TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 14423:2025

Xuất bản lần 1

AN NINH MẠNG - YÊU CẦU ĐỐI VỚI HỆ THỐNG THÔNG TIN QUAN TRỌNG

Cyber security - Requirements for critical information system

HÀ NỘI – 2025

Mục lục

Lời nói đầu

TCVN 14423:2025 được xây dựng trên cơ sở tham khảo Tiêu chuẩn quốc tế CIS Critical Security Control phiên bản 8, ban hành bởi Trung tâm An ninh Internet, Hoa Kỳ (Center for Internet Security - CIS) năm 2021, có điều chỉnh, sửa đổi, bổ sung để phù hợp với điều kiện của Việt Nam.

TCVN 14423:2025 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 của cơ quan nhà nước, hệ thống thông tin quan trọng về an ninh quốc gia, 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 – Yêu cầu đối với hệ thống thông tin quan trọng

Cyber security – Requirements for critial information system

1 Phạm vi áp dụng

Tiêu chuẩn này quy định các yêu cầu cơ bản về an ninh mạng cho hệ thống thông tin của cơ quan nhà nước và hệ thống thông tin quan trọng về an ninh quốc gia.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau rất cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi, bổ sung (nếu có).

TCVN 11930:2017 (ISO/IEC 27001:2013) *Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ*

3 Thuật ngữ, định nghĩa và chữ viết tắt

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

3.1 Thuật ngữ và định nghĩa

3.1.1

An ninh mạng (cyber security)

Sự bảo đảm 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.

3.1.2

Hệ thống thông tin (information system)

Tập hợp phần cứng, phần mềm và cơ sở 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.

3.1.3

Dữ liệu quan trọng (important data)

Dữ liệu trong hệ thống, được cơ quan, tổ chức xác định là quan trọng, cần được ưu tiên bảo vệ. Dữ liệu quan trọng bao gồm nhưng không giới hạn các loại dữ liệu chứa các thông tin sau: thông tin nghiệp vụ, thông tin bí mật nhà nước, thông tin riêng và các loại thông tin quan trọng khác (nếu có).

3.1.4

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 có có thể gây gián đoạn hoạt động của hệ thống và làm mất tính khả dụng của hệ thống thông tin.

3.1.5

Nhật ký hệ thống (system log)

Những sự kiện được hệ thống ghi lại liên quan đến trạng thái hoạt động, sự cố, sự kiện an ninh mạng và các thông tin khác liên quan đến hoạt động của hệ thống (nếu có).

3.1.6

Phần mềm độc hại (malware)

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

3.1.7

Phương tiện lưu trữ (media storage)

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

3.1.8

Xác thực đa nhân 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...)..

3.1.9

Tiến trình (process)

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

3.1.10

Khôi phục (roll back)

Thao tác đưa hệ thống về một trạng thái cũ.

3.1.11

Biện pháp kiểm soát (control)

Việc thiết lập các tiêu chuẩn đo lường kết quả thực hiện, so sánh kết quả với các tiêu chuẩn, phát hiện sai lệch và nguyên nhân, tiến hành các điều chỉnh nhằm làm cho kết quả cuối cùng phù hợp với mục tiêu đã được xác định.

3.1.12

Rủi ro an ninh mạng (cyber security risk)

Khả năng bị lộ hoặc mất mát do một cuộc tấn công mạng hoặc vi phạm dữ liệu trong cơ quan, tổ chức, đơn vị. Rủi ro an ninh mạng không chỉ nằm ở khả năng xảy ra một cuộc tấn công mạng mà còn là những hậu quả tiềm ẩn, ví dụ như tổn thất tài chính, thiệt hại về danh tiếng hoặc gián đoạn hoạt động.

3.1.13

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.

3.1.14

Cứng hóa (hardening)

Quá trình nâng cao tính bảo mật cho một hệ thống bằng các quy tắc, thiết lập bảo mật máy chủ và hệ thống.

3.1.15

Phần mềm trái phép (unauthorized software)

Những phần mềm 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.

3.1.16

Thiết bị di động (mobile device)

Thiết bị số có thể cầm tay, có hệ điều hành, có khả năng xử lý, kết nối mạng và có màn hình hiển thị như máy tính xách tay, máy tính bảng, điện thoại di động thông minh.

3.1.17

Lỗ hổng bảo mật (security vulnerability)

Một 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.

3.1.18

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.

3.1.19

Phân quyền dữ liệu (data decentralization)

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.

3.1.20

Nhà cung cấp (supplier)

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

3.1.21

Không gian mạng (cyberspace)

Mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu; là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian.

3.1.22

Phần mềm thuê khoán (outsource 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.

3.1.23

Vùng DMZ (demilitarized zone)

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

3.1.24

Vùng mạng biên (outside zone)

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

3.1.25

Vùng máy chủ nội bộ (internal server zone)

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

3.1.26

Vùng mạng nội bộ (LAN - 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.

3.1.27

Vùng quản trị (management zone)

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

3.1.28

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.

3.1.29

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

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

3.1.30

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).

3.1.31

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.

3.1.32

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.

3.2 Chữ viết tắt

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
SOC	Trung tâm điều hành an ninh	Security Operations Center
ISP	Doanh nghiệp cung cấp dịch vụ Internet	Internet Service Provider
SIEM	Hệ thống quản lý nhật ký và sự kiện tập trung	Security Information and Event Management
CNTT	Công nghệ thông tin	

4 Yêu cầu đối với hệ thống thông tin của cơ quan nhà nước

4.1 Quản lý rủi ro an ninh mạng

4.1.1 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.

4.1.2 Yêu cầu cụ thể

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

a) Xây dựng, ban hành và đảm bảo tuân thủ 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 tài liệu.

4.1.2.2 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 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...).

4.1.2.3 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.

4.1.2.4 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 06 tháng đánh giá và cải thiện hiệu quả của các biện pháp kiểm soát được sử dụng để giảm thiểu rủi ro.

4.1.2.5 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.

4.1.2.6 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.

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 02 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) Tất cả tài sản vật lý phải được kiểm tra an ninh bởi cơ quan, tổ chức có thẩm quyền theo quy định của pháp luật trước khi 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 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) Xây dựng, ban hành và đảm bảo tuân thủ 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.

4.2.2.3 Quản lý tài sản thanh lý/ hư hỏng

Xây dựng, ban hành và đảm bảo tuân thủ quy trình thanh lý/ tiêu hủy tài sản CNTT, đảm bảo xóa không thể khôi phục toàn bộ dữ liệu của cơ quan, tổ chức trước khi tiến hành thanh lý/ tiêu hủy.

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 02 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) Xây dựng, ban hành và đảm bảo tuân thủ quy trình phát hiện và xử lý các phần mềm trái phép định kỳ tối thiểu 01 lần/quý.

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.

4.4 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) Xây dựng, ban hành và đảm bảo tuân thủ 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 (*thực hiện theo quy định của Luật Bảo vệ bí mật nhà nước*).

c) Xây dựng quy trình yêu cầu truy cập, thêm mới, sửa, xoá 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/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 hoá dữ liệu quan trọng

a) Mã hoá dữ liệu quan trọng được lưu trữ trong các tài sản phần cứng và phần mềm của cơ quan, tổ chức.

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

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) Xây dựng, ban hành và đảm bảo tuân thủ quy định, quy trình cấu hình an toàn cho các tài sản phần cứng và phần mềm của cơ quan, tổ chức.

b) Xây dựng, ban hành và đảm bảo tuân thủ các tài liệu cấu hình tiêu chuẩn, tài liệu cấu hình bảo mật nâng cao 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) 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 khoá phiên làm việc trên các tài sản phần cứng và phần mềm

a) Tự động khoá phiên làm việc trên các tài sản sau một khoảng thời gian không sử dụng.

- Đối với máy tính người dùng: không quá 15 min.

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

- Đối với thiết bị di động: không quá 02 min.

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

b) Tự động khoá 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 xử lý và lưu trữ dữ liệu quan trọng: tối đa 05 lần.

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

4.5.2.3 Phát triển phần mềm thuê khoán

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. Trong đó, yêu cầu cung cấp mã nguồn phần mềm.

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

4.6.1 Khái quát

a) Thiết lập, tuân thủ và duy trì quy trình, sử dụng 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) Xây dựng và thực thi 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 hoá 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.

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

a) Xây dựng, ban hành và đảm bảo tuân thủ quy định sử dụng mật khẩu an toàn trong tổ chức, đáp ứng các yêu cầu 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 đa nhân tố, quy định mật khẩu có tối thiểu 08 ký tự.

- Đối với các hệ thống không sử dụng xác thực đa nhân tố, 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.

b) Đối với tài khoản quản trị cần đảm bảo tuân thủ các quy định bổ sung:

- Thay đổi mật khẩu định kỳ 01 lần/02 tháng.

- Mật khẩu mới không được trùng với 10 mật khẩu trước đó.

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

Xây dựng, ban hành và đảm bảo tuân thủ 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.

- Quy định về quản lý thiết bị lưu khóa bí mật và khóa bí mật.

- Xoá hoặc vô hiệu hoá các tài khoản không hoạt động sau 45 ngày hoặc ngay khi có thay đổi về nhân sự quản lý 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

Xây dựng, ban hành và đảm bảo tuân thủ 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 đa nhân tố 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.

4.6.2.5 Xây dựng và tuân thủ quy trình cấp mới, thay đổi và thu hồi quyền truy cập

a) Xây dựng, ban hành và đảm bảo tuân thủ 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.

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 doạ, lỗ hổng bảo mật mới từ nhiều nguồn.

4.7.2 Yêu cầu cụ thể

4.7.2.1 Thiết lập, tuân thủ và duy trì quy trình quản lý lỗ hổng bảo mật

a) Xây dựng, ban hành và đảm bảo tuân thủ 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: Thiết lập và duy trì 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: Xây dựng phương án, 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 và cập nhật quy trình tối thiểu 01 lần/năm hoặc khi xảy ra thay đổi trong tổ chức ảnh hưởng đến quy trình này.

4.7.2.2 Thiết lập, tuân thủ và duy trì quy trình quản lý bản vá

Xây dựng, ban hành và đảm bảo tuân thủ 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.

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, tuân thủ và duy trì một quy trình quản lý nhật ký an ninh mạng

a) Xây dựng, ban hành và đảm bảo tuân thủ 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: đia 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.

- Nhật ký tiến trình hoạt động tối thiểu bao gồm: thông tin thiết bị (IP/ tên thiết bị, tên miền), 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.

- Đảm bảo việc thu thập nhật ký được áp dụng trên toàn bộ tài sản CNTT chứa dữ liệu nhạy cảm của tổ chức.

- 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 12 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/tuần.

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 doạ 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) Ban hành 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 tối thiểu 01 lần/tháng thông qua nhà cung cấp.

4.9.2.2 Sử dụng dịch vụ lọc tên miền (DNS Filtering)

Triển khai sử dụng dịch vụ lọc tên miền (DNS Filtering) 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) Xây dựng 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 trình phần mềm, giải pháp phòng chống mã độc

a) Triển khai và duy trì phần mềm, giải pháp phòng, chống mã độc 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 hoá tính năng tự động thực thi (autorun, autoplay…) đối với các phương tiện lưu trữ di động như ổ cứng, thẻ nhớ, USB…

4.10.2.3 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).

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) Xây dựng, ban hành, đảm bảo tuân thủ 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 thay đổi trong tổ chức ảnh hưởng đến quy định.

4.11.2.2 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 sao lưu dữ liệu tự động.

4.11.2.3 Bảo vệ bản sao lưu dữ liệu

a) 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.

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

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

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, an toàn thông tin.

d) 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.

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.

- Có phương án kiểm soát truy cập giữa các vùng mạng; kiểm soát truy cập thiết bị đầu cuối, máy tính người dùng kết nối vào mạng.

- 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: có phân vùng mạng riêng cho máy chủ của hệ thống thông tin; có phân vùng mạng trung gian (DMZ) để cung cấp dịch vụ trên mạng Internet; có phân vùng mạng riêng để cung cấp dịch vụ mạng không dây; có phân vùng mạng riêng đối với máy chủ cơ sở dữ liệu; có vùng mạng nội bộ; có vùng mạng biên; có vùng mạng WAN diện rộng.

4.12.2.3 Sử dụng các giao thức truyền thông và quản trị mạng an toàn

Sử dụng các giao thức truyền thông và quản trị mạng an toàn.

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

Xây dựng và áp dụng chính sách quản lý truy cập từ xa đáp ứng các yêu cầu sau:

- Sử dụng mạng riêng ảo VPN 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 đa nhân tố để kết nối VPN và các dịch vụ xác thực khác 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.

4.12.2.5 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.

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) 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, an toàn thông tin 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) Thiết lập và duy trì một 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.

4.13.2.3 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.

c) Định kỳ tổ chức sát hạch các cá nhân tham gia bảo vệ an ninh mạng cho hệ thống thông tin.

4.14 Quản lý nhà cung cấp sản phẩm, dịch vụ

4.14.1 Khái quát

Xây dựng, phát triển và duy trì 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

Thiết lập và duy trì bản kiểm kê các nhà cung cấp sản phẩm, dịch vụ. Bao gồm:

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

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

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

d) 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

Xây dựng 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.

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 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.

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

a) Thiết lập và duy trì một 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) Thiết lập và duy trì một 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.

4.15.2.4 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.

5 Yêu cầu đối với hệ thống thông tin quan trọng về an ninh quốc gia

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) Xây dựng, ban hành và đảm bảo tuân thủ 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 tài liệu.

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 hàng 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 06 tháng 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

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.

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 02 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) Tất cả tài sản vật lý phải được kiểm tra an ninh bởi cơ quan, tổ chức có thẩm quyền theo quy định của pháp luật trước khi 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 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) Xây dựng, ban hành và đảm bảo tuân thủ 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.

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

a) Xây dựng, ban hành và đảm bảo tuân thủ 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.

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/tháng.

5.2.2.5 Quản lý tài sản thanh lý/ hư hỏng

Xây dựng, ban hành và đảm bảo tuân thủ quy trình thanh lý/ tiêu hủy tài sản CNTT, đảm bảo xóa không thể khôi phục toàn bộ dữ liệu của cơ quan, tổ chức trước khi tiến hành thanh lý/tiêu hủy.

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 02 lần/năm.

5.3.2 Yêu cầu chi tiết

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) Xây dựng, ban hành và đảm bảo tuân thủ 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 02 lần/năm hoặc khi xảy ra các thay đổi trong tổ chức ảnh hưởng đến danh sách.

5.3.2.3 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 02 lần/năm.

5.3.2.4 Xử lý các tài sản phần mềm trái phép

a) Xây dựng, ban hành và đảm bảo tuân thủ quy trình phát hiện và xử lý các phần mềm trái phép định kỳ tối thiểu 01 lần/quý.

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, 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) Xây dựng, ban hành và đảm bảo tuân thủ 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 đơn vị.

- 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 (*thực hiện theo quy định của Luật Bảo vệ bí mật nhà nước*).

c) Xây dựng quy trình yêu cầu truy cập, thêm mới, sửa, xoá dữ liệu để kiểm soát nhật ký 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/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 hoá dữ liệu quan trọng

a) Mã hoá dữ liệu quan trọng được lưu trữ trong các tài sản phần cứng và phần mềm của tổ chức.

b) Mã hoá dữ liệu quan trọng trong quá trình truyền gửi để đảm bảo tính toàn vẹn của dữ liệu.

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

5.4.2.5 Tài liệu hoá luồng dữ liệu

a) Có tài liệu mô tả các luồng dữ liệu quan trọng.

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.

5.4.2.6 Tách biệt quá trình xử lý và lưu trữ dữ liệu theo mức độ nhạy cảm

a) Xây dựng, ban hành và đảm bảo tuân thủ 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 với dữ liệu có độ nhạy cảm thấp (cả về mặt logic và vật lý). 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.

5.4.2.7 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 mức 03 trở lên được lưu trữ, xử lý trong hệ thống thông tin.

5.4.2.8 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: bao gồm các hành vi chỉnh sửa, huỷ bỏ dữ liệu đối với mức 03, các hành vi xem, chỉnh sửa, huỷ bỏ dữ liệu đối với mức 04.

b) Rà soát nhật ký thường xuyên, tối thiểu định kỳ 01 lần/tháng để phát hiện sớm những hành vi truy cập trái phép.

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

Việc sử dụng chữ ký số khi trao đổi thông tin số, dữ liệu số quan trọng đáp ứng quy định tại 8.2.3.5 của TCVN 11930:2017 về Chống chối bỏ.

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) Xây dựng, ban hành và đảm bảo tuân thủ quy định, quy trình cấu hình an toàn cho các tài sản phần cứng và phần mềm của cơ quan, tổ chức.

b) Xây dựng, ban hành và đảm bảo tuân thủ 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) 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.

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

a) Tự động khoá phiên làm việc trên các tài sản sau một khoảng thời gian không sử dụng.

- Đối với máy tính người dùng: không quá 15 min.

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

- Đối với thiết bị di động: không quá 02 min.

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

b) Tự động khoá 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 h, tối đa 30 ngày.

5.5.2.3 Gỡ bỏ hoặc vô hiệu hoá các tính năng, dịch vụ không cần thiết trên các tài sản phần cứng và phần mềm

Xây dựng, ban hành và đảm bảo tuân thủ quy định gỡ bỏ hoặc vô hiệu hoá các tính năng, dịch vụ không cần thiết trên các tài sản phần cứng và phần mềm.

5.5.2.4 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.

5.5.2.5 Thiết lập khả năng xoá sạch dữ liệu từ xa trên thiết bị di động cấp cho người dùng

Xây dựng và triển khai giải pháp xoá sạch dữ liệu từ xa trên thiết bị di động cấp cho người dùng.

5.5.2.6 Phân tách các không gian làm việc riêng biệt trên các thiết bị di động cấp cho người dùng

a) Xây dựng, ban hành và đảm bảo tuân thủ 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.

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

5.6.1 Khái quát

a) Thiết lập, tuân thủ và duy trì quy trình, sử dụng 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) Xây dựng và thực thi 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 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 hoá 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.

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

a) Xây dựng, ban hành và đảm bảo tuân thủ quy định sử dụng mật khẩu an toàn trong tổ chức, đáp ứng các yêu cầu 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 đa nhân tố, quy định mật khẩu có tối thiểu 08 ký tự.

- Đối với các hệ thống không sử dụng xác thực đa nhân tố, 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.

b) Đối với tài khoản quản trị cần đảm bảo tuân thủ các quy định bổ sung:

- Thay đổi mật khẩu định kỳ 01 lần/02 tháng.

- 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

Xây dựng, ban hành và đảm bảo tuân thủ 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.

- Quy định về quản lý thiết bị lưu khóa bí mật và khóa bí mật.

- Xoá hoặc vô hiệu hoá các tài khoản không hoạt động sau 45 ngày hoặc ngay khi có thay đổi về nhân sự quản lý 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

Xây dựng, ban hành và đảm bảo tuân thủ 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 đa nhân tố 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.

5.6.2.5 Xây dựng và tuân thủ quy trình cấp mới, thay đổi và thu hồi quyền truy cập

a) Xây dựng, ban hành và đảm bảo tuân thủ 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.

5.7 Quản lý lỗ hổng bảo mật

5.7.1 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 doạ, lỗ hổng bảo mật mới từ nhiều nguồn.

5.7.2 Yêu cầu cụ thể

5.7.2.1 Thiết lập, tuân thủ và duy trì quy trình quản lý lỗ hổng bảo mật

a) Xây dựng, ban hành và đảm bảo tuân thủ 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: Thiết lập và duy trì 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: Xây dựng phương án, 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 và cập nhật quy trình tối thiểu 01 lần/năm hoặc khi xảy ra thay đổi trong tổ chức ảnh hưởng đến quy trình này.

5.7.2.2 Thiết lập, tuân thủ và duy trì quy trình quản lý bản vá

Xây dựng, ban hành và đảm bảo tuân thủ 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, tuân thủ và duy trì một quy trình quản lý nhật ký an ninh mạng

a) Xây dựng, ban hành và đảm bảo tuân thủ 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: đia 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.

- Nhật ký tiến trình hoạt động tối thiểu bao gồm: thông tin thiết bị (IP/ tên thiết bị, tên miền), 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.

- Đảm bảo việc thu thập nhật ký được áp dụng trên toàn bộ tài sản CNTT chứa dữ liệu nhạy cảm của tổ chức.

- 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 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 hệ thống từ đối tượng giám sát về hệ thống giám sát.

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

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

5.8.2.2 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.

5.8.2.3 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.

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 doạ 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) Ban hành 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 và dịch vụ thư điện tử được rà soát, cập nhật bản vá lỗ hổng bảo mật tối thiểu 01 lần/tháng thông qua nhà cung cấp.

5.9.2.2 Sử dụng dịch vụ lọc tên miền (DNS Filtering)

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

5.9.2.3 Thực thi, cập nhật các bộ lọc URL và giới hạn số lượng kết nối đến các ứng dụng, dịch vụ

a) 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.

b) Giới hạn số lượng kết nối đồng thời bên ngoài mạng (bên ngoài vùng mạng cài đặt, quản trị ứng dụng, dịch vụ) 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

5.9.2.4 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.

5.9.2.5 Triển khai giải pháp xác thực email

Triển khai giải pháp xác thực email thông qua DMARC (Domain-based Message Authentication, Reporting & Conformance) để tăng cường bảo mật và ngăn chặn các cuộc tấn công lừa đảo, giả mạo đối với các tên miền của tổ chức.

5.9.2.6 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.

5.9.2.7 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.

5.10 Phòng chống phần mềm độc hại

5.10.1 Khái quát

a) Xây dựng 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.

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 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

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

b) Đáp ứng yêu cầu tại 9.2.2.5 của TCVN 11930:2017 về Phòng chống phần mềm độc hại.

5.10.2.3 Quản lý tập trung các phần mềm phòng, chống mã độc

Đáp ứng yêu cầu tại 9.2.2.5 của TCVN 11930:2017 về Phòng chống phần mềm độc hại.

5.10.2.4 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).

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

a) Triển khai giải pháp phòng và chống mã độc dựa trên hành vi (EDR - Endpoint Detection and Response).

b) Kết nối về hệ thống quản lý nhật ký và sự kiện tập trung (SIEM) để thực hiện giám sát theo thời gian thực và đưa ra cảnh báo kịp thời.

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) Xây dựng, ban hành và đảm bảo tuân thủ 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.

- 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 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 sao lưu dữ liệu tự động.

5.11.2.3 Bảo vệ bản sao lưu dữ liệu

a) 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.

b) Thực hiện mã hoá 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

a) 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.

b) Đáp ứng yêu cầu tại 9.2.4.3 của TCVN 11930:2017 về Sao lưu dự phòng.

5.11.2.5 Kiểm tra khả năng khôi phục dữ liệu

Kiểm tra khả năng khôi phục bản sao lưu dữ liệu tối thiểu 01 lần/quý.

5.12 Quản lý hạ tầng mạng

5.12.1 Khái quát

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. 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, an toàn thông tin trước khi triển khai thực hiện.

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, an toàn thông tin.

d) Xây dựng phương án và thực hiện quản lý và bảo vệ tài liệu, hồ sơ thiết kế.

e) 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.

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 dự phòng 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 kết nối mạng Internet từ các ISP sử dụng hạ tầng kết nối trong nước khác nhau.

- Có phương án kiểm soát truy cập giữa các vùng mạng; kiểm soát truy cập thiết bị đầu cuối, máy tính người dùng kết nối vào mạng.

- 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.

b) Chia tách thành các vùng mạng khác nhau theo đối tượng sử dụng, mục đích sử dụng, tối thiểu: có phân vùng mạng riêng cho máy chủ của hệ thống thông tin; có phân vùng mạng trung gian (DMZ) để cung cấp dịch vụ trên mạng Internet; có phân vùng mạng riêng để cung cấp dịch vụ mạng không dây; có phân vùng mạng riêng đối với máy chủ cơ sở dữ liệu; có vùng mạng nội bộ; có vùng mạng biên; có vùng mạng WAN diện rộng.

5.12.2.3 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.

5.12.2.4 Sử dụng các giao thức truyền thông và quản trị mạng an toàn

Sử dụng các giao thức truyền thông và quản trị mạng an toàn.

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

Xây dựng và áp chính sách quản lý truy cập từ xa đáp ứng các yêu cầu sau:

- Sử dụng mạng riêng ảo VPN 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 đa nhân tố để kết nối VPN và các dịch vụ xác thực khác 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.

5.12.2.6 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.

5.12.2.7 Kiểm thử và nghiệm thu hệ thống

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

b) Có đơn vị độc lập hoặc bộ phận độc lập thuộc đơn vị thực hiện tư vấn, giám sát quá trình thử nghiệm và nghiệm thu hệ thống.

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

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 doạ.

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, an toàn thông tin 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 giải pháp quản lý tập trung các sự kiện an ninh mạng 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, an toàn hệ thống thông tin 24/7.

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 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.

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

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

5.13.2.5 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.

5.13.2.6 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.

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.

5.14.2.2 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) Thiết lập và duy trì một 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.

5.14.2.3 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.

5.14.2.4 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.

5.15 Quản lý nhà cung cấp sản phẩm, dịch vụ

5.15.1 Khái quát

Xây dựng, phát triển và duy trì 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

5.15.2.1 Thiết lập và duy trì bản kiểm kê các nhà cung cấp sản phẩm, dịch vụ

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

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

c) Các nhà cung cấp sản phẩm, dịch vụ an ninh mạng phải đủ điều kiện kinh doanh sản phẩm, dịch vụ an ninh mạng theo Luật An ninh mạng.

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

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

5.15.2.2 Thiết lập và duy trì quy định quản lý nhà cung cấp dịch vụ

a) Xây dựng, ban hành và đảm bảo tuân thủ 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.

5.15.2.3 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.

5.15.2.4 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.

5.15.2.5 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.

5.16 Phát triển ứng dụng an toàn

5.16.1 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.

5.16.2 Yêu cầu cụ thể

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

a) Xây dựng, ban hành và đảm bảo tuân thủ 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. Trong đó, yêu cầu cung cấp mã nguồn phần mềm.

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

a) Xây dựng, ban hành và đảm bảo tuân thủ 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.

5.16.2.3 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.

5.16.2.4 Thiết lập và quản trị hệ thống kiểm kê 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.

5.16.2.5 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.

5.16.2.6 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.

5.16.2.7 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.

5.16.2.8 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 hoá được chuẩn hoá và đánh giá rộng rãi.

c) Ghi nhật ký kiểm toán hành vi của người dùng trong sản phẩm.

5.16.2.9 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 (component, extension...) 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.

5.17 Quản trị ứng phó sự cố an ninh mạng

5.17.1 Khái quát

Xây dựng 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.

5.17.2 Yêu cầu cụ thể

5.17.2.1 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.

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

a) Thiết lập và duy trì một 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.

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

a) Thiết lập và duy trì một 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) Quy trình ứng phó sự cố an ninh mạng cần tuân thủ quy định tại Điều 17 Nghị định 53/2022/NĐ-CP quy định chi tiết một số điều của Luật 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.

5.17.2.4 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.

5.17.2.5 Thực hiện đánh giá sau sự cố an ninh mạng

Thực hiện đánh giá sau sự cố an ninh mạng.

5.17.2.6 Định kỳ diễn tập ứng phó sự cố an ninh mạng

Lập kế hoạch và thực hiện diễn tập các kịch bản ứng phó sự cố định kỳ tối thiểu 01 lần/năm.

5.17.2.7 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.

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, đặc biệt là hệ thống thông tin quan trọng về an ninh quốc gia 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; đánh giá xâm nhập hệ thống thông tin.

5.18.2 Yêu cầu chi tiết

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

a) Thiết lập và duy trì một 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 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 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.

5.18.2.3 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.

5.18.2.4 Rà soát các biện pháp bảo mật

Kiểm tra các biện pháp bảo mật sau mỗi lần thực hiện kiểm thử xâm nhập.

5.18.2.5 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.

5.18.2.6 Thực hiện đánh giá xâm nhập hệ thống

Định kỳ thực hiện đánh giá xâm nhập để tìm kiếm, xác định các dấu vết tấn công và xâm nhập đang diễn ra hoặc đã xảy ra trong hệ thống thông tin (nếu có) tối thiểu 01 lần/năm.

Thư mục tài liệu tham khảo

[1] CIS (Center for Internet Security) Critical Security Controls Version 8, 2021.

[2] NIST SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations), September 23, 2021.
