**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

**HƯỚNG DẪN MÔ HÌNH BẢO ĐẢM AN TOÀN THÔNG TIN CẤP BỘ, TỈNH**

(*Kèm theo Công văn số 235/CATTT-ATHTTT ngày 08 tháng 04 năm 2020
của Cục An toàn thông tin)*

**Hà Nội, 2020**

# I. ĐẶT VẤN ĐỀ

# Trong thời gian vừa qua, công tác bảo đảm an toàn thông tin cho hệ thống thông tin, đặc biệt là bảo đảm an toàn thông tin phục vụ Chính phủ điện tử (CPĐT), Chính quyền điện tử (CQĐT) và Đô thị thông minh (ĐTTM) đã được các bộ, ngành, địa phương quan tâm. Tình hình an toàn thông tin tại Việt Nam đã ghi nhận nhiều chuyển biến tích cực.

Tuy nhiên, công tác bảo đảm an toàn thông tin chưa được triển khai một cách tổng thể, đồng bộ và thống nhất với với Khung kiến trúc Chính phủ điện tử Việt Nam, phiên bản 2.0 (Khung CPĐT 2.0) và các hướng dẫn khác của Bộ Thông tin và Truyền thông có liên quan; Mức độ quan tâm của người đứng đầu còn hạn chế; Việc triển khai công tác bảo đảm an toàn thông tin còn chưa đúng cách. Do đó, công tác bảo đảm an toàn thông tin nói chung cần tiếp tục thực hiện một cách tổng thể, đồng bộ và thống nhất, tuân thủ các quy định của pháp luật.

# II. MỤC ĐÍCH

1. Đảm bảo công tác an toàn thông tin trong phát triển CPĐT, CQĐT và ĐTTM tuân thủ các quy định của pháp luật, đáp ứng các yêu cầu bảo đảm an toàn thông tin theo quy định và phù hợp với Khung CPĐT 2.0.

2. Thống nhất, đồng bộ công tác, mô hình bảo đảm an toàn thông tin phục vụ phát triển CPĐT, CQĐT và ĐTTM tại các bộ, ngành, địa phương.

# III. QUAN ĐIỂM, NGUYÊN TẮC XÂY DỰNG VÀ TRIỂN KHAI

1. Công tác bảo đảm an toàn, an ninh mạng là điều kiện cơ bản, là yếu tố sống còn, không thể tách rời công tác chuyển đổi số, phát triển CPĐT, CQĐT và ĐTTM.

2. Việc thực thi bảo đảm an toàn thông tin phải tuân thủ các quy định của pháp luật; phương án bảo đảm an toàn thông tin phải đáp ứng các yêu cầu an toàn cơ bản theo quy định, phù hợp với Khung CPĐT 2.0 và các văn bản liên quan.

3. Công tác bảo đảm an toàn thông tin phải bảo đảm tính thống nhất, đồng bộ, tận dụng, chia sẻ hạ tầng, tài nguyên sẵn có.

4. Gắn kết an toàn thông tin trong quá trình chuyển đổi số tránh đầu tư trùng lặp, lãng phí.

5. Việc tổ chức bảo đảm an toàn thông tin phải tuân thủ nguyên tắc chỉ huy tại chỗ, lực lượng tại chỗ, thiết bị tại chỗ, hậu cần tại chỗ.

# IV. MÔ HÌNH ĐIỂN HÌNH ATTT CHÍNH QUYỀN ĐIỆN CẤP TỈNH

1. Cách tiếp cận xây dựng mô hình

Mô hình được xây dựng dựa trên phương pháp tiếp cận như sau:

- Hướng dẫn chi tiết Khung CPĐT 2.0 đối với nội dung về bảo đảm an toàn thông tin, nhằm tạo ra sự thống nhất, đồng bộ trong công tác bảo đảm an toàn thông tin phục vụ phát triển CQĐT,CPĐT và ĐTTM.

- Hướng dẫn chi tiết việc thực thi bảo đảm an toàn thông tin trong việc phát triển CQĐT, CPĐT và ĐTTM nhằm tuân thủ theo quy định của pháp luật và đáp ứng các tiêu chuẩn, quy chuẩn quốc gia về an toàn thông tin.

## 2. Mô hình bảo đảm an toàn thông tin cấp bộ, tỉnh

### 2.1. Mô hình đảm an toàn thông tin tổng thể cấp bộ, tỉnh



*Hình 1: Mô hình đảm bảo an toàn thông tin tổng thể cấp bộ, tỉnh*

Mô hình đảm an toàn thông tin tổng thể cấp bộ, tỉnh bao gồm các thành phần: (1) Hệ thống thông tin phục vụ phát triển CPĐT, CQĐT và ĐTTM cấp bộ, tỉnh; (2) Trung tâm điều hành an toàn, an ninh mạng; (3) Mô hình tổ chức “04 lớp” bảo đảm an toàn thông tin; (4) Mô hình tham chiếu về biện pháp quản lý an toàn thông tin; (5) Mô hình tham chiếu về giải pháp, công nghệ; (6) Mô hình tham chiếu Trung tâm điều hành an toàn, an ninh mạng.

Mỗi bộ, tỉnh thiết lập một Trung tâm điều hành an toàn, an ninh mạng và thực hiện kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia phục vụ hoạt động hỗ trợ giám sát, phòng chống tấn công mạng và điều phối ứng cứu sự cố an toàn thông tin.

### 2.2. Thành phần bảo đảm an toàn thông tin

Việc bảo đảm an toàn thông tin phục vụ phát triển CPĐT phải thống nhất, đồng bộ các hệ thống thành phần trong mô hình. Các hệ thống thành phần cần bảo đảm an toàn thông tin phục vụ CPĐT cấp bộ, tỉnh và ĐTTM cấp tỉnh bao gồm nhưng không giới hạn các thành phần sau:

(1) Cổng Thông tin điện tử;

(2) Cổng Dịch vụ công/Hệ thống thông tin một cửa điện tử;

(3) Hệ thống Quản lý văn bản và điều hành;

(4) Hệ thống thông tin báo cáo;

(5) Nền tảng chia sẻ, tích hợp dùng chung (LGSP);

(6) Các hệ thống cơ sở dữ liệu phục vụ phát triển CPĐT, CQĐT và ĐTTM;

(7) Các hệ thống thông tin khác phục vụ phát triển CPĐT, CQĐT và ĐTTM;

(8) Trung tâm điều hành an toàn, an ninh mạng (SOC).

### 2.3. Mô hình tổ chức “04 lớp” bảo đảm an toàn thông tin

Công tác bảo đảm an toàn thông tin nói chung và công tác bảo đảm an toàn thông tin trong CPĐT, CQĐT và ĐTTM phải được thực hiện một cách tổng thể, đồng bộ theo chỉ đạo của Thủ tướng Chính phủ tại Chỉ thị số 14/CT-TTg ngày 06/7/2019. Theo đó, cơ quan, tổ chức triển khai bảo đảm an toàn thông tin cho hệ thống thông tin thuộc phạm vi quản lý theo mô **“4 lớp”**: (1) Lực lượng tại chỗ, (2) Tổ chức hoặc doanh nghiệp giám sát, bảo vệ chuyên nghiệp, (3) Tổ chức hoặc doanh nghiệp độc lập kiểm tra, đánh giá định kỳ, (4) Kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia.

a) Lực lượng tại chỗ

Thực hiện kiện toàn lực lượng tại chỗ để thực hiện giám sát, bảo vệ: (1) Người đứng đầu các bộ, ngành, địa phương trực tiếp quan tâm, chỉ đạo công tác an toàn, an ninh mạng theo đúng chỉ đạo của Thủ tướng Chính phủ, hoặc có thể phân công một Lãnh đạo cấp phó giúp theo dõi, điều hành; (2) Chỉ định, kiện toàn đầu mối đơn vị chuyên trách về an toàn thông tin mạng để làm tốt công tác tham mưu, tổ chức thực thi và kiểm tra, đôn đốc thực hiện các quy định của pháp luật về bảo đảm an toàn, an ninh mạng; (3) Thành lập Bộ phận chuyên trách về an toàn thông tin/Đội Ứng cứu sự cố an toàn thông tin mạng để thực thi nhiệm vụ bảo đảm an toàn thông tin và ứng cứu sự cố an toàn thông tin mạng với sự tham gia của đại diện các cơ quan, tổ chức trực thuộc do đơn vị chuyên trách làm thường trực; (4) Đăng ký tham gia Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia do Trung tâm VNCERT/CC, Cục An toàn thông tin làm điều phối.

b) Tổ chức hoặc doanh nghiệp giám sát, bảo vệ chuyên nghiệp

Tổ chức hoặc doanh nghiệp giám sát, bảo vệ chuyên nghiệp: Bên cạnh lực lượng tại chỗ, mỗi hệ thống thông tin từ cấp độ 3 trở lên cần có sự giám sát, bảo vệ của lực lượng chuyên nghiệp. Lực lượng chuyên nghiệp có thể là doanh nghiệp được Bộ Thông tin và Truyền thông cấp phép hoặc đơn vị chuyên trách của Bộ Quốc phòng (Bộ Tư lệnh 86, Ban Cơ yếu Chính phủ), Bộ Công an (Cục An ninh mạng và phòng chống tội phạm công nghệ cao), Bộ Thông tin và Truyền thông (Cục An toàn thông tin).

c) Tổ chức hoặc doanh nghiệp độc lập kiểm tra, đánh giá định kỳ

Tổ chức hoặc thuê doanh nghiệp độc lập kiểm tra, đánh giá định kỳ: Định kỳ tối thiểu 1 năm một lần có tổ chức hoặc doanh nghiệp độc lập với tổ chức hoặc doanh nghiệp giám sát, bảo vệ để thực hiện kiểm tra, đánh giá, rà quét, phát hiện lỗ hổng, điểm yếu, kiểm thử xâm nhập hệ thống để từ đó có biện pháp phòng ngừa, khắc phục phù hợp.

d) Kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia

Thực hiện kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia của Cục An toàn thông tin, Bộ Thông tin và Truyền thông. Đăng ký đầy đủ với Trung tâm Giám sát an toàn không gian mạng quốc gia, Cục An toàn thông tin các dải địa chỉ IP public của các hệ thống thông tin trong cơ quan, tổ chức nhà nước phục vụ việc theo dõi, cảnh báo các kết nối bất thường, độc hại.

### 2.4. Mô hình tham chiếu về biện pháp quản lý an toàn thông tin

Mô hình dưới đây mô tả các yêu cầu về quản lý an toàn thông tin theo tiêu chuẩn quốc gia TCVN 11930:2017.



*Hình 2: Mô hình các yêu cầu về quản lý an toàn thông tin*

Các yêu cầu cụ thể được xác định dựa vào cấp độ của hệ thống thông tin tương ứng cần bảo vệ và được chia ra làm 05 nhóm: (1) Chính sách an toàn thông tin, (2) Tổ chức bảo đảm an toàn thông tin, (3) Bảo đảm nguồn nhân lực, (4) Quản lý thiết kế, xây dựng hệ thống, (5) Quản lý vận hành an toàn hệ thống thông tin, chi tiết tham khảo tại Phụ lục hướng dẫn này.

### 2.5. Mô hình tham chiếu biện pháp kỹ thuật bảo đảm an toàn thông tin

Mô hình dưới đây mô tả các yêu cầu về kỹ thuật bảo đảm an toàn thông tin theo tiêu chuẩn quốc gia TCVN 11930:2017.



*Hình 3: Mô hình yêu cầu về kỹ thuật đảm bảo an toàn thông tin*

Các yêu cầu cụ thể được xác định dựa vào cấp độ của hệ thống thông tin tương ứng cần bảo vệ và được chia làm 04 nhóm: (1) An toàn hạ tầng mạng, (2) An toàn máy chủ, (3) An toàn ứng dụng, (4) An toàn dữ liệu, chi tiết thảm khảo tại Phụ lục hướng dẫn này.

***2.6. Mô hình tham chiếu về giải pháp, công nghệ***

Mô hình tham chiếu này đưa ra thành phần giải pháp, công nghệ và sản phẩm được sử dụng nhằm bảo đảm an toàn thông tin cho các hệ thống thông tin phục vụ phát triển CPĐT, CQĐT và ĐTTM.

Các sản phẩm cụ thể được phân chia làm 08 nhóm, bao gồm: (1) Sản phẩm an toàn cho thiết bị đầu cuối; (2) Sản phẩm an toàn lớp mạng; (3) Sản phẩm an toàn lớp ứng dụng; (4) Sản phẩm bảo vệ dữ liệu; (5) Nhóm giải pháp định hướng phát triển theo hình thức cung cấp dịch vụ; (6) Sản phẩm trình duyệt; (7) Sản phẩm nền tảng tích hợp, chia sẻ dữ liệu (LGSP); (8) Sản phẩm nền tảng điện toán đám mây phục vụ chính phủ điện tử.



*Hình 4: Mô hình tham chiếu về giải pháp và công nghệ*

Danh mục, chức năng chi tiết của từng nhóm sản phẩm tham khảo tại Phụ lục hướng dẫn này.

### 2.7. Mô hình tham chiếu Trung tâm điều hành an toàn, an ninh mạng

Mô hình SOC bao gồm 03 thành phần cơ bản như hình dưới đây:



*Hình 5: Mô hình Trung tâm điều hành an toàn, an ninh mạng SOC*

Trong đó:

Công nghệ là các phương án, giải pháp kỹ thuật được sử dụng để bảo đảm việc giám sát an toàn thông tin đáp ứng các yêu cầu về kỹ thuật và tính hiệu quả.

Quy trình là những quy định trong quy chế, chính sách bảo đảm an toàn thông tin của cơ quan, tổ chức được xây dựng để phục vụ việc quản lý, vận hành hệ thống an toàn.

Con người là việc tổ chức nhân sự cán bộ chuyên trách, chuyên gia và các đội ngũ khác (nếu có) để vận hành quản lý hệ thống SOC và các thành phần liên quan.

Theo Khung CPĐT 2.0, hệ thống SOC sau khi được thiết lập cần được kết nối, chia sẻ thông tin với hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia phục vụ hoạt động hỗ trợ giám sát và phòng chống tấn công mạng và điều phối ứng cứu sự cố an toàn thông tin. Việc kết nối chia sẻ thông tin được thực hiện theo hướng dẫn của Bộ Thông tin và Truyền thông về việc triển khai hoạt động giám sát an toàn thông tin trong cơ quan, tổ chức nhà nước tại Công văn số 2973/BTTTT-CATTT ngày 04/9/2019.

Chi tiết mô hình tham chiếu Trung tâm điều hành an toàn, an ninh mạng tại phụ lục kèm theo.

## 3. Thực thi bảo đảm an toàn thông tin cho hệ thống thông tin phục vụ phát triển CPĐT

***3.1. Xây dựng Hồ sơ đề xuất cấp độ và triển khai phương án bảo đảm an toàn thông tin theo cấp độ***

Việc xác định và xây dựng HSĐXCĐ là điều kiện bắt buộc đối với cơ quan, tổ chức trong việc tuân thủ các quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ. Căn cứ vào cấp độ của hệ thống thông tin cho phép cơ quan, tổ chức xác định được các hệ thống thông tin quan trọng cần ưu tiên bảo vệ và xây dựng phương án bảo vệ phù hợp.

Để có phương án bảo vệ phù hợp, cơ quan tổ chức xác định các yêu cầu an toàn đối với cấp độ tương ứng của hệ thống thông tin theo quy định tại Thông tư số 03/2017/TT-BTTTT ngày 24/04/2017 và hướng dẫn chi tiết tại tiêu chuẩn quốc gia TCVN 11930:2017.

Sau khi xác định được cấp độ của hệ thống và xây dựng phương án bảo vệ tương ứng, cơ quan, tổ chức hoàn thiện HSĐXCĐ trình cấp có thẩm quyền thẩm định và phê duyệt theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ.

Sau khi HSĐXCĐ được phê duyệt, cơ quan, tổ chức triển khai phương án bảo đảm an toàn hệ thống thông tin theo phương án đã được phê duyệt trong HSĐXCĐ, trong đó, cơ quan, tổ chức cần chú ý: (1) Phương án bảo đảm an toàn thông tin trong HSĐXCĐ là sở cứ để đề nghị đầu tư nâng cấp hệ thống thông tin trong trường hợp hệ thống hiện tại chưa đáp ứng các yêu cầu an toàn theo quy định; (2) Phương án và kết quả thực hiện phương án bảo vệ trong HSĐXCĐ là cơ sở để cơ quan có thẩm quyền kiểm tra, đánh giá sự tuân thủ của cơ quan tổ chức đối với các quy định về bảo đảm an toàn hệ thống thông tin theo cấp độ và đánh giá hiệu quả của phương án bảo vệ.

Hướng dẫn cụ thể liên quan đến việc xác định và thực thi bảo đảm an toàn hệ thống thông tin theo cấp độ được Bộ Thông tin và Truyền thông hướng dẫn tại Công văn số 713/CATTT-TĐQLGS ngày 25/7/2019.

***3.2. Triển khai Trung tâm điều hành an toàn, an ninh mạng***

Việc triển khai hệ thống giám sát, điều hành an toàn, an ninh mạng tập trung (SOC) cho một bộ, ngành, địa phương là hết sức cần thiết. Tuy nhiên, ngay từ khi triển khai, cơ quan, tổ chức cần nhận thức rất rõ: Việc triển khai một hệ thống SOC hiệu quả mấu chốt nằm ở đội ngũ nhân sự, chuyên gia phân tích, vận hành, khai thác theo quy trình chuyên nghiệp. Lực lượng nhân sự này chủ yếu nằm ở các doanh nghiệp.

Vì vậy, việc triển khai hệ thống SOC cần được cân nhắc trên quan điểm tổng thể, tránh việc chỉ đơn giản đầu tư, mua sắm giải pháp, trang thiết bị mà không khai thác, vận hành hiệu quả.

Trong quá trình triển khai hệ thống SOC, đề nghị cơ quan, tổ chức tham vấn ý kiến của Bộ Thông tin và Truyền thông về thiết kế kỹ thuật, bảo đảm sự hoạt động liên thông, kết nối, chia sẻ thông tin với Trung tâm Giám sát an toàn không gian mạng quốc gia, Cục An toàn thông tin. Trong số các đối tác tham gia triển khai, lựa chọn đối tác có đủ năng lực chuyên môn về an toàn, an ninh mạng để bảo đảm triển khai hiệu quả.

***3.3. Kiểm tra, đánh giá an toàn thông tin***

Cơ quan, tổ chức thực hiện kiểm tra, đánh giá an toàn thông tin theo quy định tại Thông tư 03/2017/TT-BTTTT. Nội dung kiểm tra đánh giá bao gồm: (1) Kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ; (2) Đánh giá hiệu quả của biện pháp bảo đảm an toàn hệ thống thông tin; (3) Đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống.

Đối với việc kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ, chủ quản hệ thống thông tin chỉ đạo, giao đơn vị chuyên trách về an toàn thông tin tổ chức kiểm tra, đánh giá theo quy định.

Đối với việc đánh giá hiệu quả của biện pháp bảo đảm an toàn hệ thống thông tin và đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống, Bộ TT&TT đề nghị cơ quan, tổ chức thực hiện kiểm tra, đánh giá theo tinh thần chỉ đạo của Thủ tướng Chính phủ tại Chỉ thị số 14/CT-TTg ngày 25/5/2018 quy định như sau: “Đối với công tác kiểm tra, đánh giá an toàn thông tin mạng cho hệ thống thông tin thuộc quyền quản lý: 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 toàn thông tin mạng đối với hệ thống thông tin cấp độ 3 trở lên thuộc quyền quản lý hoặc kiểm tra, đánh giá đột xuất khi có yêu cầu theo quy định của pháp luật”.

Kết quả kiểm tra đánh giá được giám sát và đánh giá bởi một đơn vị độc lập (đơn vị chức năng, đơn vị chuyên trách về an toàn thông tin hoặc một đơn vị độc lập khác) để phục vụ việc kiểm tra, giám sát của cơ quan có thẩm quyền.

Thẩm quyền, phạm vi và nội dung kiểm tra đánh giá phù hợp với quy định tại Điều 11, 12 và 13 Thông tư 03/2017/TT-BTTTT ngày 24/4/2017.

Nội dung kiểm tra, đánh giá an toàn thông tin cơ bản bao gồm các nội dung sau: (1) Kiểm tra, đánh giá về thiết kế, cấu hình bảo mật của hạ tầng mạng; (2) Kiểm tra, đánh giá lỗ hổng, điểm yếu an toàn thông tin trên thiết bị mạng, thiết bị bảo mật; (3) Kiểm tra, đánh giá lỗ hổng, điểm yếu an toàn thông tin trên máy chủ; (4) Kiểm tra, đánh giá lỗ hổng, điểm yếu an toàn thông tin trên ứng dụng; (5) Kiểm tra, đánh giá lỗ hổng, điểm yếu an toàn thông tin trên các thiết bị đầu cuối.

***3.4. Xây dựng phương án ứng cứu sự cố an toàn thông tin mạng***

Tổ chức xây dựng và triển khai kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng theo quy định tại Điều 16, Quyết định số 05/2017/NĐ-CP ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia. Theo đó, cơ quan, tổ chức cần thực hiện:

a) Khảo sát và thực đánh giá rủi ro để xác định các nguy cơ, sự cố an toàn thông tin có thể xảy ra đối với hệ thống;

b) Đánh giá và phân loại các nguy cơ, sự cố an toàn thông tin;

c) Xây dựng phương án, quy trình xử lý các sự cố, bao gồm nhưng không giới hạn các nhóm sự cố sau:

- Sự cố do bị tấn công mạng: Tấn công từ chối dịch vụ, Tấn công giả mạo, Tấn công sử dụng mã độc, Tấn công truy cập trái phép, chiếm quyền điều khiển, Tấn công thay đổi giao diện, Tấn công mã hóa phần mềm, dữ liệu, thiết bị, Tấn công phá hoại thông tin, dữ liệu, phần mềm, Tấn công nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu, Tấn công tổng hợp sử dụng kết hợp nhiều hình thức.

- Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật: Sự cố nguồn điện, Sự cố đường kết nối Internet, Sự cố do lỗi phần mềm, phần cứng, ứng dụng của hệ thống thông tin, Sự cố liên quan đến quá tải hệ thống, Sự cố khác do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật.

- Tình huống sự cố do lỗi của người quản trị, vận hành hệ thống: Lỗi trong cập nhật, thay đổi, cấu hình phần cứng, Lỗi trong cập nhật, thay đổi, cấu hình phần mềm; Lỗi liên quan đến chính sách và thủ tục an toàn thông tin, Lỗi liên quan đến việc dừng dịch vụ vì lý do bắt buộc, Lỗi khác liên quan đến người quản trị, vận hành hệ thống.

d) Xây dựng kịch bản và tổ chức diễn tập để thực hành phương án ứng cứu sự cố được xây dựng.

***3.5. Phòng, chống phần mềm độc hại***

Tổ chức triển khai các biện pháp tăng cường năng lực phòng chống phần mềm độc hại theo chỉ đạo của Thủ tướng Chính phủ tại Chỉ thị số 14/CT-TTg ngày 25/5/2018, cụ thể:

- Bảo đảm 100% máy chủ, máy trạm, thiết bị đầu cuối (nếu được hỗ trợ bởi phần mềm phòng chống mã độc) được cài đặt giải pháp phòng chống mã độc đáp ứng yêu cầu tại Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ;

- Giải pháp, phần mềm sử dụng đáp ứng các yêu cầu kỹ thuật tối thiểu bao gồm: Có chức năng cho phép quản trị tập trung; có dịch vụ, giải pháp hỗ trợ kỹ thuật 24/7, có khả năng phản ứng kịp thời trong việc phát hiện, phân tích và gỡ bỏ phần mềm độc hại; có thể chia sẻ thông tin, dữ liệu thống kê tình hình lây nhiễm mã độc với hệ thống kỹ thuật của cơ quan chức năng có thẩm quyền, tuân thủ theo tiêu chuẩn, quy chuẩn kỹ thuật, hướng dẫn nghiệp vụ của Bộ Thông tin và Truyền thông và quy định của pháp luật;

- Trong các dự án đầu tư ứng dụng công nghệ thông tin phải có cấu phần phù hợp cho giải pháp bảo đảm an toàn thông tin, giải pháp phòng, chống mã độc;

- Tổ chức theo dõi, thống kê chỉ số lây nhiễm mã độc trên các thiết bị đầu cuối, các hệ thống thông tin trong phạm vi bộ, ngành, địa phương mình, định kỳ hàng quý báo cáo về Bộ Thông tin và Truyền thông;

- Đăng ký đầy đủ với Trung tâm Giám sát an toàn không gian mạng quốc gia, Cục An toàn thông tin các dải địa chỉ IP public của các hệ thống thông tin trong cơ quan, tổ chức nhà nước phục vụ việc theo dõi, cảnh báo các kết nối bất thường, độc hại;

- Tuân thủ yêu cầu báo cáo, yêu cầu kết nối, chia sẻ thông tin về Trung tâm Giám sát an toàn không gian mạng quốc gia, Cục An toàn thông tin theo đúng chỉ đạo của Thủ tướng Chính phủ và văn bản hướng dẫn của Bộ Thông tin và Truyền thông.

PHỤ LỤC

**CHI TIẾT CÁC MÔ HÌNH THAM CHIẾU AN TOÀN THÔNG TIN**

# I. Mô hình tham chiếu về quản lý an toàn thông tin

Mô hình dưới đây mô tả các yêu cầu về quản lý an toàn thông tin theo tiêu chuẩn quốc gia TCVN 11930:2017. Các yêu cầu cụ thể được xác định dựa vào cấp độ của hệ thống thông tin tương ứng cần bảo vệ.



*Hình tham chiếu hình 2 trang 05: Mô hình các yêu cầu về quản lý an toàn thông tin*

Các yêu cầu về quản lý được chia ra làm 05 nhóm: (1) Chính sách an toàn thông tin, (2) Tổ chức bảo đảm an toàn thông tin, (3) Bảo đảm nguồn nhân lực, (4) Quản lý thiết kế, xây dựng hệ thống, (5) Quản lý vận hành an toàn hệ thống thông tin, cụ thể như sau:

### 1.1. Chính sách an toàn thông tin

Chính sách an toàn thông tin bao gồm các nội dung cơ bản như:

- Mục tiêu, nguyên tắc bảo đảm an toàn thông tin;

- Trách nhiệm bảo đảm an toàn thông tin: Mô tả trách nhiệm bảo đảm an toàn thông tin của đơn vị chuyên trách về an toàn thông tin và các đối tượng thuộc phạm vi điều chỉnh của chính sách an toàn thông tin;

- Phạm vi chính sách an toàn thông tin: Mô tả phạm vi chính sách, đối tượng áp dụng chính sách bảo đảm an toàn thông tin của tổ chức;

### 1.2. Tổ chức bảo đảm an toàn thông tin

Cung cấp thông tin về cơ cấu, tổ chức bảo đảm an toàn thông tin của tổ chức, bao gồm: Đơn vị chuyên trách về an toàn thông tin; Cơ chế, đầu mối phối hợp với cơ quan/tổ chức có thẩm quyền trong hoạt động bảo đảm an toàn thông tin.

### 1.3. Bảo đảm nguồn nhân lực

Đưa ra chính sách/quy trình thực hiện quản lý bảo đảm nguồn nhân lực an toàn thông tin của tổ chức, bao gồm: Tuyển dụng cán bộ; quy chế/quy định bảo đảm an toàn thông tin trong quá trình làm việc và chấm dứt hoặc thay đổi công việc.

### 1.4. Quản lý thiết kế, xây dựng hệ thống

Đưa ra 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.

### 1.5. Quản lý vận hành an toàn hệ thống

Quản lý vận hành an toàn hệ thống bao gồm 09 nội dung quản lý:

- Quản lý an toàn mạng: Đưa ra 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.

- Quản lý an toàn máy chủ và ứng dụng: Đưa ra chính sách/quy trình thực hiện quản lý 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.

- Quản lý an toàn dữ liệu: Đưa ra chính sách/quy trình thực hiện quản lý an toàn dữ liệu 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.

- Quản lý an toàn thiết bị đầu cuối: Đưa ra chính sách/quy trình thực hiện quản lý 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 toàn thông tin cho thiết bị đầu cuối.

- Quản lý phòng chống phần mềm độc hại: Đưa ra 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.

- Quản lý giám sát an toàn hệ thống thông tin: Đưa ra chính sách/quy trình thực hiện quản lý phòng chống phần mềm độc hại 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.

- Quản lý điểm yếu an toàn thông tin:Đưa ra chính sách/quy trình thực hiện quản lý điểm yếu an toàn thông tin của tổ chức, bao gồm: Quản lý thông tin các thành phần có trong hệ thống có khả năng tồn tại điểm yếu an toàn thông tin; Quản lý, cập nhật nguồn cung cấp điểm yếu an toàn thông tin; 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 toàn thông tin trước khi đưa hệ thống vào sử dụng; Quy trình khôi phục lại hệ thống.

- Quản lý sự cố an toàn thông tin: Đưa ra chính sách/quy trình thực hiện quản lý sự cố an toàn thông tin của tổ chức, bao gồm: Phân nhóm sự cố an toàn thông tin; Phương án tiếp nhận, phát hiện, phân loại và xử lý thông tin; Kế hoạch ứng phó sự cố an toàn thông tin; Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin; Quy trình ứng cứu sự cố an toàn thông tin thông thường; Quy trình ứng cứu sự cố an toàn thông tin nghiêm trọng; Cơ chế phối hợp trong việc xử lý, khắc phục sự cố an toàn thông tin; Diễn tập phương án xử lý sự cố an toàn thông tin.

- Quản lý an toàn người sử dụng đầu cuối: Đưa ra chính sách/quy trình thực hiện quản lý 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.

# II. Mô hình tham chiếu phương án kỹ thuật bảo đảm an toàn thông tin

Mô hình dưới đây mô tả các yêu cầu về kỹ thuật bảo đảm an toàn thông tin theo tiêu chuẩn quốc gia TCVN 11930:2017. Các yêu cầu cụ thể được xác định dựa vào cấp độ của hệ thống thông tin tương ứng cần bảo vệ.



*Hình tham chiếu hình 3 trang 05: Mô hình yêu cầu về kỹ thuật đảm bảo*

*an toàn thông tin*

Các yêu cầu được nhóm lại thành 04 nhóm: (1) An toàn hạ tầng mạng, (2) An toàn máy chủ, (3) An toàn ứng dụng, (4) An toàn dữ liệu, cụ thể như sau:

### 2.1. Bảo đảm an toàn mạng

- Thiết kế phương án bảo đảm an toàn thông tin: Đưa ra các phương án thiết kế các vùng mạng trong hệ thống theo chức năng, các vùng mạng; Phương án quản lý truy cập, quản trị hệ thống từ xa an toàn; Phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập; Phương án cân bằng tải, dự phòng nóng cho các thiết bị mạng; Phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu; Phương án chặn lọc phần mềm độc hại trên môi trường mạng; Phương án phòng chống tấn công từ chối dịch vụ; Phương án giám sát hệ thống thông tin tập trung; Phương án giám sát an toàn hệ thống thông tin tập trung; Phương án quản lý sao lưu dự phòng tập trung; Phương án quản lý phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng tập trung; Phương án phòng, chống thất thoát dữ liệu; Phương án bảo đảm an toàn cho mạng không dây; Phương án quản lý tài khoản đặc quyền; Phương án dự phòng hệ thống ở vị trí địa lý khác nhau.

- Kiểm soát truy cập từ bên ngoài mạng: Đưa ra phương án 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 từ 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.

- Kiểm soát truy cập từ bên trong mạng: Đưa ra phương án 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.

- Nhật ký hệ thống: Đưa ra phương án 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.

- Phòng chống xâm nhập: Đưa ra phương án triển khai/thiết lập cấu hình của thiết bị phòng, chống xâm nhập IDS/IPS hoặc chức năng IDS/IPS trên thiết bị tường lửa có trong hệ thống nhằm đáp ứng yêu cầu an toàn.

- Phòng chống phần mềm độc hại trên môi trường mạng: Đưa ra phương án triển khai/thiết lập cấu hình của thiết bị để thực hiện chức năng phòng chống phần mềm độc hại trên môi trường mạng đáp ứng yêu cầu an toàn.

- Bảo vệ thiết bị hệ thống: Đưa ra phương án triển khai/thiết lập cấu hình chức năng bảo mật trên các thiết bị có trong hệ thống nhằm bảo đảm an toàn cho thiết bị trong quá trình sử dụng và quản lý vận hành.

### 2.2. Bảo đảm an toàn máy chủ

- Xác thực: Đưa ra phương án thiết lập chính sách xác thực trên máy chủ để bảo đảm việc xác thực khi đăng nhập vào máy chủ an toàn.

- Kiểm soát truy cập: Đưa ra phương án thiết lập chính sách 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.

- Nhật ký hệ thống: Đưa ra phương án quản lý 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.

- Phòng chống xâm nhập: Đưa ra phương án thiết lập cấu hình bảo mật trên máy chủ để bảo vệ tấn công xâm nhập từ bên ngoài.

- Phòng chống phần mềm độc hại: Đưa ra phương án thiết lập cấu hình bảo mật 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.

- Xử lý máy chủ khi chuyển giao: Đưa ra phương án xóa sạch dữ liệu; sao lưu dự phòng dữ liệu khi chuyển giao hoặc thay đổi mục đích sử dụng.

### 2.3. Bảo đảm an toàn ứng dụng

- Xác thực: Đưa ra phương án thiết lập chính sách xác thực trên ứng dụng để bảo đảm việc xác thực khi đăng nhập vào máy chủ an toàn.

- Kiểm soát truy cập: Đưa ra phương án thiết lập chính sách 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.

- Nhật ký hệ thống: Đưa ra phương án quản lý 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.

- Bảo mật thông tin liên lạc: Đưa ra phương án mã hóa và sử dụng giao thức mạng hoặc kênh kết nối mạng an toàn khi trao đổi dữ liệu qua môi trường mạng.

- Chống chối bỏ: Đưa ra phương án dùng 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.

- An toàn ứng dụng và mã nguồn: Đưa ra phương án cấu hình/thiết lập chức năng bảo mật cho ứng dụng và phương án bảo vệ mã nguồn ứng dụng.

### 2.4. Bảo đảm an toàn dữ liệu

- Nguyên vẹn dữ liệu: Đưa ra phương án lưu trữ, quản lý thay đổi, khôi phục dữ liệu bảo đảm tính nguyên vẹn của dữ liệu.

- Bảo mật dữ liệu: Đưa ra phương án lưu trữ, quản lý thay đổi, khôi phục dữ liệu bảo đảm tính bí mật của dữ liệu.

- Sao lưu dự phòng: Đưa ra phương án 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…

# III. Mô hình tham chiếu về giải pháp, công nghệ

Mô hình tham chiếu này đưa ra thành phần giải pháp, công nghệ và sản phẩm được sử dụng nhằm bảo đảm an toàn thông tin cho các hệ thống thông tin phục vụ phát triển CPĐT, ĐTTM.

Các sản phẩm cụ thể được phân chia làm 08 nhóm, bao gồm:

- Sản phẩm an toàn cho thiết bị đầu cuối;

- Sản phẩm an toàn lớp mạng;

- Sản phẩm an toàn lớp ứng dụng;

- Sản phẩm bảo vệ dữ liệu;

- Nhóm giải pháp định hướng phát triển theo hình thức cung cấp dịch vụ;

- Sản phẩm trình duyệt;

- Sản phẩm nền tảng tích hợp, chia sẻ dữ liệu (LGSP);

- Sản phẩm nền tảng điện toán đám mây phục vụ CPĐT, ĐTTM.



*Hình tham chiếu hình 4 trang 06: Mô hình tham chiếu về giải pháp và công nghệ*

| **TT** | **Tên sản phẩm** | **Loại hình** | **Tính năng chính** |
| --- | --- | --- | --- |
| **I** | **Sản phẩm an toàn cho thiết bị đầu cuối** |
| 1 | Bảo vệ máy tính cá nhân/máy chủ (PC/Laptop/Server Security) | Phần mềm  | - Chống virus, mã độc hại- Phát hiện và ngăn chặn các loại tấn công có chủ đích (ATP) đến thiết bị đầu cuối- Tường lửa, phát hiện, chống tấn công (IPS/IDS)- Kiểm soát truy nhập- Giám sát hoạt động của thiết bị; hỗ trợ cập nhật bản vá phần mềm- Hỗ trợ mã hóa dự liệu, sao lưu dữ liệu trên thiết bị đầu cuối |
| 2 | Bảo vệ thiết bị di động (Mobile Security) | Phần mềm | - Chống virus, mã độc hại- Phát hiện và ngăn chặn các loại tấn công có chủ đích (ATP) đến thiết bị đầu cuối- Tường lửa, phát hiện, chống tấn công (IPS/IDS)- Kiểm soát truy nhập- Giám sát hoạt động của thiết bị; hỗ trợ cập nhật bản vá phần mềm- Hỗ trợ mã hóa dự liệu, sao lưu dữ liệu trên thiết bị di động |
| **II** | **Sản phẩm an toàn lớp mạng** |
| 1 | Sản phẩm kiểm soát truy cập mạng (Network Access Control) | Phần mềm/phần cứng | - Kiểm soát truy cập mạng- Quản lý định danh, xác thực và cấp quyền truy cập- Phân chia vùng mạng- Áp dụng thực thi chính sách an toàn mạng |
| 2 | Tường lửa bảo vệ lớp mạng (Network-base Firewall) | Phần mềm/phần cứng | - Ngăn chặn các tấn công trên hệ thống mạng- Quản lý, thiết lập các chính sách kiểm soát truy cập mạng- Phân tích, đánh giá dữ liệu trên đường truyền  |
| 3 | Sản phẩm phát hiện và ngăn chặn xâm nhập - Intrusion Prevention/ Detection System (IPS/IDS) | Phần mềm/phần cứng/giải pháp | - Phát hiện, ngăn chặn xâm nhập dựa trên:- Hành vi- Dữ liệu nhận dạng (signature)- Các chính sách được thiết lập- Nhật ký hệ thống |
| 4 | Sản phẩm chống tấn công từ chối dịch vụ (DDoS Prevention) | Phần mềm/phần cứng/giải pháp | - Chống tấn công từ chối dịch vụ, từ chối dịch vụ phân tán |
| 5 | Sản phẩm an toàn mạng Internet kết nối vạn vật (IoT Security) | Phần mềm | - Bảo đảm an toàn thông tin cho các thiết bị, hệ thống IoT |
| 6 | Sản phẩm quản lý sự kiện và an toàn thông tin (SIEM) | Phần mềm/phần cứng/giải pháp | - Quản lý sự kiện an toàn thông tin - Quản lý an toàn thông tin- Theo dõi, phân tích, cảnh báo theo thời gian thực các sự kiện mất an toàn thông tin xảy ra trên hệ thông tin- Thu thập, quản lý tập trung nhật ký sự kiện an toàn thông tin của các thiết bị trong hệ thống  |
| 7 | Thiết bị quản lý nguy cơ mất an toàn thông tin đa dụng (UTM) | Phần mềm/phần cứng | - Tích hợp đa dạng các tính năng bảo đảm an toàn thông tin (tường lửa, IPS/IDS, mạng riêng ảo, lọc thư rác, anti-virus,…)- Hỗ trợ quản lý, vận hành đơn giản, phù hợp với các hệ thống thông tin của tổ chức, doanh nghiệp vừa và nhỏ |
| 8 | Sản phẩm giám sát mạng (Network Monitoring) | Phần mềm/phần cứng | - Giám sát, phân tích gói tin truyền trên hệ thống mạng- Phát hiện các dấu hiệu, nguy cơ mất an toàn thông tin- Cảnh báo cho người quản trị |
| 9 | Mạng riêng ảo (VPN) | Phần mềm/phần cứng | - Tạo kênh kết nối riêng giữa các thiết bị, hệ thống mạng có mã hóa đường truyền- Chống các loại hình tấn công, nghe lén thông tin trên đường truyền- Xác thực các đối tượng tham gia trao đổi thông tin |
| **III** | **Sản phẩm an toàn lớp ứng dụng** |
| 1 | Tường lửa cho hệ thống cho các hệ thống ứng dụng trên nền tảng web (Web Application Firewall) | Phần mềm/phần cứng | - Chống các loại tấn công đối với ứng dụng trên nền tảng ứng dụng web - Hỗ trợ mã hóa thông tin giữa máy chủ web và người truy cập- Xác thực máy chủ web- Hạn chế thất thoát dữ liệu, xâm nhập bất hợp pháp vào máy chủ và ứng dụng web |
| 2 | Tường lửa cho hệ thống thư điện tử (Email Firewall) | Phần mềm/phần cứng | - Ngăn chặn các tấn công trên hệ thống thư điện tử- Thiết lập các bộ lọc thư điện tử, ngăn chặn thư điện tử rác, chứa mã độc,…- Quản lý, tăng cường sự tin cậy của hệ thống thư điện tử- Phân tích, đánh giá dữ liệu gửi và nhận từ hệ thống thư điện tử |
| 3 | Hệ thống kiểm soát người truy cập web | Phần mềm/phần cứng | - Kiểm soát người dùng truy cập Web/Ứng dụng Web- Phát hiện và ngăn chặn kết nối độc hại- Xác thực, định danh và phân quyền người dùng- Ngăn chặn thất thoát dữ liệu qua kênh upload- Ngăn chặn lừa đảo qua Internet |
| **IV** | **Sản phẩm bảo vệ dữ liệu** |
| 1 | Tường lửa cho hệ thống cơ sở dữ liệu (Database Firewall) | Phần mềm/phần cứng | - Bảo vệ cơ sở dữ liệu- Kiểm soát các truy vấn bất thường vào hệ thống cơ sở dữ liệu- Chống các loại hình tấn công, xâm nhập đặc thù vào cơ sở dữ liệu |
| 2 | Sản phẩm chống thất thoát dữ liệu (DLP) | Phần mềm/phần cứng | - Phân tích nội dung gói tin- Ngăn chặn các truy cập bất hợp pháp vào các dữ liệu nhạy cảm- Thiết lập và quản lý các chính sách chia sẻ, truy cập dữ liệu- Mã hóa dữ liệu- Phân quyền truy cập dữ liệu  |
| 3 | Sản phẩm mã hóa, an toàn dữ liệu lưu | Phần mềm/phần cứng | - Áp dụng các kỹ thuật mật mã tiên tiến mã hóa dữ liệu khi lưu trữ, chỉa sẻ |
| **V** | **Nhóm giải pháp định hướng phát triển theo hình thức cung cấp dịch vụ** |
| 1 | Giải pháp thu thập thông tin nguy cơ, đe dọa thông minh (Threat Intelligence) | Giải pháp | * Thiết lập, duy trì, cập nhật hệ thống cơ sở dữ liệu các mối đe dọa, điểm yếu trên toàn cầu
* Thu thập, phân tích, đánh giá chủ động các điểm yếu, sự cố xảy ra trong hệ thống
* Hỗ trợ chia sẻ, kết nối với các hệ thống giám sát, quản lý an toàn thông tin tập trung khác
 |
| 2 | Giải pháp giám sát an toàn thông tin tập trung (SOC) | Giải pháp | * Giám sát, quản lý tập trung các sự kiện có nguy cơ mất an toàn thông tin xảy ra trong hệ thống
* Phân tích, cảnh báo tức thời cho các đối tượng liên quan
 |
| 3 | Giải pháp kiểm tra, đánh giá an toàn thông tin mạng | Giải pháp | * Kiểm tra, đánh giá các nguy cơ, điểm yếu mất an toàn thông tin của hệ thống, ứng dụng, phần mềm
 |
| 4 | Giải pháp điều tra và xử lý sự cố | Giải pháp | * Điều tra, tìm vết các sự cố an toàn thông tin
* Xác định nguyên nhân, đối tượng và phương án xử lý
* Quản lý và theo dõi các tiến trình xử lý sự cố
 |
| **VI** | **Sản phẩm trình duyệt** | Phần mềm |  |
| **VII** | **Sản phẩm nền tảng tích hợp, chia sẻ dữ liệu (LGSP)** | Phần mềm | - Nền tảng kết nối liên thông các hệ thống thông tin phục vụ chính phủ điện tử, đô thị thông minh- Hỗ trợ tích hợp, chia sẻ cơ sở dữ liệu dùng chung |
| **VIII** | **Sản phẩm nền tảng điện toán đám mây phục vụ chính phủ điện tử** | Phần mềm | - Hệ thống nền tảng điện toán đám mây phục vụ chính phủ điện tử- Hỗ trợ dạng hạ tầng, nền tảng và dịch vụ |

# IV. Mô hình tham chiếu Trung tâm điều hành an toàn, an ninh mạng

Mô hình SOC bao gồm 03 thành phần cơ bản như hình dưới đây:



*Hình tham chiếu hình 5 trang 07: Mô hình Trung tâm điều hành an toàn,*

*an ninh mạng SOC*

Trong đó:

Công nghệ là các phương án, giải pháp kỹ thuật được sử dụng để bảo đảm việc giám sát an toàn thông tin đáp ứng các yêu cầu về kỹ thuật và tính hiệu quả.

Quy trình là những quy định trong quy chế, chính sách bảo đảm an toàn thông tin của cơ quan, tổ chức được xây dựng để phục vụ việc quản lý, vận hành hệ thống an toàn.

Con người là việc tổ chức nhân sự cán bộ chuyên trách, chuyên gia và các đội ngũ khác (nếu có) để vận hành quản lý hệ thống SOC và các thành phần liên quan.

### 4.1. Công nghệ

Công nghệ, giải pháp kỹ thuật được sử dụng trong SOC cần phải đáp ứng yêu cầu kỹ thuật theo quy định tại Điều 5, khoản 1 Thông tư số 31/2017/TT-BTTTT bao gồm nhưng không giới hạn các chức năng sau:

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 chức năng giám sát hệ thống

Hệ thống SOC cần có khả năng để giám sát các đối tượng giám sát tối thiểu 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:

Giám sát lớp mạng là việc thu thập, quản lý và giám sát các sự kiện từ các thiết bị mạng, thiết bị bảo mật như: Router, Switch, Firewall/IPS/IDS, Sandbox, WAF, Network APT...;

Giám sát lớp máy chủ là việc thu thập, quản lý và giám sát các sự kiện từ các máy chủ hệ thống (cả máy chủ vật lý và ảo hóa) trên các nền tảng khác nhau như: Windows, Linux, Unix…;

Giám sát lớp ứng dụng là việc thu thập, quản lý và giám sát các sự kiện từ các ứng dụng như: (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 ...;

Giám sát lớp thiết bị đầu cuối là việc thu thập, quản lý và giám sát các sự kiện từ các thiết bị như: Máy tính người sử dụng, máy in, máy fax, IP Phone, IP Camera…;

Giám sát trên đường truyền là việc thu thập, quản lý và giám sát các sự kiện từ: 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.

d) 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, bảo vệ, 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.

đ) 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;

- Hỗ trợ và tích hợp các công nghệ Big data & Machine learning, Kill-chain, Advanced malware analysis, AI.

### 4.2. Quy trình

Quy trình trong một hệ thống SOC cơ bản bao gồm 02 nhóm quy trình: quy trình quản lý, vận hành hệ thống và quy trình giám sát bảo vệ các hệ thống cần được bảo vệ như dưới đây.

a) Quy trình quản lý, vận hành bảo đảm an toàn thông tin cho hệ thống SOC

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.

b) Quy trình giám sát, bảo vệ hệ thống thông tin

- Giám sát quản lý các sự kiện và cảnh báo an toàn thông tin: Thực hiện giám sát 24/7 các sự kiện từ các hệ thống cần bảo vệ; Giám sát màn hình cảnh báo; kiểm tra và phân loại cảnh báo; Tạo phiếu yêu cầu, gán yêu cầu xử lý cho bộ phận tương ứng; Theo dõi quá trình xử lý, đóng các ticket xử lý xong.

- Xử lý sự cố an toàn thông tin: Phân tích sơ bộ log, các dấu hiệu tấn công, truy cập trái phép; nhận diện và xác định mức độ của sự cố; Xác định các hành động cần thiết và hướng dẫn (hoặc xử lý trực tiếp) bộ phận chuyên trách của đơn vị chủ quản thực hiện các hành động ứng cứu, ngăn chặn ngay khi có dấu hiệu sự cố; Phân tích sâu, khoanh vùng, điều tra nguyên nhân gốc; xác định phương án và thực hiện khắc phục triệt để sự cố.

- Tối ưu cảnh báo: Tối ưu cảnh báo trên hệ thống giám sát để tăng hiệu quả của việc vận hành, giảm thiểu tối đa cảnh báo sai.

- Điều tra, phân tích các nguy cơ mất an toàn thông tin: Cập nhật, cung cấp thông tin cho đơn vị chủ quản nguy cơ mất an toàn thông tin; Đánh giá ảnh hưởng, đề xuất và hướng các biện pháp để phòng ngừa; Định kỳ thực hiện tìm kiếm chủ động (threat-hunting) phát hiện các nguy cơ mất an toàn thông tin có thể xảy ra với hệ thống của đơn vị chủ quản.

### 4.3. Con người

Đơn vị vận hành hệ thống SOC cần tổ chức và bố trí nhân sự thực hiện quản lý, vận hành hệ thống và giám sát an toàn thông tin, bao gồm các nhóm 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.

- Theo 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.

Trên cơ sở đó, các nhóm nhân sự được tổ chức thành các khâu như sau:

- Phân tích cảnh báo (Tier 1 – Alert Analyst)

Được thực hiện bởi bên vận hành SOC, có trách nhiệm thực hiện hoạt động giám sát 24/7. Chịu trách nhiệm về việc giám sát, phân tích sơ bộ nhằm nhận diện và phân loại các sự kiện được cung cấp từ hệ thống các công cụ và từ các bộ phận, quy trình hoạt động khác. Thực hiện các hành động theo quy trình nhằm ngăn chặn nhanh chóng các sự cố, tránh gây thiệt hại về mặt kinh tế, dữ liệu, hình ảnh,.. của hệ thống cần bảo vệ. Theo dõi quá trình xử lý, kết thúc các yêu cầu (ticket) xử lý xong.

- Tiếp nhận và xử lý sự cố (Tier 2).

Là đơn vị, bộ phận chuyên trách của đơn vị chủ quản có trách nhiệm quản lý, vận hành hệ thống thông tin cần được bảo vệ. Bộ phận này có trách nhiệm xử lý cảnh báo theo hướng dẫn xử lý của Tier 1.

- Ứng cứu, xử lý sự cố (Tier 3 – Incident Responder )

Là bộ phần của đơn vị vận hành SOC thực hiện xử lý các vấn đề ngoài khả năng xử lý của Tier 2 như: Phân tích mã độc chuyên sâu; Phân tích điều tra sâu về nguồn tấn công, phát hiện đề phòng các tấn công; Phân tích xử lý các sự cố mới, phức tạp.

- Tối ưu, chuẩn hóa hệ thống (Content Analysis)

Là bộ phần của đơn vị vận hành SOC thực hiện việc tối ưu cảnh báo để tăng hiệu quả của việc vận hành, giảm thiểu tối đa cảnh sai; Phân tích thông tin sự cố nội bộ và bên ngoài tạo cảnh báo, tối ưu hóa luật.

- Chủ động tìm kiếm nguy cơ mất an toàn thông tin (Threat Hunter)

Là bộ phần của đơn vị vận hành SOC thực hiện việc theo dõi các nguồn tin về lỗ hổng mới; Phân tích để cập nhật chính sách trên tất cả các giải pháp triển khai cho hệ thống được bảo vệ; Phân tích, gỡ bỏ mã độc và định kỳ rà soát và gỡ bỏ các mã độc trong hệ thống.

- Quản lý vận hành SOC (SOC Manager)

Là bộ phần của đơn vị vận hành SOC thực hiện việc quản lý điều hành việc xử lý các cảnh báo, sự cố theo KPI, đảm bảo chất lượng dịch vụ theo thoả thuận ký kết đối với đơn vị chủ quản; Báo cáo, đánh giá các công tác hoạt động của SOC.