##### **Phụ lục 2**

**Dự thảo**

**Tháng 07/2021**

**6/2021**

## **Mô tả nhiệm vụ chuyên trách kỹ thuật về an toàn thông tin**

 *(Ban hành kèm theo Thông tư số /2021/TT-BTTTT*

*ngày tháng năm 2021 của Bộ trưởng Bộ Thông tin và Truyền thông)*

1. **Tiếp nhận và phân loại sự cố ATTT**

a) Tiếp nhận, thu thập thông tin về sự cố mạng có liên quan hoặc do Việt Nam quản lý trên nhiều nguồn khác nhau;

b) Xác định các nguồn gửi thông tin sự cố, bao gồm các nguồn chủ yếu như:

+ Nguồn từ người dùng gửi về qua website;

+ Nguồn từ người dùng gửi về qua hệ thống email;

+ Nguồn từ người dùng gửi về qua điện thoại;

+ Nguồn từ các tổ chức khác trong mạng lưới gửi về;

+ Nguồn từ các tổ chức công bố trên hệ thống của họ.

c) Phân tích sơ bộ sự cố, các mối liên quan và phân loại sự cố theo các tiêu chí và quy định cụ thể;

d) Chuyển giao thông tin sự cố cho các cá nhân, đơn vị có liên quan;

đ) Nghiên cứu, tìm tòi, đào tạo và tự đào tạo, nâng cao kiến thức, kỹ năng liên quan đến công việc và nhiệm vụ được giao.

1. **Ứng cứu sự cố ATTT**
* Phối hợp và cung cấp hỗ trợ kỹ thuật cho các kỹ thuật viên của cơ quan, tổ chức để giải quyết các sự cố ATTT mạng;
* Đối chiếu dữ liệu sự cố để xác định các lỗ hổng cụ thể và đưa ra các khuyến nghị cho phép khắc phục nhanh chóng sự cố ATTT mạng;
* Thực hiện phân tích các tệp nhật ký (log) từ nhiều nguồn khác nhau (ví dụ: nhật ký máy chủ, nhật ký lưu lượng mạng, nhật ký tường lửa [Firewall] và nhật ký hệ thống phát hiện xâm nhập [IDS]) để xác định các nguy cơ, mối đe dọa có thể đối với an toàn, an ninh mạng;
* Thực hiện xử lý sự cố ATTT mạng, bao gồm xác định phạm vi, mức độ khẩn cấp và tác động tiềm năng, xác định lỗ hổng cụ thể và đưa ra các khuyến nghị cho phép khắc phục nhanh chóng sự cố;
* Thực hiện phân tích và báo cáo hướng xử lý sự cố ATTT mạng;
* Thực hiện ứng cứu sự cố ban đầu, thu thập hình ảnh điều tra số và kiểm tra để cô lập, giảm thiểu/khắc phục sự cố có thể xảy ra trên các hệ thống;
* Thực hiện xử lý sự cố ATTT mạng (ví dụ: tập hợp bằng chứng số, đồng bộ thông tin xâm nhập trái phép và theo dõi, phân tích mối đe dọa và trực tiếp khắc phục hệ thống) để hỗ trợ các Đội ứng cứu sự cố triển khai nhiệm vụ;
* Tiếp nhận và phân tích cảnh báo mạng từ nhiều nguồn khác nhau trong tổ chức và xác định nguyên nhân có thể của các cảnh báo đó;
* Theo dõi và ghi lại các sự cố ATTT mạng từ phát hiện ban đầu cho đến khi kết thúc;
* Xây dựng và đề xuất các báo cáo kỹ thuật, hướng dẫn và báo cáo về ATTT mạng thuộc phạm vi được giao;
* Phối hợp với các cán bộ Phân tích nguy cơ/tình báo để đồng bộ dữ liệu đánh giá các mối đe dọa;
* Ghi lại và các hành động đã thực hiện;
* Giám sát các nguồn dữ liệu bên ngoài (ví dụ: các trang web của nhà cung cấp sản phẩm, dịch vụ ATTT mạng, Đội ứng cứu sự cố,...) để duy trì cập nhật các mối nguy cơ ATTT mạng và xác định vấn đề an toàn thông tin, bảo mật có thể ảnh hưởng đến hệ thống của cơ quan, tổ chức;
* Phối hợp thực hiện chức năng ứng phó sự cố ATTT theo quy định.
1. **Kiểm soát và đánh giá điểm yếu (Vulnerability Assessment and Management)**
2. Tìm kiếm, phát hiện, liệt kê các điểm không phù hợp, các điểm yếu, lỗ hổng bảo mật trong hệ thống, như:

+ Hạ tầng mạng: Switch, Router...;

+ Hệ thống và các thiết bị bảo vệ: Firewall, IDS/IPS...;

+ Máy chủ, máy trạm, thiết bị IoT;

+ Ứng dụng: ứng dụng web, ứng dụng thiết bị di động, ứng dụng trên thiết bị IoT...;

+ Điểm yếu về nhận thức của người dùng;

+ Điểm yếu trong các quy trình, quy định về ATTT.

1. Phân tích, đánh giá, đo lường (định lượng, định tính) về mức độ nghiêm trọng của lỗ hổng bảo mật;

c) Đánh giá phân loại tài sản thông tin;

d) Phân tích, đánh giá tác động của mối đe dọa đối với lỗ hổng bảo mật và tài sản thông tin;

đ) Phân tích, đánh giá rủi ro an toàn thông tin và đưa ra các biện pháp giảm xử lý, giảm thiểu rủi ro;

e) Nghiên cứu đánh giá an toàn thông tin đối với các dòng thiết bị mạng (router, switch), thiết bị bảo mật (Firewall, IPS/IDS), các thiết bị phục vụ kiểm tra đánh giá, phân tích mã độc/virus, phòng chống thư rác…của các hãng bảo mật;

g) Đảm bảo tuân thủ quy định của pháp luật, các quy tắc đạo đức nghề nghiệp trong lĩnh vực an toàn thông tin.

1. **Phân tích/giám sát ATTT(Cybersecurity Analysis)**

**4.1.** **Giám sát an toàn mạng**

a) Vận hành, quản trị và các thiết bị quan trắc cơ sở;

b) Giám sát sự kiện ATTT diễn ra trên các thiết bị quan trắc cơ sở;

c) Lọc ra các sự kiện có khả năng gây ra rủi ro mất ATTT cao để cung cấp cho bộ phận phân tích, điều tra xử lý;

d) Thu thập, tổng hợp thông tin về thủ đoạn tấn công, thông tin về sự cố, thông tin về các điểm yếu kỹ thuật v.v... từ các nguồn khác nhau;

e) Phối hợp chặt chẽ với một số cơ quan, đơn vị chức năng trong và ngoài nước để phân tích, tìm nguyên nhân gây sự cố an toàn mạng;

f) Đề xuất hỗ trợ khắc phục sự cố an toàn mạng;

g) Thực hiện công tác báo cáo, thống kê theo chức năng nhiệm vụ được giao;

h) Xử lý kịp thời các sự cố nếu phát hiện sự cố xảy ra. Lưu sổ nhật ký theo dõi;

i) Đảm bảo tuân thủ pháp luật, thực hiện đầy đủ các quy định về đảm bảo bí mật nhà nước, quy tắc đạo đức nghề nghiệp lĩnh vực an toàn thông tin và các quy trình điều phối, ứng cứu, xử lý sự cố;

k) Nghiên cứu, tìm tòi, đào tạo và tự đào tạo, nâng cao kiến thức, kỹ năng liên quan đến công việc và nhiệm vụ được giao;

l) Thực hiện phân tích, điều tra chuyên sâu đối với từng thủ đoạn tấn công có khả năng gây ra rủi ro mất ATTT.

**4.2.** **Điều tra và Phân tích sự kiện/sự cố ATTT phục vụ giám sát ATTT**

a) Giả lập/tái hiện lại các thủ đoạn tấn công để thu thập bằng chứng phục vụ công tác xử lý sự cố;

b) Xác minh và cập nhật tình hình sự cố với đối tượng được giám sát;

c) Đề xuất hỗ trợ khắc phục sự cố an toàn mạng;

d) Thu thập, tổng hợp thông tin về kết quả phân tích, xử lý sự cố;

đ) Phối hợp chặt chẽ với một số cơ quan, đơn vị chức năng trong và ngoài nước để phân tích, tìm nguyên nhân gây sự cố an toàn mạng;

e) Xây dựng báo cáo sự cố an toàn mạng, các điểm yếu kỹ thuật tồn tại trên hệ thống của cơ quan, tổ chức;

g) Xây dựng biện pháp, tài liệu hướng dẫn phòng, chống, ngăn chặn hiệu quả;

h) Đảm bảo tuân thủ pháp luật, thực hiện đầy đủ các quy định về đảm bảo bí mật nhà nước, quy tắc đạo đức nghề nghiệp lĩnh vực an toàn thông tin và các quy trình điều phối, ứng cứu, xử lý sự cố;

i) Thực hiện công tác báo cáo, thống kê theo chức năng nhiệm vụ được giao;

k) Nghiên cứu, tìm tòi, đào tạo và tự đào tạo, nâng cao kiến thức, kỹ năng liên quan đến công việc và nhiệm vụ được giao.

1. **An toàn cơ sở hạ tầng thông tin (Cybersecurity Infrastructure Support)**

a) Đề xuất mô hình triển khai và trang thiết bị dự kiến cần lắp đặt tại điểm giám sát;

b) Cấu hình kết nối thiết bị quan trắc để đổ dữ liệu về hệ thống giám sát ATM Trung tâm;

c) Vận hành, quản trị và giám sát các thiết bị quan trắc và hoạt động của hệ thống cảnh báo, giám sát;

d) Nghiên cứu, xây dựng và cập nhật các luật giám sát phù hợp với đối tượng được giám sát;

đ) Thực hiện phân tích, điều tra đối với các thủ đoạn tấn công có khả năng gây ra rủi ro mất ATTT;

e) Thu thập thông tin về các nguy cơ, sự cố mất ATTT mạng liên quan đến đối tượng cần giám sát từ các nguồn khác nhau;

f) Thu thập, tổng hợp thông tin về kết quả phân tích, xử lý sự cố;

g) Nghiên cứu các loại mã độc, lỗ hổng bảo mật và xu hướng tấn công mới;

h) Cập nhật phiên bản, bản vá định kỳ cho hệ thống giám sát trung tâm và các thiết bị quan trắc cơ sở;

i) Lập kế hoạch bảo trì, bảo dưỡng định kỳ, cập nhật license cho các thiết bị thuộc hệ thống giám sát ATTT;

k) Thực hiện công tác thống kê, báo cáo về các loại lỗ hổng bảo mật, các nguy cơ, các sự kiện và sự cố mất an toàn thông tin.

1. **Phân tích nguy cơ/tình báo ATTT (Threat Analysis)**

a) Bảo mật thông tin bằng các thuật toán mã hóa và giải mã, các kỹ thuật bảo mật không sử dụng các thuật toán mã hóa;

b) Nghiên cứu các thuật toán mã hóa, các phương thức bảo vệ dữ liệu chống lộ lọt;

c) Nghiên cứu các giải pháp mật mã và bảo vệ dữ liệu áp dụng trong cơ quan, tổ chức;

d) Nghiên cứu mô hình triển khai PKI và các mô hình khác;

đ) Khảo sát phân tích nhu cầu, khả năng áp dụng mật mã và các biện pháp bảo mật dữ liệu;

e) Tư vấn triển khai các giải pháp bảo mật dữ liệu;

f) Đề xuất mô hình triển khai và trang thiết bị dự kiến cần lắp đặt;

g) Cài đặt, vận hành và tối ưu hệ thống theo mô hình dự kiến;

h) Vận hành, bảo trì hệ thống bảo mật dữ liệu;

i) Đảm bảo tuân thủ các quy định của pháp luật và các quy định về đảm bảo bí mật nhà nước, quy tắc đạo đức nghề nghiệp lĩnh vực an toàn thông tin;

k) Thực hiện công tác báo cáo, thống kê theo chức năng nhiệm vụ được giao.

1. **Tư vấn ATTT (Cybersecurity Advisor)**

a) Nghiên cứu các giải pháp/sản phẩm bảo mật (giải pháp thương mại và giải pháp nguồn mở);

b) Nghiên cứu kiến trúc, mô hình, giải pháp bảo mật bao gồm các giải pháp tổng thể và giải pháp cho nhóm dịch vụ cụ thể;

c) Tư vấn giải pháp bảo mật, bảo đảm an toàn thông tin cho các cơ quan, doanh nghiệp;

d) Lập kế hoạch khảo sát và khảo sát hệ thống mạng, bảo mật của các cơ quan, đơn vị theo yêu cầu;

e) Lập báo cáo khảo sát, đề xuất kiến nghị các biện pháp, giải pháp đảm bảo an toàn thông tin cho các cơ quan, đơn vị theo yêu cầu;

f) Nghiên cứu, tìm hiểu văn bản QPPL, quy định, tiêu chuẩn kỹ thuật về đảm bảo an toàn thông tin;

g) Xây dựng và triển khai các chính sách, quy trình sử dụng và vận hành, hệ thống mạng;

h) Nghiên cứu, tìm tòi, đào tạo và tự đào tạo, nâng cao kiến thức, kỹ năng liên quan đến công việc và nhiệm vụ được giao.

1. **Đào tạo, huấn luyện an toàn thông tin (Cybersecurity Trainer)**

**8.1. Đào tạo, huấn luyện, bồi dưỡng kỹ năng về an toàn thông tin cho đội ngũ kỹ thuật**

a) Xây dựng đề cương chương trình đào tạo, huấn luyện, bồi dưỡng kỹ năng về an toàn thông tin từ cơ bản, nâng cao đến chuyên sâu cho đội ngũ kỹ thuật;

b) Xây dựng các bài lab thực hành các kỹ năng về an toàn thông tin cho đội ngũ kỹ thuật;

c) Thực hiện đào tạo, huấn luyện, bồi dưỡng các kiến thức và kỹ năng từ cơ bản, nâng cao đến chuyên sâu cho đội ngũ kỹ thuật;

d) Nghiên cứu, tìm tòi, đào tạo và tự đào tạo, nâng cao kiến thức, kỹ năng liên quan đến công việc và nhiệm vụ được giao.

**8.2.** **Đào tạo, huấn luyện, bồi dưỡng kiến thức về an toàn thông tin cho người dùng, cán bộ lãnh đạo, quản lý**

a) Xây dựng đề cương chương trình đào tạo, huấn luyện, bồi dưỡng kỹ năng về an toàn thông tin cho người dùng, cán bộ lãnh đạo, quản lý;

b) Xây dựng các bài thực hành các kỹ năng đảm bảo an toàn thông tin cho người dùng máy tính, cho cán bộ lãnh đạo quản lý;

c) Thực hiện đào tạo, huấn luyện, bồi dưỡng các kiến thức và kỹ năng cho người dùng, cán bộ lãnh đạo quản lý;

d) Nghiên cứu, tìm tòi, đào tạo và tự đào tạo, nâng cao kiến thức, kỹ năng liên quan đến công việc và nhiệm vụ được giao.

1. **Điều tra số (Digital Forensics)**

Phân tích bằng chứng số và điều tra sự cố ATTT để đưa ra các thông tin hữu ích nhằm hỗ trợ giảm thiểu lỗ hổng, điểm yếu của hệ thống thông tin/mạng, cụ thể:

* Tiến hành phân tích các tệp nhật ký, bằng chứng và thông tin khác để xác định các phương pháp tốt nhất để xác định (các) thủ phạm xâm nhập mạng;
* Xác nhận những gì đã biết về một vụ xâm nhập và khám phá thông tin mới, nếu có thể, sau khi xác định xâm nhập thông qua phân tích động;
* Tạo một bản sao số của bằng chứng (hình ảnh bằng chứng số) để đảm bảo bằng chứng ban đầu không bị vô tình sửa đổi, để sử dụng cho quá trình phân tích và khôi phục dữ liệu. Điều này bao gồm, nhưng không giới hạn ở các ổ đĩa cứng, đĩa mềm, CD, PDA, điện thoại di động, GPS và tất cả các định dạng băng;
* Giải mã dữ liệu thu thập được bằng các phương tiện kỹ thuật;
* Cung cấp tóm tắt kỹ thuật các kết quả phát hiện được tương ứng với quy trình báo cáo;
* Kiểm tra dữ liệu phục hồi để biết thông tin liên quan đến vấn đề đang có;
* Xác định bằng chứng số để kiểm tra và phân tích theo cách để tránh sự thay đổi không chủ ý;
* Thực hiện phân tích động để khởi động hình ảnh của một ổ đĩa (mà không nhất thiết phải có ổ đĩa gốc) để xem sự xâm nhập như người dùng có thể đã nhìn thấy, trong một môi trường tự nhiên;
* Thực hiện phân tích chữ ký tập tin;
* Thực hiện so sánh băm với cơ sở dữ liệu được thiết lập;
* Thực hiện phân tích điều tra số theo thời gian thực (ví dụ: sử dụng Helix kết hợp với LiveView;
* Thực hiện phân tích dòng thời gian;

-Thực hiện xử lý sự cố ATTT mạng (ví dụ: tập hợp bằng chứng số, đối chiếu thông tin xâm nhập trái phép và theo dõi, phân tích mối đe dọa và trực tiếp khắc phục hệ thống) để hỗ trợ các Đội ứng cứu sự cố triển khai nhiệm vụ;

* Thực hiện phân tích phương tiện tĩnh;
* Thực hiện phân tích phần mềm độc hại cấp 1, 2 và 3;
* Chuẩn bị phương tiện kỹ thuật số để sao chụp ảnh đảm bảo tính toàn vẹn dữ liệu (ví dụ: sử dụng công cụ chống ghi theo quy trình chuẩn);
* Cung cấp hỗ trợ kỹ thuật về các vấn đề bằng chứng kỹ số cho nhân viên thích hợp;
* Nhận biết và báo cáo chính xác các bằng chứng số tương ứng của một hệ điều hành cụ thể;
* Trích xuất dữ liệu bằng các kỹ thuật khắc dữ liệu (ví dụ: Bộ công cụ điều tra số [FTK], ...);
* Nắm bắt và phân tích lưu lượng mạng liên quan đến các hoạt động độc hại bằng cách sử dụng công cụ giám sát mạng;
* Sử dụng các thiết bị và kỹ thuật chuyên dụng để lập danh mục, tài liệu, trích xuất, thu thập, đóng gói và lưu giữ bằng chứng số;
* Tiến hành phân tích nhị phân chữ thảo;
* Thực hiện quét virus trên phương tiện kỹ thuật số;
* Thực hiện phân tích điều tra số hệ thống;
* Thực hiện phân tích tĩnh để gắn "hình ảnh" của ổ đĩa (không nhất thiết phải có ổ đĩa gốc);
* Thực hiện phân tích phần mềm độc hại tĩnh;
* Sử dụng bộ công cụ điều tra số có thể triển khai để hỗ trợ các hoạt động khi cần thiết;
* Phối hợp với các nhà phân tích tình báo để đồng bộ dữ liệu, đánh giá các nguy cơ, mối đe dọa;
* Xử lý hình ảnh với các công cụ thích hợp tùy thuộc vào mục tiêu của nhà phân tích;
* Thực hiện phân tích sổ đăng ký Windows (Windows Registry);
* Thực hiện giám sát tệp và đăng ký trên hệ thống đang chạy sau khi xác định xâm nhập thông qua phân tích động;
* Nhập thông tin phương tiện vào cơ sở dữ liệu theo dõi (ví dụ: Công cụ theo dõi sản phẩm) cho phương tiện kỹ thuật số đã được mua;
* Đồng bộ dữ liệu sự cố và thực hiện báo cáo phòng thủ không gian mạng;
* Duy trì bộ công cụ ATTT mạng có thể triển khai (ví dụ: phần mềm / phần cứng ứng phó sự cố ATTT chuyên dụng) để hỗ trợ nhiệm vụ của Đội ứng cứu sự cố;
* Thu thập và phân tích dấu vết xâm nhập (ví dụ: mã nguồn, phần mềm độc hại và cấu hình hệ thống) và sử dụng dữ liệu được phát hiện để cho phép giảm thiểu các sự cố ATTT mạng tiềm ẩn;
* Xây dựng và đưa ra các khuyến nghị, báo cáo về ATTT mạng thuộc trách nhiệm được giao.
1. **Quản trị, tổng hợp an toàn thông tin (Cybersecurity administrator)**

a) Chủ trì và chịu trách nhiệm chung về hoạt động quản trị, tổng hợp an toàn thông tin, công tác điều phối, ứng cứu, xử lý sự cố; duy trì hệ thống bảo mật và ngăn chặn phá hoại, ăn cắp dữ liệu của hệ thống thông tin của tổ chức chủ quản thuộc phạm vi được phân công;

b) Đảm bảo an toàn, bảo mật cho hệ thống thông tin và triển khai các biện pháp phòng, chống tấn công của các tin tặc;

c) Phối hợp chặt chẽ với các thành viên khác trong Đội trong thực hiện nhiệm vụ; trực tiếp giám sát toàn bộ hoạt động của Đội về kỹ thuật và nhân sự, kịp thời phát hiện, tổng hợp, báo cáo sự không phù hợp và đề xuất phương hướng xử lý thuộc phạm vi được phân công;

d) Hỗ trợ Lãnh đạo Đội trong công tác quản lý và điều hành việc tổ chức, hoạt động Đội Ứng cứu sự cố và duy trì công việc đảm bảo an toàn thông tin trong toàn bộ tổ chức thuộc Chủ quản Đội và/hoặc các đối tượng có liên quan hoặc nếu đứng độc lập,..../.