BỘ CÔNG AN	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 565 /BCA-A05 V/v tham gia ý kiến dự thảo Hướng dẫn bảo đảm an ninh mạng hệ thống thông tin giải quyết thủ tục hành chính	*Hà Nội, ngày 10 tháng 02 năm 2026*

Kính gửi: ..... UBND tỉnh Điện Biên .....

Thực hiện các nhiệm vụ của Bộ Công an tại Nghị định số 118/2025/NĐ-CP ngày 09/6/2025 về thực hiện thủ tục hành chính theo cơ chế một cửa, một cửa liên thông tại bộ phận một cửa và Cổng dịch vụ công quốc gia, Bộ Công an đã dự thảo "Tài liệu hướng dẫn bảo đảm an ninh mạng cho hệ thống thông tin giải quyết thủ tục hành chính cấp bộ, cấp tỉnh". Căn cứ chức năng nhiệm vụ được giao, Bộ Công an đề nghị các đơn vị tham gia ý kiến dự thảo tài liệu hướng dẫn (*dự thảo kèm theo*) và trao đổi bằng văn bản về Bộ Công an (*qua Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, địa chỉ: E2 Dương Đình Nghệ, Cầu Giấy, Hà Nội*) trước ngày 27/02/**2026** để tập hợp.

Bộ Công an cử đồng chí Đại úy Nguyễn Hồng Hải - Cán bộ Phòng Bảo vệ an ninh hệ thống mạng thông tin quốc gia, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an (*điện thoại: 0904.855.495*) là đầu mối liên hệ, phối hợp.

Bộ Công an trao đổi các đơn vị để phối hợp./.

Nơi nhận:
- Như trên;
- Đ/c Bộ trưởng (để báo cáo);
- Lưu: VT, A05(P7).NHH.55b.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Thượng tướng Phạm Thế Tùng

BỘ CÔNG AN

DỰ THẢO

TÀI LIỆU HƯỚNG DẪN
BẢO ĐẢM AN NINH MẠNG CHO HỆ THỐNG THÔNG TIN GIẢI QUYẾT THỦ TỤC HÀNH CHÍNH CẤP BỘ, TỈNH

(*Kèm theo Công văn số /BCA-A05 ngày tháng năm 2026 của Bộ Công an*)

Hà Nội, 2026

MỤC LỤC

THUẬT NGỮ, TỪ VIẾT TẮT

STT	Từ viết tắt	Nghĩa đầy đủ
1	Nghị định 85/2016/NĐ- CP	Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ
2	Thông tư 12/2022/TT- BTTTT	Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an ninh, an toàn hệ thống thông tin theo cấp độ
3	TCVN 11930:2017	Tiêu chuẩn quốc gia TCVN 11930:2017 về Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ
4	TCVN 14423:2025	Tiêu chuẩn quốc gia TCVN 14423:2025 về An ninh mạng - Yêu cầu đối với hệ thống thông tin quan trọng
5	CNTT	Công nghệ thông tin
6	WAN	Mạng tin học diện rộng
7	LAN	Mạng nội bộ
8	HSĐXCĐ	Hồ sơ đề xuất cấp độ

TÀI LIỆU HƯỚNG DẪN
BẢO ĐẢM AN NINH MẠNG CHO HỆ THỐNG THÔNG TIN GIẢI QUYẾT THỦ TỤC HÀNH CHÍNH

I. HƯỚNG DẪN CHUNG

1.1. Căn cứ xây dựng và phạm vi điều chỉnh

Tài liệu này hướng dẫn việc thực thi tổng thể, đồng bộ các biện pháp bảo đảm an ninh mạng cho các hệ thống thông tin giải quyết thủ tục hành chính (TTHC) thuộc phạm vi quản lý cấp bộ, tỉnh. Nội dung được hướng dẫn trong tài liệu này bao gồm các nội dung chính sau:

(1) Triển khai các biện pháp bảo vệ theo phương án (*bao gồm phương án quản lý và phương án kỹ thuật*) được phê duyệt trong Hồ sơ đề xuất cấp độ (*tối thiểu cấp độ 3 cho phục vụ hoạt động của các cơ quan, tổ chức trong phạm vi một ngành, một tỉnh*);

(2) Tổ chức bảo đảm an ninh mạng cho hệ thống thông tin giải quyết TTHC các bộ, ngành, địa phương theo mô hình tổ chức, bộ máy mới.

Nội dung trong hướng dẫn này được xây dựng dựa trên các văn bản và các tài liệu kỹ thuật sau đây:

- Luật An ninh mạng số 24/2018/QH14; Luật An toàn thông tin mạng số 86/2015/QH13 (*có hiệu lực đến ngày 01/7/2026*);

- Luật An ninh mạng số 116/2025/QH15 (*có hiệu lực từ ngày 01/7/2026*);

- Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an ninh, an toàn hệ thống thông tin theo cấp độ;

- Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toànhệ thống thông tin theo cấp độ;

- Nghị định số 118/2025/NĐ-CP ngày 09/06/2025 của Chính phủ về thực hiện thủ tục hành chính theo cơ chế một cửa, một cửa liên thông tại bộ phận một cửa và Cổng dịch vụ công quốc gia;

- Nghị định số 367/2025/NĐ-CP ngày 31/12/2025 của Chính phủ về sửa đổi, bổ sung một số điều của Nghị định số 118/2025/NĐ-CP ngày 09/06/2025 của Chính phủ về thực hiện thủ tục hành chính theo cơ chế một cửa, một cửa liên thông tại bộ phận một cửa và Cổng dịch vụ công quốc gia;

- Tiêu chuẩn quốc gia TCVN 11930:2017 về Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ;

- Tiêu chuẩn quốc gia TCVN 14423:2025 về An ninh mạng - Yêu cầu đối với hệ thống thông tin quan trọng.

- Các nghị định, thông tư, tiêu chuẩn quốc gia TCVN 11930:2017, TCVN 14423:2025 có hiệu lực đến khi có các văn bản khác thay thế, có hiệu lực.

1.2. Đối tượng áp dụng

Tài liệu này được xây dựng để hướng dẫn và khuyến nghị áp dụng đối với cơ quan, tổ chức là chủ quản hệ thống thông tin, đơn vị chuyên trách về an ninh mạng và đơn vị quản trị, vận hành, khai thác, sử dụng hệ thống thông tin giải quyết TTHC thuộc phạm vi quản lý cấp bộ. Đối với hệ thống thông tin giải quyết TTHC cấp tỉnh có thể áp dụng hướng dẫn này trong giai đoạn từ nay đến khi hoàn thiện theo Mô hình Kiến trúc Hệ thống thông tin giải quyết thủ tục hành chính cấp bộ, cấp tỉnh (*Mô hình 5721*). Ngoài ra, các cơ quan, tổ chức khác có thể tham khảo tài liệu hướng dẫn này để bảo đảm an ninh mạng hệ thống thông tin tổng thể, đồng bộ, hiệu quả.

II. TRIỂN KHAI CÁC BIỆN PHÁP BẢO VỆ THEO PHƯƠNG ÁN ĐƯỢC PHÊ DUYỆT TRONG HỒ SƠ ĐỀ XUẤT CẤP ĐỘ

2.1. Hướng dẫn chung

Hồ sơ đề xuất cấp độ (*HSĐXCĐ*) của Hệ thống thông tin giải quyết thủ tục hành chính cấp bộ, tỉnh phải được phê duyệt phương án (*bao gồm phương án quản lý và phương án kỹ thuật*) đáp ứng yêu cầu bảo đảm an toàn hệ thống thông tin tối thiểu cấp độ 3. Do đó, cơ quan, tổ chức cần triển khai đầy đủ các biện pháp bảo đảm an ninh mạng hệ thống thông tin theo quy định tại Điều 9, Điều 10 Thông tư số 12/2022/TT-BTTTT.

Phương án bảo đảm an ninh mạng về quản lý đưa ra các yêu cầu an toàn để bảo đảm an ninh, an toàn hệ thống thông tin trong quá trình vận hành, khai thác. Để đáp ứng các yêu cầu an toàn về quản lý, cơ quan, tổ chức cần xây dựng Quy chế bảo đảm an ninh mạng. Trong đó, Quy chế bao gồm các quy định, quy trình bảo đảm an ninh mạng nhằm đáp ứng toàn bộ các yêu cầu về quản lý theo quy định.

Phương án bảo đảm an ninh mạng về kỹ thuật đưa ra các yêu cầu về thiết kế, thiết lập hệ thống thông tin. Các yêu cầu kỹ thuật là cơ sở để cơ quan, tổ chức xác định được các biện pháp bảo đảm an ninh mạng cần triển khai làm cơ sở để xác định các hạng mục cần đầu tư, trang bị. Yêu cầu kỹ thuật cũng đưa ra yêu cầu về việc thiết lập cấu hình bảo mật trên từng thiết bị, máy chủ, ứng dụng và cơ sở dữ liệu trước khi đưa vào sử dụng.

2.2. Hướng dẫn triển khai các biện pháp về quản lý

Cơ quan, tổ chức cần xây dựng và ban hành Quy chế bảo đảm an ninh mạng; trong đó, bao gồm các quy định, quy trình bảo đảm an ninh mạng nhằm đáp ứng toàn bộ các yêu cầu về quản lý theo quy định, do cấp có thẩm quyền ban hành, trước khi đưa hệ thống vào vận hành, khai thác.

Quy chế bảo đảm an ninh mạng cần quy định tối thiểu các nội dung sau để đáp ứng các yêu cầu an ninh, an toàn về quản lý, bao gồm các nội dung:

(1) Mục tiêu, nguyên tắc bảo đảm an ninh mạng.

(2) Phạm vi chính sách an ninh mạng.

(3) Quy định việc xây dựng, cập nhật và sửa đổi Quy chế.

(4) Trách nhiệm bảo đảm an ninh mạng.

(5) Đầu mối phối hợp với cơ quan/tổ chức có thẩm quyền trong hoạt động bảo đảm an ninh mạng.

(6) Bảo đảm nguồn nhân lực: Quy định/quy trình thực hiện quản lý bảo đảm nguồn nhân lực an ninh mạng của tổ chức, bao gồm: Tuyển dụng cán bộ; quy chế/quy định bảo đảm an ninh mạng trong quá trình làm việc và chấm dứt hoặc thay đổi công việc (*Các quy định đưa ra phải đáp ứng các yêu cầu tại Mục 7.1.3 Tiêu chuẩn quốc gia TCVN 11930:2017*).

(7) Quản lý thiết kế, xây dựng hệ thống: Quy định chính sách/quy trình thực hiện quản lý thiết kế, xây dựng hệ thống của tổ chức, bao gồm: Thiết kế an toàn hệ thống thông tin; Phát triển phần mềm thuê khoán; Thử nghiệm và nghiệm thu hệ thống (*Các quy định đưa ra phải đáp ứng các yêu cầu tại Mục 7.1.4 Tiêu chuẩn quốc gia TCVN 11930:2017*).

(8) Quản lý vận hành hệ thống:

- *Quản lý an ninh, an toàn mạng*: Quy định chính sách/quy trình thực hiện quản lý an toàn hạ tầng mạng của tổ chức, bao gồm: Quản lý vận hành hoạt động bình thường của hệ thống; Cập nhật, sao lưu dự phòng và khôi phục hệ thống sau khi xảy ra sự cố; Truy cập và quản lý cấu hình hệ thống; Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) trước khi đưa vào vận hành, khai thác (*Các quy định đưa ra phải đáp ứng các yêu cầu tại Mục 7.1.5.1 Tiêu chuẩn quốc gia TCVN 11930:2017*).

- *Quản lý an ninh, an toàn máy chủ và ứng dụng*: Quy định chính sách/quy trình thực hiện quản lý an ninh, an toàn máy chủ và ứng dụng của tổ chức, bao gồm: Quản lý vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ; Truy cập mạng của máy chủ; Truy cập và quản trị máy chủ và ứng dụng; Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố; Cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống; Kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống; Cấu hình tối ưu và tăng cường bảo mật cho hệ thống máy chủ trước khi đưa vào vận hành, khai thác (*Các quy định đưa ra phải đáp ứng các yêu cầu tại Mục 7.1.5.2 Tiêu chuẩn quốc gia TCVN 11930:2017*).

- *Quản lý an ninh, an toàn dữ liệu*: Quy định chính sách/quy trình thực hiện quản lý an ninh, an toàn dữ liệu, thông tin nhạy cảm (dữ liệu cá nhân, tổ chức) của tổ chức, bao gồm: Yêu cầu an toàn đối với phương pháp mã hóa; Phân loại, quản lý và sử dụng khóa bí mật và dữ liệu mã hóa; Cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu; Trao đổi dữ liệu qua môi trường mạng và phương tiện lưu trữ; Sao lưu dự phòng và khôi phục dữ liệu; Cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ (*Các*

quy định đưa ra phải đáp ứng các yêu cầu tại Mục 7.1.5.3 Tiêu chuẩn quốc gia TCVN 11930:2017).

- *Quản lý an ninh, an toàn thiết bị đầu cuối*: Quy định chính sách/quy trình thực hiện quản lý an ninh, an toàn thiết bị đầu cuối của tổ chức, bao gồm: Quản lý vận hành hoạt động bình thường cho thiết bị đầu cuối; Kết nối, truy cập và sử dụng thiết bị đầu cuối từ xa; Cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống; Cấu hình tối ưu và tăng cường bảo mật cho máy tính người sử dụng; Kiểm tra, đánh giá, xử lý điểm yếu an ninh mạng cho thiết bị đầu cuối (*Các quy định đưa ra phải đáp ứng các yêu cầu tại Mục 7.1.5.4 Tiêu chuẩn quốc gia TCVN 11930:2017*).

- *Quản lý phòng chống phần mềm độc hại*: Quy định chính sách/quy trình thực hiện quản lý phòng chống phần mềm độc hại của tổ chức, bao gồm: Cài đặt, cập nhật, sử dụng phần mềm phòng chống mã độc; Cài đặt, sử dụng phần mềm trên máy tính, thiết bị di động và việc truy cập các trang thông tin trên mạng; Gửi nhận tập tin qua môi trường mạng và các phương tiện lưu trữ di động; Thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; Kiểm tra và xử lý phần mềm độc hại (*Các quy định đưa ra phải đáp ứng các yêu cầu tại Mục 7.1.5.5 Tiêu chuẩn quốc gia TCVN 11930:2017*).

- *Quản lý giám sát an ninh, an toàn hệ thống thông tin*: Quy định chính sách/quy trình thực hiện quản lý giám sát an ninh, an toàn hệ thống thông tin của tổ chức, bao gồm: Quản lý vận hành hoạt động bình thường của hệ thống giám sát; Đối tượng giám sát bao gồm; Kết nối và gửi nhật ký hệ thống; Truy cập và quản trị hệ thống giám sát; Loại thông tin cần được giám sát; Lưu trữ và bảo vệ thông tin giám sát; Theo dõi, giám sát và cảnh báo sự cố; Bố trí nguồn lực và tổ chức giám sát (*Các quy định đưa ra phải đáp ứng các yêu cầu tại Mục 7.1.5.6 Tiêu chuẩn quốc gia TCVN 11930:2017*).

- *Quản lý điểm yếu an ninh mạng*: Quy định chính sách/quy trình thực hiện quản lý điểm yếu an ninh mạng của tổ chức, bao gồm: Quản lý thông tin các thành phần có trong hệ thống có khả năng tồn tại điểm yếu an ninh mạng; Quản lý, cập nhật nguồn cung cấp điểm yếu an ninh mạng; Phân nhóm và mức độ của điểm yếu; Cơ chế phối hợp với các nhóm chuyên gia; Kiểm tra, đánh giá và xử lý điểm yếu an ninh mạng trước khi đưa hệ thống vào sử dụng; Quy trình khôi phục lại hệ thống (*Các quy định đưa ra phải đáp ứng các yêu cầu tại Mục 7.1.5.7 Tiêu chuẩn quốc gia TCVN 11930:2017*).

- *Quản lý sự cố an ninh mạng*: Quy định chính sách/quy trình thực hiện quản lý sự cố an ninh mạng của tổ chức, bao gồm: Phân nhóm sự cố an ninh mạng; Phương án tiếp nhận, phát hiện, phân loại và xử lý thông tin; 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 trong việc xử lý, khắc phục sự cố an ninh mạng; Diễn tập phương án xử lý sự cố an ninh mạng (*Các quy định*

đưa ra phải đáp ứng các yêu cầu tại Mục 7.1.5.8 Tiêu chuẩn quốc gia TCVN 11930:2017).

- *Quản lý an ninh, an toàn người sử dụng đầu cuối*: Quy định chính sách/quy trình thực hiện quản lý an ninh, an toàn người sử dụng đầu cuối của tổ chức, bao gồm: Quản lý truy cập, sử dụng tài nguyên nội bộ; Quản lý truy cập mạng và tài nguyên trên Internet; Cài đặt và sử dụng máy tính an toàn (*Các quy định đưa ra phải đáp ứng các yêu cầu tại Mục 7.1.5.9 Tiêu chuẩn quốc gia TCVN 11930:2017*).

2.3. Hướng dẫn triển khai các biện pháp về kỹ thuật

2.3.1. Thiết lập cấu hình bảo mật để đáp ứng các yêu cầu an ninh, an toàn về thiết kế hệ thống

a) Quản lý truy cập, quản trị hệ thống từ xa đảm bảo an ninh, an toàn

Thiết lập cấu hình cho sản phẩm quản lý truy cập, quản trị hệ thống từ xa an toàn (VPN) hoặc chức năng VPN được tích hợp trên tường lửa lớp mạng. Một số thiết lập, cấu hình VPN cụ thể: Cấu hình tính năng xác thực 2 lớp khi đăng nhập VPN; Thiết lập cấu hình VPN truy cập hệ thống thông qua máy chủ trung gian (Jump Server); Kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể; Phân quyền và cấp quyền truy cập từ bên ngoài vào hệ thống theo từng người dùng hoặc nhóm người dùng căn cứ theo yêu cầu nghiệp vụ, yêu cầu quản lý; Cấu hình chặn các IP nước ngoài truy cập đối với các hệ thống đặc thù… Nhật ký hệ thống của sản phẩm/chức năng VPN được quản lý tập trung trên Hệ thống Quản lý và phân tích sự kiện an ninh mạng (SIEM).

b) Quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập

Thiết lập cấu hình cho sản phẩm phòng chống xâm nhập hoặc chức năng phòng chống xâm nhập được tích hợp trên tường lửa lớp mạng. Việc thiết lập cấu hình sản phẩm/chức năng phòng chống xâm nhập phải bảo đảm đầy đủ về độ phủ của các vùng mạng theo cấp độ tương ứng, bao gồm: Vùng mạng nội bộ; Vùng mạng biên; Vùng DMZ; Vùng máy chủ nội bộ; Vùng mạng không dây (nếu có) tách riêng, độc lập với các vùng mạng khác; Vùng mạng máy chủ cơ sở dữ liệu; Vùng quản trị; Vùng quản trị thiết bị hệ thống. Nhật ký hệ thống của thiết bị/giải pháp được quản lý tập trung trên SIEM.

c) Cân bằng tải, dự phòng nóng cho các thiết bị mạng/thiết bị mạng chính

Thiết lập cấu hình chức năng cân bằng tải, dự phòng nóng trên thiết bị mạng/thiết bị mạng chính. Các thiết bị mạng chính tối thiểu bao gồm: Thiết bị chuyển mạch trung tâm hoặc tương đương; Thiết bị tường lửa trung tâm; Tường lửa ứng dụng web; Tường lửa cơ sở dữ liệu (*nếu có*).

d) Bảo đảm an ninh mạng cho máy chủ cơ sở dữ liệu

Thiết lập cấu hình cho tường lửa cơ sở dữ liệu để bảo vệ cơ sở dữ liệu của

hệ thống. Các cơ sở dữ liệu cần bảo vệ được xác định dựa vào Danh mục ứng dụng được đưa ra trong HSĐXCĐ. Ngoài ra, cấu hình tăng cường bảo mật cho hệ điều hành và cơ sở dữ liệu (*Cơ quan, tổ chức có thể tham khảo tài liệu SP800-123 Guide to General Server Security của Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ - NIST để thực hiện*) như: Thiết lập cấu hình tường lửa hệ điều hành máy chủ cơ sở dữ liệu để quản lý truy cập giữa các máy chủ trong cùng một vùng mạng; Thiết lập cấu hình hệ thống để định kỳ tự động thực hiện sao lưu dự phòng cơ sở dữ liệu trên hệ thống lưu trữ độc lập… Nhật ký hệ thống của tường lửa cơ sở dữ liệu được thiết lập và quản lý tập trung trên SIEM.

đ) Chặn lọc phần mềm độc hại trên môi trường mạng

Thiết lập cấu hình cho sản phẩm hoặc chức năng phòng, chống mã độc trên môi trường mạng được tích hợp trên tường lửa lớp mạng/thiết bị phòng, chống xâm nhập. Việc thiết lập cấu hình phòng, chống mã độc trên môi trường mạng phải bảo đảm đầy đủ về độ phủ của các vùng mạng theo cấp độ tương ứng, bao gồm: Vùng mạng nội bộ; Vùng mạng biên; Vùng DMZ; Vùng máy chủ nội bộ; Vùng mạng không dây (nếu có) tách riêng, độc lập với các vùng mạng khác; Vùng mạng máy chủ cơ sở dữ liệu; Vùng quản trị; Vùng quản trị thiết bị hệ thống. Nhật ký hệ thống của sản phẩm được thiết lập và quản lý tập trung trên SIEM.

e) Phòng chống tấn công từ chối dịch vụ

Thiết lập cấu hình trên sản phẩm phòng chống tấn công từ chối dịch vụ hoặc có giải pháp tương đương hoặc thuê dịch vụ chuyên nghiệp của doanh nghiệp để phòng, chống tấn công từ chối dịch vụ lớp mạng và lớp ứng dụng. Nhật ký hệ thống của sản phẩm được thiết lập và quản lý tập trung trên SIEM.

g) Phòng chống tấn công mạng cho ứng dụng web

Thiết lập cấu hình cho sản phẩm tường lửa ứng dụng web để bảo vệ toàn bộ ứng dụng (*theo Danh mục ứng dụng được đưa ra trong HSĐXCĐ*) của hệ thống, được cung cấp dịch vụ ra bên ngoài. Tường lửa ứng dụng web là thiết bị mạng chính, do đó cần cấu hình chức năng cân bằng tải, dự phòng nóng cho thiết bị này. Nhật ký hệ thống của sản phẩm này được thiết lập và quản lý tập trung trên SIEM.

h) Bảo đảm an ninh mạng cho hệ thống thư điện tử

Thiết lập cấu hình trên sản phẩm bảo đảm an ninh mạng cho hệ thống thư điện tử để bảo vệ hệ thống thư điện tử. Nhật ký hệ thống của sản phẩm được thiết lập và quản lý tập trung trên SIEM.

i) Quản lý truy cập lớp mạng

Thiết lập cấu hình cho sản phẩm quản lý truy cập lớp mạng để quản lý thông tin, truy cập của máy chủ, máy trạm và thiết bị hệ thống trong mạng; Thiết lập cấu hình bảo mật trên thiết bị chuyển mạch lớp 2 cho phép phát hiện và quản lý truy cập mạng lớp 2 đối với các thiết bị kết nối vào hệ thống. Nhật ký hệ

thống của sản phẩm được thiết lập và quản lý tập trung trên SIEM.

k) Giám sát hệ thống thông tin tập trung

Thiết lập cấu hình trên sản phẩm/giải pháp giám sát hệ thống thông tin tập trung đáp ứng tối thiểu các yêu cầu sau: Giám sát được trạng thái hoạt động của thiết bị, máy chủ và ứng dụng được thuyết minh trong HSĐXCĐ; Cấu hình các chức năng cảnh báo bất thường, ảnh hưởng tới hoạt động bình thường của thiết bị, máy chủ và ứng dụng qua tin nhắn, thư điện tử… Trạng thái giám sát tối thiểu bao gồm các thông tin hiệu năng của CPU, RAM, Storage và các giao diện mạng.

l) Giám sát an ninh mạng hệ thống thông tin tập trung

Thiết lập cấu hình trên sản phẩm SIEM hoặc sản phẩm có chức năng tương đương để quản lý tập trung nhật ký hệ thống của thiết bị hệ thống, máy chủ, máy trạm, ứng dụng và các thành phần khác của hệ thống (nếu có). Danh mục các thiết bị hệ thống, máy chủ, máy trạm, ứng dụng được đưa ra trong HSĐXCĐ. Một số yêu cầu tối thiểu đối với hệ thống SIEM bao gồm:

- Có chức năng quản trị: Chức năng phân tích tương quan (Correlation), Chức năng lọc (Filters), Tạo các luật (Rules), Chức năng hiển thị (Dashboards), Chức năng cảnh báo và báo cáo (Alerts and Reports), Chức năng cảnh báo thời gian thực (Real Time Alert).

- Có chức năng nhận nhật ký (log): Cho phép nhận log từ các nguồn với nhiều định dạng khác nhau từ các thiết bị mạng, máy chủ và ứng dụng; định dạng, chuẩn hóa log nhận được theo các trường thông tin tùy biến theo nhu cầu sử dụng.

- Sử dụng máy chủ thời gian NTP Server (Network Time Protocol Server) hoặc máy chủ thời gian (Master Clock) để đồng bộ thời gian giữa các thiết bị mạng, thiết bị đầu cuối và các thành phần khác trong hệ thống giám sát.

m) Quản lý sao lưu dự phòng tập trung

Thiết lập cấu hình trên hệ thống quản lý sao lưu dự phòng tập trung để quản lý sao lưu dự phòng tập trung, sử dụng giải pháp như SAN, NAS… Việc thiết lập cấu hình trên hệ thống quản lý sao lưu dự phòng tập trung cần đáp ứng các yêu cầu sau: Tối thiểu các dữ liệu sau được lưu trữ trên hệ thống quản lý tập trung (*Ảnh hệ điều hành của các máy chủ trong hệ thống, tệp tin cấu hình các thiết bị hệ thống, cơ sở dữ liệu và dữ liệu nghiệp vụ nếu có*). Ngoài ra, triển khai giải pháp mã hóa với những tệp tin sao lưu dữ liệu quan trọng (*cơ sở dữ liệu, dữ liệu nghiệp vụ*).

n) Quản lý phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng tập trung

Thiết lập cấu hình hệ thống quản lý phần mềm phòng chống mã độc đáp ứng các yêu cầu: Có chức năng quản lý tập trung, thiết lập lịch quét (scan), quản lý thiết bị ngoại vi; ưu tiên sử dụng giải pháp có tích hợp EDR (*Endpoint Detection*

and Response). Toàn bộ các máy chủ, máy trạm trong hệ thống được cài đặt sản phẩm và được quản lý trên hệ thống quản lý tập trung. Đối với các máy chủ chuyên dụng mà không có sản phẩm phòng chống mã độc trên thị trường hỗ trợ thì cần có phương án tương đương để hỗ trợ phòng, chống mã độc như: Phòng, chống mã độc trên môi trường mạng; cấu hình tăng cường bảo mật…

o) Phòng, chống thất thoát dữ liệu

Thiết lập cấu hình sản phẩm, giải pháp Phòng, chống thất thoát dữ liệu đáp ứng tối thiểu các máy chủ cơ sở dữ liệu, máy chủ trung gian (Jump Server), máy tính quản trị cơ sở dữ liệu, máy tính phục vụ hoạt động nghiệp vụ xử lý dữ liệu được triển khai các giải pháp phòng, chống thất thoát dữ liệu; Thiết lập cấu hình tường lửa hệ điều hành máy chủ cơ sở dữ liệu để quản lý truy cập giữa các máy chủ trong cùng một vùng mạng. Bên cạnh đó cần cấu hình tăng cường bảo mật cho hệ điều hành, cơ sở dữ liệu và các máy tính quản trị cơ sở dữ liệu, máy tính phục vụ hoạt động nghiệp vụ xử lý dữ liệu.

p) Dự phòng kết nối mạng Internet cho các máy chủ dịch vụ

Thiết lập cấu hình hệ thống để dự phòng kết nối mạng Internet cho các máy chủ dịch vụ; sử dụng phương án duy trì 02 kết nối Internet của hai nhà cung cấp khác nhau. Hệ thống có dải địa chỉ IP Public và có số hiệu mạng ASN riêng khi kết nối định tuyến với các nhà cung cấp khác nhau.

q) Phương án bảo đảm an ninh, an toàn cho mạng không dây

Thiết lập cấu hình hệ thống để bảo mật cho mạng không dây sử dụng giải pháp chuyên dụng hoặc việc thiết lập cấu hình bảo mật trên hệ thống để bảo đảm an ninh, an toàn cho mạng không dây. Mạng khách và mạng dành cho cán bộ, công chức, viên chức tiếp nhận, xử lý TTHC cần được tách biệt độc lập.

2.3.2. Thiết lập cấu hình thiết bị hệ thống

a) Kiểm soát truy cập ngoại mạng

Thiết lập cấu hình trên thiết bị hệ thống để quản lý truy cập từ các mạng bên ngoài theo chiều đi vào hệ thống tới các máy chủ dịch vụ bên trong mạng, bao gồm: Các dịch vụ/ứng dụng cho phép truy cập từ bên ngoài; Thời gian mất kết nối; Phân quyền truy cập; Giới hạn kết nối; Thiết lập chính sách ưu tiên. Phương án cần mô tả chính sách đó được thiết lập trên thiết bị hệ thống nào. Thiết lập cấu hình trên thiết bị hệ thống phải đáp ứng các yêu cầu tại Mục 7.2.1.2 Tiêu chuẩn quốc gia TCVN 11930:2017.

b) Kiểm soát truy cập nội mạng

Thiết lập cấu hình trên thiết bị hệ thống để quản lý truy cập từ các máy tính/máy chủ bên trong mạng theo chiều đi ra các mạng bên ngoài và các mạng khác bên trong mạng, bao gồm: Các ứng dụng/dịch vụ nào được truy cập; Quản lý truy cập theo địa chỉ thiết bị; Phương án ưu tiên truy cập. Phương án cần mô tả chính sách đó được thiết lập trên thiết bị hệ thống nào. Thiết lập cấu hình trên thiết bị hệ thống phải đáp ứng các yêu cầu tại Mục 7.2.1.3 Tiêu chuẩn quốc gia TCVN 11930:2017.

c) Nhật ký hệ thống

Thiết lập cấu hình trên thiết bị hệ thống để quản lý nhật ký hệ thống (log) trên các thiết bị hệ thống về bật chức năng ghi log; thông tin ghi log; thời gian, dung lượng ghi log; quản lý log. Thiết lập cấu hình trên thiết bị hệ thống phải đáp ứng các yêu cầu Tiêu chuẩn quốc gia TCVN 11930:2017.

d) Phòng chống xâm nhập

Thiết lập cấu hình trên thiết bị phòng, chống xâm nhập (IDS/IPS) hoặc chức năng IDS/IPS trên thiết bị tường lửa có trong hệ thống, đáp ứng các yêu cầu tại Mục 7.2.1.5 Tiêu chuẩn quốc gia TCVN 11930:2017.

đ) Phòng chống phần mềm độc hại trên môi trường mạng

Thiết lập cấu hình trên thiết bị hệ thống để thực hiện chức năng phòng chống phần mềm độc hại trên môi trường mạng, đáp ứng các yêu cầu tại Mục 7.2.1.6 Tiêu chuẩn quốc gia TCVN 11930:2017.

e) Bảo vệ thiết bị hệ thống

Thiết lập cấu hình trên thiết bị hệ thống để bảo đảm bảo đảm an ninh, an toàn cho thiết bị trong quá trình sử dụng và quản lý vận hành, đáp ứng các yêu cầu tại Mục 7.2.1.7 Tiêu chuẩn quốc gia TCVN 11930:2017.

g) Cấu hình tường lửa

Việc thiết lập cấu hình sản phẩm tường lửa lớp mạng phải bảm đảm đầy đủ về độ phủ của các vùng mạng theo cấp độ tương ứng, bao gồm: Vùng mạng nội bộ; Vùng mạng biên; Vùng DMZ; Vùng máy chủ nội bộ; Vùng mạng không dây (nếu có) tách riêng, độc lập với các vùng mạng khác; Vùng mạng máy chủ cơ sở dữ liệu; Vùng quản trị; Vùng quản trị thiết bị hệ thống. Thiết lập chính sách trường lửa theo nguyên tắc quyền tối thiểu, chỉ mở những cổng, giao thức, dịch vụ thật sự cần. Nhật ký hệ thống của tường lửa được thiết lập và quản lý tập trung trên SIEM.

2.3.3. Thiết lập cấu hình bảo mật cho máy chủ

a) Xác thực

Thiết lập cấu hình chức năng xác thực trên máy chủ để bảo đảm việc xác thực khi đăng nhập vào máy chủ an toàn, đáp ứng các yêu cầu tại Mục 7.2.2.1 Tiêu chuẩn quốc gia TCVN 11930:2017.

b) Kiểm soát truy cập

Thiết lập cấu hình chức năng kiểm soát truy cập trên máy chủ để bảo đảm việc truy cập, sử dụng máy chủ an toàn sau khi đăng nhập thành công, đáp ứng các yêu cầu tại Mục 7.2.2.2 Tiêu chuẩn quốc gia TCVN 11930:2017.

c) Nhật ký hệ thống

Thiết lập cấu hình chức năng ghi nhật ký hệ thống (log) trên các máy chủ về: Bật chức năng ghi log; Thông tin ghi log; Thời gian, Dung lượng ghi log;

Quản lý log. Thiết lập cấu hình trên máy chủ phải đáp ứng các yêu cầu tại Mục 7.2.2.3 Tiêu chuẩn quốc gia TCVN 11930:2017.

d) Phòng chống xâm nhập

Thiết lập cấu hình bảo mật trên máy chủ để bảo bảo vệ tấn công xâm nhập từ bên ngoài, đáp ứng các yêu cầu tại Mục 7.2.2.4 Tiêu chuẩn quốc gia TCVN 11930:2017.

đ) Phòng chống phần mềm độc hại

Thiết lập cấu hình chức năng phòng, chống mã độc trên máy chủ về: Cài đặt phần mềm phòng chống mã độc; Dò quét mã độc; Xử lý mã độc; Quản lý tập trung phần mềm phòng chống mã độc... để phòng chống mã độc cho máy chủ. Thiết lập cấu hình trên máy chủ phải đáp ứng các yêu cầu tại Mục 7.2.2.5 Tiêu chuẩn quốc gia TCVN 11930:2017.

e) Xử lý máy chủ khi chuyển giao

Mô tả phương án kỹ thuật, công cụ để cho phép xóa sạch dữ liệu; sao lưu dự phòng dữ liệu khi chuyển giao hoặc thay đổi mục đích sử dụng. Thiết lập cấu hình trên máy chủ phải đáp ứng các yêu cầu tại Mục 7.2.2.6 Tiêu chuẩn quốc gia TCVN 11930:2017.

2.3.4. Thiết lập cấu hình bảo mật cho ứng dụng

a) Xác thực

Thiết lập cấu hình chức năng xác thực trên ứng dụng để bảo đảm việc xác thực khi đăng nhập vào ứng dụng an toàn. Tài khoản cán bộ thực hiện xây dựng TTHC cần được cấu hình xác thực đa nhân tố (MFA). Thiết lập cấu hình trên ứng dụng phải đáp ứng các yêu cầu tại Mục 7.2.3.1 Tiêu chuẩn quốc gia TCVN 11930:2017 và Mục 4.6.2.2 Xây dựng và tuân thủ quy định sử dụng mật khẩu TCVN 14423:2025.

b) Kiểm soát truy cập

Thiết lập cấu hình chức năng kiểm soát truy cập trên ứng dụng để bảo đảm việc truy cập, sử dụng ứng dụng an toàn sau khi đăng nhập thành công. Thiết lập cấu hình trên ứng dụng phải đáp ứng các yêu cầu tại Mục 7.2.3.2 Tiêu chuẩn quốc gia TCVN 11930:2017.

c) Nhật ký hệ thống

Thiết lập cấu hình chức năng ghi nhật ký hệ thống (log) trên các ứng dụng về: Bật chức năng ghi log; Thông tin ghi log; Thời gian, dung lượng ghi log; Quản lý log. Thiết lập cấu hình trên ứng dụng phải đáp ứng các yêu cầu tại Mục 7.2.3.3 Tiêu chuẩn quốc gia TCVN 11930:2017.

d) Bảo mật thông tin liên lạc

Thiết lập cấu hình trên ứng dụng để mã hóa và sử dụng giao thức mạng

hoặc kênh kết nối mạng an toàn khi trao đổi dữ liệu qua môi trường mạng. Thiết lập cấu hình trên ứng dụng phải đáp ứng các yêu cầu tại Mục 7.2.3.4 Tiêu chuẩn quốc gia TCVN 11930:2017.

đ) Chống chối bỏ

Thiết lập cấu hình trên ứng dụng để sử dụng và bảo vệ chữ ký số để bảo vệ tính bí mật và chống chối bỏ khi gửi/nhận thông tin quan trọng qua mạng. Thiết lập cấu hình trên ứng dụng phải đáp ứng các yêu cầu tại Mục 7.2.3.5 Tiêu chuẩn quốc gia TCVN 11930:2017.

e) An toàn ứng dụng và mã nguồn

Cấu hình/thiết lập chức năng bảo mật cho ứng dụng và phương án bảo vệ mã nguồn ứng dụng đáp ứng các yêu cầu tại Mục 7.2.3.6 Tiêu chuẩn quốc gia TCVN 11930:2017.

2.3.5. Thiết lập cấu hình bảo mật cho dữ liệu

a) Nguyên vẹn dữ liệu

Thiết lập cấu hình trên hệ thống lưu trữ để lưu trữ, quản lý thay đổi, khôi phục dữ liệu bảo đảm tính nguyên vẹn của dữ liệu, đáp ứng các yêu cầu tại Mục 7.2.4.1 Tiêu chuẩn quốc gia TCVN 11930:2017.

b) Bảo mật dữ liệu

Thiết lập cấu hình trên hệ thống lưu trữ để lưu trữ, quản lý thay đổi, khôi phục dữ liệu bảo đảm tính bí mật của dữ liệu, đáp ứng các yêu cầu tại Mục 7.2.4.2 Tiêu chuẩn quốc gia TCVN 11930:2017.

c) Sao lưu dự phòng

Thiết lập cấu hình trên hệ thống lưu trữ để sao lưu dự phòng dữ liệu: Các thông tin yêu cầu sao lưu dự phòng; Phân loại dữ liệu sao lưu dự phòng; Hệ thống sao lưu dự phòng… Thiết lập cấu hình trên hệ thống lưu trữ phải đáp ứng các yêu cầu tại Mục 7.2.4.3 Tiêu chuẩn quốc gia TCVN 11930:2017.

III. TỔ CHỨC BẢO ĐẢM AN NINH MẠNG

3.1. Hướng dẫn chung

Hệ thống thông tin sau khi được phê duyệt HSĐXCĐ, cần triển khai đầy đủ phương án bảo đảm an ninh mạng bao gồm: Thiết kế, thiết lập hệ thống; quản lý, vận hành hệ thống theo Quy chế bảo đảm an ninh mạng được ban hành cùng HSĐXCĐ. Để triển khai phương án an ninh mạng cho hệ thống thông tin một cách tổng thể, đồng bộ và hiệu quả, cơ quan tổ chức cần tổ chức triển khai toàn diện, thực chất công tác bảo đảm an ninh mạng bao gồm: ***(1)*** Lực lượng tại chỗ; ***(2)*** Giám sát, bảo vệ; ***(3)*** Kiểm tra, đánh giá an ninh mạng; ***(4)*** Kết nối, chia sẻ dữ liệu.

3.2. Lực lượng tại chỗ

Lực lượng tại chỗ giúp cơ quan, tổ chức kiện toàn nhận lực và nâng cao năng lực của cán bộ chuyên trách để triển khai bảo đảm an ninh mạng cho hệ thống TTHC cấp bộ, tỉnh, bao gồm các nội dung: ***(1)*** Kiện toàn lực lượng tại chỗ; ***(2)*** Nâng cao năng lực.

3.2.1. Kiện toàn lực lượng tại chỗ

Một số nội dung trọng tâm cơ quan, tổ chức cần triển khai để kiện toàn lực lượng tại chỗ bao gồm:

a) Người đứng đầu cơ quan, tổ chức trực tiếp chỉ đạo, trong trường hợp cần thiết có thể giao thêm 01 Lãnh đạo cấp phó của mình đảm nhận nhiệm vụ thường trực, giúp người đứng đầu;

b) Người đứng đầu đơn vị chuyên trách trực tiếp chỉ đạo, trong trường hợp cần thiết có thể giao thêm 01 Lãnh đạo cấp phó của mình đảm nhận nhiệm vụ thường trực, giúp người đứng đầu;

c) Chỉ định bộ phận chuyên trách về an ninh mạng thuộc đơn vị chuyên trách về công nghệ thông tin, trong trường hợp chưa có đơn vị chuyên trách về an ninh mạng độc lập;

d) Thành lập Tổ/Đội bảo đảm an ninh mạng/Ứng cứu sự cố liên ngành theo hướng chuyên nghiệp, cơ động với sự tham gia của đại diện các cơ quan, tổ chức trực thuộc do đơn vị chuyên trách làm thường trực.

3.2.2. Nâng cao năng lực

Một số nội dung trọng tâm cơ quan, tổ chức cần triển khai để nâng cao năng lực tại chỗ bao gồm:

a) Khuyến nghị bố trí tối thiểu 05 chuyên gia an ninh mạng (*bao gồm cả chuyên gia thuê ngoài*) đáp ứng chuẩn kỹ năng về an ninh mạng quy định tại Thông tư 17/2021/TT-BTTTT ngày 30/11/2021 của Bộ Thông tin và Truyền thông.

b) Xây dựng kế hoạch và tổ chức đào tạo chuyên sâu về an ninh mạng cho nhân sự chuyên trách; hàng năm tổ chức đào tạo, tuyên truyền tới toàn thể cán bộ, công chức, viên chức, người lao động thuộc phạm vi quản lý theo chỉ đạo của Thủ tướng Chính phủ tại Quyết định số 21/QĐ-TTg ngày 06/11/2021.

c) Xây dựng kế hoạch và hàng năm tổ chức tuyên truyền, nâng cao nhận thức và phổ biến kiến thức về an ninh mạng tới toàn thể cán bộ, công chức, viên chức, người lao động thuộc phạm vi quản lý theo chỉ đạo của Thủ tướng Chính phủ tại Quyết định số 1907/QĐ-TTg ngày 23/11/2020.

d) Tổ chức diễn tập thực chiến tối thiểu 01 lần/năm đối với hệ thống thông tin cấp độ 3 trở lên theo chỉ đạo của Thủ tướng Chính phủ tại Quyết định số 18/CT-TTg ngày 13/10/2022.

3.3. Giám sát, bảo vệ

3.3.1. Hướng dẫn chung về giám sát, bảo vệ

Giám sát, bảo vệ giúp cơ quan, tổ chức triển khai giải pháp giám sát, bảo vệ chuyên nghiệp cho hệ thống thông tin TTHC cấp bộ, tỉnh. Một số điểm cơ quan, tổ chức cần lưu ý khi triển khai lớp giám sát, bảo vệ như sau:

- Mỗi hệ thống thông tin được xác định, phê duyệt đầy đủ các biện pháp bảo đảm an ninh, an toàn hệ thống thông tin theo cấp độ. Việc triển khai giám sát, bảo vệ hệ thống thông tin là việc tổ chức triển khai các giải pháp nhằm đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong HSĐXCĐ.

- Hệ thống thông tin có các máy chủ ứng dụng cần được triển khai tập trung tại Trung tâm dữ liệu của bộ, ngành hoặc tỉnh để được giám sát, bảo vệ tập trung.

- Mỗi bộ, ngành, địa phương triển khai một Trung tâm giám sát, điều hành an ninh mạng (SOC) theo chỉ đạo của Thủ tướng Chính phủ tại Quyết định 942/QĐ-TTg ngày 15/6/2021. Hệ thống SOC được thiết lập cho phép đơn vị chủ quản có thể nhìn được tổng thể các nguy cơ tấn công mạng đối với các hệ thống thông tin trên địa bàn. Theo phương án này, nhật ký từ các hệ thống thông tin sẽ được gửi về và được quản lý tại hệ thống quản lý tập trung tại hệ thống SOC.

3.3.2. Hướng dẫn giám sát bảo vệ đối với hệ thống thông tin TTHC cấp bộ, tỉnh

Triển khai đầy đủ biện pháp bảo đảm an ninh mạng yêu cầu đối với hệ thống thông tin:

- Đáp ứng các quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT;

- Đáp ứng các yêu cầu tại Mục 5 TCVN 14423:2025 yêu cầu đối với hệ thống thông tin quan trọng về an ninh quốc gia;

- Đáp ứng các yêu cầu theo hướng dẫn đảm bảo an ninh mạng, triển khai bảo mật đối với hệ thống thông tin khi thực hiện sáp nhập các tỉnh, thành phố theo mô hình hai cấp tại Điều 4 Chương II Phụ lục Hướng dẫn triển khai hạ tầng kỹ thuật, các hệ thống thông tin khi thực hiện sáp nhập các tỉnh, thành phố theo mô hình hai cấp tại Công văn số 14939-CV/VPTW, ngày 21/5/2025 của Văn phòng Trung ương Đảng.

3.3.3. Hướng dẫn triển khai Trung tâm điều hành an ninh mạng SOC

a) Hướng dẫn triển khai hệ thống SOC

Như đã được hướng dẫn ở trên, mỗi bộ, ngành, địa phương triển khai một Trung tâm SOC theo chỉ đạo của Thủ tướng Chính phủ tại Quyết định 942/QĐ-TTg ngày 15/6/2021. Hệ thống SOC được thiết lập để giám sát, bảo vệ tập trung các hệ thống thông tin thuộc phạm vi quản lý của mỗi bộ, ngành, địa phương. Hệ thống SOC thuộc loại hình hệ thống cơ sở hạ tầng thông tin. Hệ thống SOC khi triển khai giám sát, bảo vệ tập trung cho các hệ thống thông tin thuộc bộ, ngành,

địa phương có cấp độ an ninh mạng tối thiểu cấp độ 3. Do đó, hệ thống SOC phải triển khai đầy đủ các biện phạm bảo vệ theo quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và bổ sung các thành phần để giám sát, bảo vệ tập trung các hệ thống thông tin khác. Hệ thống SOC có thể được triển khai theo một số phương án tùy thuộc vào hiện trạng hiện có của mỗi bộ, ngành, địa phương như sau:

Trường hợp, bộ, ngành, địa phương đã có Trung tâm dữ liệu (TTDL) thì hệ thống SOC nên được triển khai trên hệ thống TTDL và coi như một hệ thống hợp phần của TTDL và bổ sung các phương án giám sát, bảo vệ để đáp ứng các yêu cầu kỹ thuật được hướng dẫn tại văn bản này. Tuy nhiên, khi triển khai theo phương án này thì yêu cầu đơn vị vận hành phải có đủ năng lực để vận hành, khai thác hiệu quả của hệ thống SOC.

Trong trường hợp cơ quan, tổ chức chưa triển khai TTDL hoặc đơn vị vận hành không đủ năng lực vận hành, khai thác hiệu quả hệ thống SOC thì có thể xem xét phương án triển khai SOC theo hình thức thuê dịch vụ. Trong trường hợp này, bên cung cấp dịch vụ sẽ cung cấp hạ tầng và giải pháp. Bên sử dụng chỉ đầu tư các thành phần đầu cuối cơ bản như màn hình, máy tính quản trị và cơ sở hạ tầng liên quan để phục vụ việc thực hiện quản lý, vận hành SOC từ xa.

Yêu cầu về năng lực đối với bên cung cấp dịch vụ SOC cơ quan, tổ chức có thể kham khảo tại tại Quyết định 1356/QĐ-BTTTT ngày 07/7/2022 Ban hành Tiêu chí đánh giá giải pháp, dịch vụ Trung tâm giám sát điều hành an ninh mạng (SOC).

b) Các thành phần chính đối với hệ thống SOC

Giám sát hoạt động mạng 24/7 nhằm phát hiện sớm và phản ứng kịp thời với các sự cố an ninh mạng. Hệ thống giám sát, đảm bảo an ninh mạng SOC cần đảm bảo các thành phần chính như sau:

- Điều phối, tự động hóa và ứng phó sự cố an ninh mạng - SOAR (*Security Orchestration, Automation and Response*): Là tập hợp các dịch vụ và công cụ tự động hóa hoạt động ngăn chặn cuộc tấn công qua mạng và đưa ra biện pháp ứng phó. Quá trình tự động hóa này được thực hiện bằng cách hợp nhất các tích hợp, xác định cách chạy tác vụ và phát triển kế hoạch ứng phó sự cố phù hợp với nhu cầu của đơn vị (*Danh mục Yêu cầu kỹ thuật cơ bản đối với sản phẩm SOAR được ban hành kèm theo Quyết định số 1907/QĐ-BTTTT ngày 02 tháng 12 năm 2021 của Bộ Thông tin và Truyền thông*).

- Sản phẩm Quản lý và phân tích sự kiện an ninh mạng - SIEM, đáp ứng các yêu cầu: Phải bảo đảm năng lực thu thập và quản lý nhật ký hệ thống của toàn bộ các nguồn log gửi về từ các hệ thống thông tin trên địa bàn hoặc thuộc phạm vi quản lý. Nhật ký hệ thống bao gồm đầy đủ log của thiết bị mạng, thiết bị bảo mật. máy chủ, ứng dụng của hệ thống SOC và các hệ thống được giám sát, bảo vệ bởi hệ thống SOC (*Danh mục Yêu cầu kỹ thuật cơ bản đối với sản phẩm SIEM được ban hành kèm theo Quyết định số 1127/QĐ-BTTTT ngày 30 tháng 07 năm 2021 của Bộ Thông tin và Truyền thông*).

- Hệ thống cảm biến mạng (*Smart Network Sensor*): Thực hiện thu thập toàn bộ các tệp nhật ký (log) từ các nguồn như máy chủ, thiết bị mạng, thiết bị bảo đảm an ninh mạng, ứng dụng, thiết bị đầu cuối trong các hệ thống mạng. Các thông tin thu thập được đẩy về hệ thống SIEM để phân tích, giám sát, cảnh báo sự cố an ninh mạng.

- Hệ thống chống tấn công APT (*Advanced Persistent Threat*): Là tập hợp các giải pháp bảo mật sử dụng phần mềm và phần cứng chuyên dụng để phát hiện, ngăn chặn và đối phó hiệu quả với các cuộc tấn công mạng tinh vi, có chủ đích, kéo dài và khó phát hiện, nhắm vào các tổ chức lớn để đánh cắp thông tin nhạy cảm hoặc phá hoại hạ tầng.

- Giải pháp phát hiện và phản hồi điểm cuối (EDR) quản lý tập trung được toàn bộ máy chủ, máy trạm phục vụ hoạt động của hệ thống SOC và từ các hệ thống thuộc phạm vi bảo vệ của hệ thống SOC. Giải pháp EDR có chức năng kết nối, chia sẻ thông tin về Trung tâm Giám sát an ninh mạng quốc gia.

3.4. Kiểm tra, đánh giá an ninh mạng

3.4.1. Hướng dẫn chung

Chủ quản hệ thống thông tin chỉ đạo đơn vị chuyên trách về an ninh mạng chủ trì tổ chức, kiểm tra đánh giá, tổng hợp và xây dựng báo cáo việc tuân thủ các quy định của pháp luật về bảo đảm an ninh mạng hệ thống thông tin theo trách nhiệm của chủ quản hệ thống thông tin.

Đơn vị chuyên trách về an ninh mạng tổ chức kiểm tra, đánh giá việc tuân thủ các quy định của pháp luật về bảo đảm an ninh, an toàn hệ thống thông tin đối với các đơn vị vận hành trên địa bàn; tổng hợp và chuẩn bị nội dung báo cáo đánh giá tuân thủ cho chủ quản hệ thống thông tin.

Đơn vị vận hành tự thực hiện kiểm tra, đánh giá hoặc thuê dịch vụ chuyên nghiệp của doanh nghiệp thực hiện. Hệ thống cấp độ 3 phải do tổ chức chuyên môn được cơ quan có thẩm quyền cấp phép; tổ chức sự nghiệp nhà nước có chức năng, nhiệm vụ phù hợp hoặc do tổ chức chuyên môn được cấp có thẩm quyền chỉ định thực hiện. Đơn vị cung cấp dịch vụ được cấp Giấy phép kinh doanh sản phẩm, dịch vụ an ninh mạng có thể tư vấn xây dựng hồ sơ đánh giá tuân thủ và/hoặc xác nhận kết quả kiểm tra, đánh giá theo yêu cầu của bên sử dụng dịch vụ. Đối với công tác kiểm tra, đánh giá an ninh mạng cho hệ thống thông tin thuộc quyền quản lý cần lựa chọn tổ chức, doanh nghiệp độc lập với tổ chức, doanh nghiệp giám sát, bảo vệ để định kỳ kiểm tra, đánh giá an ninh mạng đối thuộc quyền quản lý hoặc kiểm tra, đánh giá đột xuất khi có yêu cầu theo quy định của pháp luật.

Hồ sơ đánh giá tuân thủ các quy định của pháp luật về bảo đảm an ninh mạng hệ thống thông tin bao gồm: ***(1)*** Quyết định phê duyệt HSĐXCĐ và quy chế bảo đảm an ninh mạng; ***(2)*** Báo cáo kết quả kiểm tra, đánh giá hiệu quả của các biện pháp bảo đảm an ninh mạng theo phương án bảo đảm an ninh mạng được

phê duyệt trong HSĐXCĐ; *(3)* Báo cáo kết quả kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thông tin.

3.4.2. Hướng dẫn thực hiện kiểm tra, đánh giá hiệu quả của các biện pháp bảo đảm an ninh mạng

a) Kiểm tra tính đầy đủ và phù hợp của quy chế bảo đảm an ninh mạng theo phương án bảo đảm an ninh mạng về quản lý trong HSĐXCĐ được phê duyệt:

Quy chế bảo đảm an ninh mạng được đánh giá là phù hợp khi nội dung quy chế bao gồm đầy đủ các quy định và quy trình đáp ứng các yêu cầu về quản lý được quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và các yêu cầu tại Tiêu chuẩn quốc gia TCVN 11930:2017, TCVN 14423:2025, bao gồm:

- Các quy định trong Quy chế: *(1)* Thiết lập chính sách an ninh, an toàn; *(2)* Tổ chức bảo đảm an ninh mạng; *(3)* Bảo đảm nguồn nhân lực; *(4)* Quản lý thiết kế, xây dựng hệ thống; *(5)* Quản lý vận hành hệ thống.

- Các quy trình kèm theo Quy chế: *(1)* Quy trình tuyển dụng cán bộ; *(2)* Quy trình chấm dứt hoặc thay đổi công việc; *(3)* Quy trình thử nghiệm và nghiệm thu hệ thống; *(4)* Quản lý an ninh, an toàn mạng; *(5)* Quản lý an ninh, an toàn máy chủ và ứng dụng; *(6)* Quản lý an ninh, an toàn dữ liệu; *(7)* Quản lý an ninh, an toàn thiết bị đầu cuối; *(8)* Quản lý phòng chống phần mềm độc hại; *(9)* Quản lý giám sát an ninh, an toàn hệ thống thông tin; *(10)* Quản lý điểm yếu an ninh mạng; *(11)* Quản lý sự cố an ninh mạng; *(12)* Quản lý an ninh, an toàn người sử dụng đầu cuối; *(13)* Quản lý rủi ro an ninh mạng; *(14)* Kết thúc vận hành, khai thác, thanh lý, hủy bỏ.

b) Đánh giá việc tuân thủ các quy định, quy trình trong quy chế bảo đảm an ninh mạng trong quá trình vận hành, khai thác, kết thúc hoặc hủy bỏ hệ thống thông tin:

- Đơn vị vận hành cần có nhật ký quản lý vận hành hệ thống theo các quy định và quy trình ban hành theo quy chế bảo đảm an ninh mạng.

- Báo cáo đánh giá tuân thủ cần có các tài liệu minh chứng hệ thống được quản lý, vận hành theo quy chế được ban hành và nhật ký vận hành hệ thống.

c) Đánh giá việc thiết kế hệ thống theo phương án được phê duyệt trong HSĐXCĐ:

Báo cáo đánh giá tuân thủ cần có sơ đồ vật lý, sơ đồ logic và minh chứng cấu hình trên thiết bị hệ thống để chứng minh hệ thống được thiết kế đúng theo phương án được phê duyệt trong HSĐXCĐ.

d) Đánh giá việc thiết lập, cấu hình hệ thống theo phương án trong Hồ sơ đề xuất cấp độ được phê duyệt:

Mỗi thành phần trong hệ thống như thiết bị hệ thống, máy chủ, ứng dụng được đưa ra tại các Danh mục trong HSĐXCĐ cần có một báo cáo minh chứng

việc thiết lập, cấu hình hệ thống theo phương án trong HSĐXCĐ được phê duyệt.

3.4.3. Hướng dẫn kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thông tin

a) Phạm vi, đối tượng đánh giá: Toàn bộ thành phần trong hệ thống như thiết bị hệ thống, máy chủ, ứng dụng được đưa ra tại các Danh mục trong HSĐXCĐ.

b) Tiêu chí đánh giá:

- *Thiết bị mạng lớp 2*: Đánh giá vai trò thiết bị trong hệ thống; Kiểm tra, đánh giá cấu hình lớp an ninh; Kiểm tra, đánh giá cấu hình quản trị; Kiểm tra, đánh giá cấu hình chung (*phiên bản, lỗ hổng của thiết bị*); Kiểm tra, đánh giá cấu hình chính sách tài khoản; Kiểm tra chính sách kết nối quản trị; Kiểm tra cấu hình nhật ký, giám sát.

- *Thiết bị mạng lớp 3*: Đánh giá vai trò thiết bị trong hệ thống; Kiểm tra, đánh giá cấu hình lớp an ninh; Kiểm tra, đánh giá cấu hình quản trị; Kiểm tra, đánh giá cấu hình chung (*phiên bản, lỗ hổng của thiết bị*); Kiểm tra, đánh giá cấu hình chính sách tài khoản; Kiểm tra chính sách kết nối quản trị; Kiểm tra cấu hình nhật ký, giám sát; Kiểm tra, đánh giá cấu hình định tuyến (*thiết bị mạng*).

- *Thiết bị bảo mật*: Đánh giá vai trò thiết bị trong hệ thống; Kiểm tra, đánh giá cấu hình lớp an ninh; Kiểm tra, đánh giá cấu hình quản trị; Kiểm tra, đánh giá cấu hình chung (*phiên bản, lỗ hổng của thiết bị*); Kiểm tra, đánh giá cấu hình chính sách tài khoản; Kiểm tra chính sách kết nối quản trị; Kiểm tra cấu hình nhật ký, giám sát; Kiểm tra, đánh giá cấu hình định tuyến; Kiểm tra chính sách, cấu hình ngăn chặn tấn công trên thiết bị.

- *Đối với máy chủ*: Kiểm tra bản vá và cập nhật hệ điều hành; Kiểm tra cấu hình hệ điều hành; Kiểm tra cấu hình chứng thực; Kiểm tra cấu hình nhật ký, giám sát; Kiểm tra các cấu hình chính sách nội bộ; Kiểm tra, đánh giá cấu hình chính sách tài khoản; Kiểm tra chính sách kết nối quản trị; Kiểm tra các giải pháp về phòng, chống mã độc; Kiểm tra, đánh giá phát hiện mã độc thủ công.

- *Đối với ứng dụng*: Kiểm tra an ninh, an toàn của các thư viện mã nguồn; Kiểm tra, đánh giá quản lý cấu hình và triển khai; Kiểm tra, đánh giá quản lý định danh; Kiểm tra, đánh giá xác thực; Kiểm tra, đánh giá phân quyền; Kiểm tra, đánh giá quản lý phiên; Kiểm tra, đánh giá sàng lọc dữ liệu đầu vào; Kiểm tra, đánh giá cơ chế xử lý lỗi; Kiểm tra, đánh giá thuật toán mã hóa; Kiểm tra, đánh giá logic nghiệp vụ; Kiểm tra xử lý phía người dùng; Kiểm tra, đánh giá khả năng tồn tại các lỗ hổng bảo mật (*Overflows, SQL Injection, Race Conditions*…).

c) *Phương pháp đánh giá*:

- *Kiểm tra, đánh giá hộp đen (Black box)*: Đơn vị đánh giá sẽ thực hiện kiểm tra hệ thống từ bên ngoài và không được cung cấp các thông tin về hệ thống mục tiêu như nền tảng hệ thống, phiên bản ứng dụng, sơ đồ kiến trúc, tài khoản

đăng nhập…

- *Kiểm tra, đánh giá hộp xám (Gray box)*: Đơn vị đánh giá được cung cấp một số thông tin về hệ thống được đánh giá. Hình thức này có lợi thế cho phép đánh giá được các vùng chức năng đòi hỏi phải đăng nhập mới có thể tiếp cận, kết quả kiểm tra, đánh giá an ninh, an toàn sẽ đầy đủ hơn so với phương pháp blackbox.

- *Kiểm tra, đánh giá hộp trắng (White box)*: Đơn vị đánh giá sẽ được cung cấp đầy đủ thông tin và được tiếp cận trực tiếp với về hệ thống, ứng dụng, mã nguồn, cấu hình để thực hiện một đánh giá tổng thể và đầy đủ nhất.

3.5. Kết nối, chia sẻ dữ liệu

3.5.1. Hướng dẫn chung

Kết nối, chia sẻ dữ liệu giám sát về Trung tâm An ninh mạng quốc gia nhằm mục đích hỗ trợ đảm bảo an ninh, an toàn không gian mạng quốc gia và hỗ trợ cơ quan, tổ chức trong việc giám sát bảo vệ hệ thống thông tin, đảm bảo các yêu cầu kỹ thuật: ***(1)*** Dữ liệu chia sẻ phải bảo đảm thường xuyên, liên tục. Không mất kết nối quá 01 ngày; ***(2)*** Đối với dữ liệu giám sát cần chia sẻ đầy đủ các cảnh báo có mức độ nguy hiểm từ thấp đến nghiêm trọng, yêu cầu đơn vị đảm bảo chia sẻ đầy đủ 100% các cảnh báo mức cao và nghiêm trọng.

Kết nối chia sẻ dữ liệu của cơ quan, tổ chức bao gồm:

- Chia sẻ dữ liệu giám sát hệ thống giám sát tập trung của các bộ, ngành, địa phương về Trung tâm an ninh mạng quốc gia, Bộ Công an.

- Chia sẻ dữ liệu phòng, chống mã độc tập trung của các bộ, ngành, địa phương về Trung tâm an ninh mạng quốc gia, Bộ Công an.

3.5.2. Kết nối, chia sẻ dữ liệu giám sát an ninh mạng về Trung tâm An ninh mạng quốc gia

Việc kết nối, chia sẻ thông tin từ hệ thống của cơ quan, tổ chức với Trung tâm An ninh mạng quốc gia, Bộ Công an (*Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao*), giúp phát hiện và cảnh báo sớm nguy cơ mất an ninh mạng có thể xảy ra với cơ quan, tổ chức và phục vụ công tác của Bộ Công an.

3.5.3. Kết nối đối với chia sẻ dữ liệu phòng, chống mã độc tập trung với Trung tâm An ninh mạng quốc gia

Các bộ, ngành, địa phương có giải pháp phòng, chống mã độc được đầu tư mới hoặc nâng cấp cần có chức năng cho phép quản trị tập trung, chia sẻ thông tin, dữ liệu thống kê tình hình lây nhiễm mã độc với hệ thống kỹ thuật của Bộ Công an (*Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao*). Do vậy mỗi cơ quan, tổ chức khi triển khai các giải pháp phòng, chống mã độc cần có máy chủ quản lý tập trung về tình hình lây nhiễm, phòng chống mã độc

của các máy tính, thiết bị mạng trong nội bộ cơ quan, tổ chức và chia sẻ thông tin cơ bản với hệ thống kỹ thuật của Bộ Công an.

Việc kết nối, chia sẻ thông tin về mã độc giúp cập nhật tình hình lây nhiễm mã độc chung tại Việt Nam. Các cơ quan tổ chức gửi thông tin về Bộ Công an (*Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao*) có thể cập nhật tình hình của đơn vị mình và đơn vị khác thông qua bản đồ lây nhiễm mã độc tại Việt Nam. Với các mẫu, thông tin mã độc thu thập được, thông qua xử lý và chia sẻ lại của Bộ Công an (*Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao*) sẽ hỗ trợ cơ quan, tổ chức khác có thể phòng, chống, ngăn chặn nguy cơ tấn công tương tự khi bị đối tượng tấn công sử dụng cùng mẫu mã độc, giúp tăng cường bảo đảm an ninh mạng.

Về phương thức kết nối: Việc chia sẻ thông tin giữa máy chủ quản lý tập trung của các đơn vị với hệ thống kỹ thuật của Bộ Công an được ký số và truyền đi qua kênh mã hoá HTTPS.

IV. HỖ TRỢ BẢO ĐẢM AN NINH MẠNG

1. Đơn vị chuyên trách về an ninh mạng tại địa phương (Công an tỉnh/thành phố) có nhiệm vụ tham mưu cho Ủy ban nhân dân tỉnh/thành phố trong công tác bảo đảm an ninh mạng. Tiến hành kiểm tra, đánh giá an ninh mạng đối với hệ thống thông tin, thiết bị đầu cuối…; kiểm tra hoạt động sử dụng, khai thác hệ thống thông tin giải quyết TTHC tại các sở, ban, ngành, Uỷ ban nhân dân cấp xã.

2. Đơn vị chuyên trách về an ninh mạng tại các bộ, ngành có nhiệm vụ tham mưu, hướng dẫn cơ quan chủ quản và cán bộ thực hiện công tác tiếp nhận, giải quyết TTHC tuân thủ các quy định, quy chế bảo đảm an ninh mạng khi khai thác, sử dụng hệ thống.

3. Trường hợp có khó khăn, vướng mắc trong công tác bảo đảm an ninh mạng, các bộ, ngành, địa phương trao đổi về Bộ Công an (*Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao*) để được hỗ trợ, hướng dẫn./.