BỘ THÔNG TIN VÀ TRUYỀN THÔNG

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 1973/BTTTT-CATTT
V/v hướng dẫn triển khai hoạt động giám sát an toàn thông tin trong cơ quan, tổ chức nhà nước

Hà Nội, ngày 04 tháng 9 năm 2019

Kính gửi:
- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương;
- Các tập đoàn kinh tế, tổng công ty Nhà nước.

Thực hiện chức năng quản lý nhà nước về an toàn thông tin của Bộ Thông tin và Truyền thông tại Nghị định số 17/2017/NĐ-CP ngày 17 tháng 02 năm 2017 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;

Triển khai Quyết định số 1017/QĐ-TTg ngày 14 tháng 8 năm 2018 của Thủ tướng Chính phủ phê duyệt Đề án giám sát an toàn thông tin mạng đối với hệ thống, dịch vụ công nghệ thông tin phục vụ Chính phủ điện tử đến năm 2020, định hướng đến 2025, Bộ Thông tin và Truyền thông công bố Tài liệu hướng dẫn triển khai hoạt động giám sát an toàn thông tin trong cơ quan, tổ chức nhà nước.

Tài liệu này hướng dẫn cơ quan, tổ chức triển khai phương án giám sát an toàn thông tin; thiết lập, quản lý vận hành hệ thống giám sát an toàn hệ thống thông tin; thuê dịch vụ giám sát an toàn thông tin và hướng dẫn kết nối, chia sẻ thông tin giám sát với hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia.

Bản mềm tài liệu hướng dẫn có thể được tải về từ cổng thông tin điện tử của Bộ Thông tin và Truyền thông tại địa chỉ: http://www.mic.gov.vn hoặc tại địa chỉ: https://www.ais.gov.vn/huong-dan-trien-khai-hoat-dong-giam-sat-thong-tin.htm.

Chi tiết liên hệ:

- Ông Nguyễn Tiến Đức, Cục An toàn thông tin, Điện thoại: 0934578162; Thư điện tử: ntduc@mic.gov.vn;

- Ông Nguyễn Phú Dũng, Cục An toàn thông tin, Điện thoại: 0376611700; Thư điện tử: npdung@mic.gov.vn.

Trong quá trình thực hiện, nếu có điều gì vướng mắc, đề nghị các cơ quan, tổ chức, phản ánh về Bộ Thông tin và Truyền thông (Cục An toàn thông tin) để được hướng dẫn thực hiện./. Tien

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Các Thứ trưởng;
- Cổng Thông tin điện tử Chính phủ;
- Đơn vị chuyên trách về CNTT của các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Đơn vị chuyên trách về CNTT của Văn phòng Trung ương Đảng, Văn phòng Chủ tịch nước, Văn phòng Quốc hội, Tòa án nhân dân tối cao, Viện kiểm sát nhân dân tối cao, Kiểm toán nhà nước;
- Đơn vị chuyên trách về CNTT của Cơ quan Trung ương của các đoàn thể;
- Sở TT&TT các tỉnh, thành phố trực thuộc Trung ương;
- Cổng thông tin điện tử Bộ TT&TT;
- Lưu: VT, CATTT.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Thành Hưng

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

TÀI LIỆU HƯỚNG DẪN
TRIỂN KHAI HOẠT ĐỘNG GIÁM SÁT AN TOÀN THÔNG TIN TRONG CƠ QUAN, TỔ CHỨC NHÀ NƯỚC

(Kèm theo Công văn số 2973/BTTTT-CATTT ngày 04 tháng 9 năm 2019 của Bộ Thông tin và Truyền thông)

Hà Nội, 2019

Chương I
PHẠM VI, ĐỐI TƯỢNG ÁP DỤNG

1.1 Phạm vi áp dụng

Tài liệu này hướng dẫn triển khai hoạt động giám sát trong cơ quan, tổ chức nhà nước bao gồm các nội dung: Hướng dẫn phương án triển khai hoạt động giám sát an toàn thông tin; thiết lập, quản lý vận hành hệ thống giám sát an toàn hệ thống thông tin; thuê dịch vụ giám sát an toàn thông tin và hướng dẫn kết nối với hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia.

1.2 Đối tượng áp dụng

- Tài liệu này áp dụng đối với cơ quan, tổ chức, cá nhân có liên quan đến hoạt động giám sát an toàn thông tin cho các hệ thống thông tin trong các cơ quan, tổ chức nhà nước.

- Các cơ quan trực thuộc Bộ Quốc phòng, Bộ Công an không thuộc đối tượng áp dụng của Hướng dẫn này.

- Khuyến khích tổ chức, cá nhân liên quan khác áp dụng Hướng dẫn này.

1.3 Thuật ngữ và định nghĩa

1. Giám sát an toàn hệ thống thông tin: Hoạt động lựa chọn đối tượng, công cụ giám sát, thu thập, phân tích thông tin trạng thái của đối tượng giám sát, báo cáo, cảnh báo hành vi xâm phạm an toàn thông tin hoặc có khả năng gây ra sự cố an toàn thông tin đối với hệ thống thông tin.

2. Hệ thống lọc phần mềm độc hại: Tập hợp phần cứng, phần mềm được kết nối vào hệ thống mạng để phát hiện, ngăn chặn, lọc và thống kê phần mềm độc hại.

3. Nhật ký hệ thống (log): Những sự kiện được hệ thống ghi lại liên quan đến trạng thái hoạt động, sự cố, sự kiện an toàn thông tin và các thông tin khác liên quan đến hoạt động của hệ thống (nếu có).

4. Phần mềm độc hại: 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.

5. Phần mềm phòng chống mã độc: Phần mềm có chức năng phát hiện, cảnh báo và xử lý phần mềm độc hại.

6. Sự cố an toàn thông tin/Sự cố: Việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng tới tính bí mật, tính nguyên vẹn hoặc tính khả dụng.

7. Vùng quản trị: 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.

8. Vùng quản trị thiết bị hệ thống: 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.

9. Phát hiện, ngăn chặn tấn công có chủ đích: Phát hiện, ngăn chặn loại hình tấn công được thiết kế nhằm đột nhập vào một hệ thống thông tin cụ thể.

10. Phòng chống tấn công từ chối dịch vụ: Ngăn chặn tác dụng của các cuộc tấn công trên mạng nhằm làm suy giảm hoặc gián đoạn hoạt động của một trang tin, ứng dụng, dịch vụ hoặc hệ thống mạng, dẫn đến người dùng không thể sử dụng trang tin, ứng dụng, dịch vụ hoặc hệ thống mạng này.

11. Phòng chống xâm nhập: phát hiện, ngăn chặn các hoạt động vào, ra trên hệ thống thông tin được bảo vệ có dấu hiệu gây hại hoặc vi phạm chính sách an toàn mạng.

12. Tường lửa: Hệ thống cho phép hoặc không cho phép thiết lập kết nối mạng giữa thiết bị thuộc vùng mạng này và thiết bị thuộc vùng mạng khác theo chính sách an toàn mạng của đơn vị.

13. Tường lửa ứng dụng web: Hệ thống ngăn chặn các tấn công nhằm vào các điểm yếu của lớp ứng dụng web.

14. Hệ thống quan trắc cơ sở là tập hợp các thiết bị, phần mềm có khả năng theo dõi, thu thập, phân tích, cung cấp thông tin nhật ký, trạng thái, cảnh báo cho hoạt động giám sát trung tâm phục vụ cho việc phân tích, phát hiện các sự cố, điểm yếu, nguy cơ, lỗ hổng an toàn thông tin mạng.

Chương II
HƯỚNG DẪN TRIỂN KHAI HOẠT ĐỘNG GIÁM SÁT

2.1 Phương án triển khai giám sát

Cơ quan, tổ chức có thể triển khai hoạt động giám sát theo một trong các phương án sau:

- Thuê dịch vụ giám sát chuyên nghiệp của doanh nghiệp.

- Tự đầu tư, xây dựng hệ thống và quản lý vận hành.

Cơ quan, tổ chức căn cứ vào điều kiện thực tế về hạ tầng, nhu cầu, nguồn lực của mình để lựa chọn phương án triển khai phù hợp theo một trong các phương án ở trên.

Trong quá trình triển khai thực hiện, Bộ Thông tin và Truyền thông đề nghị cơ quan, tổ chức thực hiện:

- Lồng ghép nội dung về phương án giám sát trong Hồ sơ đề xuất cấp độ của hệ thống thông tin và thực hiện thẩm định và phê duyệt theo quy định.

- Xin ý kiến của chuyên môn của Bộ Thông tin và Truyền thông trước khi phê duyệt phương án triển khai thực hiện, căn cứ theo chỉ đạo của Thủ tướng Chính phủ tại điểm b, Khoản 3, Phần II, Điều 1 Quyết định số 1017/QĐ-TTg ngày 14/8/2018 về phê duyệt Đề án giám sát an toàn thông tin mạng đối với hệ thống, dịch vụ công nghệ thông tin phục vụ Chính phủ điện tử đến năm 2020, định hướng đến năm 2025 (Quyết định số 1017/QĐ-TTg).

- Cung cấp thông tin về hoạt động giám sát, chuẩn bị cổng kết nối và các điều kiện cần thiết cho Bộ Thông tin và Truyền thông thực hiện giám sát khi cần thiết theo quy định tại khoản 3, khoản 5 Điều 14 Thông tư số 31/2017/TT-BTTTT.

- Thực hiện kết nối, chia sẻ thông tin hệ thống hệ thống quan trắc cơ sở với hệ thống kỹ thuật của Bộ Thông tin và Truyền thông theo chỉ đạo của Thủ tướng Chính phủ tại Mục II, Khoản 3, điểm a Quyết định số 1017/QĐ-TTg.

- Ưu tiên lựa chọn giải pháp giám sát do doanh nghiệp Việt Nam làm chủ về công nghệ, sử dụng dịch vụ của các doanh nghiệp trong nước đáp ứng các yêu cầu kỹ thuật theo quy định, theo chỉ đạo của Thủ tướng Chính phủ tại điểm đ, Khoản 1 Chỉ thị số 14/CT-TTg ngày 07/6/2019 về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam. Trong đó, cơ quan, tổ chức ưu tiên lựa chọn các doanh nghiệp: (1) Được Bộ Thông tin và Truyền thông cấp Cấp giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng; (2) Các doanh nghiệp trong Liên minh xử lý mã độc và phòng, chống tấn công mạng; (3) Các sản phẩm do Bộ Thông tin và Truyền thông đánh giá và khuyến nghị sử dụng.

Cơ quan, tổ chức tham khảo hướng dẫn cụ thể về thiết lập và quản lý vận hành hệ thống giám sát tại Chương 2 Hướng dẫn này để có thông tin đầu tư, xây dựng hoặc thuê dịch vụ giám sát an toàn thông tin.

Bộ Thông tin và Truyền thông đề nghị cơ quan, tổ chức khẩn trương triển khai giám sát theo một trong hai phương án đầu tư, xây dựng hoặc thuê dịch vụ giám sát an toàn thông tin. Tuy nhiên, trong trường hợp cơ quan, tổ chức chưa được trang bị công nghệ, giải pháp giám sát và chưa bố trí được nguồn lực để triển khai phương án giám sát, có thể đề nghị hỗ trợ từ Bộ Thông tin và Truyền thông (Cục An toàn thông tin) theo hướng dẫn chi tiết tại Phụ lục 1.

2.2 Triển khai phương án giám sát theo hình thức đầu tư

Cơ quan, tổ chức khi thực hiện phương án đầu tư cần xem xét một số vấn đề sau:

Về ưu điểm: Cơ quan, tổ chức sẽ chủ động hoàn toàn về giải pháp công nghệ, con người và quy trình trong hoạt động giám sát.

Về hạn chế: Chi phí đầu tư ban đầu lớn, việc nâng cấp mở rộng hoặc thay đổi giải pháp, công nghệ khó khả thi vì phụ thuộc vào quá trình đầu tư.

Trường hợp cơ quan, tổ chức có bộ phân chuyên môn đủ năng lực thực hiện giám sát thì có thể xem xét triển khai phương án giám sát theo hình thức này để phù hợp với những yêu cầu đặc thù của mình và giảm thiểu sự phụ thuộc vào các đơn vị ngoài.

Để xác định phạm vi đầu tư, cơ quan tổ chức cần xác định phạm vi, đối tượng giám sát và các yêu cầu an toàn đối với hệ thống thông tin của mình theo cấp độ. Cơ quan tổ chức có thể tham khảo hướng dẫn cụ thể tại Chương 2 Hướng dẫn này và tiêu chuẩn quốc gia TCVN 11930:2017 để xác định các yêu cầu an toàn hạ tầng mạng, máy chủ, ứng dụng và dữ liệu (Ví dụ hệ thống giám sát, hệ thống lưu trữ tập trung, nhật ký hệ thống…) để xác định phạm vi và đối tượng giám sát phù hợp.

Giải pháp, công nghệ cho hệ thống giám sát cần đáp ứng các yêu cầu cụ thể tại chương 2 và các quy định tại Điều 5 Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 quy định hoạt động giám sát an toàn hệ thống thông tin (Thông tư số 31/2017/TT-BTTTT). Cơ quan tổ chức có thể tham khảo hướng dẫn cụ thể tại Chương 2 Hướng dẫn này để có thêm thông tin lựa chọn giải pháp, công nghệ.

Nội dung đầu tư liên quan đến lưu trữ nhật ký hệ thống cũng là nội dung đầu tư quan trọng phục vụ hoạt động của hệ thống giám sát. Cơ quan, tổ chức căn cứ vào quy mô, phạm vi, đối tượng và năng lực xử lý của hệ thống giám sát để tính toán tương đối số lượng sự kiện hệ thống có thể xử lý trong 01 giây, từ đó tính toán dung lượng lưu trữ theo từng tháng mà hệ thống phải lưu trữ. Thời gian lưu trữ nhật ký hệ thống tối thiểu tính theo tháng, đối với từng hệ thống theo cấp độ cần đáp ứng các yêu cầu tối thiểu theo quy định tại Thông tư số 03/2017/TT-BTTTT ngày 24/04/2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ (Thông tư số 03/2017/TT-BTTTT).

Cơ quan, tổ chức có thể căn cứ vào chỉ đạo của Thủ tướng Chính phủ tại điểm e, Khoản 1 Chỉ thị số 14/CT-TTg ngày 07/6/2019 về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam liên quan đến tỉ lệ kinh phí chi cho sản phẩm, dịch vụ bảo đảm an toàn, an ninh mạng, căn cứ quy định của pháp luật về đầu tư để làm căn cứ xây dựng dự án.

2.3 Triển khai phương án giám sát theo hình thức thuê dịch vụ

Cơ quan, tổ chức khi thực hiện phương án thuê dịch vụ giám sát an toàn thông tin cần xem xét một số vấn đề sau:

Về ưu điểm: Chi phí ban đầu để triển khai hệ thống không lớn; tận dụng được đội ngũ chuyên gia chuyên nghiệp có trình độ cao của doanh nghiệp; hỗ trợ việc giám sát 24/7/365; dễ dàng mở rộng hay thay đổi công nghệ giám sát theo khả năng cung cấp dịch vụ của doanh nghiệp và không mất nhiều thời gian như hình thức triển khai đầu tư hệ thống.

Về hạn chế: Hiệu quả của hoạt động giám sát phụ thuộc hoàn toàn vào năng lực của bên cung cấp dịch vụ; thông tin giám sát có thể cần gửi về hệ thống giám sát của bên cung cấp dịch vụ tiềm ẩn nguy cơ lộ lọt dữ liệu của hệ thống ra bên ngoài.

Cơ quan, tổ chức căn cứ vào yêu cầu thực tế của mình để xác định phạm vi cung cấp dịch vụ, yêu cầu đối với bên cung cấp dịch vụ cũng như trách nhiệm của bên thuê và bên cung cấp dịch vụ. Trong đó, một số nội dung sau cần được xác định:

a) Xác định phạm vi thuê dịch vụ giám sát

Để xác định được phạm vi thuê dịch vụ giám sát, cơ quan tổ chức cần khảo sát hệ thống và chuẩn bị các thông tin sau: Phạm vi, đối tượng giám sát; Thông tin sơ đồ, quy hoạch hệ thống; Danh mục các thiết bị, máy chủ và ứng dụng; Các giải pháp bảo đảm an toàn thông tin mà hệ thống đã có; Các nguy cơ mất an toàn thông tin mà cơ quan, tổ chức được xác định thông qua việc kiểm tra, đánh giá và quản lý rủi ro an toàn thông tin; Thông tin về các sự cố mất an toàn thông tin của hệ thống đã ghi nhận trước khi thuê dịch vụ.

Căn cứ vào các thông tin có được ở trên, cơ quan tổ chức có cơ sở để xác định phạm vi thuê dịch vụ giám sát cũng như xác định các yêu cầu đối với bên cung cấp dịch vụ.

Nội dung khảo sát để phục vụ hoạt động thuê dịch vụ tham khảo tại phần Phụ lục Hướng dẫn này.

b) Yêu cầu đối với bên cung cấp dịch vụ

Căn cứ vào hiện trạng và yêu cầu giám sát cụ thể đối với từng hệ thống, cơ quan tổ chức cần đưa ra yêu cầu cụ thể đối với bên cung cấp dịch vụ. Về cơ bản yêu cầu đối với bên cung cấp dịch vụ bao gồm các yêu cầu sau:

- Yêu cầu trang thiết bị hạ tầng thông tin; Bảo đảm về cơ sở hạ tầng, trang thiết bị và các giải pháp kỹ thuật đáp ứng các bài toán đặt ra của bên sử dụng dịch vụ;

- Giải pháp kỹ thuật cần cung cấp đầy đủ các thông tin: Thông tin liên tục về trạng thái các sự cố, cảnh báo; Thông tin, dữ liệu nhật ký hệ thống phục vụ quá trình điều tra, truy vết; Thông tin đo lường về hiệu quả công việc của các chuyên gia phân tích; Thông tin về các trạng thái kết nối trong hệ thống mạng; Thông tin tổng hợp, trực quan về trạng thái của hệ thống; Kênh truyền kết nối giữa hệ thống cần giám sát với hệ thống giám sát trung tâm của bên cung cấp dịch vụ bảo đảm tính sẵn sàng và an toàn thông qua kênh truyền được mã hóa; Yêu cầu đáp ứng kết nối về hệ thống kỹ thuật của Bộ Thông tin và Truyền thông theo Hướng dẫn.

- Yêu cầu về nhân lực: Đơn vị cung cấp dịch vụ cần bảo đảm về đội ngũ nhân sự đủ kinh nghiệm, kiến thức chuyên môn và khả năng đáp ứng yêu cầu giám sát 24/7. Bộ phận nhân sự được tổ chức bảo đảm các yêu cầu: Theo dõi quá trình thực hiện việc giám sát, tiếp nhận các cảnh báo, báo cáo về tình trạng sự cố và báo cáo về tình hình an toàn thông tin, tiếp nhận các yêu cầu liên quan đến phản ứng, xử lý sự cố và điều phối nhân sự trong quá trình xử lý sự cố; vận hành các hệ thống thông tin có trách nhiệm phối hợp và trực tiếp thực hiện việc xử lý sự cố liên quan đến hệ thống được phụ trách;

- Yêu cầu về quy trình: Bên cung cấp dịch vụ cần có các quy trình quản lý vận hành hệ thống như được đề cập ở mục 3.5.

c) Các điều kiện bên sử dụng dịch vụ cần chuẩn bị

Các thông tin cần thiết để cung cấp cho bên cung cấp dịch vụ tại điểm a mục này;

Các điều kiện về hạ tầng, mặt bằng, cổng kết nối đáp ứng các yêu cầu của bên cung cấp dịch vụ để triển khai giám sát;

Bộ phận phối hợp triển khai dịch vụ giám sát; Tổ chức giám sát hoạt động giám sát của bên cung cấp dịch vụ; Đầu mối tiếp nhận thông tin và phối hợp xử lý sự cố;

Các yêu cầu cụ thể khác (nếu có) của bên cung cấp dịch vụ đề nghị.

d) Cam kết giữa bên sử dụng và bên cung cấp dịch vụ

Bên sử dụng dịch vụ cần cam kết bảo đảm các điều kiện cần thiết như điểm c mục này và các yêu cầu cụ thể khác theo thỏa thuận hai bên.

Bên cung cấp dịch vụ cần cam kết về chất lượng dịch vụ, trách nhiệm và các cam kết khác theo thỏa thuận của hai bên. Về cơ bản, bên cung cấp dịch vụ cần cam kết các nội dung sau:

- Bảo mật thông tin hệ thống của bên sử dụng dịch vụ;

- Bảo mật dữ liệu giám sát ghi nhận được;

- Chất lượng dịch vụ như: Các tuân thủ về chính sách, quy trình và các tiêu chuẩn; Thời gian và mức độ xử lý sự cố; Tư vấn phương án xử lý; Chế độ báo cáo và tổng hợp thông tin;

- Các cam kết khác theo đề nghị của mỗi bên.

đ) Căn cứ pháp lý để xây dựng dự toán thuê dịch vụ giám sát an toàn thông tin

Cơ quan, tổ chức có thể căn cứ vào quy định liên quan tại các văn bản sau để làm căn cứ xây dựng dự toán thuê dịch vụ giám sát an toàn thông tin:

- Thông tư số 121/2018/TT-BTC ngày 12/12/2018 của Bộ Tài chính quy định về lập dự toán, quản lý, sử dụng và quyết toán kinh phí để thực hiện công tác ứng cứu sự cố, bảo đảm an toàn thông tin mạng;

- Quyết định số 80/2014/QĐ-TTg ngày 30/12/2014 của Thủ tướng Chính phủ quy định thí điểm về thuê dịch vụ công nghệ thông tin trong cơ quan nhà nước;

- Văn bản số 3575/BTTTT-THH ngày 23/10/2018 của Bộ Thông tin và Truyền thông về hướng dẫn một số nội dung của Quyết định số 80/2014/QĐ-TTg.

Bộ Thông tin và Truyền thông khuyến nghị cơ quan, tổ chức lựa chọn doanh nghiệp được Bộ Thông tin và Truyền thông đã cấp Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng khi sử dụng dịch vụ giám sát an toàn thông tin. Danh sách các doanh nghiệp đã được Bộ Thông tin và Truyền thông cấp phép tại địa chỉ: https://ais.gov.vn/thong-tin-doanh-nghiep-dc-cap-phep/danh-sach-doanh-nghiep-da-duoc-cap-giay-phep-kinh-doanh-san-pham-dich-vu-an-toan-thong-tin-mang.htm.

Chương III
THIẾT LẬP VÀ QUẢN LÝ VẬN HÀNH HỆ THỐNG GIÁM SÁT

3.1 Hướng dẫn chung

Để thiết lập hệ thống giám sát, trước hết cơ quan, tổ chức phải xác định phạm vi và đối tượng và các yêu cầu đối với hệ thống giám sát làm cơ sở để lựa chọn giải pháp, công nghệ và năng lực xử lý phù hợp.

Giải pháp giám sát cần triển khai kết hợp nhiều lớp giám sát khác nhau một cách đồng bộ, thống nhất tối thiểu bao gồm: Giám sát ở lớp mạng; giám sát lớp máy chủ; giám sát lớp ứng dụng; giám sát lớp thiết bị đầu cuối.

Ngoài các nội dung liên quan đến giải pháp giám sát, cơ quan tổ chức cần xác định dung lượng lưu trữ cần thiết để lưu trữ nhật ký hệ thống căn cứ vào phạm vi và quy mô giám sát và tổng số tương đối sự kiện của hệ thống phải xử lý trong 01 giây.

Để lựa chọn giải pháp, công nghệ phù hợp, cơ quan, tổ chức xem hướng dẫn tại Mục 2.2 Hướng dẫn này.

Dưới đây là nội dung hướng dẫn cụ thể cho việc thiết lập và quản lý vận hành hệ thống giám sát.

3.2 Đối tượng, phạm vi giám sát

3.2.1 Xác định phạm vi giám sát

Về cơ bản, phạm vi giám sát có thể là một hệ thống thông tin, nhiều hệ thống thông tin, một vùng mạng hoặc một đối tượng giám sát cụ thể.

Phạm vi giám sát được xác định dựa vào thẩm quyền, phạm vi quản lý các đối tượng giám sát của cơ quan, tổ chức.

Trường hợp phạm vi giám sát là một hệ thống thông tin là trường hợp hệ thống được triển khai tập trung tại một khu vực địa lý bao gồm các kết nối mạng nội bộ và mạng Internet mà không có kết nối mạng diện rộng đi các mạng khác thuộc phạm vi quản lý của cơ quan, tổ chức.

Trường hợp phạm vi giám sát là nhiều hệ thống thông tin là trường hợp một hệ thống thông tin tổng thể thuộc phạm vi quản lý của cơ quan, tổ chức nhưng có các hệ thống thành phần khác nhau ở khu vực địa lý khác nhau và có kết nối mạng diện rộng về hệ thống trung tâm.

Trường hợp phạm vi giám sát là một vùng mạng như vùng DMZ, vùng Cơ sở dữ liệu, vùng quản trị…thì các máy chủ, ứng dụng trong đó sẽ được coi là đối tượng thành phần trong đối tượng giám sát là vùng mạng.

Trường hợp phạm vi giám sát là một đối tượng giám sát cụ thể. Ví dụ trường hợp thuê dịch vụ giám sát cho máy chủ hay một ứng dụng cụ thể.

3.2.2 Xác định đối tượng giám sát

Đối tượng giám sát về cơ bản bao gồm máy chủ, thiết bị mạng, thiết bị bảo mật, máy chủ, dịch vụ, ứng dụng, các thiết bị đầu cuối và điểm giám sát trên đường truyền, cụ thể:

Hình 1. Đối tượng và lớp giám sát

a) Các thiết bị mạng, thiết bị bảo mật như: Router, Switch, Firewall/IPS/IDS, Sandbox, WAF, Network APT...

b) Các máy chủ hệ thống (cả máy chủ vật lý và ảo hóa) trên các nền tảng khác nhau: Windows, Linux, Unix…;

c) Các ứng dụng: (1) Ứng dụng phục vụ hoạt động của hệ thống: DHCP, DNS, NTP, VPN, Proxy Server…; (2) Ứng dụng cung cấp dịch vụ: Web, Mail, FPT, TFTP và các hệ quản trị cơ sở dữ liệu Oracle, SQL, MySQL ...;

d) Các thiết bị đầu cuối: Máy tính người sử dụng, máy in, máy fax, IP Phone, IP Camera…;

đ) Điểm giám sát trên đường truyền: Điểm giám sát biên tại giao diện kết nối của thiết bị định tuyến biên với các mạng bên ngoài; điểm giám sát tại mỗi vùng mạng của hệ thống.

3.2.3 Triển khai giám sát ở lớp mạng

Việc triển khai giám sát ở lớp mạng cho phép phát hiện:

- Các kết nối, truy vấn tới các máy chủ điều khiển mạng botnet (C&C Server);

- Các file mã độc, URL nguy hiểm được truyền qua môi trường mạng (với các giao thức không mã hóa) bằng cách giải mã giao thức, bóc tách dữ liệu dạng file, URL đưa vào các hệ thống phân tích tự động;

- Các Shellcode, payload tấn công khai thác lỗ hổng phần mềm, dịch vụ trong dữ liệu truyền tải trên mạng thông qua phân tích các dấu hiệu đặc trưng;

- Các hành vi bất thường như dò quét mạng, dò quét tài khoản mật khẩu mặc định, mật khẩu yếu…

Phương án triển khai giám sát trên môi trường mạng phù hợp với việc giám sát lưu lượng mạng không sử dụng các giao thức mã hóa (SSH, VPN, TLS, SSL…). Trường hợp, phương án kỹ thuật yêu cầu cần giám sát lưu lượng mạng có mã hóa thì các thiết bị bảo mật phải có chức năng giải mã hoặc sử dụng thiết bị giải mã chuyên dụng.

Để triển khai giám sát trên môi trường mạng, phương án kỹ thuật yêu cầu phải thiết lập các điểm giám sát như đã được mô tả trong mục 3.2.2.

Tại mỗi điểm giám sát có thể triển khai hai hình thức Inline và Passive. Mỗi hình thức triển khai có ưu, nhược điểm khác nhau.

Với hình thức Inline, lưu lượng giám sát sẽ đi qua thiết bị giám sát, bảo vệ như Firewall, IDS/IPS…Ưu điểm của hình thức triển khai này là có thể vừa phát hiện và thực hiện ngăn chặn tấn công mạng trực tiếp. Tuy nhiên, điểm hạn chế của hình thức triển khai này là ảnh hưởng đến hiệu năng, thông lượng của lưu lượng mạng do mọi gói tin phải được kiểm tra hợp lệ mới được cho phép đi qua thiết bị bảo vệ. Trường hợp hiệu năng của thiết bị bảo vệ không đủ so với lưu lượng thực tế của hệ thống sẽ làm tắc nghẽn hoặc gây gián đoạn hoạt động của hệ thống nếu thiết bị bảo vệ xảy ra sự cố. Trường hợp triển khai theo phương án này thì giải pháp bảo vệ cần bảo đảm đủ hiệu năng, có phương án cân bằng tải, dự phòng nóng và có chức năng bypass traffic khi thiết bị quá tải hoặc có sự cố.

Với hình thức Passive, lưu lượng mạng sẽ được trích rút ra để phân tích bằng cách sử dụng thiết bị trích rút dữ liệu (Network-TAP) hoặc sử dụng chức năng span port trên các Switch. Ưu điểm hình thức triển khai này là không làm ảnh hưởng đến hiệu năng, thông lượng lưu lượng mạng. Tuy nhiên, hình thức này không ngăn chặn trực tiếp được các tấn công mạng mà chỉ đưa ra cảnh báo. Để giải quyết vấn đề này, giải pháp sử dụng cần có chức năng tương tác với các thiết bị mạng, thiết bị bảo mật hay máy chủ để ngăn chặn tấn công.

Việc sử dụng Network-TAP hay span port cần chú ý là dữ liệu trích rút cần có hai chiều (từ ngoài vào hệ thống và bên trong hệ thống đi ra). Một số thiết bị Network-TAP chỉ trích rút dữ liệu theo từng chiều và đưa ra cổng ra tương ứng. Do đó trường hợp thiết bị bảo vệ chỉ có 01 cổng phân tích thì sẽ chỉ phân tích được một lưu lượng

mạng một chiều. Do đó, Network-TAP cần được lựa chọn loại có chức năng Aggregator để cho phép trích rút hai chiều lưu lượng mạng và đưa vào 01 cổng ra.

3.2.4 Triển khai giám sát lớp máy chủ

Việc triển khai giám sát ở lớp máy chủ cho phép phát hiện:

- Các hành vi vi phạm chính sách truy cập, quản lý, thiết lập cấu hình hệ điều hành, các dịch vụ hệ thống;

- Các kết nối của máy chủ ra các địa chỉ IP độc hại;

- Các hình thức tấn công mạng như tấn công khai thác điểm yếu, tấn công dò quét và các dạng tấn công tương tự khác;

- Sự thay đổi trái phép của các tệp tin hệ thống;

- Các tiền trình có dấu hiệu bất thường về hành vi và việc sử dụng tài nguyên máy chủ;

Việc triển khai giám sát ở lớp máy chủ cho phép giải quyết được vấn đề của triển khai giám sát lớp mạng là thường không phụ thuộc vào các lưu lượng mạng có mã hóa. Tuy nhiên, việc triển khai giám sát lớp máy chủ sẽ ảnh hưởng đến tài nguyên của máy chủ và khả năng mở rộng phạm vi giám sát khi số lượng máy chủ lớn. Do đó, cần lựa chọn các giải pháp cho phép quản lý tập trung để giảm thiểu việc xử lý trực tiếp các chức năng giám sát trên từng máy chủ.

Việc triển khai giám sát lớp máy chủ có thể triển khai theo hai hình thức sau:

- Cài đặt phần mềm giám sát có chức năng phát hiện tấn công trực tiếp trên máy chủ như Host IDS, AV, DLP…Hình thức này chức năng phát hiện tấn công hay các hành vi vi phạm được phát hiện trực tiếp và gửi nhật ký cảnh báo về hệ thống quản lý tập trung;

- Gửi log về hệ thống giám sát tập trung như SIEM. Hình thức này chức năng phát hiện tấn công mạng được thực hiện trên hệ thống quản lý tập trung thông qua việc phân tích dấu hiệu, luật tương quan hay sử dụng công nghệ dữ liệu lớn. Việc gửi log về hệ thống giám sát tập trung có thể thực hiện thông qua các giao thức hệ điều hành hỗ trợ như Syslog, SNMP hoặc các Agent của những giải pháp cụ thể.

Hình thức gửi log về hệ thống giám sát tập trung sẽ ít ảnh hưởng đến hiệu năng của máy chủ so với hình thức trên. Tuy nhiên, hình thức này sẽ không thể phát hiện được một số dạng tấn công mà giải pháp sử dụng cần phân tích nhiều thông tin tương quan khác trên máy chủ.

Trường hợp gửi log về hệ thống giám sát tập trung thì cần lựa chọn nguồn log có thông tin để phục vụ các giải pháp phát hiện tấn công. Nguồn log gửi về cần tối thiểu có các thông tin sau:

- Thông tin kết nối mạng tới máy chủ (Firewall log);
- Thông tin đăng nhập vào máy chủ;
- Lỗi phát sinh trong quá trình hoạt động (nhật ký trạng thái hoạt động của máy chủ);
- Thông tin về các tiến trình hệ thống;
- Thông tin về sự thay đổi các tập tin, thư mục trên hệ thống;
- Thông tin thay đổi cấu hình máy chủ.

3.2.5 Triển khai giám sát lớp ứng dụng

Việc triển khai giám sát lớp ứng dụng cho phép phát hiện:

- Các dạng tấn công vào lớp ứng dụng như SQLi, XSS...;
- Tấn công dò quét, vét cạn mật khẩu, thư mục và khai thác thông tin;
- Tấn công thay đổi giao diện;
- Tấn công Phishing và cài cắm mã độc trên ứng dụng;
- Tấn công từ chối dịch vụ.

Việc triển khai giám sát ở mức mạng cũng có thể phát hiện các dạng tấn công ở trên trong trường hợp lưu lượng mạng không có mã hóa.

Hình thức triển khai giám sát lớp ứng dụng cũng được thực hiện tương tự đối với lớp hệ điều hành. Chỉ khác là lựa chọn phần mềm và giải pháp phù hợp cho phát hiện tấn công lớp ứng dụng. Ví dụ để phát hiện tấn công ứng dụng web có thể sử dụng phần mềm tường lửa ứng dụng web hoặc phần mềm Host IDS được cài đặt trực tiếp trên máy chủ.

Trường hợp gửi log về hệ thống giám sát tập trung thì cần lựa chọn nguồn log có thông tin để phục vụ các giải pháp phát hiện tấn công. Nguồn log gửi về cần tối thiểu có các thông tin sau:

- Thông tin truy cập ứng dụng;
- Thông tin đăng nhập khi quản trị ứng dụng;
- Thông tin các lỗi phát sinh trong quá trình hoạt động;
- Thông tin thay đổi cấu hình ứng dụng.

3.2.6 Triển khai giám sát lớp thiết bị đầu cuối

Các thiết bị đầu cuối ngoài máy tính người sử dụng thì các thiết bị khác không hỗ trợ cài đặt các phần mềm bảo vệ trên thiết bị. Việc giám sát bảo vệ máy tính của người sử dụng có thể thực hiện tương tự như đối với máy chủ.

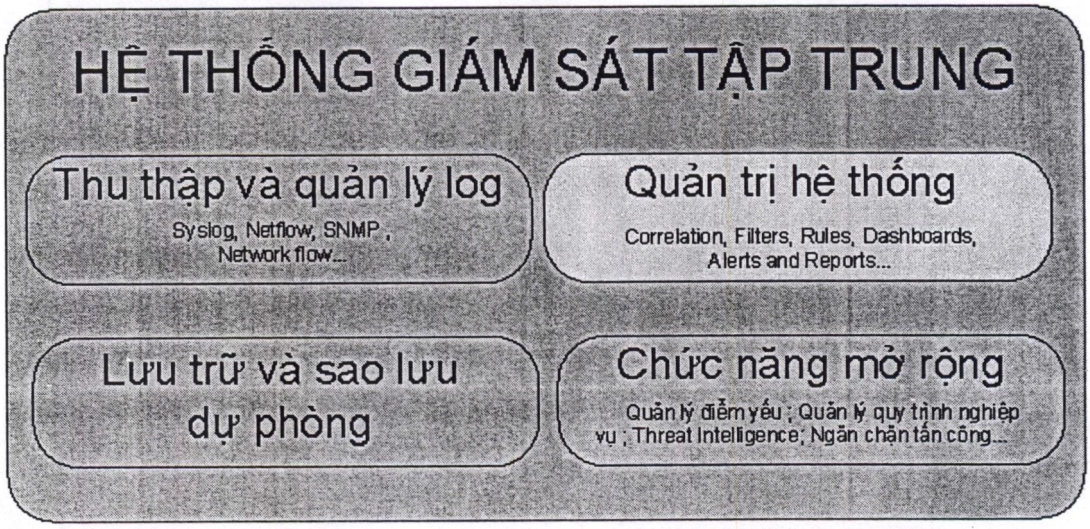
Các thiết bị đầu cuối khác không hỗ trợ cài đặt phần mềm bảo vệ thì có thể triển khai giám sát theo hai hình thức sau: Bật chức năng gửi Syslog trên thiết bị hoặc kết nối, lấy dữ liệu về để phân tích sử dụng giao thức SNMP (hoặc giao thức có chức năng tương đương).

Việc giám sát thiết bị đầu cuối nên kết hợp với giám sát thiết bị quản lý truy cập NAC để phát hiện các thiết bị đầu cuối vi phạm chính sách của hệ thống. Ngoài ra cần đồng bộ với việc cấp phát địa chỉ IP của máy chủ DHCP để có thể xác định các thiết bị đầu cuối vi phạm chính sách dựa vào địa chỉ MAC.

3.3 Hệ thống quản lý tập trung

3.3.1 Yêu cầu cơ bản đối với hệ thống quản lý tập trung

Yêu cầu đối với hệ thống quản lý tập trung cần đáp ứng các yêu cầu theo quy định tại Điều 5, khoản 1 Thông tư số 31/2017/TT-BTTTT và các yêu cầu cụ thể dưới đây:



Hình 2. Yêu cầu chức năng đối với hệ thống quản lý tập trung

a) Chức năng quản trị

- Chức năng phân tích tương quan (Correlation): Chức năng này cho phép phân tích tương quan thông tin giữa các log nhận được từ các đối tượng giám sát khác nhau;

- Chức năng lọc (Filters): Cho phép lọc ra log cần truy vấn dựa theo nội dung của từng trường thông tin mà nguồn log đã được chuẩn hóa và lưu trữ;

- Tạo các luật (Rules): Cho phép người quản trị thiết lập các luật kết hợp giữa chức năng Filter và các luật tương quan để phát hiện ra tấn công mạng hay hành vi bất thường của người sử dụng;

- Chức năng hiển thị (Dashboards): Cung cấp giao diện quản trị hệ thống, thông tin thống kê và quản lý sự kiện nhận được theo thời gian thực;

- Chức năng cảnh báo và báo cáo (Alerts and Reports): Cho phép quản lý thông tin cảnh báo và tạo báo cáo;

- Chức năng cảnh báo thời gian thực (Real Time Alert) cho phép gửi thông tin cảnh báo thời gian thực từ hệ thống ngay khi có sự cố xảy ra.

b) Chức năng nhận log

- Cho phép nhận log từ các nguồn với nhiều định dạng khác nhau từ các thiết bị mạng, máy chủ và ứng dụng;

- Cung cấp các chức năng cho phép định dạng, chuẩn hóa log nhận được theo các trường thông tin tùy biến theo nhu cầu sử dụng;

- Cho phép nhận log trực tiếp qua các giao thức mạng như: Syslog, Netflow, SNMP và các giao thức có chức năng tương đương theo thiết kế của từng hãng cụ thể. Giao thức truyền, nhận log qua môi trường mạng cần hỗ trợ chức năng mã hóa dữ liệu, nén dữ liệu;

- Cho phép tải các tệp tin log theo các định dạng khác nhau lên hệ thống để chuẩn hóa và phân tích.

c) Yêu cầu về lưu trữ

Yêu cầu lưu trữ đối với hệ thống quản lý tập trung cần bảo đảm thời gian tối thiểu để lưu trữ nhật ký hệ thống căn cứ vào cấp độ (Điều 9 Thông tư số 03/2017/TT-BTTTT) của hệ thống thông tin được triển khai giám sát, cụ thể:

- Hệ thống thông tin cấp độ 1 hoặc 2 là 01 tháng.

- Hệ thống thông tin cấp độ 3 là 03 tháng.

- Hệ thống thông tin cấp độ 4 là 06 tháng.

- Hệ thống cấp độ 5 là 12 tháng.

d) Chức năng mở rộng

- Quản lý điểm yếu an toàn thông tin;

- Quản lý quy trình nghiệp vụ xử lý sự cố an toàn thông tin;

- Tích hợp, tổng hợp và phân tích thông tin từ hệ thống Threat Intelligence;

- Tự động tương tác với thiết bị mạng và máy chủ để ngăn chặn tấn công.

3.3.2 Nguyên lý hoạt động cơ bản

Hệ thống quản lý tập trung cho phép nhận quản lý tập trung log từ nhiều nguồn và định dạng của các thiết bị, máy chủ và ứng dụng khác nhau. Việc quản lý log trên một hệ thống tập trung ngoài việc cho phép quản lý tổng thể các sự kiện xảy ra trong hệ thống còn cho phép phân tích, truy vết và phát hiện tấn công mạng. Về cơ bản, hoạt động của hệ thống như sau:

a) Đối tượng giám sát gửi log về hệ thống giám sát tập trung bằng một trong các hình thức sau:

- Đối với đối tượng giám sát là các thiết bị mạng, thiết bị bảo mật phải thiết lập chức năng gửi log về hệ thống tập trung sử dụng một số giao thức mà thiết bị đó hỗ trợ. Giao thức phổ biến mà thiết bị hỗ trợ là Syslog, SNMP và Netflow.

- Đối tượng giám sát là các máy chủ hoặc các thiết bị khác cho phép cài đặt Agent (do hãng cung cấp giải pháp phát triển) để gửi log về hệ thống tập trung. Hình thức này cho phép tùy biến cao các nguồn log có thể gửi về hệ thống tập trung như log của hệ điều hành, ứng dụng, tường lửa mềm…Các Agent cung cấp chức năng nén, mã hóa dữ liệu trước khi gửi log về hệ thống tập trung.

Trường hợp khi số lượng đối tượng giám sát lớn và nằm phân tán ở nhiều hệ thống mạng khác nhau thì các đối tượng giám sát xem xét được chia thành từng nhóm theo từng hệ thống mạng và được thiết lập gửi log về một điểm trung gian. Điểm nhận log trung gian này cho phép nhận log từ các điểm giám sát nén và mã hóa dữ liệu trước khi gửi về hệ thống tập trung.

b) Dữ liệu nhận được từ hệ thống tập trung sẽ được chuẩn hóa theo từng định dạng mà hệ thống đó hỗ trợ. Trường hợp định dạng log mới mà hệ thống chưa hỗ trợ thì sẽ có chức năng cho phép người sử dụng tự định nghĩa định dạng log để chuẩn hóa. Ngoài chức năng chuẩn hóa dữ liệu, hệ thống quản lý tập trung còn cung cấp chức năng cho phép lọc bỏ các log trùng lặp hoặc không cần thiết trước khi lưu vào cơ sở dữ liệu.

Dữ liệu log sau khi được chuẩn hóa và lưu vào cơ sở dữ liệu cho phép người sử dụng quản lý, phân tích để truy vết và phát hiện tấn công mạng.

Hệ thống quản lý tập trung thường tích hợp các chức năng tự động phát hiện tấn công trên cơ sở phân tích log nhận được. Chức năng phát hiện tấn công có thể được thiết lập dựa vào các luật phân tích tương quan, các dấu hiệu tấn công; sử dụng hệ thống Threat Intelligence hoặc áp dụng công nghệ: AI, Data mining, Big Data…

Tấn công mạng sau khi được phát hiện, hệ thống quản lý tập trung sẽ thực hiện các hành động cụ thể theo chính sách của người sử dụng đưa vào như: gửi cảnh báo

qua email, SMS hoặc tương tác với các thiết bị mạng, thiết bị bảo mật để tự động ngăn chặn tấn công. Các hành động cụ thể được hiển thị dưới dạng các cảnh báo theo thời gian thực cho phép người quản trị giám sát, theo dõi.

3.4 Thiết lập hệ thống

3.4.1 Cài đặt hệ thống

Việc cài đặt thành phần xử lý tập trung phụ thuộc vào gói giải pháp được đầu tư. Đối với các giải pháp được đầu tư tích hợp cùng phần cứng của hãng dưới dạng thiết bị chuyên dụng thì không yêu cầu quá trình cài đặt mà chỉ cần thiết lập cấu hình để sử dụng.

Đối với gói giải pháp dưới dạng phần mềm được cài đặt trên hệ điều hành thì trước hết cần lựa chọn hệ điều hành phù hợp và tiến hành cài đặt. Căn cứ vào yêu cầu về năng lực xử lý của phần mềm giám sát đối với máy chủ để lựa chọn máy chủ và không gian lưu trữ phù hợp. Khuyến khích cơ quan, tổ chức triển khai cài đặt giải pháp trên nền tảng ảo hóa để dễ dạng mở rộng, nâng cấp và sao lưu dự phòng.

Chú ý việc cài đặt hệ thống cần thực hiện trên môi trường độc lập với hệ thống đang hoạt động của cơ quan, tổ chức để tránh các ảnh hưởng không cần thiết đến hệ thống đang hoạt động.

Sau khi cài đặt thiết lập hệ thống thì cần nâng cấp phiên bản, cập nhật các bản vá và thực hiện kiểm tra đánh giá an toàn thông tin cho hệ thống trước khi đưa vào sử dụng. Thông tin về các điểm yếu an toàn thông tin có thể được tham khảo tại địa chỉ: https://ti.khonggianmang.vn/, https://www.cvedetails.com/...

3.4.2 Thiết lập cấu hình hệ thống

Để đưa hệ thống giám sát vào hệ thống, thì người quản trị cần quy hoạch địa chỉ IP, vùng mạng và các chính sách truy cập trên các thiết bị bảo vệ trước khi kết nối hệ thống giám sát vào hệ thống.

Hệ thống giám sát cần được đưa vào một vùng mạng riêng (vùng quản trị thiết bị hệ thống). Vùng mạng này sẽ được quy hoạch địa chỉ IP cho giao diện quản trị trên các thiết bị/máy chủ và giao diện của hệ thống giám sát cho phép việc gửi/nhận log được gửi trực tiếp giữa các giao diện trong vùng mạng này mà không qua các thiết bị mạng trung gian để không ảnh hưởng đến các kết nối mạng khác trong hệ thống.

Hệ thống giám sát cần được bảo vệ với các thiết bị bảo mật và được thiết lập cấp hình bảo mật tối thiểu bao gồm: Kiểm soát truy cập từ các vùng mạng khác đi vào vùng quản trị thiết bị hệ thống; Kiểm soát truy cập từ vùng quản trị thiết bị hệ thống đi ra

các vùng mạng khác; Phòng chống xâm nhập; Phòng chống phần mềm độc hại trên môi trường mạng.

Vùng mạng quản trị cần được thiết lập riêng để đặt các máy tính quản trị, vận hành hệ thống giám sát. Các thiết bị bảo mật cần được thiết lập chỉ cho phép các máy tính quản trị được truy cập, quản lý hệ thống giám sát.

Trường hợp cần quản trị hệ thống giám sát từ xa thì cần thiết lập cấu hình hệ thống để cho phép truy cập gián tiếp từ các máy bên ngoài vào các máy quản trị thông qua các giao thức mạng có mã hóa, bảo mật như VPN, SSH, TLS, SSL …

3.4.3 Kiểm thử nghiệm thu hệ thống giám sát

Hệ thống giám sát cần được cài đặt trên môi trường độc lập, sau khi cài đặt và kiểm thử hệ thống thì mới đưa vào khai thác, vận hành trong môi trường thực tế.

Căn cứ vào các yêu cầu đối với hệ thống giám sát, cơ quan, tổ chức yêu cầu đơn vị cung cấp giải pháp xây dựng kịch bản kiểm thử để đánh giá khả năng đáp ứng của hệ thống. Trong đó, kịch bản kiểm thử cần đáp ứng tối thiểu các nội dung sau:

- Các hình thức tiếp nhận log từ các thiết bị giám sát, trực tiếp qua các giao thức mạng hoặc gián tiếp qua việc tải tệp tin log lên hệ thống;

- Khả năng nhận và chuẩn hóa định dạng log của các thiết bị, máy chủ, ứng dụng và dịch vụ khác nhau (đối với định dạng hệ thống đã hỗ trợ) và khả năng tùy biến để chuẩn hóa định dạng log mới (đối với định dạng hệ thống chưa hỗ trợ);

- Số lượng sự kiện tối đa mà hệ thống có thể tiếp nhận và xử lý trong một giây;

- Các chức năng của hệ thống để đáp ứng các yêu cầu về mặt chức năng như được mô tả tại mục 3.3.1 như: Lọc, phân tích tương quan, thiết lập luật trên thành phần quản lý tập trung; phân tích thống kê; cảnh báo và báo cáo.

3.5 Quản lý, vận hành hệ thống

Để đưa hệ thống giám sát vào vận hành, khai thác hiệu quả thì cơ quan, tổ chức cần xây dựng quy định, quy trình quản lý vận hành hệ thống giám sát. Các quy định này có thể được đưa vào Quy chế bảo đảm an toàn thông tin của tổ chức để triển khai thực hiện.

Cơ quan, tổ chức có thể tham khảo tiêu chuẩn quốc gia TCVN 11930:2017, để xây dựng các quy định và quy trình liên quan đến quản lý, vận hành hệ thống giám sát bao gồm:

3.5.1 Quản lý, vận hành hoạt động bình thường của hệ thống

Các quy định, quy trình liên quan đến quản lý, vận hành hoạt động bình thường của hệ thống giám sát là các quy định, quy trình nhằm bảo đảm hệ thống giám sát hoạt động ổn định, có tính chịu lỗi cao và sẵn sàng khôi phục lại trạng thái bình thường khi xảy ra sự cố. Các quy định, quy trình cần tối thiểu bao gồm các nội dung:

- Khởi động và tắt hệ thống giám sát;
- Thay đổi cấu hình và các thành phần của hệ thống giám sát;
- Quy trình xử lý các sự cố liên quan đến hoạt động của hệ thống giám sát;
- Quy trình sao lưu, dự phòng cấu hình hệ thống và log của hệ thống;
- Quy trình bảo trì, nâng cấp hệ thống giám sát;
- Quy trình khôi phục hệ thống sau sự cố.

3.5.2 Kết nối và gửi log từ đối tượng giám sát về hệ thống quản lý tập trung

Đối tượng giám sát của hệ thống có nhiều loại khác nhau, mỗi loại có định dạng log và chức năng hỗ trợ gửi log cũng khác nhau. Thêm nữa, đối tượng giám sát có thể nằm phân tán ở nhiều vị trí khác nhau. Do đó, cần có quy định và quy trình gửi log từ đối tượng giám sát về hệ thống quản lý tập trung. Quy định, quy trình liên quan đến nội dung này có thể bao gồm:

- Loại log mà hệ thống có thể tiếp nhận;
- Giao thức gửi nhận log hệ thống hỗ trợ;
- Quy định về quy tắc xác định nguồn gửi log như đặt tên thiết bị theo quy tắc;
- Số lượng sự kiện tối đa từ một đối tượng giám sát có thể gửi;
- Chính sách hệ thống để quản lý các nguồn log gửi về;
- Quy định về chuẩn mã hóa, nén dữ liệu.

3.5.3 Truy cập và quản trị hệ thống

Hệ thống giám sát lưu trữ nhiều thông tin quan trọng của hệ thống. Do đó, việc truy cập và quản trị hệ thống giám sát cần được quy định và có các quy trình để thực hiện. Các quy định, quy trình liên quan đến nội dung này có thể bao gồm:

- Chính sách truy cập, quản trị hệ thống từ mạng bên trong hệ thống và từ xa;
- Quản lý tài khoản và phân quyền truy cập, quản trị hệ thống;
- Truy cập và quản lý tập tin cấu hình và log lưu trữ trên hệ thống;
- Quyền thiết lập cấu hình và quản lý các đối tượng giám sát.

3.5.4 Lưu trữ và bảo vệ log hệ thống

Log hệ thống là dữ liệu quan trọng của cơ quan, tổ chức cần bảo vệ. Việc lộ lọt dữ liệu log hệ thống có thể là cơ sở để tin tặc khai thác thông tin của hệ thống phục vụ việc thực hiện các cuộc tấn công mạng. Do đó, việc lưu trữ và bảo về log hệ thống cần được quy định và có quy trình để thực hiện. Các quy định, quy trình liên quan đến nội dung này có thể bao gồm:

- Loại log và thông tin cấu hình hệ thống cần lưu trữ;

- Tần suất sao lưu, dự phòng tập tin cấu hình và log hệ thống;

- Gán nhãn dữ liệu (quy cách đặt tên, nơi lưu trữ…), mã hóa, nén dữ liệu log;

- Khôi phục và bảo vệ log hệ thống khi xảy ra sự cố theo phương án và năng lực xử lý của cơ quan, tổ chức.

3.5.5 Theo dõi, giám sát, cảnh báo và xử lý tấn công mạng

Một trong những nội dung quan trọng liên quan đến quản lý, vận hành hệ thống giám sát là quy định, quy trình theo dõi, giám sát, cảnh báo và xử lý tấn công mạng. Các hình thức tấn công mạng tùy thuộc vào mức độ nghiêm trọng sẽ có các phương án xử lý khác nhau. Để chủ động đối phó với các dạng tấn công mạng được ghi nhận trên hệ thống, cơ quan tổ chức cần quy định và có quy trình xử lý. Các quy định, quy trình liên quan đến nội dung này có thể bao gồm:

- Quy định trách nhiệm của cán bộ trong việc thực hiện theo dõi, giám sát, cảnh báo và xử lý tấn công mạng;

- Quy trình thực hiện theo dõi, giám sát, cảnh báo và xử lý tấn công mạng;

- Quy trình thu thập thông tin và quản lý, cập nhật xử lý các sự cố mới;

- Quy định về các mức độ sự cố tấn công mạng và xây dựng quy trình xử lý tấn công mạng đối với các dạng tấn công cụ thể, tối thiểu bao gồm:

+ Tấn công dò, quét và khai thác thông tin hệ thống;

+ Tấn công mã độc, tấn công có chủ đích;

+ Tấn công khai thác điểm yếu, chiếm quyền điều khiển hệ thống;

+ Tấn công thay đổi giao diện;

+ Tấn công đánh cắp dữ liệu hoặc phá hoại dữ liệu;

+ Tấn công từ chối dịch vụ.

- Quy định về việc định kỳ tổ chức thực hành, diễn tập xử lý sự cố tấn công mạng.

- Quy định về chế độ báo cáo khi phát hiện và xử lý sự cố tấn công mạng.

3.5.6 Bố trí nguồn lực và tổ chức giám sát

Cơ quan, tổ chức cần bố trí cán bộ và tổ chức giám sát 24/7 (đối với hệ thống thông tin cấp độ 3 trở lên). Tùy thuộc vào nguồn nhân lực của mỗi cơ quan, tổ chức mà các cán bộ được bố trí làm cán bộ chuyên trách hay kiêm nhiệm các nhiệm vụ trong việc vận hành hệ thống giám sát hoặc một cán bộ có thể thực hiện nhiệm vụ của nhiều nhóm khác nhau.

Về cơ bản các nhiệm vụ trong quá trình quản lý vận hành hệ thống giám sát được phân làm các nhóm công việc sau:

a) Nhóm quản lý vận hành hệ thống giám sát

- Có nhiệm vụ quản lý vận hành bảo đảm các hoạt động bình thường của hệ thống giám sát. Nhóm này có thể nằm trong nhóm quản lý vận hành chung cho toàn bộ hạ tầng của hệ thống.

- Có kiến thức về mạng, nắm được thiết kế hệ thống, thiết lập cấu hình bảo mật trên các thiết bị, máy chủ.

- Phảitheo dõi, thường xuyên, liên tục trạng thái hoạt động của hệ thống, tài nguyên, băng thông, trạng thái kết nối để bảo đảm hệ thống hoạt động bình thường, có tính sẵn sàng cao.

b) Nhóm theo dõi và cảnh báo

- Có nhiệm vụ theo dõi, giám sát các sự kiện, tấn công mạng ghi nhận được trên hệ thống. Xác định và phân loại mức độ sự cố và xác định hành động phù hợp tiếp theo hoặc cảnh báo cho nhóm xử lý sự cố thực hiện.

- Có kiến thức về các lỗ hổng mới, mã độc mới, chiến dịch, hình thức tấn công mới; có thể phân loại và xác định mức độ của các sự cố và tìm kiếm, truy vấn thông tin từ các nguồn dữ liệu bên ngoài như hệ thống Threat Intelligence.

- Thực hiện định kỳ phân tích bộ luật, cảnh báo sai thực hiện whitelist, chỉnh sửa luật không cho những cảnh báo sai lập lại để tối ưu khả năng phát hiện tấn công, sự cố của hệ thống, giảm thiểu nhận diện nhầm.

c) Nhóm xử lý sự cố

- Có nhiệm vụ tiếp nhận cảnh báo, xác minh và thực hiện các hành động để xử lý sự cố, bao gồm một số hành động cụ thể như sau:

- Xác định các hành động ứng cứu khẩn cấp: Phản ứng chặn kênh kết nối điều khiển, bổ sung luật ngăn chặn sớm tấn công hoặc cô lập hệ thống.

- Xử lý các lỗ hổng, điểm yếu, cập nhật bản vá và bóc gỡ mã độc trên hệ thống;

Nâng cấp hoặc khôi phục hệ thống sau sự cố.

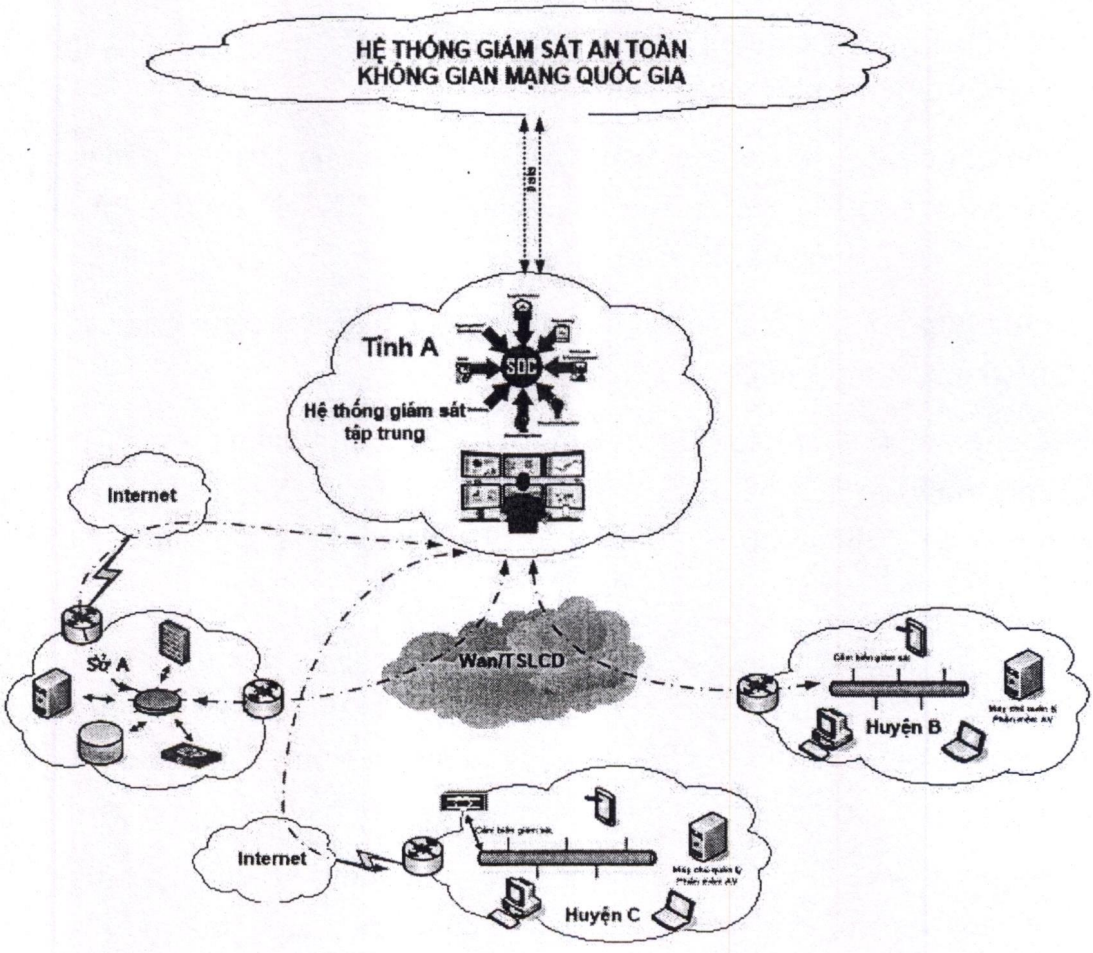
d) Nhóm điều tra, phân tích

- Có nhiệm vụ phân tích chuyên sâu các cảnh báo, các sự cố để tìm ra nguồn gốc, nguyên nhân và các dấu hiệu nhận biết tấn công.

- Kết quả đầu ra của nhóm này là chứng cứ số, các dấu hiệu cho phép thiết lập các tập luật trên hệ thống để ngăn chặn các dạng tấn công tương tự tiếp theo đến hệ thống.

3.6 Mô hình tham khảo về giám sát an toàn thông tin cấp tỉnh

Về cơ bản, mỗi địa phương thường có nhiều hệ thống thông tin nằm phân tán tại các đơn vị khác nhau như các sở, quận, huyện…Nếu đầu tư hệ thống giám sát và bố trí nguồn lực để quản lý vận hành cho mỗi hệ thống này sẽ rất tốn kèm và không hiệu quả do tính phân tán, không đồng bộ.



Hình 3. Mô hình tham khảo giám sát tập trung của tỉnh A

Việc triển khai hệ thống giám sát tập trung cho phép đơn vị vận hành có thể nhìn được tổng thể các nguy cơ tấn công mạng đối với các hệ thống thông tin trên địa bàn, thậm chí đến từng máy tính cụ thể bên trong mỗi hệ thống. Việc này sẽ giảm thiểu được

chi phí đầu tư và tận dụng và tập trung được nguồn nhân lực có trình độ cao tập trung tại các hệ thống trung tâm.

Do đó, mỗi tỉnh có thể triển khai một hệ thống giám sát tập trung để giám sát và bảo vệ các hệ thống thông tin trên địa bàn. Theo phương án này, log từ các hệ thống thông tin sẽ được gửi về và được quản lý tại hệ thống quản lý tập trung. Hệ thống quản lý tập trung thường đặt tại trung tâm dữ liệu của tỉnh và do Sở Thông tin và Truyền thông quản lý vận hành.

Các hệ thống thông tin trên địa bàn có hai loại hình triển khai phổ biến:

a) Hệ thống cung cấp dịch vụ trực tuyến và có người sử dụng. Hệ thống này có hệ thống máy chủ để cung cấp dịch vụ mà có mạng LAN của người sử dụng (Sở A).

Thông thường các hệ thống này đã được triển khai các hệ thống quan trắc cơ sở, có thể có hệ thống giám sát tập trung và có kết nối mạng Internet độc lập. Đối với trường hợp này, log của hệ thống quan trắc cơ sở sẽ được gửi về hệ thống giám sát tập trung theo một trong hai phương án sau:

- Trường hợp Sở A có kết nối mạng WAN về hệ thống giám sát tập trung thì log sẽ được ưu tiên gửi qua kết nối mạng này. Kết nối WAN cần ưu tiên sử dụng mạng truyền số liệu chuyên dùng (TSLCD).

- Trường hợp Sở A không có kết nối WAN thì log sẽ được gửi qua mạng Internet về hệ thống giám sát tập trung.

Để có phương án tối ưu trong việc gửi log về hệ thống giám sát tập trung, log cần được gửi tập trung về một hệ thống tại Sở A (sử dụng Syslog hoặc giải pháp tương đương) được lọc lấy thông tin cần thiết, nén và mã hóa trước khi gửi về hệ thống tập trung.

Trường hợp hệ thống của Sở A chưa có hệ thống quan trắc thì hệ thống này cần thiết lập tối thiểu cảm biến giám sát và hệ thống quản lý phần mềm phòng chống phần mềm độc hại tập trung và gửi log về hệ thống giám sát trung tâm. Cảm biến giám sát cần được thiết lập để có thể giám sát được cả hai kết nối mạng Internet và WAN.

b) Trường hợp hệ thống chỉ có mạng LAN của người sử dụng. Trường hợp này, hệ thống chỉ có máy tính của người sử dụng và có kết nối mạng Internet.

Kết nối mạng Internet có thể triển khai theo một trong hai phương án sau:

- Hệ thống có kết nối Internet độc lập và không có kết nối WAN (Huyện C). Trường hợp này log của hệ thống quan trắc cơ sở (nếu có) hoặc từ cảm biến giám sát sẽ được gửi về hệ thống giám sát tập trung qua mạng Internet. Chú ý rằng, trường hợp

hệ thống có kết nối WAN thì cần ưu tiên sử dụng kết nối này để gửi log về hệ thống giám sát tập trung.

- Hệ thống không có kết nối Internet trực tiếp mà kết nối qua mạng WAN (Huyện B). Trường hợp này, cảm biến giám sát không cần thiết phải triển khai tại Huyện B mà có thể triển khai cảm biến giám sát tập trung tại cổng ra Internet tập trung của các đơn vị. Trường hợp này yêu cầu hệ thống tại các đơn vị không cấu hình NAT trên các thiết bị mạng để cho phép tại điểm giám sát, cảm biến giám sát có thể thấy được địa chỉ IP thật của mỗi máy tính trong mạng. Việc cấu hình NAT sẽ được thực hiện tại thiết bị định tuyến biên của cổng kết nối Internet tập trung.

Các máy tính trong hệ thống thông tin của Huyện B cần cài đặt phần mềm phòng, chống phần mềm độc hại và được quản lý tập trung bởi một máy tính/máy chủ bên trong hệ thống và gửi log về hệ thống giám sát tập trung.

Các hệ thống thông tin trên địa bàn tỉnh A cần ưu tiên phương án sử dụng kết nối mạng Internet qua kết nối WAN qua cổng kết nối Internet tập trung để có thể triển khai biện pháp giám sát và bảo vệ tập trung nhằm giảm thiểu chi phí đầu tư và tăng hiệu quả giám sát và bảo vệ.

Mỗi hệ thống sử dụng giải pháp phòng, chống phần mềm độc hại có chức năng quản lý tập trung và có thể kết nối, chia sẻ thông tin với hệ thống giám sát an toàn không gian mạng quốc gia.

Hệ thống giám sát tập trung tại tỉnh A cần kết nối chia sẻ dữ liệu với hệ thống giám sát an toàn không gian mạng quốc gia theo hướng dẫn cụ thể tại Chương 4.

Chương IV
KẾT NỐI CHIA SẺ THÔNG TIN VỚI TRUNG TÂM GIÁM SÁT AN TOÀN KHÔNG GIAN MẠNG QUỐC GIA

4.1 Hướng dẫn chung

Việc kết nối chia sẻ thông tin với Trung tâm Giám sát an toàn không gian mạng quốc gia thực hiện phù hợp với quy định trong Luật An toàn thông tin mạng; Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ; Thông tư số 31/2017-BTTTT ngày 15/11/2017 quy định về hoạt động giám sát an toàn hệ thống thông tin, Chỉ thị số 14/CT-TTg ngày 07/6/2019 về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam.

Việc kết nối, chia sẻ thông tin tuân thủ theo Thông tư số 39/2017/TT-BTTTT ngày 15/12/2017 của Bộ Thông tin và Truyền thông ban hành Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước; Thông tư số

13/2017/TT-BTTTT Quy định các yêu cầu kỹ thuật về kết nối các hệ thống thông tin, cơ sở dữ liệu với cơ sở dữ liệu quốc gia.

Tham chiếu áp dụng Quy chuẩn kỹ thuật quốc gia QCVN 102:2016/BTTTT về cấu trúc mã định danh.

Việc kết nối, chia sẻ thông tin từ hệ thống của cơ quan, tổ chức với Hệ thống xử lý tấn công mạng Internet Việt Nam (Hệ thống tiếp nhận và xử lý dữ liệu giám sát quốc gia) của Bộ Thông tin và Truyền thông, giúp phát hiện và cảnh báo sớm nguy cơ mất an toàn thông tin có thể xảy ra với cơ quan, tổ chức và phục vụ công tác quản lý nhà nước của Bộ Thông tin và Truyền thông.

Địa chỉ hệ thống kỹ thuật tiếp nhận thông tin:

- Địa chỉ trên Internet: https://monitor.soc.gov.vn.

- Địa chỉ trên mạng truyền số liệu chuyên dùng: https://10.21.124.2

Để kết nối chia sẻ thông tin, tổ chức cung cấp thông tin (theo Phụ lục 5) Cục An toàn thông tin sẽ cấp tài khoản xác thực. Trong quá trình thực hiện, nếu cần hỗ trợ có thể liên hệ đầu mối kỹ thuật của Cục An toàn thông tin để được hướng dẫn kỹ thuật cụ thể theo thư điện tử: ais@mic.gov.vn; điện thoại: 02432091616.

4.2 Nguyên tắc kết nối và chia sẻ thông tin

- Hệ thống giám sát trung tâm cấp Bộ, ngành, địa phương thực hiện chia sẻ thông tin với Hệ thống tiếp nhận và xử lý dữ liệu giám sát quốc gia theo nguyên tắc:

- Phù hợp với các quy định trong Luật An toàn thông tin mạng; Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ; Thông tư số 31/2017-BTTTT ngày 15/11/2017 quy định về hoạt động giám sát an toàn hệ thống thông tin, Chỉ thị số 14/CT-TTg ngày 07/6/2019 về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam.

- Thông tin chia sẻ giữa Hệ thống giám sát trung tâm cấp Bộ, ngành, địa phương với Hệ thống tiếp nhận và xử lý dữ liệu giám sát quốc gia được thực hiện một chiều, trên kênh mã hoá và bảo đảm an toàn thông tin.

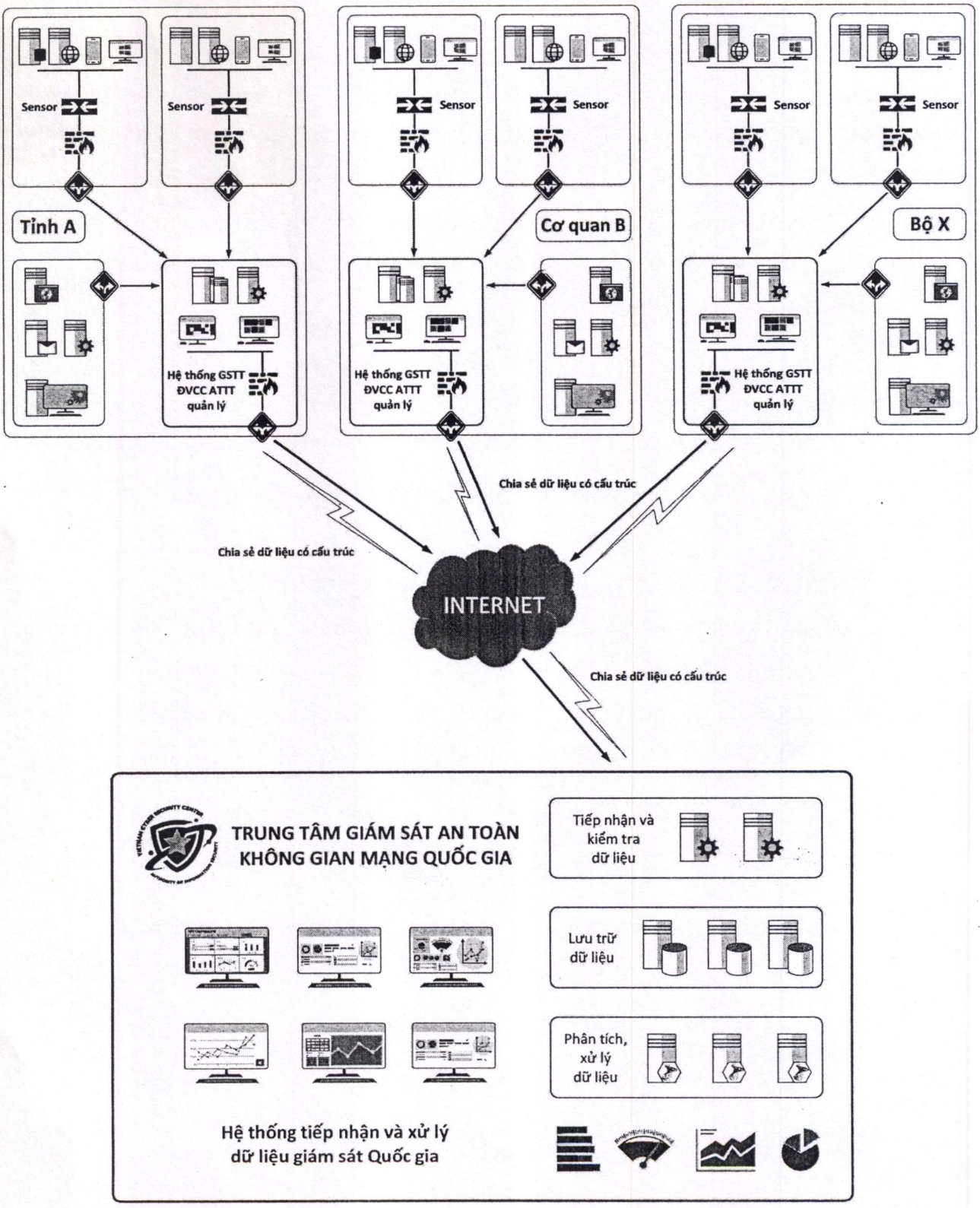
- Thông tin chia sẻ theo định dạng dữ liệu có cấu trúc với các trường dữ liệu quy định tại Phụ lục 3: Định dạng dữ liệu chia sẻ

- Hệ thống tiếp nhận và xử lý dữ liệu giám sát quốc gia tiếp nhận thông tin chia sẻ từ Hệ thống giám sát trung tâm cấp bộ, ngành, địa phương và không chia sẻ thông tin này với bên thứ ba.

- Thông tin chia sẻ định kỳ và thời điểm cập nhật thông tin do Cục An toàn thông tin xây dựng và thông báo đến các tổ chức để bảo đảm hiệu năng của hệ thống kỹ thuật.

- Khi có thay đổi thông tin về máy chủ chia sẻ thông tin, các cơ quan, đơn vị, tổ chức thông báo về Cục An toàn thông tin để cập nhật kết nối chia sẻ.

4.3 Mô hình kết nối



Hình 4. Mô hình kết nối hệ thống

- Mỗi Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Uỷ ban nhân dân các tỉnh, thành phố trực thuộc Trung ương có 01 hệ thống giám sát tập trung và giao cho đơn vị chuyên trách về an toàn thông tin quản lý, gọi là Hệ thống giám sát trung tâm cấp bộ, ngành, địa phương.

- Nếu các đơn vị trực thuộc bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Uỷ ban nhân dân các tỉnh, thành phố trực thuộc Trung ương có hệ thống giám sát tập trung của riêng đơn vị thì thực hiện kết nối về Hệ thống giám sát trung tâm cấp bộ, ngành, địa phương.

- Hệ thống tiếp nhận và xử lý dữ liệu giám sát Quốc gia do Trung tâm Giám sát an toàn không gian mạng quốc gia, Cục An toàn thông tin quản lý và vận hành.

4.4 Phương thức kết nối

Việc chia sẻ thông tin giữa Hệ thống giám sát trung tâm cấp bộ, ngành, địa phương của các cơ quan đơn vị với Hệ thống tiếp nhận và xử lý dữ liệu giám sát quốc gia của Bộ Thông tin và Truyền thông được truyền đi qua kênh mã hoá HTTPS.

Thông tin chia sẻ bao gồm các trường được mô tả trong Phụ lục 3 và đóng gói theo chuẩn JSON.

4.5 Hướng dẫn về định dạng thông tin, dữ liệu chia sẻ

Việc kết nối, chia sẻ thông tin giữa các hệ thống kỹ thuật thực hiện trên cơ sở áp dụng định dạng dữ liệu JSON với các trường dữ liệu theo quy định tại Phụ lục 3. Việc xác định quy cách đóng gói gói tin do doanh nghiệp cung cấp giải pháp quyết định dựa trên cơ sở đáp ứng yêu cầu do cơ quan có nhu cầu khai thác đặt ra.

PHỤ LỤC 1:
HƯỚNG DẪN VỀ VIỆC HỖ TRỢ TRIỂN KHAI GIÁM SÁT CỦA BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Các cơ quan tổ chức có thể đề nghị cơ quan chức năng của Bộ Thông tin và Truyền thông (Cục An toàn thông tin) hỗ trợ phối hợp cùng giám sát một phần song hành cùng với hệ thống gián sát của các cơ quan tổ chức đang triển khai (tự đầu tư hoặc thuê dịch vụ của doanh nghiệp) để nâng cao khả năng phát hiện các tấn công mạng, mã độc và bổ sung đa dạng góc nhìn về các nguy cơ rủi ro.

Phương án hỗ trợ triển khai giám sát an toàn thông tin được Bộ Thông tin và Truyền thông (Cục An toàn thông tin) thực hiện theo 02 hình thức đặt cảm biến giám sát hoặc giám sát thụ động từ xa.

Trường hợp triển khai cảm biến giám sát, thì cảm biến giám sát sẽ được thiết lập tại điểm kết nối của hệ thống ra Internet (giám sát thụ động). Cảm biến giám sát sẽ được kết nối, chia sẻ trực tiếp thông tin giám sát với hệ thống của Bộ Thông tin và Truyền thông (Cục An toàn thông tin) để hỗ trợ phối hợp để cùng chủ quản thực hiện việc giám sát.

Trường hợp giám sát gián tiếp từ xa, thì cơ quan, tổ chức cần đăng ký và cung cấp các thông tin liên quan đối với các dịch vụ trực tuyến theo yêu cầu của Cục An toàn thông tin. Hệ thống giám sát trung tâm của Bộ Thông tin và Truyền thông (Cục An toàn thông tin) sẽ theo dõi thụ động từ xa để phát hiện một số dạng tấn công mạng phổ biến đối với các hệ thống trực tuyến của cơ quan, tổ chức.

Cơ quan, tổ chức có nhu cầu hỗ trợ giám sát từ Bộ Thông tin và Truyền thông cần đáp ứng các yêu cầu sau:

- Cung cấp thông tin cho Bộ Thông tin và Truyền thông theo hướng dẫn tại điểm g, Khoản 3, Điều 5 Thông tư số 31/2017/TT-BTTTT.

- Chuẩn bị máy chủ cài đặt cảm biến giám sát, thiết lập điểm giám sát theo hướng dẫn của Bộ Thông tin và Truyền thông đối với từng hệ thống cụ thể.

- Thiết lập cấu hình hệ thống để cho phép cảm biến giám sát có thể cập nhật dấu hiệu phát hiện tấn công mạng và chia sẻ thông tin giám sát tới hệ thống của Trung tâm giám sát an toàn thông gian mạng quốc gia.

- Cung cấp thông tin đầu mối phối hợp với cơ quan chức năng của Bộ Thông tin và Truyền thông (Cục An toàn thông tin) để phối hợp triển khai hệ thống, tiếp nhận cảnh báo và xử lý sự cố.

Trường hợp, cơ quan, tổ chức cần hỗ trợ triển khai giám sát, cơ quan, tổ chức có văn bản đề nghị Bộ Thông tin và Truyền thông (Cục An toàn thông tin) và gửi kèm theo thông tin liên quan như hướng dẫn ở trên.

PHỤ LỤC 2:
NỘI DUNG KHẢO SÁT PHỤC VỤ HOẠT ĐỘNG THUÊ DỊCH VỤ GIÁM SÁT AN TOÀN THÔNG TIN MẠNG

STT	NỘI DUNG CÂU HỎI KHẢO SÁT
I	***QUY HOẠCH HỆ THỐNG MẠNG***
	Cung cấp thông tin về sơ đồ vật lý và logic của hệ thống, quy hoạch các vùng mạng và địa chỉ IP.
II	***GIẢI PHÁP ATTT***
1	**Lớp mạng biên**
	a. Anti-DDoS/DDoS Mitigation (phòng chống/giảm thiểu tấn công từ chối dịch vụ)
	Giải pháp đang sử dụng (nếu có).
	Giải pháp (nếu có) chống được tấn công băng thông ở layer 4 (Volume-based) không?
	Số lượng dịch vụ/website cần bảo vệ?
	Thông tin về băng thông kết nối Internet của hệ thống.
	b. Tường lửa lớp mạng biên
	Có trang bị Firewall kiểm soát kết nối vào/ra Internet/WAN?
	Giải pháp đang sử dụng (nếu có).
	Có trang bị Firewall kiểm soát kết nối giữa các vùng mạng trong trung tâm dữ liệu?
	Băng thông giữa các vùng mạng?
	c. Phát hiện và phòng chống xâm nhập ở lớp mạng biên
	Có trang bị IPS/IDS phòng chống, phát hiện tấn công cho vùng Internet/WAN?
	Giải pháp đang sử dụng (nếu có).
	Có trang bị IPS/IDS phòng chống, phát hiện tấn công cho vùng mạng trong trung tâm dữ liệu?

STT	NỘI DUNG CÂU HỎI KHẢO SÁT
	Băng thông giữa các vùng mạng?
	d. Giải pháp bảo vệ chống tấn công vào hệ thống website, ứng dụng web
	Có trang bị giải pháp bảo vệ chuyên dụng cho website/cổng thông tin/ứng dụng web?
	Giải pháp đang sử dụng (nếu có).
	Mô hình mạng hiện tại có đáp ứng được các traffic web được đưa qua hệ thống WAF không?
	Số lượng website cần triển khai? (bao nhiêu website nội bộ, bao nhiêu website quảng bá ra ngoài Internet)
	e. Giải pháp kiểm soát người dùng truy cập Web
	Có trang bị giải pháp bảo vệ chuyên dụng để kiểm soát người dùng truy cập Web, proxy/caching?
	Giải pháp đang sử dụng (nếu có).
	Số lượng người dùng Internet hiện tại?
	f. Giải pháp bảo vệ hệ thống thư điện tử
	Có trang bị giải pháp bảo vệ , chặn lọc cho hệ thống Email?
	Giải pháp đang sử dụng (nếu có).
	Các tính năng chính của hệ thống Email Secuity đang sử dụng (Antispam, Antivirus, Antiphishing,…)
	Số lượng tài khoản người dùng? Lượng mail trung bình/ngày (MB)
2	**Lớp máy chủ và ứng dụng**
	a. Tường lửa lớp mạng lõi
	Có trang bị Firewall kiểm soát kết nối giữa các vùng mạng trong trung tâm dữ liệu?
	Giải pháp đang sử dụng (nếu có).
	Băng thông giữa các vùng mạng?
	b. Phát hiện và phòng chống xâm nhập

STT	NỘI DUNG CÂU HỎI KHẢO SÁT
	Có trang bị IPS/IDS phòng chống, phát hiện tấn công cho vùng mạng lõi trong trung tâm dữ liệu?
	Giải pháp đang sử dụng (nếu có).
	Băng thông giữa các vùng mạng?
	c. Phần mềm bảo vệ cài đặt trên máy chủ như Anti-virus, Device Control
	Số lượng máy chủ?
	Đã có hệ thống Endpoint Security cho máy chủ (Server) hay chưa? Nếu đã có thì đang dùng của hãng nào?
	d. Database Security
	Đã có giải pháp bảo vệ, giám sát đánh giá cho Cơ sở dữ liệu chưa?
	Giải pháp đang sử dụng (nếu có).
	Số lượng cơ sở dữ liệu cần bảo vệ, TPS cho mỗi Database Server?
3	**Phòng chống tấn công có chủ đích (Advanced Persistent Threats - APT)**
	Đã có giải pháp phát hiện tấn công APT ở mức Endpoint? Nếu có, đang sử dụng của hãng nào?
	Đã có giải pháp phát hiện tấn công APT qua Email? Nếu có, đang sử dụng của hãng nào?
	Đã có giải pháp phát hiện tấn công APT ở mức mạng? Nếu có, đang sử dụng của hãng nào?
	Đã có giải pháp phân tích mã độc APT tập trung, sandboxing? Nếu có, đang sử dụng của hãng nào?
4	**Lớp quản lý tập trung**
	a. Quản lý lỗ hổng bảo mật, bản vá tập trung
	Đã triển khai quản lý lỗ hổng bảo mật tập trung cho OS và các ứng dụng văn phòng trên máy trạm (MS office, Adobe…). Nếu có, đang sử dụng của hãng nào?
	b. Quản lý cấu hình thiết bị

STT	NỘI DUNG CÂU HỎI KHẢO SÁT
	Đã triển khai quản lý cấu hình các thiết bị (Mạng, bảo mật, máy chủ)?
	Liệt kê số lượng thiết bị cần quản lý?
	c. Thu thập, quản lý và phân tích sự kiện an ninh thông tin tập trung (SIEM)
	Đã triển khai quản lý và phân tích sự kiện an ninh thông tin tập trung? Nếu có, đang sử dụng của hãng nào?
5	**Lớp người dùng**
	a. Lớp người dùng đầu cuối
	Có triển khai hệ thống AD/LDAP hay ko? Nếu có, đang sử dụng của hãng nào?
	Có triển khai hệ thống Web Proxy/Web Gateway? Nếu có, đang sử dụng của hãng nào?
	b. Lớp người dùng quản trị
	Có giải pháp quản lý User Admin (tài khoản quản trị) riêng? Nếu có, đang sử dụng của hãng nào?
	Số lượng tài khoản quản trị cần quản lý?
	c. Endpoint Security for PC/Desktop/Laptop (phần mềm bảo vệ cài đặt trên máy tính người dùng như Anti-virus, Device Control)
	Số lượng máy trạm (PC, Desktop, Laptop)
	Đã có hệ thống Endpoint Security cho máy trạm hay chưa? Nếu đã có thì đang dùng của hãng nào?
	d. Network Access Control (kiểm soát truy cập và kết nối cho thiết bị vào hệ thống mạng nội bộ: PC, laptop, mobile)
	Có trang bị giải pháp Network Access Control - NAC? Nếu có, đang sử dụng của hãng nào?
	Số lượng Endpoint cần bảo vệ?

PHỤ LỤC 3:
ĐỊNH DẠNG DỮ LIỆU CHIA SẺ

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
1	vendor_id	string	Mã tổ chức thực hiện giám sát. Mã này do Cục An toàn thông tin cung cấp sau khi tổ chức đăng ký tài khoản.	Bắt buộc	
2	unit_id	string	Mã tổ chức được giám sát. Mã này do Cục An toàn thông tin cung cấp sau khi tổ chức đăng ký tài khoản.	Bắt buộc	QCVN 102:2016/BTTTT
3	sensor_id	string	Mã sensor, Mã này do Cục An toàn thông tin cung cấp sau khi tổ chức đăng ký tài khoản.	Bắt buộc	Đây là thiết bị hoặc hệ thống giám sát (sensor) chia sẻ dữ liệu về Hệ thống tiếp nhận và xử lý dữ liệu giám sát Quốc gia.
4	timestamp	float	Thời gian mà sensor ghi nhận được sự kiện.	Bắt buộc	Sử dụng định dạng UNIX Time
5	category	number	Phân loại cảnh báo vào loại hình tấn công	Bắt buộc	Category được phân loại theo chuẩn của chuẩn của MITRE

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
					1: Initial Access 2: Execution 3: Persistence 4: Privilege Escalation 5: Defense Evasion 6: Credential Access 7: Discovery 8: Lateral Movement 9: Collection 10: Command and Control 11: Exfiltration 12: Impact Tham khảo https://attack.mitre.org/matrices/enterprise/
6	action	number	Hành động của sensor đối với gói tin. Ví dụ Allowed là cho phép gói tin được đi qua	Bắt buộc	1: Allowed 2: Drop 3: Alerted 4: Suspended 5: Archived 6: Other

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
7	signature	string	Dấu hiệu nhận biết liên quan đến cảnh báo	Bắt buộc	Định dạng Signature tùy thuộc vào từng nhà chung cấp dịch vụ giám sát. Khuyến nghị chia sẻ thông tin chi tiết, tuy nhiên có thể chia sẻ thông tin mô tả.
8	severity	number	Mức độ nghiêm trọng/ưu tiên của cảnh báo Khuyến nghị chỉ chia sẻ cảnh báo từ mức 2 đến mức 4	Bắt buộc	1: Low 2: Medium 3: High 4: Critical
9	direction	number	Hướng của gói tin	Bắt buộc	0: outbound 1: inbound 2: local
10	dest_ip	string	Địa chỉ IP đích của gói tin	Bắt buộc	
11	dest_port	number	Địa chỉ cổng đích của gói tin	Bắt buộc	
12	src_ip	string	Địa chỉ IP nguồn của gói tin	Bắt buộc	
13	src_port	number	Địa chỉ cổng nguồn của gói tin	Bắt buộc	
14	proto	string	Giao thức sử dụng để truyền tải gói tin	Bắt buộc	Chiều dài từ 2-10 ký tự HTTP, TCP, DNS, UNDEFINED

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
15	domain	string	Tên miền của máy chủ điều khiển C&C	Tùy chọn	
16	host	string	Tên của sensor	Bắt buộc	
17	data_leak	[string]	Danh sách dữ liệu bị lộ, lọt	Tùy chọn	
18	tags	number	Trường thông tin về geoip	Bắt buộc	1: có tìm thấy geoip, 0: không tìm thấy geoip
19	geoip	object	Vị trí địa lý của IP public (có thể là địa chỉ nguồn hoặc địa chỉ đích của gói tin) không thuộc hệ thống được giám sát. Giá trị này phụ thuộc vào trường tags. Chỉ khi trường tags trả về giá trị 1 thì mới có các thuộc tính của đối tượng này. Các trường hợp khác các thuộc tính là NULL.	Tùy chọn	
19.1	lat	number	Vĩ độ	Bắt buộc	
19.2	lon	number	Kinh độ	Bắt buộc	

STT	Tên trường	Định dạng dữ liệu	Mô tả	Thuộc tính	Ghi chú
19.3	ip	string	Địa chỉ IP public (có thể là địa chỉ nguồn hoặc địa chỉ đích của gói tin) không thuộc hệ thống được giám sát.	Bắt buộc	
19.4	city_name	string	Tên thành phố	Bắt buộc	
19.5	country_name	string	Tên quốc gia	Bắt buộc	
19.6	country_code	string	Mã quốc gia theo chuẩn mới nhất	Bắt buộc	
19.7	timezone	string	Múi giờ	Bắt buộc	
19.8	region_name	string	Tên vùng	Bắt buộc	

PHỤ LỤC 4:
VÍ DỤ VỀ DỮ LIỆU CHIA SẺ


```
{
  "timestamp": 1565835901.01232356,
  "vendor_id": "VD.00.01.211",
  "unit_id": "00.01.133.H26",
  "sensor_id": "ad2bd838f1977b46636b81c9",
  "category": 8,
  "action": 6,
  "signature": "APT",
  "dest_ip": "81.182.250.130",
  "dest_port": 1435,
  "src_ip": "192.168.71.238",
  "src_port": 57879,
  "proto": "SMTP",
  "severity": 3,
  "direction": 0,
  "domain": "orlando.com",
  "host": "CYQPTL",
  "tags": 1,
  "geoip": {
    "region_name": "Nancy Hunt",
    "timezone": "Sam Hammack",
```

```
        "city_name": "Kreitzer",
        "lat": -68.195,
        "country_name": "Darlene",
        "lon": -121.5345,
        "ip": "81.182.250.130"
      }
}
```

PHỤ LỤC 5:
PHIẾU ĐĂNG KÝ THÔNG TIN PHỤC VỤ KẾT NỐI, CHIA SẺ DỮ LIỆU GIÁM SÁT

TÊN CƠ QUAN, TỔ CHỨC
TÊN ĐƠN VỊ

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày ... tháng ... năm ...

PHIẾU ĐĂNG KÝ THÔNG TIN

(Chỉ cung cấp cho Cục ATTT để phục vụ kết nối, chia sẻ thông tin với Hệ thống tiếp nhận và xử lý dữ liệu giám sát Quốc gia)

1. Thông tin chung

- Tên đơn vị: .....
- Địa chỉ: .....
- Số điện thoại : ..... Fax: .....
- Email: .....Website (nếu có): .....
- Mã số thuế (tùy chọn):.....
- Đơn vị cung cấp dịch vụ giám sát: .....
- Đại diện hợp pháp của cơ quan/tổ chức:
  - Họ tên (nếu có): .....
  - Email (nếu có): .....
- Đầu mối kỹ thuật giám sát của cơ quan/tổ chức:
  - Họ tên: .....
  - Email: .....
  - Số điện thoại: .....
  - Địa chỉ: .....

2. Thông tin các điểm giám sát(sensor) của đơn vị

STT	Địa chỉ giám sát	Tên Sensor *(đặt theo đơn vị đặt sensor)*	Đơn vị cung cấp dịch vụ giám sát
1	Tầng 16, 115 Trần Duy Hưng, Hà Nội	Trung tâm Giám sát an toàn không gian mạng quốc gia	Trung tâm Giám sát an toàn không gian mạng quốc gia
2	Tầng 8, 115 Trần Duy Hưng, Hà Nội	Sensor1_Cục ATTT	BKAV
3	Tầng 8, 115 Trần Duy Hưng, Hà Nội	Sensor2_Cục ATTT	Viettel
...	...	...	...

Ghi chú: *Bản mềm gửi về hòm thư ais@mic.gov.vn*

ĐẠI DIỆN LÃNH ĐẠO ĐƠN VỊ

(Ghi rõ chức danh, họ tên, ký và đóng dấu)