên ngoài hệ thống.

7.12.2.6 Xây dựng và áp dụng chính sách quản lý truy cập từ xa

Có chính sách quản lý truy cập từ xa đáp ứng các yêu cầu sau:

- Sử dụng mạng riêng ảo VPN, giải pháp ZTNA hoặc phương án tương đương và yêu cầu xác thực cho việc truy cập từ xa vào hệ thống đối với người dùng quản trị, người dùng tác nghiệp hệ thống.

- Yêu cầu người dùng xác thực MFA để kết nối truy cập từ xa và xác thực bổ sung trước khi truy cập vào hệ thống.

- Không cho phép quản trị, cấu hình thiết bị trực tiếp từ các mạng bên ngoài, trường hợp bắt buộc phải quản trị thiết bị từ xa phải thực hiện gián tiếp thông qua các máy quản trị trong hệ thống và sử dụng kết nối mạng an toàn.

- Giới hạn các dải địa chỉ mạng hoặc thiết bị cụ thể được phép kết nối để thực hiện quản trị từ xa đối với tài sản phần cứng và phần mềm.

- Các thiết bị được phép truy cập từ xa phải đảm bảo các yêu cầu về bảo mật: cài đặt phần mềm phòng chống mã độc, cấu hình bảo mật theo chính sách an ninh, an toàn đã ban hành của tổ chức.

7.12.2.7 Thiết lập và duy trì tài nguyên hệ thống dành riêng cho công tác quản trị

Thiết lập và duy trì các nguồn tài nguyên dành riêng cho công tác quản trị, tách biệt về mặt vật lý hoặc logic; được phân tách với mạng chính của hệ thống và không kết nối với Internet.

7.12.2.8 Kiểm thử và nghiệm thu hệ thống

a) Thực hiện thử nghiệm và nghiệm thu hệ thống trước khi bàn giao và đưa vào sử dụng.

b) Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống.

c) Có đơn vị độc lập hoặc bộ phận độc lập thuộc cơ quan, tổ chức thực hiện tư vấn, giám sát quá trình thử nghiệm và nghiệm thu hệ thống.

d) Thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng.

e) Có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng.

7.13 Giám sát và phòng thủ an ninh mạng

7.13.1 Khái quát

Xây dựng, vận hành các quy trình và công cụ để thiết lập, duy trì giám sát mạng toàn diện và bảo vệ hệ thống mạng khỏi các mối đe dọa.

7.13.2 Yêu cầu cụ thể

7.13.2.1 Thực hiện giám sát và quản lý tập trung các cảnh báo và sự kiện an ninh mạng

a) Triển khai giám sát an ninh mạng đối với tối thiểu các đối tượng: thiết bị hệ thống, máy chủ, ứng dụng, dịch vụ và các thành phần khác trong hệ thống (nếu có).

b) Triển khai SIEM để liên kết các sự kiện liên quan, phân tích theo hướng dẫn, yêu cầu và quy định của cơ quan, tổ chức có thẩm quyền.

c) Bố trí nguồn lực và tổ chức giám sát an ninh mạng 24/7.

7.13.2.2 Thiết lập và sử dụng tính năng về tường lửa, cảnh báo phát hiện và ngăn chặn xâm nhập của hệ điều hành và hệ thống

Thiết lập và sử dụng tính năng về tường lửa, cảnh báo phát hiện, ngăn chặn xâm nhập của hệ điều hành và hệ thống (nếu có).

7.13.2.3 Triển khai giải pháp, thiết bị chuyên dụng để bảo mật hệ thống mạng của cơ quan, tổ chức

Triển khai các giải pháp, thiết bị chuyên dụng có chức năng lọc gói tin giữa các phân đoạn mạng, lọc tầng ứng dụng, cảnh báo phát hiện và ngăn chặn xâm nhập trong hệ thống mạng của cơ quan, tổ chức.

7.13.2.4 Thiết lập cấu hình kiểm soát truy cập các cổng kết nối mạng

a) Thiết lập cấu hình trên các thiết bị mạng để kiểm soát truy cập các cổng kết nối mạng nếu thiết bị hỗ trợ.

b) Thay đổi, tách biệt cổng quản trị ứng dụng với cổng cung cấp dịch vụ ứng dụng.

7.13.2.5 Thu thập thông tin dữ liệu mạng

Thu thập nhật ký luồng dữ liệu mạng và/ hoặc dữ liệu lưu lượng từ các thiết bị mạng để rà soát và đưa ra các cảnh báo.

7.13.2.6 Điều chỉnh các ngưỡng cảnh báo sự kiện an ninh mạng

Điều chỉnh ngưỡng cảnh báo sự kiện an ninh mạng tối thiểu 01 lần/ tháng.

7.14 Nhân sự vận hành, quản trị hệ thống, bảo vệ an ninh mạng

7.14.1 Khái quát

a) Có cơ chế hoạt động độc lập về chuyên môn giữa các bộ phận vận hành, quản trị, bảo vệ an ninh mạng.

b) Có chương trình đào tạo nâng cao nhận thức an ninh mạng và kỹ năng an ninh mạng.

c) Có trình độ chuyên môn phù hợp với các bộ phận vận hành, quản trị, bảo vệ an ninh mạng.

7.14.2 Yêu cầu cụ thể

7.14.2.1 Có bộ phận phụ trách về vận hành, quản trị hệ thống và bảo vệ an ninh mạng

a) Thành lập các bộ phận riêng biệt vận hành, quản trị hệ thống và bảo vệ an ninh mạng.

b) Có cơ chế hoạt động độc lập về chuyên môn giữa các bộ phận vận hành, quản trị hệ thống và bảo vệ an ninh mạng.

7.14.2.2 Thiết lập và duy trì chương trình đào tạo tổng quan để nâng cao nhận thức an ninh mạng cho cán bộ, nhân viên

a) Có chương trình nâng cao nhận thức an ninh mạng cho toàn bộ cán bộ, nhân viên có sử dụng hệ thống thông tin.

b) Cán bộ chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của tổ chức.

c) Có quy trình và thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.

d) Có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc.

e) Tiến hành đào tạo tối thiểu 01 lần/ năm.

7.14.2.3 Thực hiện đào tạo kiến thức an ninh mạng theo từng vị trí, vai trò cụ thể

a) Thực hiện đào tạo kiến thức chuyên môn an ninh mạng theo từng vị trí, vai trò cụ thể. Đào tạo nhận thức về quy định pháp luật liên quan, trách nhiệm pháp lý cho các cá nhân tham gia bảo vệ an ninh mạng.

b) Tiến hành đào tạo tối thiểu 01 lần/ năm hoặc khi có thay đổi về các nhân sự liên quan trong tổ chức.

7.14.2.4 Xây dựng khung năng lực cho nhân sự chuyên trách

a) Xây dựng khung năng lực tương ứng từng vị trí việc làm, làm cơ sở cho việc tuyển dụng nhân sự chuyên trách vận hành, quản trị hệ thống, bảo vệ an ninh mạng.

b) Thực hiện đánh giá, kiểm tra trình độ chuyên môn đảm bảo phù hợp với vị trí làm việc.

7.15 Quản lý nhà cung cấp sản phẩm, dịch vụ

7.15.1 Khái quát

Có quy trình để đánh giá nhà cung cấp sản phẩm, dịch vụ an ninh mạng, lưu trữ, xử lý dữ liệu nhạy cảm hoặc chịu trách nhiệm về các quy trình, nền tảng quan trọng của hệ thống.

7.15.2 Yêu cầu cụ thể

7.15.2.1 Thiết lập và duy trì bản kiểm kê các nhà cung cấp sản phẩm, dịch vụ

Có phương án thiết lập và duy trì bản kiểm kê các nhà cung cấp sản phẩm, dịch vụ. Tối thiểu bao gồm:

- Lập danh sách, theo dõi, cập nhật trạng thái các nhà cung cấp sản phẩm, dịch vụ.

- Thực hiện phân loại các nhà cung cấp dịch vụ trong danh sách quản lý.

- Các nhà cung cấp sản phẩm, dịch vụ an ninh mạng phải đủ điều kiện kinh doanh sản phẩm, dịch vụ an ninh mạng.

- Có văn bản xác định rõ phạm vi trách nhiệm của nhà cung cấp và tổ chức.

- Xem xét và cập nhật danh sách tối thiểu 01 lần/ năm hoặc khi xảy ra thay đổi ảnh hưởng đến danh sách này.

7.15.2.2 Thiết lập và duy trì quy định quản lý nhà cung cấp dịch vụ

a) Có quy định quản lý các nhà cung cấp dịch vụ.

b) Đánh giá và cập nhật quy định tối thiểu 01 lần/ năm hoặc khi xảy ra thay đổi ảnh hưởng đến quy định này.

7.15.2.3 Đảm bảo các hợp đồng cung cấp dịch vụ có kèm theo các yêu cầu bảo mật

a) Đảm bảo các hợp đồng với nhà cung cấp dịch vụ an ninh mạng bao gồm đầy đủ yêu cầu về bảo mật.

b) Đánh giá và cập nhật hợp đồng của nhà cung cấp dịch vụ khi gia hạn để đảm bảo đầy đủ các yêu cầu bảo mật.

7.15.2.4 Thực hiện theo dõi các nhà cung cấp dịch vụ

Giám sát các nhà cung cấp dịch vụ thực hiện quy định quản lý cung cấp dịch vụ của tổ chức.

7.15.2.5 Rà soát vấn đề bảo mật khi kết thúc hợp đồng với các nhà cung cấp dịch vụ

Rà soát vấn đề bảo mật khi kết thúc hợp đồng với các nhà cung cấp dịch vụ.

7.16 Phát triển ứng dụng an toàn

7.16.1 Khái quát

Quản lý vòng đời bảo mật của các phần mềm ứng dụng để phòng ngừa, phát hiện và xử lý các điểm yếu, lỗ hổng bảo mật.

7.16.2 Yêu cầu cụ thể

7.16.2.1 Thiết lập và duy trì quy trình phát triển ứng dụng an toàn

a) Có quy trình phát triển ứng dụng an toàn.

b) Đánh giá và cập nhật quy trình tối thiểu 01 lần/ năm hoặc khi xảy ra các thay đổi có thể ảnh hưởng đến quy trình.

c) Đối với các phần mềm phát triển thuê khoán, yêu cầu:

- Có biên bản, hợp đồng và cam kết bảo mật đối với bên thuê khoán các nội dung liên quan đến phát triển phần mềm thuê khoán.

- Yêu cầu nhà phát triển cung cấp mã nguồn phần mềm. Trong trường hợp không thể cung cấp mã nguồn phần mềm, chủ quản hệ thống phải yêu cầu các bên thuê khoán cung cấp chứng chỉ đánh giá an

toàn độc lập hoặc thực hiện các biện pháp kiểm thử xâm nhập, giám sát rủi ro thay thế và ký cam kết chịu trách nhiệm pháp lý về tính an toàn của phần mềm.

- Kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng.

- Kiểm tra, đánh giá an ninh mạng của phần mềm trước khi đưa vào sử dụng.

- Khi thay đổi mã nguồn, kiến trúc phần mềm thực hiện kiểm tra, đánh giá an ninh mạng cho phần mềm.

- Có cam kết của bên phát triển về bảo đảm tính bí mật và bản quyền của phần mềm phát triển.

7.16.2.2 Thiết lập và duy trì quy trình tiếp nhận và xử lý lỗ hổng bảo mật phần mềm

a) Có quy trình tiếp nhận và xử lý báo cáo về lỗ hổng bảo mật phần mềm, bao gồm cả việc cung cấp phương tiện để các cá nhân, tổ chức bên ngoài báo cáo.

b) Quản lý, theo dõi lỗ hổng bảo mật phần mềm bao gồm xếp hạng mức độ nghiêm trọng và chỉ số đo lường thời gian để xác định, phân tích và khắc phục các lỗ hổng.

c) Đánh giá và cập nhật quy trình tối thiểu 01 lần/ năm hoặc khi xảy ra các thay đổi có thể ảnh hưởng đến quy trình.

7.16.2.3 Thực hiện phân tích nguyên nhân cốt lõi của lỗ hổng bảo mật

Thực hiện phân tích nguyên nhân cốt lõi của các lỗ hổng bảo mật.

7.16.2.4 Thiết lập, quản lý các cấu thành phần mềm của bên thứ ba

a) Thiết lập và quản lý một danh sách cập nhật các thành phần của bên thứ ba được sử dụng trong quá trình phát triển (thư viện, mô-đun…) và các thành phần dự kiến sẽ sử dụng trong tương lai để phát triển phần mềm.

b) Danh sách bao gồm các rủi ro an ninh mạng mà mỗi thành phần bên thứ ba có thể gây ra.

c) Đánh giá và cập nhật danh sách tối thiểu 01 lần/ tháng.

7.16.2.5 Tách biệt môi trường cho các hoạt động phát triển, kiểm thử và vận hành

Duy trì việc tách biệt môi trường vận hành chính thức, môi trường kiểm thử và môi trường phát triển. Trong đó yêu cầu không lưu trữ thông tin xác thực, thông tin bí mật trên mã nguồn ứng dụng.

7.16.2.6 Đào tạo về bảo mật và lập trình an toàn

a) Đảm bảo tất cả nhân viên phát triển phần mềm được đào tạo về trách nhiệm và phương thức phát triển phần mềm an toàn đối với từng môi trường/giải pháp cụ thể.

b) Thực hiện đào tạo tối thiểu 01 lần/ năm.

7.16.2.7 Kết hợp các nguyên tắc bảo mật trong kiến trúc ứng dụng

Kết hợp các nguyên tắc bảo mật trong quá trình xây dựng kiến trúc ứng dụng. Trong đó bao gồm nhưng không giới hạn các yêu cầu:

- Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý.

- Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu ra trước khi gửi về máy yêu cầu.

- Có phương án bảo vệ ứng dụng chống lại những dạng tấn công phổ biến.

- Có chức năng kiểm soát lỗi, thông báo lỗi từ ứng dụng.

- Không lưu trữ thông tin xác thực, thông tin bí mật trên mã nguồn ứng dụng.

- Có chức năng tạo lập, duy trì và quản lý phiên làm việc an toàn.

7.16.2.8 Tận dụng các mô-đun hoặc dịch vụ đã được kiểm chứng cho các thành phần bảo mật ứng dụng

a) Tận dụng mô-đun hoặc dịch vụ đã được kiểm chứng cho các thành phần bảo mật của ứng dụng.

b) Chỉ sử dụng thuật toán mã hóa mạnh (chưa được các tổ chức quốc tế công bố điểm yếu), được chuẩn hóa và đánh giá rộng rãi.

c) Ghi nhật ký kiểm toán hành vi của người dùng trong sản phẩm.

7.16.2.9 Tiến hành kiểm tra an ninh, an toàn các ứng dụng

a) Kiểm tra các lỗ hổng bảo mật trong mã nguồn được phát triển, lỗ hổng trong các thư viện, thành phần mở rộng của bên thứ ba mà ứng dụng sử dụng.

b) Kiểm thử xâm nhập và khắc phục các lỗ hổng bảo mật trước khi đưa vào vận hành chính thức.

7.17 Quản trị ứng phó sự cố an ninh mạng

7.17.1 Khái quát

Có kế hoạch, chương trình để phát triển và duy trì khả năng ứng phó sự cố bao gồm chính sách, kế hoạch, thủ tục, vai trò, đào tạo, kênh liên lạc.

7.17.2 Yêu cầu cụ thể

7.17.2.1 Thành lập lực lượng ứng phó sự cố an ninh mạng

a) Chỉ định một người chủ chốt và ít nhất một người dự phòng để quản lý quy trình ứng phó sự cố an ninh mạng.

b) Thiết lập và duy trì đầu mối liên lạc để báo cáo sự cố. Xác minh thông tin liên hệ hàng năm để đảm bảo rằng thông tin được cập nhật.

c) Phân công vị trí, vai trò và trách nhiệm chính của từng thành viên trong lực lượng tham gia ứng phó sự cố.

d) Quy định về trách nhiệm phối hợp với lực lượng ứng phó sự cố an ninh mạng của các phòng ban có liên quan.

7.17.2.2 Thiết lập và duy trì quy trình nội bộ để báo cáo sự cố an ninh mạng

a) Có quy trình nội bộ để báo cáo sự cố an ninh mạng.

b) Thực hiện phân nhóm sự cố an ninh mạng.

c) Đánh giá và cập nhật quy trình tối thiểu 01 lần/ năm hoặc khi xảy ra các thay đổi ảnh hưởng đến quy trình.

7.17.2.3 Thiết lập và duy trì quy trình ứng phó sự cố an ninh mạng

a) Có quy trình ứng phó sự cố, đảm bảo có cơ chế phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ khắc phục sự cố an ninh mạng.

b) Đánh giá và cập nhật quy trình tối thiểu 01 lần/ năm hoặc khi xảy ra các thay đổi ảnh hưởng đến quy trình.

7.17.2.4 Thiết lập cơ chế (kênh kỹ thuật) liên lạc trong quá trình xử lý sự cố

a) Thiết lập cơ chế chính và cơ chế phụ sử dụng để giao tiếp và báo cáo trong xử lý sự cố an ninh mạng.

b) Đánh giá và cập nhật cơ chế liên lạc tối thiểu 01 lần/ năm hoặc khi xảy ra các thay đổi ảnh hưởng đến cơ chế.

7.17.2.5 Thực hiện đánh giá sau sự cố an ninh mạng

Thực hiện đánh giá sau sự cố an ninh mạng.

7.17.2.6 Định kỳ diễn tập ứng phó sự cố an ninh mạng

Có kế hoạch và thực hiện diễn tập các kịch bản ứng phó sự cố định kỳ tối thiểu 01 lần/ năm.

7.17.2.7 Triển khai và duy trì các ngưỡng sự cố an ninh mạng

a) Thiết lập và duy trì các ngưỡng sự cố an ninh mạng.

b) Đánh giá và cập nhật ngưỡng tối thiểu 01 lần/ 06 tháng hoặc khi xảy ra các thay đổi ảnh hưởng đến ngưỡng.

7.18 Quản lý kiểm tra an ninh mạng

7.18.1 Khái quát

Xác định tính hiệu quả trong năng lực phòng vệ và khả năng phục hồi của các tài sản thông qua việc đánh giá khả năng khai thác các điểm yếu trong quy trình kiểm soát về con người, quy trình, công nghệ; mô phỏng lại các mục tiêu và hành động tấn công; khắc phục các tồn tại phát hiện được qua kết quả kiểm thử xâm nhập.

7.18.2 Yêu cầu cụ thể

7.18.2.1 Thiết lập và duy trì một chương trình kiểm thử xâm nhập

a) Có chương trình kiểm thử xâm nhập phù hợp với quy mô, mức độ phức tạp và trạng thái của tổ chức.

b) Chương trình kiểm thử xâm nhập cần đáp ứng một số nội dung sau:

- Về yêu cầu: hoạt động kiểm thử xâm nhập phải được phê duyệt về phạm vi, thời gian, phương pháp, đầu mối phối hợp, phương án đảm bảo an ninh mạng và phương án xử lý dữ liệu thu được; đối với hệ

thống đang vận hành, phải chọn thời điểm và cách thức kiểm thử phù hợp để không làm gián đoạn dịch vụ, ưu tiên thực hiện trên môi trường phát triển hoặc trong thời gian đã được phê duyệt.

- Về phạm vi tiến hành: kiểm tra một phần hoặc toàn bộ hạ tầng công nghệ thông tin của tổ chức.

- Về tần suất: hàng quý, nửa năm, một năm hoặc đột xuất.

- Về các giới hạn: xác định các hành vi tấn công bị cấm (tấn công vật lý, tấn công lừa đảo, tấn công phi kỹ thuật…).

- Về cách phản ứng của tổ chức: có thực hiện việc ngăn chặn hay không, cơ chế kiểm soát thông tin (về cuộc kiểm thử) trong nội bộ.

7.18.2.2 Định kỳ thực hiện kiểm thử xâm nhập từ bên ngoài

a) Định kỳ thực hiện kiểm thử xâm nhập từ bên ngoài tối thiểu 01 lần/ 06 tháng.

b) Áp dụng với các ứng dụng, dịch vụ của tổ chức được công khai ra mạng Internet.

7.18.2.3 Khắc phục các tồn tại phát hiện được qua việc kiểm thử xâm nhập

Khắc phục các tồn tại phát hiện được qua kiểm thử xâm nhập dựa trên chính sách của tổ chức về phạm vi và mức độ ưu tiên khắc phục.

7.18.2.4 Rà soát các biện pháp bảo mật

Kiểm tra, đánh giá hiệu quả các biện pháp bảo mật sau mỗi lần thực hiện kiểm thử xâm nhập.

7.18.2.5 Định kỳ thực hiện kiểm thử xâm nhập từ bên trong

a) Định kỳ thực hiện kiểm thử xâm nhập từ bên trong tối thiểu 01 lần/ 06 tháng.

b) Áp dụng với các tài nguyên nội bộ trong hệ thống thông tin của tổ chức.

Phụ lục A

Yêu cầu cơ bản về an toàn vật lý cho hệ thống thông tin theo cấp độ

A.1 Yêu cầu vật lý cho hệ thống thông tin cấp độ 1

A.1.1 Kiểm soát truy cập vật lý

Thiết lập cổng bảo vệ để kiểm soát vào, ra phòng máy chủ.

A.1.2 Chống trộm, chống phá hoại

Thiết bị hệ thống phải được đặt trong máy chủ và có tủ bảo vệ (tủ rack), được đặt cố định và gắn nhãn mô tả.

A.1.3 Chống cháy

Phòng máy chủ được trang bị hệ thống phòng cháy, chữa cháy.

A.1.4 Nguồn cung cấp

Nguồn điện trong phòng máy chủ phải được đảm bảo ổn định có ổn áp, chống quá tải.

A.2 Yêu cầu vật lý cho hệ thống thông tin cấp độ 2

A.2.1 Kiểm soát truy cập vật lý

a) Thiết lập hệ thống cổng bảo vệ để kiểm soát vào, ra phòng máy chủ.

b) Thiết lập hệ thống camera giám sát, ghi lại thông tin vào ra phòng máy chủ.

A.2.2 Chống trộm, chống phá hoại

Thiết bị hệ thống phải được đặt trong phòng máy chủ và có tủ bảo vệ (tủ rack), được đặt cố định và gắn nhãn mô tả.

A.2.3 Chống sét

Tòa nhà đặt phòng máy chủ phải được thiết lập hệ thống chống sét.

A.2.4 Chống cháy

Phòng máy chủ phải lắp đặt hệ thống cảnh báo và chữa cháy tự động.

A.2.5 Kiểm soát nhiệt độ và độ ẩm

Có hệ thống điều hòa, bảo đảm về nhiệt độ, độ ẩm ổn định trong phòng máy chủ.

A.2.6 Nguồn cung cấp

a) Nguồn điện trong phòng máy chủ phải được đảm bảo ổn định có ổn áp, chống quá tải.

b) Có hệ thống UPS đảm bảo hoạt động liên tục của các thiết bị mạng chính và các máy chủ quan trọng.

A.3 Yêu cầu vật lý cho hệ thống thông tin cấp độ 3

A.3.1 Lựa chọn vị trí vật lý

Vị trí phòng máy chủ không được nằm ở các tầng cao của tòa nhà; không được đặt dưới tầng hầm hoặc dưới các nơi chứa, đựng nước.

A.3.2 Kiểm soát truy cập vật lý

a) Thiết lập hệ thống cổng điện tử để kiểm soát vào, ra phòng máy chủ.

b) Thiết lập hệ thống camera giám sát, ghi lại thông tin vào ra phòng máy chủ. Dữ liệu nhật ký camera phải được lưu trữ tối thiểu 03 tháng.

c) Có phương án kiểm soát các thiết bị, vật dụng được mang ra, vào phòng máy chủ.

A.3.3 Chống trộm, chống phá hoại

a) Thiết bị hệ thống phải được đặt trong phòng máy chủ và có tủ bảo vệ (tủ rack), được đặt cố định và gắn nhãn mô tả.

b) Kết nối vật lý (cáp mạng, điện thoại…) trong phòng phải được đi ngầm và có đường ống bảo vệ.

c) Thiết lập hệ thống báo động chống trộm tự động.

A.3.4 Chống sét

a) Tòa nhà đặt phòng máy chủ phải được thiết lập hệ thống chống sét và được nghiệm thu, kiểm tra kỹ thuật của ban quản lý tòa nhà.

b) Các thiết bị, tủ kỹ thuật trong phòng máy chủ phải được nối đất.

A.3.5 Chống cháy

a) Phòng máy chủ phải lắp đặt hệ thống cảnh báo và chữa cháy tự động.

b) Phòng máy chủ phải được xây dựng sử dụng các vật liệu chịu lửa.

A.3.6 Chống ẩm và chống thấm

a) Tường và sàn nhà của phòng máy chủ có các đường ống thoát nước; đường ống thoát nước không được đi qua trần, sàn phòng máy chủ.

b) Trần và các cửa, cửa sổ phòng máy chủ phải được thiết kế đảm bảo không bị nước mưa hắt vào.

c) Có biện pháp ngăn không cho nước mưa thấm qua trần và tường vào phòng máy, tích tụ nước và di chuyển nước tích tụ trong phòng máy.

A.3.7 Chống tĩnh điện

a) Có biện pháp chống tĩnh điện đối với các thiết bị mạng chính.

b) Sàn phòng máy chủ cần phải được lắp đặt sàn chống tĩnh điện.

A.3.8 Kiểm soát nhiệt độ và độ ẩm

Có hệ thống điều hòa trung tâm, bảo đảm về nhiệt độ, độ ẩm ổn định trong phòng máy chủ.

A.3.9 Nguồn cung cấp

a) Nguồn điện trong phòng máy chủ phải được đảm bảo ổn định có ổn áp, chống quá tải.

b) Có nguồn cung cấp điện dự phòng, có thể thay thế nguồn cung cấp điện chính.

c) Có hệ thống UPS đảm bảo hoạt động liên tục của các thiết bị hệ thống và máy chủ.

A.3.10 Bảo vệ điện từ

a) Đường điện và cáp tín hiệu (cáp mạng, thoại…) phải được đặt cách ly để tránh nhiễu điện từ đường điện sang cáp tín hiệu.

b) Có phương án che chắn, cách ly các nguồn nhiễu điện từ như: các máy biến áp, các động cơ và máy phát điện, thiết bị X quang, các máy phát ra-đa hoặc vô tuyến, thiết bị hàn nhiệt.

A.4 Yêu cầu vật lý cho hệ thống thông tin cấp độ 4

A.4.1 Lựa chọn vị trí vật lý

a) Vị trí phòng máy chủ không được nằm ở các tầng cao của tòa nhà; không được đặt dưới tầng hầm hoặc dưới các nơi chứa, đựng nước.

b) Vị trí đặt phòng máy chủ cần tránh khu vực dễ phát sinh lửa như khu vực gần kho dầu, vật dễ cháy, khu vực có điện trường và từ trường mạnh.

A.4.2 Kiểm soát truy cập vật lý

a) Thiết lập hệ thống cổng điện tử để kiểm soát vào, ra phòng máy chủ.

b) Thiết lập hệ thống camera giám sát, ghi lại thông tin vào ra phòng máy chủ; hệ thống phải được quản lý tập trung và được theo dõi, giám sát 24/7. Dữ liệu nhật ký camera phải được lưu trữ tối thiểu 06 tháng.

c) Thiết lập khu vành đai giữa phòng máy chủ với các khu vực khác trong tòa nhà.

d) Các khu vực trong phòng máy chủ đặt thiết bị mạng chính và máy chủ quan trọng phải có hệ thống camera giám sát và có tủ bảo vệ.

A.4.3 Chống trộm, chống phá hoại

a) Thiết bị hệ thống phải được đặt trong phòng máy chủ và có tủ bảo vệ (tủ rack), được đặt cố định và gắn nhãn mô tả.

b) Kết nối vật lý (cáp mạng, điện thoại…) trong phòng phải được đi ngầm và có đường ống bảo vệ.

c) Thiết lập hệ thống báo động chống trộm tự động sử dụng kỹ thuật quang điện hoặc những kỹ thuật khác tương đương.

A.4.4 Chống sét

a) Tòa nhà đặt phòng máy chủ phải được thiết lập hệ thống chống sét và được nghiệm thu, kiểm tra kỹ thuật của ban quản lý tòa nhà.

b) Có phương án phòng chống sét lan truyền cho các thiết bị hệ thống, các thiết bị phụ trợ và nguồn cung cấp điện.

c) Kết nối mạng giữa các thiết bị hệ thống có cơ chế phòng chống sét lan truyền.

A.4.5 Chống cháy

a) Phòng máy chủ phải lắp đặt hệ thống cảnh báo và chữa cháy tự động; có các hình thức phát tín hiệu cảnh báo cháy khác nhau (bằng âm thanh, ánh sáng...).

b) Phòng máy chủ phải được xây dựng sử dụng các vật liệu chịu lửa.

c) Khu vực máy chủ quan trọng và thiết bị mạng chính phải đặt cách ly và có biện pháp cách lửa với các khu vực khác.

A.4.6 Chống ẩm và chống thấm

a) Tường và sàn nhà của phòng máy chủ có các đường ống thoát nước; đường ống thoát nước không được đi qua trần, sàn phòng máy chủ.

b) Trần và các cửa, cửa sổ phòng máy chủ phải được thiết kế đảm bảo không bị nước mưa hắt vào.

c) Có biện pháp ngăn không cho nước mưa thấm qua trần và tường vào phòng máy, tích tụ nước và di chuyển nước tích tụ trong phòng máy.

A.4.7 Chống tĩnh điện

a) Có biện pháp chống tĩnh điện đối với các thiết bị trong phòng máy chủ.

b) Sàn phòng máy chủ cần phải được lắp đặt sàn chống tĩnh điện.

A.4.8 Kiểm soát nhiệt độ và độ ẩm

a) Có hệ thống điều hòa trung tâm, bảo đảm về nhiệt độ, độ ẩm ổn định trong phòng máy chủ.

b) Hệ thống điều hòa không khí tại phòng máy phải riêng biệt hoàn toàn với các hệ thống điều hòa khác trong tòa nhà.

c) Có thiết bị đo độ ẩm và cảnh báo khi độ ẩm trong phòng máy chủ vượt mức cho phép.

d) Có thiết bị hút ẩm để ngăn chặn sự ngưng tụ hơi nước ở phòng máy chủ và thẩm thấu nước đã tích tụ ở sàn phòng máy chủ.

A.4.9 Nguồn cung cấp

a) Nguồn điện trong phòng máy chủ phải được đảm bảo ổn định có ổn áp, chống quá tải.

b) Sử dụng hai nguồn cung cấp kéo từ hai trạm điện khác nhau.

c) Có hệ thống UPS đảm bảo hoạt động liên tục của các thiết bị hệ thống và máy chủ.

A.4.10 Bảo vệ điện từ

a) Đường điện và cáp tín hiệu (cáp mạng, thoại…) phải được đặt cách ly để tránh nhiễu điện từ đường điện sang cáp tín hiệu.

b) Có phương án che chắn, cách ly các nguồn nhiễu điện từ như: các máy biến áp, các động cơ và máy phát điện, thiết bị X quang, các máy phát ra-đa hoặc vô tuyến, thiết bị hàn nhiệt.

c) Có tấm chắn điện từ cho khu vực máy chủ quan trọng và thiết bị mạng chính.

A.5 Yêu cầu vật lý cho hệ thống thông tin cấp độ 5

A.5.1 Lựa chọn vị trí vật lý

a) Vị trí phòng máy chủ không được nằm ở các tầng cao của tòa nhà; không được đặt dưới tầng hầm hoặc dưới các nơi chứa, đựng nước.

b) Vị trí đặt phòng máy chủ cần tránh khu vực dễ phát sinh lửa như khu vực gần kho dầu, vật dễ cháy, khu vực có điện trường và từ trường mạnh.

c) Vị trí xây dựng phòng máy chủ phải tránh được các điều kiện khắc nghiệt của thời tiết như: bão, thiên tai và các điều kiện khác.

A.5.2 Kiểm soát truy cập vật lý

a) Thiết lập hệ thống cổng điện tử để kiểm soát vào, ra phòng máy chủ, có ít nhất 02 yếu tố xác thực khi vào phòng máy chủ hoặc truy cập vật lý các thiết bị mạng chính.

b) Thiết lập hệ thống camera giám sát, ghi lại thông tin vào ra phòng máy chủ; hệ thống phải được quản lý tập trung và được theo dõi, giám sát 24/7. Dữ liệu nhật ký camera phải được lưu trữ tối thiểu 12 tháng.

c) Thiết lập khu vành đai giữa phòng máy chủ với các khu vực khác trong tòa nhà.

d) Các khu vực trong phòng máy chủ đặt thiết bị mạng chính và máy chủ quan trọng phải có hệ thống camera giám sát và có tủ bảo vệ.

A.5.3 Chống trộm, chống phá hoại

a) Thiết bị hệ thống phải được đặt trong phòng máy chủ và có tủ bảo vệ (tủ rack), được đặt cố định và gắn nhãn mô tả.

b) Kết nối vật lý (cáp mạng, điện thoại…) trong phòng phải được đi ngầm và có đường ống bảo vệ.

c) Thiết lập hệ thống báo động chống trộm tự động sử dụng kỹ thuật quang điện hoặc những kỹ thuật khác tương đương.

d) Thiết lập lớp bảo vệ vật lý thứ 2 cho khu vực máy chủ quan trọng, thiết bị mạng chính; có hệ thống kiểm soát vào, ra khu vực này, sử dụng tối thiểu 02 yếu tố xác thực.

A.5.4 Chống sét

a) Tòa nhà đặt phòng máy chủ phải được thiết lập hệ thống chống sét và được nghiệm thu, kiểm tra kỹ thuật của ban quản lý tòa nhà.

b) Có phương án phòng chống sét lan truyền cho các thiết bị hệ thống, các thiết bị phụ trợ và nguồn cung cấp điện.

c) Kết nối mạng giữa các thiết bị hệ thống có cơ chế phòng chống sét lan truyền.

d) Có phương án quản lý, giám sát tập trung hệ thống chống sét.

A.5.5 Chống cháy

a) Phòng máy chủ phải lắp đặt hệ thống cảnh báo và chữa cháy tự động; có các hình thức phát tín hiệu cảnh báo cháy khác nhau (bằng âm thanh, ánh sáng...).

b) Phòng máy chủ phải được xây dựng sử dụng các vật liệu chịu lửa.

c) Khu vực máy chủ quan trọng và thiết bị mạng chính phải đặt cách ly và có biện pháp cách lửa với các khu vực khác.

d) Có phương án quản lý, giám sát tập trung hệ thống chống cháy; bố trí nguồn lực và tổ chức giám sát 24/7.

A.5.6 Chống ẩm và chống thấm

a) Tường và sàn nhà của phòng máy chủ có các đường ống thoát nước; đường ống thoát nước không được đi qua trần, sàn phòng máy chủ.

b) Trần và các cửa, cửa sổ phòng máy chủ phải được thiết kế đảm bảo không bị nước mưa hắt vào.

c) Có biện pháp ngăn không cho nước mưa thấm qua trần và tường vào phòng máy, tích tụ nước và di chuyển nước tích tụ trong phòng máy.

A.5.7 Chống tĩnh điện

a) Có biện pháp chống tĩnh điện đối với các thiết bị trong phòng máy chủ.

b) Sàn phòng máy chủ cần phải được lắp đặt sàn chống tĩnh điện.

c) Có phương án giảm thiểu sự phát sinh tĩnh điện cho các máy chủ quan trọng và thiết bị mạng chính.

d) Các vật liệu sử dụng xây dựng phòng máy chủ phải sử dụng loại vật liệu cách điện hoặc sinh ra tĩnh điện nhỏ.

A.5.8 Kiểm soát nhiệt độ và độ ẩm

a) Có hệ thống điều hòa trung tâm, bảo đảm về nhiệt độ, độ ẩm ổn định trong phòng máy chủ.

b) Hệ thống điều hòa không khí tại phòng máy phải riêng biệt hoàn toàn với các hệ thống điều hòa khác trong tòa nhà.

c) Có thiết bị đo độ ẩm và cảnh báo khi độ ẩm trong phòng máy chủ vượt mức cho phép.

d) Có thiết bị hút ẩm để ngăn chặn sự ngưng tụ hơi nước ở phòng máy chủ và thẩm thấu nước đã tích tụ ở sàn phòng máy chủ.

e) Có phương án quản lý, giám sát tập trung hệ thống kiểm soát nhiệt độ và độ ẩm; bố trí nguồn lực và tổ chức giám sát 24/7.

A.5.9 Nguồn cung cấp

a) Nguồn điện trong phòng máy chủ phải được đảm bảo ổn định có ổn áp, chống quá tải.

b) Sử dụng hai nguồn cung cấp kéo từ hai trạm điện khác nhau.

c) Có hệ thống UPS đảm bảo hoạt động liên tục của các thiết bị hệ thống và máy chủ.

d) Có phương án quản lý, giám sát tập trung hệ thống nguồn cung cấp; bố trí nguồn lực và tổ chức giám sát 24/7.

A.5.10 Bảo vệ điện từ

a) Đường điện và cáp tín hiệu (cáp mạng, thoại…) phải được đặt cách ly để tránh nhiễu điện từ đường điện sang cáp tín hiệu.

b) Có phương án che chắn, cách ly các nguồn nhiễu điện từ như: các máy biến áp, các động cơ và máy phát điện, thiết bị X quang, các máy phát ra-đa hoặc vô tuyến, thiết bị hàn nhiệt.

c) Có tấm chắn điện từ cho khu vực máy chủ quan trọng và thiết bị mạng chính.

Thư mục tài liệu tham khảo

[1] CIS (Center for Internet Security) Critical Security Controls Version 8.1, 2024.

[2] NIST SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations), September 23, 2021.

[3] TCVN 14423:2025 An ninh mạng - Yêu cầu đối với hệ thống thông tin quan trọng.

[4] TCVN ISO 31000:2018 Quản lý rủi ro - Hướng dẫn.

[5] TCVN 11930:2017 Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ.
