BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập - Tự do - Hạnh phúc
Số: /2018/TT-BTTTT	*Hà Nội, ngày tháng năm 2018*

Dự thảo
V 0.5-2018

THÔNG TƯ

Quy định về tổ chức, hoạt động của đội ứng cứu sự cố và các chức danh công việc ứng cứu sự cố an toàn thông tin mạng

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ 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;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Quyết định số 1622/QĐ-TTg ngày 25 tháng 10 năm 2017 của Thủ tướng Chính phủ Phê duyệt Đề án đẩy mạnh hoạt động của mạng lưới ứng cứu sự cố, tăng cường năng lực cho các cán bộ, bộ phận chuyên trách ứng cứu sự cố an toàn thông tin mạng trên toàn quốc đến 2020, định hướng đến 2025;

Theo đề nghị của Giám đốc Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam,

Bộ trưởng Bộ Thông tin và Truyền thông ban hành Thông tư quy định tổ chức, vận hành các đội ứng cứu sự cố an toàn thông tin mạng:

Chương I
NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi và đối tượng áp dụng

Thông tư này quy định về tổ chức và hoạt động các đội ứng cứu sự cố an toàn thông tin mạng; năng lực và kỹ năng các cán bộ chuyên trách ứng cứu sự cố và trách nhiệm của các tổ chức, cá nhân có liên quan tới hoạt động ứng cứu sự cố an toàn thông tin mạng.

Điều 2. Giải thích thuật ngữ

Trong văn bản này, các thuật ngữ dưới dây được hiểu như sau:

1. Sự cố an toàn thông tin mạng là việc thông tin, hệ thống thông tin bị tấn công hoặc gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng (sau đây gọi tắt là Sự cố).

2. Sự kiện bảo mật là một sự kiện có khả năng liên quan đến an toàn thông tin mạng, nhưng chưa được xác định chính xác là một sự cố an toàn thông tin

mạng.

3. Sự cố nghiêm trọng là sự cố đáp ứng các tiêu chí quy định tại Điều 9 Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia (sau đây gọi tắt là Quyết định số 05/2017/QĐ-TTg).

4. Ứng cứu sự cố an toàn thông tin mạng là hoạt động nhằm xử lý, khắc phục sự cố gây mất an toàn thông tin mạng gồm: theo dõi, thu thập, phân tích, phát hiện, cảnh báo, điều tra, xác minh sự cố, ngăn chặn sự cố, khôi phục dữ liệu và khôi phục hoạt động bình thường của hệ thống thông tin.

5. Ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia là hoạt động ứng cứu sự cố trong tình huống xảy ra sự cố nghiêm trọng, tình huống thảm họa, hoặc theo yêu cầu của cơ quan nhà nước có thẩm quyền nhằm bảo đảm an toàn thông tin mạng quốc gia.

6. Đầu mối ứng cứu sự cố là bộ phận hoặc cá nhân được thành viên mạng lưới cử để thay mặt cho thành viên mạng lưới liên lạc và trao đổi thông tin với Cơ quan điều phối quốc gia hoặc các thành viên mạng lưới khác trong hoạt động điều phối, ứng cứu sự cố.

7. Đội ứng cứu sự cố bảo mật máy tính là một tổ chức có tên gọi thống nhất trên thế giới là Computer Security Incident Response Team (hay còn gọi tắt là CSIRT), thực hiện việc phân tích và ứng cứu đối với các sự cố an toàn thông tin mạng, tiến hành các hoạt động khác để ngăn ngừa sự cố và tăng cường chất lượng chất lượng đảm bảo an toàn thông tin mạng (sau đây gọi tắt là Đội ứng cứu sự cố hay Đội ƯCSC hay Đội).

8. *Tổ chức chủ quản* là tổ chức quản lý trực tiếp Đội ƯCSC. Tổ chức chủ quản có thể là các Bộ hoặc cơ quan ngang Bộ, Uỷ ban nhân dân cấp tỉnh hoặc thành phố trực thuộc trung ương, các nhà cung cấp dịch vụ viễn thông, Internet, các cơ quan, tổ chức, doanh nghiệp thuộc dạng đơn vị có nghĩa vụ phải tham gia mạng lưới ứng cứu sự cố quốc gia, các tổ chức hoặc các doanh nghiệp.

9. *Đối tượng phục vụ* là các bộ phận, cá nhân thuộc tổ chức chủ quản hoặc bên tổ chức bên ngoài, được Đội ƯCSC cung cấp các dịch vụ đảm bảo an toàn thông tin và xử lý sự cố của Đội.

10. *Phương tiện nhân tạo* (artifact) có thể là các tập tin hoặc đối tượng được tìm thấy trên một hệ thống có thể liên quan đến việc thăm dò hoặc tấn công hệ thống và mạng, đang được sử dụng để vượt qua các biện pháp bảo mật. Các phương tiện nhân tạo có thể là vi-rút máy tính, các chương trình trojan, sâu, các kịch bản và các công cụ khai thác.

Chương II

TỔ CHỨC, HOẠT ĐỘNG CÁC ĐỘI ỨNG CỨU SỰ CỐ AN TOÀN THÔNG TIN MẠNG

Điều 3. Chức năng, nhiệm vụ của Đội Ứng cứu sự cố

Đội ứng cứu sự cố an toàn thông tin mạng là một tổ chức không chỉ tiến hành việc phân tích và ứng cứu đối với các Sự cố đang xảy ra thực tế, mà còn tiến hành các hoạt động ngăn ngừa phát sinh hoặc tái diễn sự cố và các hoạt động tăng cường hoạt động đảm bảo an toàn thông tin mạng nhằm ngăn ngừa, khắc phục Sự cố hiệu quả, giảm thiểu những rủi ro về tính bảo mật, tính nguyên vẹn và tính sẵn sàng do Sự cố gây ra cho hệ thống thông tin.

4.1 Chức năng

- Tổ chức các hoạt động đảm bảo an toàn thông tin, giám sát và cảnh báo kịp thời cho các hệ thống thông tin của tổ chức chủ quản;

- Thực hiện các hoạt động ứng cứu, xử lý các Sự cố mất an toàn thông tin trong lĩnh vực, địa bàn, phạm vi quản lý, hoạt động của tổ chức chủ quản;

- Đầu mối tiếp nhận, phối hợp, ứng cứu, báo cáo sự cố an toàn thông tin của tổ chức chủ quản;

- Tham gia hoạt động ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia khi có yêu cầu từ Bộ Thông tin và Truyền thông hoặc Cơ quan điều phối quốc gia.

4.2 Nhiệm vụ

- Đảm bảo an toàn và giám sát an toàn cho hạ tầng công nghệ thông tin và truyền thông, hệ thống cơ sở dữ liệu quan trọng, các ứng dụng và dịch vụ trên nền tảng công nghệ thông tin của tổ chức chủ quản và các đơn vị trực thuộc;

- Kết nối với các tổ chức, các nguồn thông tin từ Intenet, các đối tác, các nhà cung cấp sản phẩm, giải pháp và dịch vụ về an toàn thông tin để thu thập thông tin về tình hình, các sự kiện, sự cố an toàn, các phương pháp và công cụ mới, các nguy cơ, các cảnh báo sớm để cập nhật và cảnh báo kỹ thuật trong phạm vi của tổ chức chủ quản và cơ quan điều phối quốc gia đối với các thông tin có khả năng gây mất an toàn cho nhiều cơ quan, tổ chức khác;

- Tổ chức đội ngũ chuyên môn kỹ thuật để cung cấp các dịch vụ đảm bảo an toàn thông tin, các dịch vụ tăng cường chất lượng hoạt động đảm bảo an toàn và các dịch vụ ứng cứu xử lý sự cố trực tiếp hoặc từ xa cho tổ chức chủ quản;

- Là đầu mối của tổ chức chủ quản để tham gia vào mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia theo hình thức thành viên có nghĩa vụ được quy định tại Quyết định 05/2017/QĐ-TTg hoặc theo hình thức thành viên tự nguyện, thực hiện các quy định về tiếp nhận, thông báo, báo cáo sự cố, và nhận triển khai yêu cầu điều phối của cơ quan điều phối quốc gia – Trung tâm Ứng cứu Khẩn cấp Máy tínhViệt Nam;

- Là đầu mối của tổ chức chủ quản phối hợp với các cơ quan chức năng và/hoặc các đơn vị khác bên ngoài trong công tác ứng cứu sự cố máy tính và an toàn thông tin mạng khi có yêu cầu;

- Tổ chức thực hiện các hoạt động diễn tập ứng cứu sự cố và phòng chống tấn công mạng; các hoạt động nâng cao nhận thức an toàn thông tin cho người dùng và cộng đồng, các tập huấn, đào tạo về kỹ năng và kiến thức cho các đối tượng công nghệ thông tin, an toàn thông tin trong phạm vi của cơ quan chủ quản;

- Thực hiện hoạt động đánh giá, kiểm thử an toàn các hệ thống thông tin thuộc cơ quan chủ quản theo định kỳ hoặc theo các yêu cầu đột xuất;

- Hợp tác với các Đội ƯCSC khác để nâng cao năng lực chuyên môn, kỹ năng cho các thành viên trong các hoạt động đảm bảo an toàn, xử lý sự cố lẫn nhau;

- Tổ chức các hoạt động nghiên cứu, phân tích các nguy cơ và công nghệ trong lĩnh vực đảm bảo an toàn thông tin;

- Cung cấp dịch vụ đảm bảo an toàn thông tin, ứng cứu sự cố cho các tổ chức, doanh nghiệp khác theo yêu cầu phù hợp với các quy định về pháp luật.

Điều 4. Mô hình tổ chức và các vị trí chuyên trách của Đội ứng cứu sự cố

1. Mô hình tổ chức

Tuỳ theo điều kiện thực tế về lĩnh vực hoạt động, quy mô và phạm vi hoạt động, yêu cầu đảm bảo an toàn, nhân lực chuyên môn về an toàn thông tin của tổ chức chủ quản mà Đội ứng cứu sự cố có thể áp dụng các mô hình tổ chức khác nhau:

1.1 Đối với tổ chức chủ quản là các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ, cơ quan Trung ương: Đội ƯCSC do đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng của tổ chức chủ quản trình thành lập và chịu trách nhiệm tổ chức hoạt động ứng cứu sự cố trong lĩnh vực, phạm vi mình quản lý. Trong đó:

- Đội trưởng Đội ƯCSC là lãnh đạo phụ trách về ứng cứu sự cố của đơn vị chuyên trách ứng cứu sự cố của Bộ, ngành;

- Thành viên gồm các thành viên chuyên trách theo quy định của mục 2 điều này và các thành viên kiêm nhiệm là các cán bộ kỹ thuật về an toàn thông tin, ứng cứu sự cố của các cơ quan, đơn vị đang tham gia vận hành các hệ thống thông tin quan trọng của tổ chức chủ quản; và cá nhân là đầu mối ứng cứu sự cố của tổ chức chủ quản.

1.2 Đối với tổ chức chủ quản là Uỷ ban nhân dân các tỉnh, thành phố trực thuộc trung ương: đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng là Sở thông tin và truyền thông cấp tỉnh, thành phố trình chủ tịch uỷ ban nhân dân cấp tỉnh, thành phố thành lập Đội ƯCSC và chịu trách nhiệm tổ chức hoạt động ứng cứu sự cố trên địa bàn, phạm vi của tỉnh, thành phố. Trong đó:

- Đội trưởng Đội ƯCSC là lãnh đạo phụ trách về ứng cứu sự cố của Sở thông tin và truyền thông cấp tỉnh, thành phố trực thuộc trung ương;

- Thành viên gồm các thành viên chuyên trách theo quy định của mục 2 điều này và các thành viên kiêm nhiệm gồm các cán bộ kỹ thuật về an toàn thông tin, ứng cứu sự cố của các cơ quan, đơn vị đang tham gia vận hành các hệ thống thông tin quan trọng của tỉnh, thành phố; và cá nhân là đầu mối ứng cứu sự cố của tổ chức chủ quản.

1.3 Đối với tổ chức chủ quản là các doanh nghiệp cung cấp dịch vụ hạ tầng viễn thông, Internet; các tổ chức, doanh nghiệp cung cấp dịch vụ trung tâm dữ liệu, cho thuê không gian lưu trữ thông tin số; đơn vị quản lý, vận hành cơ sở dữ liệu quốc gia; đơn vị chuyên trách về an toàn thông tin, công nghệ thông tin của các tổ chức ngân hàng, tài chính, kho bạc, thuế, hải quan; các tổ chức, doanh nghiệp quản lý, vận hành các hệ thống thông tin quan trọng, các hệ thống điều khiển công nghiệp (SCADA) thuộc các lĩnh vực năng lượng, công nghiệp, y tế, tài nguyên và môi trường, giáo dục và đào tạo, dân cư và đô thị: tuỳ theo quy mô, địa bàn và điều kiện thực tế mà có thể thành lập Đội ƯCSC riêng của tổ chức, hoạt động như một đơn vị hoặc bộ phận độc lập trong tổ chức. Trong đó:

- Đội trưởng Đội ƯCSC là lãnh đạo phụ trách về an toàn thông tin hoặc ứng cứu sự cố của tổ chức chủ quản;

- Thành viên gồm các thành viên chuyên trách theo quy định của mục 2 điều này và các thành viên kiêm nhiệm gồm các cán bộ kỹ thuật về an toàn thông tin, ứng cứu sự cố của các cơ quan, đơn vị đang tham gia vận hành các hệ thống thông tin quan trọng của tổ chức chủ quản; và cá nhân là đầu mối ứng cứu sự cố của tổ chức chủ quản.

1.4 Đối với tổ chức chủ quản là các tổ chức, doanh nghiệp không thuộc danh sách các đơn vị có nghĩa vụ phải tham gia mạng lưới ứng cứu sự cố quốc gia: tuỳ theo điều kiện và khả năng thực tế mà có thể thành lập Đội ƯCSC của tổ chức, doanh nghiệp như là một bộ phận hoặc đơn vị độc lập thuộc tổ chức chủ quản. Trong đó:

- Đội trưởng Đội ƯCSC là lãnh đạo phụ trách về an toàn thông tin hoặc ứng cứu sự cố của tổ chức chủ quản;

- Thành viên gồm các thành viên chuyên trách theo quy định của mục 2 điều này và các thành viên kiêm nhiệm gồm các cán bộ kỹ thuật về an toàn thông tin, ứng cứu sự cố của các cơ quan, đơn vị trực thuộc tổ chức.

2. Các vị trí chuyên trách

Để đảm bảo hoạt động ứng cứu sự cố, ngăn ngừa và tăng cường chất lượng hoạt động đảm bảo an toàn thông tin của Đội ƯCSC có hiệu quả, các thành viên của Đội có thể là các cán bộ - chuyên viên kỹ thuật về an toàn làm việc trong các bộ phận, đơn vị thuộc tổ chức chủ quản làm việc theo mô hình kiêm nhiệm, bán thời gian. Tuy nhiên, Đội ƯCSC phải có các vị trí chuyên trách - làm việc toàn thời gian cho Đội như sau:

2.1 Lãnh đạo đội ứng cứu sự cố: trong trường hợp Đội trưởng Đội ƯCSC được chỉ định kiêm nhiệm, Đội ƯCSC phải có một Đội phó hoặc chức danh tương đương làm việc chuyên trách toàn thời gian, chịu trách nhiệm tổ chức, vận hành và duy trì hoạt động của Đội ƯCSC.

2.2 Chuyên viên bảo mật

2.3 Chuyên viên xử lý Sự cố

2.4 Chuyên viên phân tích Sự cố

2.5 Chuyên viên tiếp nhận và quản lý sự kiện, sự cố an toàn thông tin

Mô tả công việc và các yêu cầu về kỹ năng của các vị trí trên được quy định trong các mục 1 đến 10 điều 10 chương III và Phụ lục 02 của thông tư này.

Các nhân sự chuyên trách cần phải đáp ứng các yêu cầu tại các điều 4, 5, 6 mục 1 - chức danh an toàn thông tin thông tư 45/2017/TT-BTTTT ngày 29/12/2018 quy định tiêu chuẩn chức danh nghề nghiệp viên chức chuyên ngành công nghệ thông tin. Ngoài ra, các vị trí chuyên trách này cần phải được huấn luyện các kỹ năng kỹ thuật thuộc nhóm các kỹ năng xử lý sự cố được nêu tại điều 8 và phụ lục 02 của thông tư này.

Điều 5. Các hoạt động chính của Đội ứng cứu sự cố

Các hoạt động của Đội ƯCSC có thể phân theo 3 nhóm sau:

1. Các hoạt động phản ứng sự cố

Các hoạt động này phát sinh tuỳ theo Sự kiện hoặc yêu cầu như báo cáo bị xâm nhập, lây nhiễm mã độc, lỗ hổng của ứng dụng, hoặc các thông tin từ hệ thống phát hiện xâm nhập hoặc nhật ký log của hệ thống, ... Đây là các hoạt động quan trọng của bất kỳ Đội ƯCSC nào. Tuỳ theo điều kiện và nguồn nhân lực hiện có mà Đội ƯCSC phải đáp ứng một phần hoặc tất cả các công việc bên dưới, gồm:

- Cảnh báo Sự cố: phổ biến thông tin mô tả về các tấn công, lỗ hổng bảo mật, cảnh báo xâm nhập, mã độc, các chiêu trò lừa đảo và các khuyến nghị giải quyết. Cảnh báo là phản ứng đối với vấn đề hiện tại để thông báo cho đối tượng

phục vụ thuộc tổ chức chủ quản hoặc tổ chức bên ngoài hướng dẫn bảo vệ hoặc khôi phục hệ thống đã bị ảnh hưởng. Thông tin này có thể do Đội ƯCSC tạo ra hoặc có thể được phân phối lại từ các nhà cung cấp, các Đội ƯCSC khác hoặc từ các chuyên gia bảo mật, từ các bộ phận khác.

- Xử lý Sự cố tại chỗ hoặc hỗ trợ xử lý từ xa: thực hiện gỡ bỏ - ngăn chặn các nguy cơ và tấn công vào hệ thống bị Sự cố, khôi phục hệ thống, đánh giá các tác động gây ra do sự cố, lập báo cáo xử lý – khắc phục. Trường hợp ở xa, Đội ƯCSC có thể cử thành viên đến nơi sự cố để xử lý hoặc hỗ trợ, hướng dẫn cho nơi bị sự cố phục hồi qua điện thoại, email hoặc tài liệu hướng dẫn để những người tại chỗ có thể thực hiện việc phục hồi Sự cố.

- Phân tích Sự cố: là đánh giá các thông tin và bằng chứng hỗ trợ có sẵn hoặc các hiện vật liên quan đến sự cố, sự kiện. Mục đích của phân tích là để xác định phạm vi của vụ việc, mức độ thiệt hại gây ra do sự số, tính chất vụ việc và cách giải quyết. Đội ƯCSC có thể dùng kết quả phân tích lỗ hổng và các công cụ sử dụng để hiểu và cung cấp các phân tích đầy đủ về những gì đã xảy ra trên một hệ thống cụ thể. Hai hoạt động sau có thể thực hiện thêm như là một phần của phân tích sự cố, tuỳ theo nhiệm vụ, mục tiêu, và quy trình của Đội:

+ Thu thập bằng chứng điều tra số: thu thập, bảo quản, phân tích bằng chứng từ hệ thống bị xâm nhập để xác định các thay đổi

+ Theo dõi hoặc truy tìm: truy tìm nguồn gốc của kẻ xâm nhập hoặc xác định các hệ thống mà kẻ xâm nhập đã truy cập. Việc này cũng có thể liên quan đến xác định danh tính của kẻ xâm nhập, có thể tự thực hiện bởi các thành viên Đội ƯCSC hoặc hợp tác với cơ quan pháp luật, nhà cung cấp dịch vụ Internet hoặc các tổ chức có liên quan.

- Điều phối phản ứng Sự cố: Đội ƯCSC điều phối các hành động phản ứng các bên có liên quan đến sự cố như nạn nhân của tấn công, các địa điểm khác có liên quan đến tấn công, và các địa điểm yêu cầu hỗ trợ phân tích tấn công. Điều phối cũng có thể liên quan đến các bên cung cấp hỗ trợ cho nạn nhân như các nhà cung cấp dịch vụ Internet, các đội ƯCSC khác; và các quản trị mạng, quản trị hệ thống của điểm bị sự cố. Điều phối cũng có thể liên quan đến thông báo và hợp tác với cơ quan điều phối quốc gia, các cơ quan thực thi pháp luật.

- Xử lý các lỗ hổng: theo dõi và cập nhật các lỗ hổng mới liên quan đến hệ thống thông tin đang vận hành, phân tích lỗ hổng, thử nghiệm đánh giá các bản vá lỗi trước khi cập nhật chính thức lên hệ thống, sao lưu trước khi cập nhật, tổ chức cập nhật các bản vá lỗi đảm bảo an toàn

- Phân tích, xử lý các phương tiện nhân tạo: khắc phục sự cố, gỡ bỏ các phương tiện nhân tạo, phân tích để phát hiện hành vi và phương pháp hoạt động, lây nhiễm. Công việc này có thể thuê một bên thứ ba độc lập để thực hiện.

2. Các hoạt động ngăn ngừa sự cố

Các hoạt động này cung cấp các hỗ trợ và thông tin giúp cho việc chuẩn bị, bảo vệ, và bảo mật các hệ thống công nghệ thông tin chống lại các tấn công, các vấn đề hoặc các Sự kiện bảo mật, giúp giảm các Sự cố trong tương lai. Đây là các hoạt động cần được thực hiện trước các hoạt động khắc phục sự cố. Đội ƯCSC có thể thực hiện một phần hoặc tất cả các hoạt động được liệt kê bên dưới:

- Cấu hình và duy trì các công cụ, ứng dụng và hạ tầng bảo mật: cung cấp các hướng dẫn về cách thức cấu hình an toàn và duy trì các công cụ, các ứng dụng và hạ tầng công nghệ thông tin. Ngoài ra, Đội ƯCSC có thể thực hiện cấu hình cập nhật và duy trì các công cụ và dịch vụ bảo mật, các hệ thống máy chủ, các máy tính để bàn hoặc xách tay, các thiết bị cá nhân, ... đảm bảo an toàn

- Giám sát để phát hiện Sự cố, sự kiện bảo mật: tổ chức các hoạt động theo dõi, giám sát trên hệ thống bảo vệ an toàn hiện có, trang bị thêm các công cụ nhằm phát hiện sớm những nguy cơ xâm nhập, tấn công mạng. Ở những nơi có yêu cầu đảm bảo hệ thống thông tin phải hoạt động liên tục 24x7 cần phải xem xét việc tổ chức phương án giám sát tương ứng, bao gồm giám sát hoạt động và giám sát bảo mật.

- Triển khai các biện pháp, giải pháp phát hiện xâm nhập: dựa trên nhật ký của các thiết bị phát hiện xâm nhập IDS, thực hiện phân tích và cảnh báo với các sự kiện chạm đến ngưỡng quy định, chuyển tiếp cảnh báo đến cá nhân hoặc tổ chức có trách nhiệm để có các phản ứng phù hợp và kịp thời. Ở những nơi có khối lượng nhật ký log lớn, cần phải có các công cụ chuyên biệt để tổng hợp và biên dịch các thông tin.

- Đánh giá, kiểm tra an toàn của hệ thống công nghệ thông tin theo định kỳ hoặc theo yêu cầu: xem xét và phân tích tính an toàn hạ tầng công nghệ thông tin dựa theo các tiêu chuẩn hoặc các định nghĩa an toàn; xem xét việc thực hiện đảm bảo an toàn của tổ chức. Công việc này có thể tự thực hiện hoặc thuê một bên thứ ba độc lập thực hiện.

- Phát triển các công cụ bảo mật: thực hiện theo yêu cầu của đối tượng phục vụ hoặc tự phát triển của Đội ƯCSC, có thể là bản vá lỗi bảo mật cho các phần mềm dùng riêng, các công cụ hoặc kịch bản phát triển để mở rộng chức năng của các công cụ bảo mật hiện tại hoặc cơ chế ngăn chặn khai thác khi lỗ hổng mới công bố chưa phát hành bản vá lỗi.

3. Các hoạt động tăng cường đảm bảo an toàn

Các hoạt động bổ sung này độc lập với các hoạt động phản ứng với Sự cố và thường được các bộ phận khác như công nghệ thông tin, đảm bảo chất lượng, đào tạo thực hiện. Tuy nhiên, nếu Đội ƯCSC thực hiện hoặc hỗ trợ các hoạt động này sẽ giúp cải thiện an toàn chung của tổ chức chủ quản và xác định được

các rủi ro, nguy cơ, và các điểm yếu của hệ thống. Các hoạt động này đóng góp gián tiếp vào việc giảm số lượng sự cố.

- Phân tích, đánh giá các rủi ro mất an toàn thông tin cho các hệ thống công nghệ thống tin, các quy trình hoạt động hoặc đánh giá các nguy cơ trong phạm vi của tổ chức chủ quản hoặc của đối tượng phục vụ để có các biện pháp và giải pháp phù hợp;

- Xây dựng và triển khai kế hoạch duy trì hoạt động liên tục và khôi phục thảm hoạ liên quan đến an toàn thông tin của tổ chức chủ quản. Tổ chức diễn tập kế hoạch định kỳ hàng năm để đảm bảo kế hoạch thực hiện được trong trường hợp Sự cố nghiêm trọng hoặc thảm hoạ;

- Huấn luyện, đào tạo, hướng dẫn về đảm bảo an toàn thông tin: tổ chức các khoá huấn luyện nâng cao nhận thức về đảm bảo an toàn thông tin cho toàn thể cán bộ, nhân viên trong toàn tổ chức chủ quản, hướng dẫn thực hiện các hoạt động về đảm bảo an toàn cho nội bộ và cho các cá nhân trong tổ chức, huấn luyện cho đội ngũ công nghệ thông tin của tổ chức chủ quản các kỹ năng cơ bản về đảm bảo an toàn và khắc phục Sự cố đơn giản;

- Triển khai kế hoạch đào tạo duy trì và/hoặc nâng cao kỹ năng chuyên môn cho các thành viên Đội ƯCSC;

- Tổ chức và/hoặc tham gia các diễn tập an toàn thông tin: định kỳ tổ chức các diễn tập đảm bảo an toàn thông tin về ứng phó kỹ thuật, chính sách trong các tình huống giả lập bị tấn công mạng, cử thành viên kỹ thuật – chính sách của Đội tham gia các diễn tập an toàn thông tin của quốc gia, khu vực hoặc do các tổ chức ứng cứu sự cố tổ chức;

- Tư vấn về an toàn thông tin: cung cấp lời khuyên và hướng dẫn thực hiện tốt nhất về an toàn cho nội bộ và cho các tổ chức bên ngoài nếu có yêu cầu. Các tư vấn có thể là các yêu cầu khi mua sắm, cài đặt hoặc bảo mật các hệ thống mới, các thiết bị mạng, các ứng dụng phần mềm, hoặc các quy trình hoạt động của tổ chức, hướng dẫn và hỗ trợ xây dựng các chính sách bảo mật của tổ chức.

Điều 6. Yêu cầu trong việc tổ chức hoạt động của Đội ứng cứu sự cố

6.1 Đội ƯCSC nên là một tổ chức độc lập trong cơ cấu tổ chức của tổ chức chủ quản, có thể sử dụng mô hình kiêm nhiệm nhưng phải đảm bảo các chức năng, nhiệm vụ của Đội phải được thực hiện;

6.2 Tuỳ theo điều kiện thực tế của mỗi tổ chức chủ quản mà bố trí nhân sự cho phù hợp, gồm các vị trí làm việc toàn thời gian và các nhân sự làm việc bán thời gian hoặc theo vụ việc. Tuy nhiên, Đội ƯCSC phải đảm bảo có nhân sự chuyên trách làm việc toàn thời gian cho các công việc quan trọng của Đội gồm lãnh đạo Đội (có thể là giám đốc/đội trưởng hoặc phó thường trực), chuyên viên điều phối sự cố an toàn thông tin, chuyên viên phản ứng sự cố, chuyên viên bảo

mật, phân tích sự cố, chuyên viên tiếp nhận và quản lý các sự kiện, sự cố.

Đối với các tổ chức chủ quản là các Bộ, ngành, các cơ quan chính phủ, cơ quan trung ương, uỷ ban nhân dân các tỉnh, thành phố thì đưa biên chế các vị trí này vào biên chế của đơn vị chuyên trách ứng cứu sự cố.

6.3 Để Đội ƯCSC hoạt động hiệu quả, cần thực hiện:

6.3.1 Đảm bảo 7 yếu tố cần thiết cho vận hành hoạt động của Đội gồm:

+ kế hoạch làm việc để đảm bảo duy trì liên tục hoạt động;

+ trang thiết bị thông tin liên lạc cần thiết, ưu tiên việc trang bị hệ thống hộp thư thoại để tiếp nhận và chuyển tiếp thông tin tự động;

+ hệ thống thư điện tử có thể tích hợp thông tin vào giải pháp quản lý luồng công việc của các cá nhân và của Đội và có thể tự động hoạt động theo các kịch bản riêng của Đội;

+ ứng dụng quản lý luồng công việc có khả năng tích hợp thông tin nhận được từ hệ thống thư điện tử, trang web, hệ thống điện thoại;

+ trang web thông tin riêng của Đội với yêu cầu tăng cường mức độ bảo mật cao hơn để tránh bị xâm hại;

+ dãi địa chỉ IP độc lập và tên miền riêng hoặc tên miền con thuộc của tên miền chính của tổ chức chủ quản;

+ bảo mật mạnh cho mạng và thiết bị với các thiết bị tường lửa loại kép có 2 bộ định tuyến độc lập cho mạng bên ngoài và bên trong, tường lửa bảo vệ cho vùng DMZ, máy tính riêng biệt co các công việc nội bộ và các tác vụ khác như kiểm tra, đánh giá, phân tích, xử lý sự cố, 2 đường kết nối Internet độc lập từ 2 nhà cung cấp dịch vụ khác nhau;

6.3.2 Xây dựng và thực hiện các quy tắc, chính sách sau:

+ bộ quy tắc ứng xử,

+ chính sách phân loại thông tin,

+ chính sách tiết lộ thông tin,

+ chính sách truyền thông,

+ chính sách bảo mật,

+ chính sách đối với lỗi do con người;

6.3.3 Đảm bảo và duy trì hoạt động liên tục của Đội, xem xét các nguy cơ có thể làm gián đoạn hoạt động của Đội do thiếu thời gian, thiếu nhân sự chính, do chuyển giao công việc, hạ tầng kỹ thuật không đủ đáp ứng hoặc do thiếu kinh phí. Duy trì liên tục hoạt động của Đội cần lưu ý đến:

+ tổ chức và vận hành hiệu quả hệ thống quản lý luồng công việc của

từng cá nhân, của Đội;

+ tổ chức và quản lý công việc ngoài giờ hành chính,

+ triển khai cho các công việc bên ngoài trụ sở của Đội;

6.3.4 Triển khai và quản lý an toàn để đảm bảo các yếu tố bảo mật, sẵn sàng, toàn vẹn, xác thực, độc quyền, riêng tư của thông tin. Các nội dung cần quan tâm và triển khai để đảm bảo an toàn cho Đội gồm:

+ sử dụng các ứng dụng mã hoá và chữ ký số trong đó ưu tiên sử dụng các hệ thống PGP đang được các Đội ứng cứu sự cố trên toàn thế giới áp dụng khi trao đổi và chia sẻ thông tin;

+ quản lý các khoá và các chứng chỉ;

+ tường lửa và bảo mật mạng;

+ mạng riêng dùng để kiểm tra;

+ cho phép truy cập từ ngoài trụ sở vào hệ thống nội bộ;

+ giải pháp bảo mật vật lý cho các vào, ra tại các khu vực;

+ bảo mật trước – trong và sau khi xử lý sự cố, thảm hoạ;

+ bảo mật cho việc xử lý sự cố bảo mật nội bộ;

6.3.5 Con người: bao gồm:

+ tổ chức và quản lý các thành viên chính thức, thành viên cộng tác của Đội ứng cứu có các kỹ năng cần thiết như đã nêu ở điều 7;

+ tuyển dụng nhân viên mới cho Đội;

+ các thủ tục cho nhân viên mới vào và các nhân viên rời khỏi Đội;

+ huấn luyện nhân viên về các kỹ năng cá nhân, kỹ năng mềm, kỹ năng chuyên môn;

+ giữ người để duy trì các thành viên có kinh nghiệm và sự ổn định của Đội;

+ phát triển và mở rộng nhân viên.

6.4 Kinh phí là yếu tố quan trọng đảm bảo sự duy trì hoạt động và liên tục của Đội ƯCSC. Ngân sách cung cấp cho Đội hoạt động gồm:

- chi phí thành lập và đầu tư trang thiết bị ban đầu,

- chi phí duy trì hoạt động hoạt động và đào tạo, cập nhật kiến thức – kỹ năng của các thành viên,

- chi phí đáp ứng các thay đổi công nghệ.

Việc cung cấp ngân sách cho Đội ƯCSC sẽ dựa trên đề án thành lập ban đầu, phê duyệt ngân sách hoạt động hàng năm và ngân sách dự phòng của tổ

chức chủ quản cho các thay đổi công nghệ.

Do hoạt động ứng cứu sự cố phụ thuộc nhiều vào kiến thức, kỹ năng, kinh nghiệm của các chuyên gia mà thực tế hiện nay đang rất thiếu, tổ chức chủ quản cần phải sắp xếp nguồn kinh phí đủ lớn cho việc tuyển dụng hoặc thu hút các chuyên gia giỏi, đào tạo thường xuyên và liên tục kỹ năng và kinh nghiệm cho các nhân sự hiện có, áp dụng ưu đãi thu nhập theo cơ chế đặc thù thí điểm của Thủ tướng đã ban hành cho đội ngũ an toàn thông tin, kinh phí cho các hoạt động hợp tác của Đội và các thành viên của Đội với các Đội ƯCSC khác có nhiều kinh nghiệm và các chuyên gia giỏi, kinh phí cho hoạt động tham gia với các nhóm quốc tế trong lĩnh vực ứng cứu sự cố.

Điều 7. Huấn luyện, đào tạo, thừa nhận, sát hạch và cấp chứng chỉ về các kỹ năng kỹ thuật liên quan đến hoạt động ứng cứu sự cố

7.1 Bộ Thông tin & Truyền thông thống nhất ban hành các nội dung huấn luyện đào tạo cơ bản và chuyên sâu được sử dụng trong hoạt động ứng cứu sự cố trong phụ lục của thông tư này;

7.2 Dựa trên đề cương các khóa đào tạo – huấn luyện đã ban hành của Bộ, các tổ chức đào tạo hoặc tổ chức có chức năng đào tạo trong nước hoặc nước ngoài có thể tổ chức các khóa đào tạo theo yêu cầu cho các đơn vị, tổ chức trong nước hoặc tổ chức các khóa học chiêu sinh công cộng. Kết thúc các khóa đào tạo, đơn vị tổ chức khóa học có thể cấp chứng nhận đã hoàn thành khóa đào tạo, huấn luyện theo quy định;

7.3 Để đảm bảo chất lượng của các kỹ năng chuyên môn kỹ thuật liên quan đến hoạt động ứng cứu sự cố, Bộ Thông tin và Truyền thông sẽ tổ chức kiểm tra sát hạch tập trung và cấp chứng chỉ. Hình thức sát hạch sẽ theo hình thức làm bài trực tuyến và có thể kết hợp kiểm tra một số kỹ năng thực tế tại các phòng thí nghiệm đủ điều kiện được chỉ định. Giao cho VNCERT – cơ quan điều phối về ứng cứu sự cố chủ trì, phối hợp với các đơn vị liên quan trong Bộ để đề xuất, xây dựng và triển khai hệ thống kiểm tra sát hạch cấp các chứng chỉ về ứng cứu sự cố;

7.4 Đối với các chứng chỉ quốc tế được nêu tại phụ lục 02 và 03 của thông tư này, Bộ Thông tin và Truyền thông sẽ xem xét và công bố thừa nhận đối với các chứng chỉ quốc tế tương đương; (*tham khảo lại thông tư 44/2017/TT-BTTTT ngày 29/12/2017 quy định về việc công nhận chứng chỉ công nghệ thông tin của tổ chức nước ngoài sử dụng ở Việt Nam đáp ứng chuẩn kỹ năng sử dụng công nghệ thông tin để quy định cho phù hợp*);

7.5 Các vị trí chuyên trách của các đội ứng cứu sự cố của các bộ, ngành, các tỉnh/thành phố trực thuộc trung ương phải đảm đảo có các chứng chỉ được yêu cầu khi tác nghiệp trong các hoạt động ứng cứu – xử lý sự cố an toàn thông tin mạng;

Chương III

CÁC CHỨC DANH CÔNG VIỆC VỀ ỨNG CỨU SỰ CỐ AN TOÀN THÔNG TIN MẠNG

Điều 8. Các kỹ năng cần thiết cho thành viên Đội ứng cứu sự cố

Một trong những nhiệm vụ chính của Đội ứng cứu sự cố là xử lý Sự cố, vì vậy đội cần các thành viên có các kỹ năng và kiến thức để phản ứng sự cố, thực hiện các nhiệm vụ phân tích và truyền thông cả trong nội bộ lẫn bên ngoài.

Dựa trên các kinh nghiệm xử lý sự cố của các tổ chức điều phối và các Đội ƯCSC trên thế giới, kinh nghiệm thực tế ở Trung tâm Ứng cứu Khẩn cấp Máy tính Việt Nam (VNCERT) và các kinh nghiệm khác từ cộng đồng, các thành viên Đội ƯCSC cần có hai nhóm kỹ năng cơ bản về các kỹ năng cá nhân và các kỹ năng kỹ thuật.

8.1 Các kỹ năng cá nhân: phục vụ cho các hoạt động hàng ngày của các thành viên xử lý sự cố, gồm:

- kỹ năng giao tiếp: viết và nói
- kỹ năng trình bày
- kỹ năng ngoại giao
- kỹ năng tuân thủ các chính sách và các quy trình
- kỹ năng đội – nhóm
- kỹ năng giữ bí mật
- biết các hạn chế, giới hạn của mình
- kỹ năng đối phó với căng thẳng
- kỹ năng giải quyết vấn đề
- kỹ năng quản lý thời gian

8.2 Các kỹ năng kỹ thuật: gồm 2 loại là kỹ năng nền tảng kỹ thuật và kỹ năng xử lý sự cố.

- Các kỹ năng nền tảng kỹ thuật: gồm
  + Các nguyên lý bảo mật
  + Lỗ hổng/điểm yếu bảo mật
  + Internet
  + Các rủi ro
  + Các giao thức mạng
  + Các ứng dụng và dịch vụ mạng

+ Các vấn đề bảo mật mạng
+ Các vấn đề bảo mật máy chủ và hệ thống
+ Mã độc hại
+ Các kỹ năng lập trình

- Các kỹ năng xử lý sự cố: gồm
+ Nắm vững các chính sách và quy trình nội bộ của Đội ƯCSC
+ Hiểu biết và xác định được các kỹ thuật xâm nhập
+ Phân tích sự cố
+ Quản lý các hồ sơ sự cố

Tham khảo Phụ lục 01 – Các kỹ năng cần thiết cho các thành viên Đội ứng cứu sự cố.

Điều 9. Danh sách các chức danh về ứng cứu sự cố an toàn thông tin mạng

- Lãnh đạo đội ứng cứu sự cố
- Chuyên viên bảo mật
- Chuyên viên xử lý Sự cố
- Chuyên viên phân tích Sự cố
- Chuyên viên tiếp nhận và quản lý sự kiện, sự cố an toàn thông tin
- Chuyên viên điều phối ứng cứu Sự cố
- Chuyên viên đánh giá an toàn
- Chuyên viên tư vấn bảo mật
- Chuyên viên pháp lý
- Chuyên viên truyền thông

Điều 10. Mô tả công việc và các yêu cầu đối với các chức danh ứng cứu sự cố an toàn thông tin mạng

1. Trưởng hoặc phó thường trực Đội ƯCSC

1.1 Mục đích công việc: Quản lý và điều hành việc tổ chức, hoạt động Đội ƯCSC và duy trì công việc đảm bảo bảo mật thông tin trong toàn bộ tổ chức chủ quản và/hoặc các đối tượng phục vụ.

1.2 Nhiệm vụ

- Xây dựng định hướng dài hạn cho đội và lập kế hoạch thực hiện định hướng hàng năm;

- Xây dựng chính sách bảo mật và chiến lượ bảo vệ thông tin cho tổ chức chủ quản và/hoặc các đối tượng phục vụ của Đội;

- Dự báo các mối nguy ảnh hưởng đến an toàn thông tin và triển khai các biện pháp giảm thiểu các nguy cơ đó;

- Giám sát việc phát triển và đảm bảo tuân thủ các chính sách, tiêu chuẩn và quy trình bảo mật của Đội, của tổ chức chủ quản, và/hoặc của các đối tượng

phục vụ;

- Làm đầu mối cho các cuộc điều tra về bảo mật CNTT và tổ chức Đội triển khai thực hiện cụ thể;

- Theo dõi hoạt động chuyên môn của các thành viên Đội để có các điều chỉnh và bổ sung phù hợp;

- Tổ chức các khoá đào tạo, tập huấn cho nhân viên; đào tạo nâng cao nhận thức của người dùng tuân thủ an toàn;

- Hợp tác với các tổ chức liên quan bên ngoài để nâng cao nâng lực hoạt động của Đội;

- Phối hợp với các quản lý cấp cao của tổ chức chủ quản, của đối tượng phục vụ để đảm bảo các chính sách, quy định bảo mật CNTT đang được vận hành, xem xét, quy trì và quản lý có hiệu quả.

1.3 Yêu cầu

- Kỹ năng nền tảng kỹ thuật: các nguyên lý bảo mật, lổ hỗng/các điểm yếu, Internet, các rủi ro, các giao thức, ứng dụng và dịch vụ mạng, các vấn đề bảo mật mạng/mảy chủ và hệ thống mức cơ bản

- Kỹ năng Ứng cứu sự cố: nắm vững các chính sách và quy trình nội bộ của Đội, hiểu biết các kỹ thuật xâm nhập – tấn công

- Kỹ năng cá nhân: các kỹ năng nói, viết, trình bày, ngoại giao, giải quyết vấn đề, quản lý thời gian, kỹ năng đội – nhóm, đàm phán

- Kỹ năng phụ trợ khác: quản lý và lãnh đạo, ngoại ngữ (tiếng Anh) nghe - nói, xây dựng mối quan hệ

2. Chuyên viên điều phối ứng cứu sự cố

2.1 Mục đích công việc:

2.2 Nhiệm vụ:

- Là đầu mối hợp tác về ứng cứu sự cố với các tổ chức bên ngoài, tiếp nhận thông tin liên quan đến Sự kiện, Sự cố từ bên ngoài

- Lập, cập nhật danh sách các tổ chức và cá nhân bên trong nội bộ và bên ngoài để phối hợp trong trường hợp có Sự cố;

- Triển khai lệnh điều phối ứng cứu khẩn cấp của quốc gia hoặc cấp trên nếu có;

- Kết nối các bên liên quan trong các Sự cố để phối hợp xử lý: nạn nhân, bộ phận CNTT hỗ trợ nạn nhân, các bộ phận có liên quan trong tổ chức chủ quản hoặc đối tượng phục vụ, các nơi có yêu cầu hỗ trợ phân tích cùng một Sự cố, các nhà cung cấp dịch vụ Internet, các Đội ƯCSC khác, các quản trị viên hệ thống/mạng, các nhà cung cấp, …

- Thông báo cho các nơi có khả năng liên quan hoặc tiềm tàng nguy cơ tương tự;

- Gửi thông báo, cảnh báo về các lỗ hổng bảo mật, các nguy cơ mới trong nội bộ, cho tổ chức chủ quản, và/hoặc đối tượng phục vụ;

- Điều phối xử lý lỗ hổng nếu có liên quan đến nhiều tổ chức, đơn vị bên ngoài: lịch phát hành các tài liệu, các bản vá và các giải pháp xử lý;

- Điều phối xử lý các phương tiện nhân tạo như mã độc, các bộ công cụ khai thác, các kịch bản thực thi, bao gồm: thông báo cho các bộ phận liên quan, tổng hợp phân tích kỹ thuật từ các nguồn, lưu trữ các mẫu, chiến lược ứng phó.

- Hợp tác với chuyên viên pháp lý, với bộ phận nhân sự hoặc bộ phận truyền thông, các cơ quan thực thi pháp luật trong các trường hợp Sự cố có ảnh hưởng đến an ninh trật tự hoặc liên quan đến nhiều tổ chức.

2.3 Yêu cầu

- Kỹ năng nền tảng kỹ thuật: các nguyên lý bảo mật, lổ hỗng/các điểm yếu, Internet, các rủi ro, các giao thức, ứng dụng và dịch vụ mạng, các vấn đề bảo mật mạng/máy chủ và hệ thống mức cơ bản

- Kỹ năng Ứng cứu sự cố: nắm vững các chính sách và quy trình nội bộ của Đội, hiểu biết các kỹ thuật xâm nhập – tấn công, quản lý các hồ sơ sự cố

- Kỹ năng cá nhân: các kỹ năng nói, viết, trình bày, ngoại giao, tuân thủ các chính sách và các quy trình, giữ bí mật, giải quyết vấn đề, đối phó với căng thẳng, quản lý thời gian, kỹ năng đội – nhóm

- Kỹ năng phụ trợ khác: ngoại ngữ (tiếng Anh) nghe – nói – đọc – viết

3. Chuyên viên phản ứng sự cố

3.1 Mục đích công việc: Chuyên viên phản ứng sự có trách nhiệm khắc phục sự cố và phòng ngừa sự cố an toàn thông tin cho tổ chức

3.2 Nhiệm vụ:

- Trực tiếp tìm hiểu nguyên nhân của sự cố, khắc phục sự cố và phòng ngừa sự cố mất an toàn thông tin cho tổ chức chủ quản, cho các đối tượng phục vụ;

- Chủ động thực hiện giám sát các hệ thống và giám sát các xâm nhập mạng;

- Xác định, nhận diện các lỗ hổng và lỗ hổng bảo mật;

- Tham gia xây dựng và vận hành quy trình phản ứng sự cố ATTT;

- Liên hệ với các tổ chức khác và các bên liên quan trong quá trình xử lý Sự cố;

- Viết các tài liệu về báo cáo sự cố, tài liệu kỹ thuật liên quan vấn đề ATTT cho tổ chức chủ quản, đối tượng phục vụ.

3.3 Yêu cầu

- Kỹ năng nền tảng kỹ thuật: các nguyên lý bảo mật, lổ hỗng/các điểm yếu, Internet, các rủi ro, các giao thức, ứng dụng và dịch vụ mạng, các vấn đề bảo mật mạng/máy chủ và hệ thống mức cơ bản, mã độc hại mức cơ bản, các kỹ năng lập trình cơ bản

- Kỹ năng Ứng cứu sự cố: nắm vững các chính sách và quy trình nội bộ của Đội, hiểu biết các kỹ thuật xâm nhập – tấn công, phân tích sự cố

- Kỹ năng cá nhân: các kỹ năng nói, viết, trình bày, tuân thủ các chính sách và các quy trình, giữ bí mật, giải quyết vấn đề, đối phó với căng thẳng, quản lý thời gian, kỹ năng đội – nhóm, biết các hạn chế - giới hạn của mình

- Kỹ năng phụ trợ khác: ngoại ngữ (tiếng Anh) nghe - nói - đọc - viết

4. Chuyên viên phân tích bảo mật

4.1 Mục đích công việc: Khám phá ra những điểm yếu của cơ sở hạ tầng (phần mềm, phần cứng và mạng) và tìm ra cách để bảo vệ nó.

4.2 Nhiệm vụ:

- Kiểm tra tất cả thông tin có sẵn, bằng chứng hỗ trợ, phương tiện nhân tạo liên quan đến Sự cố hoặc sự kiện để xác định phạm vi, các thiệt hại, bản chất của Sự cố để có chiến lược ứng phó phù hợp;

- Thực hiện điều tra số (forensics) bao gồm thu thập, bảo quản, tài liệu hoá và phân tích bằng chứng từ các hệ thống bị xâm hại để xác định các thay đổi và hỗ trợ việc khôi phục.

- Khôi phục và kiểm tra dữ liệu được lưu trữ làm bằng chứng;

- Truy tìm nguồn gốc của các kẻ xâm nhập hoặc xác định các hệ thống bị truy cập: cách xâm nhập, hệ thống và mạng bị ảnh hưởng, nơi tấn công, các hệ thống và mạng được sử dụng trong khi tấn công;

- Xây dựng các kế hoạch để bảo vệ các tập tin và hệ thống thông tin khỏi bị truy cập trái phép, bị sửa đổi hoặc bị hủy hoại;

- Giám sát truy cập;

- Thực hiện kiểm tra lỗ hổng, phân tích rủi ro và đánh giá bảo mật;

- Tiến hành đánh giá bảo mật từ bên trong và từ bên ngoài;

- Phân tích các vi phạm về an toàn thông tin để xác định nguyên nhân;

- Nghiên cứu phân tích, khuyến nghị áp dụng các công cụ, kỹ thuật chống tấn công mạng;

- Nghiên cứu, phân tích phần mềm độc hại, mã độc, các kỹ thuật phát tán phần mềm độc hại, để có các khuyến cáo và biện pháp giảm thiệu cho tổ chức chủ quản, đối tượng phục vụ;

- Phối hợp với chuyên viên pháp lý của Đội để làm nhân chứng chuyên môn trong các thủ tục của toà án khi có yêu cầu hoặc khi xác định danh tính của kẻ xâm nhập.

4.3 Yêu cầu

- Kỹ năng nền tảng kỹ thuật: các nguyên lý bảo mật, lỗ hỗng/các điểm yếu, Internet, các rủi ro, các giao thức, ứng dụng và dịch vụ mạng, các vấn đề bảo mật mạng/máy chủ và hệ thống mức cơ bản và nâng cao, mã độc hại cơ bản và nâng cao, các kỹ năng lập trình cơ bản và nâng cao

- Kỹ năng Ứng cứu sự cố: nắm vững các chính sách và quy trình nội bộ của Đội, hiểu biết các kỹ thuật xâm nhập – tấn công, phân tích sự cố

- Kỹ năng cá nhân: các kỹ năng nói, viết, trình bày, tuân thủ các chính sách và các quy trình, giữ bí mật, giải quyết vấn đề, đối phó với căng thẳng, quản lý thời gian, kỹ năng đội – nhóm, biết các hạn chế - giới hạn của mình

- Kỹ năng phụ trợ khác: ngoại ngữ (tiếng Anh) đọc – viết

5. Chuyên viên tiếp nhận, quản lý sự kiện, sự cố an toàn thông tin

5.1 Mục đích công việc: tổ chức và triển khai thực hiện việc trực tiếp nhận thông tin sự kiện, sự cố, cập nhật vào các hệ thống quản lý của Đội ƯCSC để phân bổ và có biện pháp xử lý kịp thời

5.2 Nhiệm vụ:

- Tiếp nhận thông tin các sự kiện, sự cố bảo mật từ tổ chức chủ quản hoặc bên ngoài thông báo cho Đội trong giờ làm việc và biện pháp ghi nhận thông tin báo ngoài giờ;

- Cập nhật các thông tin sự kiện, sự cố vào hệ thống thông tin quản lý của Đội;

- Cập nhật và duy trì danh sách các thành viên tương ứng với các trách nhiệm cụ thể trong Đội để chuyển tiếp trả lời thông tin hoặc xử lý trong các trường hợp khẩn cấp, ngoài giờ làm việc;

- Theo dõi và kiểm tra việc tổ chức thực hiện tiếp nhận thông tin ngoài giờ làm việc, đảm bảo thông tin được ghi nhận đầy đủ và xử lý kịp thời;

- Tập hợp, thống kê và lập báo cáo về tình hình sự cố, xử lý sự cố của Đội theo định kỳ hoặc đột xuất.

5.3 Yêu cầu

- Kỹ năng nền tảng kỹ thuật: các nguyên lý bảo mật, lỗ hỗng/các điểm yếu, Internet, các rủi ro, các giao thức, ứng dụng và dịch vụ mạng, các vấn đề bảo mật mạng/máy chủ và hệ thống mức cơ bản

- Kỹ năng Ứng cứu sự cố: nắm vững các chính sách và quy trình nội bộ của

Đội, quản lý các hồ sơ sự cố

- Kỹ năng cá nhân: các kỹ năng nói, viết, tuân thủ các chính sách và các quy trình, giữ bí mật, quản lý thời gian, kỹ năng đội – nhóm

- Kỹ năng phụ trợ khác: ngoại ngữ (tiếng Anh) nghe - nói

6. Chuyên viên đánh giá an toàn thông tin

6.1 Mục đích công việc: tìm kiếm, phát hiện, đánh giá các điểm không phù hợp, các điểm yếu của hệ thống bảo mật, của các ứng dụng, các lỗ hổng bảo mật, thực hiện khai thác các điểm yếu hoặc lỗ hổng bảo mật và thực hiện các báo cáo đánh giá bảo mật.

6.2 Nhiệm vụ:

- Lên kế hoạch, thực hiện và đánh giá bảo mật của toàn tổ chức;

- Đánh giá hiệu quả và sự tuân thủ của các quy trình hoạt động theo chính sách bảo mật của tổ chức/công ty và các quy định quản lý khác có liên quan;

- Đánh giá lại hoặc phỏng vấn nhân viên của tổ chức chủ quản, của đối tượng phục vụ để thiết lập quản lý các rủi ro bảo mật;

- Đánh giá các kết quả gây ra do thực hiện không hiệu quả hoặc thiếu kiểm soát;

- Phân tích, đánh giá mã nguồn của các ứng dụng;

- Xác định các vấn đề có thể dẫn đến truy cập trái phép hoặc rò rỉ thông tin nhạy cảm;

- Tiến hành đánh giá lỗ hổng bảo mật cho hệ thống mạng, các ứng dụng và hệ điều hành mà kẻ tấn công có thể khai thác;

- Thực hiện kiểm thử xâm nhập để xác định các lỗ hổng nguy cơ cao và thấp, để kiểm tra trên các ứng dụng dựa trên web, mạng và hệ thống máy tính;

- Xác nhận lại bằng tay các phát hiện để giảm thiểu sai sót;

- Sử dụng kỹ thuật xã hội để phát hiện các lỗ hổng, điểm yếu bảo mật như thực hiện bảo mật của người dùng yếu hoặc chính sách mật khẩu;

- Xem xét và xác định các yêu cầu cho các giải pháp đảm bảo an toàn thông tin của tổ chức chủ quản hoặc các đối tượng phục vụ;

- Cải tiến các hoạt động bảo mật, tăng cường liên tục các kỹ thuật mới và cả thiết bị hỗ trợ;

- Lập báo cáo bằng văn bản về kết quả đánh giá;

- Phản hồi và xác thực các vấn đề bảo mật để chỉnh sửa.

- Đưa ra các khuyến nghị để cải thiện bảo mật trên tất cả các lĩnh vực, kể cả cho bộ phận lập trình để viết ứng dụng an toàn và hỗ trợ huấn luyện cho các bộ

phận liên quan;

- Làm việc với các cấp quản lý để các khuyến nghị bảo mật phù hợp với quy trình của tổ chức chủ quản, của đối tượng phục vụ;

- Quản lý và duy trì cơ sở dữ liệu về các điểm yếu, các lỗ hổng, các điểm không phù hợp của hệ thống để tra cứu, huấn luyện và phục vụ các hoạt động quản lý;

- Kiểm tra, đánh giá kỹ thuật cho các hệ thống CNTT và sản phẩm CNTT;

- Kiểm tra, kiểm định các giải pháp, công nghệ bảo đảm an toàn thông tin.

6.3 Yêu cầu

- Kỹ năng nền tảng kỹ thuật: các nguyên lý bảo mật, lỗ hổng/các điểm yếu, Internet, các rủi ro, các giao thức, ứng dụng và dịch vụ mạng, các vấn đề bảo mật mạng/máy chủ và hệ thống mức cơ bản và nâng cao, mã độc hại cơ bản, các kỹ năng lập trình cơ bản

- Kỹ năng Ứng cứu sự cố: nắm vững các chính sách và quy trình nội bộ của Đội, hiểu biết các kỹ thuật xâm nhập – tấn công, phân tích sự cố, quản lý hồ sơ các sự cố

- Kỹ năng cá nhân: các kỹ năng nói, viết, trình bày, tuân thủ các chính sách và các quy trình, giữ bí mật, giải quyết vấn đề, đối phó với căng thẳng, quản lý thời gian, kỹ năng đội – nhóm, biết các hạn chế - giới hạn của mình

- Kỹ năng phụ trợ khác: ngoại ngữ (tiếng Anh) nghe – nói – đọc – viết

- Đáp ứng các yêu cầu của chức danh kiểm định viên công nghệ thông tin tại mục 3, điều 11, 12, 13 Thông tư 45/2017/TT-BTTTT ngày 29/12/2017 quy định tiêu chuẩn chức danh nghề nghiệp viên chức chuyên ngành công nghệ thông tin;

7. Chuyên viên bảo mật

7.1 Mục đích công việc: chịu trách nhiệm cho việc thiết kế, kiểm tra, triển khai và giám sát các biện pháp bảo mật cho các hệ thống của tổ chức.

7.2 Nhiệm vụ:

- Phân tích và thiết lập các yêu cầu về bảo mật cho hệ thống/mạng;

- Bảo vệ hệ thống CNTT chống lại truy cập trái phép, hiệu chỉnh hoặc hủy hoại;

- Cấu hình và hỗ trợ công cụ bảo mật như tường lửa, chống virus, hệ thống quản lý bản vá lỗi, …;

- Xác định các quyền truy cập, quyền với các cấu trúc điều khiển và quyền với tài nguyên;

- Thực hiện kiểm tra lỗ hổng, phân tích rủi ro và đánh giá bảo mật;

- Nhận dạng các bất thường và báo cáo vi phạm;

- Phát triển, cập nhật khả năng duy trì hoạt động/kinh doanh liên tục và phục hồi thảm họa;

- Đào tạo nâng cao nhận thức bảo mật người dùng, chính sách và qui trình đảm bảo an toàn thông tin;

- Thiết kế và thực hiện kiểm tra đánh giá bảo mật để đảm bảo hoạt động nghiệp vụ liên tục;

- Ứng cứu kịp thời sự cố bảo mật và cung cấp báo cáo phân tích sự cố;

- Nghiên cứu và đề xuất nâng cấp hoạt động bảo mật;

- Cung cấp các hướng dẫn kỹ thuật cho tổ chức chủ quản, đối tượng phục vụ.

7.3 Yêu cầu

- Kỹ năng nền tảng kỹ thuật: các nguyên lý bảo mật, lỗ hỗng/các điểm yếu, Internet, các rủi ro, các giao thức, ứng dụng và dịch vụ mạng, các vấn đề bảo mật mạng/máy chủ và hệ thống mức cơ bản và nâng cao, mã độc hại cơ bản, các kỹ năng lập trình cơ bản

- Kỹ năng Ứng cứu sự cố: nắm vững các chính sách và quy trình nội bộ của Đội, hiểu biết các kỹ thuật xâm nhập – tấn công, phân tích sự cố, quản lý hồ sơ các sự cố

- Kỹ năng cá nhân: các kỹ năng nói, viết, trình bày, tuân thủ các chính sách và các quy trình, giữ bí mật, giải quyết vấn đề, đối phó với căng thẳng, quản lý thời gian, kỹ năng đội – nhóm, biết các hạn chế - giới hạn của mình

- Kỹ năng phụ trợ khác: ngoại ngữ (tiếng Anh) đọc – viết

8. Chuyên viên tư vấn bảo mật

8.1 Mục đích công việc: thực hiện các hoạt động về tư vấn và hỗ trợ tổ chức, triển khai và thực hiện các công việc cụ thể về hoạt động bảo mật của tổ chức như xây dựng chính sách, triển khai các giải pháp bảo vệ, giám sát và duy trì hoạt động bảo mật, tư vấn bảo mật cho các dự án CNTT, ...

8.2 Nhiệm vụ:

- Tư vấn xây dựng, thiết kế các hệ thống CNTT có độ an toàn cao;

- Tư vấn xây dựng và triển khai các giải pháp kỹ thuật bảo đảm an toàn cho các hệ thống CNTT của Đội, của tổ chức chủ quản, và/hoặc của các đối tượng phục vụ;

- Thực hiện kiểm thử lỗ hổng/điểm yếu, phân tích rủi ro và đánh giá bảo mật;

- Nghiên cứu các tiêu chuẩn bảo mật, hệ thống bảo mật và các giao thức

xác thực;

- Kiểm tra các giải pháp bảo mật bằng việc sử dụng các tiêu chí phân tích theo tiêu chuẩn;

- Cung cấp các báo cáo kỹ thuật và hướng dẫn cho Đội, tổ chức chủ quản và đối tượng phục vụ;

- Phản ứng sớm với các sự cố liên quan đến bảo mật và cung cấp phân tích đầy đủ sau sự kiện.

8.3 Yêu cầu

- Kỹ năng nền tảng kỹ thuật: các nguyên lý bảo mật, lỗ hỗng/các điểm yếu, Internet, các rủi ro, các giao thức, ứng dụng và dịch vụ mạng, các vấn đề bảo mật mạng/máy chủ và hệ thống mức nâng cao, mã độc hại mức nâng cao, các kỹ năng lập trình nâng cao

- Kỹ năng Ứng cứu sự cố: nắm vững các chính sách và quy trình nội bộ của Đội, hiểu biết các kỹ thuật xâm nhập – tấn công, phân tích sự cố

- Kỹ năng cá nhân: các kỹ năng nói, viết, trình bày, ngoại giao, tuân thủ các chính sách và các quy trình, giữ bí mật, giải quyết vấn đề, đối phó với căng thẳng, quản lý thời gian, kỹ năng đội – nhóm, biết các hạn chế - giới hạn của mình

- Kỹ năng phụ trợ khác: ngoại ngữ (tiếng Anh) nghe - nói - đọc - viết

9. Chuyên viên pháp lý

9.1 Mục đích công việc: là đại diện Đội ƯCSC cho các hoạt động liên quan đến pháp lý, pháp luật, đạo bảo hoạt động của Đội liên quan đến thông tin, dữ liệu nhạy cảm đúng các quy định pháp luật trong nước và quốc tế khi hợp tác với các tổ chức nước ngoài

9.2 Nhiệm vụ:

- Cập nhật các quy định luật pháp để điều chỉnh và áp dụng trong các hợp đồng, thoả thuận, giao dịch của Đội với các đối tác bên ngoài, nhất là việc cung cấp thông tin liên quan đến Sự cố

- Nghiên cứu các quy định luật pháp liên quan của các nước trong các trường hợp hợp tác quốc tế, tham gia các nhóm làm việc quốc tế hoặc cung cấp dịch vụ cho tổ chức nước ngoài

- Tư vấn các vấn đề pháp lý cho các bộ phận, cá nhân trong Đội

- Hỗ trợ biên soạn, chỉnh sửa các chính sách, quy định, hợp đồng áp dụng tại Đội ƯCSC phù hợp với luật pháp

- Tham gia thương lượng, gặp gỡ các đối tác bên ngoài trong các công việc hợp tác xử lý Sự cố

- Đại diện Đội tham gia với toà án, cơ quan pháp luật trong trường hợp có yêu cầu hoặc có phát sinh từ các Sự cố

9.3 Yêu cầu

- Kỹ năng nền tảng kỹ thuật: các nguyên lý bảo mật, lỗ hỗng/các điểm yếu, Internet, các rủi ro

- Kỹ năng Ứng cứu sự cố: nắm vững các chính sách và quy trình nội bộ của Đội, hiểu biết các kỹ thuật xâm nhập – tấn công

- Kỹ năng cá nhân: các kỹ năng nói, viết, trình bày, ngoại giao, tuân thủ các chính sách và các quy trình, giữ bí mật, giải quyết vấn đề, kỹ năng đội – nhóm

- Kỹ năng phụ trợ khác: pháp lý, ngoại ngữ (tiếng Anh) nghe - nói - đọc - viết

10. Chuyên viên truyền thông

10.1 Mục đích công việc: là người đại diện của Đội để phát biểu với các tổ chức truyền thông, các cơ quan bên ngoài về mục tiêu và hoạt động của Đội, về các Sự cố mà Đội đang xử lý, về các hoạt động tuyên truyền của Đội để nâng cao nhận thức an toàn cho người dùng

10.2 Nhiệm vụ:

- Xử lý các yêu cầu của truyền thông liên quan đến hoạt động của Đội, các Sự cố đang xử lý;

- Xây dựng chính sách tiết lộ thông tin của Đội và theo dõi thực hiện;

- Thiết lập danh sách liên lạc với các cơ quan truyền thông, nhất là các nhà báo hiểu biết kỹ thuật và các ấn phẩm kỹ thuật tốt;

- Xây dựng và áp dụng các quy tắc hợp tác giữa Đội và các cơ quan truyền thông;

- Tóm lược các nội dung chính cần truyền thông của Đội;

- Chỉ định việc tiếp xúc với truyền thông trong Đội cho các trường hợp chính thức hoặc bất ngờ;

- Đào tạo cho các thành viên trong Đội tương tác với truyền thông và hiểu những gì có thể nói với truyền thông;

- Tham gia xây dựng và triển khai các hướng dẫn, đào tạo nâng cao nhận thức an toàn thông tin cho tổ chức chủ quản, đối tượng phục vụ.

10.3 Yêu cầu

- Kỹ năng nền tảng kỹ thuật: các nguyên lý bảo mật, lỗ hỗng/các điểm yếu, Internet, các rủi ro, các giao thức, ứng dụng và dịch vụ mạng, các vấn đề bảo mật mạng/máy chủ và hệ thống mức cơ bản

- Kỹ năng Ứng cứu sự cố: nắm vững các chính sách và quy trình nội bộ của Đội, hiểu biết các kỹ thuật xâm nhập – tấn công, quản lý các hồ sơ sự cố

- Kỹ năng cá nhân: các kỹ năng nói, viết, trình bày, ngoại giao, tuân thủ các chính sách và các quy trình, giữ bí mật, giải quyết vấn đề, kỹ năng đội – nhóm

- Kỹ năng phụ trợ khác: báo chí, ngoại ngữ (tiếng Anh) nghe - nói - đọc - viết

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 11.

Trung tâm Ứng cứu Khẩn cấp Máy tính Việt Nam có trách nhiệm hỗ trợ các cơ quan, đơn vị triển khai thông tư này, có các hướng dẫn chi tiết hơn về triển khai tổ chức hoạt động của các Đội ƯCSC hiện có hoặc thành lập mới, hướng dẫn và/hoặc tham gia việc huấn luyện, đào tạo các kỹ năng cho các thành viên của các Đội ƯCSC.

Điều 12. Hiệu lực thi hành

1. Thông tư này có hiệu lực thi hành kể từ ngày xx tháng xx năm 2018.

2. Trong quá trình thực hiện, nếu có vướng mắc, phát sinh tổ chức, cá nhân có liên quan kịp thời phản ánh về Bộ Thông tin và Truyền thông (qua VNCERT) để xem xét, bổ sung và sửa đổi./.

Nơi nhận:
- Thủ tướng Chính phủ, các PTTgCP (để b/c);
- Văn phòng Quốc hội;
- Văn phòng Chủ tịch nước;
- Văn phòng TW và các Ban của Đảng;
- Các Bộ và cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Toà án nhân dân tối cao;
- Viện Kiểm sát nhân dân tối cao;
- Kiểm toán Nhà nước;
- UBND các tỉnh, thành phố trực thuộc TW;
- Cơ quan Trung ương của các đoàn thể;
- Ban Chỉ đạo quốc gia về CNTT;
- Ban Chỉ đạo CNTT của cơ quan Đảng;
- Đơn vị chuyên trách về CNTT của các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc TW;
- Công báo, Cổng Thông tin điện tử Chính phủ;
- Cục Kiểm tra VBQPPL (Bộ Tư pháp);
- Bộ TTTT: Bộ trưởng và các Thứ trưởng, các cơ quan, đơn vị thuộc Bộ, Cổng Thông tin điện tử;
- Lưu: VT, VNCERT (5b).

BỘ TRƯỞNG

Nguyễn Mạnh Hùng

PHỤ LỤC 01

CÁC KỸ NĂNG CẦN THIẾT CỦA THÀNH VIÊN ĐỘI ỨNG CỨU SỰ CỐ

(Ban hành kèm theo thông tư số /2018/TT-BTTTT ngày / /2018 của Bộ Thông tin và Truyền thông)

Các Đội ƯCSC phải có một số thành viên nòng cốt cung cấp các xử lý Sự cố thông thường. Mỗi thành viên trong đội nên có một số kỹ năng cơ bản để thực hiện công việc và hiệu quả trong việc phản ứng Sự cố, cụ thể sẽ gồm các kỹ năng cá nhân và các kỹ năng kỹ thuật

1. Các kỹ năng cá nhân: là các kỹ năng hoạt động hàng ngày của các thành viên xử lý Sự cố

1.1 Kỹ năng giao tiếp

Khả năng giao tiếp hiệu quả là kỹ năng quan trọng của các thành viên Đội ƯCSC để đảm bảo họ có thể nhận được và/hoặc cung cấp thông tin cần thiết. Các thành viên Đội cần có khả năng thích ứng để phù hợp với các mức độ hiểu biết thấp hơn hoặc cao về chuyên môn của người nghe, người thảo luận. 2 kỹ năng quan trọng trong giao tiếp của thành viên Đội ƯCSC là viết và nói.

- Viết: vì phần lớn các giao tiếp của các thành viên Đội ƯCSC thông qua ngôn ngữ viết như trả lời thư điện tử liên quan đến các sự cố; viết các báo cáo sự kiện hoặc sự cố, các lỗ hổng, và các thông tin kỹ thuật khác; viết các thông báo, hướng dẫn cho nội bộ hoặc cho đối tượng phục vụ, ... nên thành viên Đội ƯCSC phải có khả năng viết rõ ràng và súc tích, mô tả chính xác các hoạt động, và cung cấp thông tin dễ hiểu cho người đọc.

- Nói: là khả năng thường xuyên sử dụng trong khi làm việc của thành viên Đội ƯCSC. Giao tiếp miệng thường qua trao đổi điện thoại hoặc thảo luận trực tiếp, có thể liên quan đến một hoặc nhiều người, nhiều đối tượng khác nhau. Trong một số trường hợp, Đội có thể chọn một hoặc một vài thành viên đóng vai trò chính trong việc liên lạc với bên ngoài hoặc làm "người phát ngôn" của Đội để phát biểu chính thức về các hoạt động và thông tin của Đội.

1.2 Kỹ năng trình bày:

Mặc dù các nhân viên xử lý sự cố của Đội ƯCSC có thể tương tác hàng ngày với các thành viên của tổ chức chủ quản, với các đối tượng phục vụ nhưng họ có thể không tự tin khi phải trình bày trước đám đông. Ngoài ta, trong tình huống khó, có tranh cãi hoặc có trở ngại thì cần phải hành xử và giải quyết để không gây tổn hại cho danh tiếng của Đội hoặc không xúc phạm người khác. Để các nhân viên có kinh nghiệm và trình bày tự tin trong các tình huống đó cần phải tốn nhiều thời gian và nỗ lực.

Ở góc độ kỹ năng "chuyên gia", Đội cần một hoặc vài thành viên có kỹ năng trình bày tốt, có thể là trình bày kỹ thuật, các vấn đề về quản trị, hoặc thảo

luận bàn tròn ở các hội thảo. Các kỹ năng của chuyên gia cũng cần được mở rộng như cung cấp lời khai chuyên gia trước pháp luật thay mặt cho Đội UCSC hoặc thay cho đối tượng phục vụ. Những thành viên có kiến thức này sẽ đại diện cho Đội UCSC và cần phải diễn giải nhiệm vụ và mục tiêu của Đội, các dịch vụ, định hướng chiến lược, ... Các chuyên gia này có thể gặp các phản ứng bất lợi về các chính sách và quy trình của Đội, về tổ chức chủ quản hoặc một bên khác có liên quan đến Đội nên phải giữ bình tĩnh trong các tình huống bất lợi đó, giữ các vấn đề theo quan điểm, đại diện cho Đội hoặc đối tượng phục vụ một cách hợp lý.

1.3 Kỹ năng ngoại giao:

Các thành viên của Đội UCSC sẽ phải tương tác với cộng đồng gồm những người có các mục tiêu và nhu cầu khác nhau. Những người này sẽ có nhiều kiến thức và mức độ quan tâm khác nhau nên cần tránh bị choáng ngợp, lo lắng, thất vọng hoặc tức giận. Trong vài trường hợp, những người khác có thể tấn công hoặc cố "lừa" nhân viên Đội UCSC cung cấp thông tin không phù hợp. Vì vậy, các nhân viên Đội UCSC phải có kỹ năng có thể lường trước các tranh chấp tiềm ẩn, có phản ứng phù hợp, duy trì quan hệ tốt và tránh gây rắc rối cho người khác. Họ cũng phải hiểu rằng họ đại diện cho Đội UCSC và/hoặc tổ chức chủ quản nên ngoại giao và khéo léo là rất cần thiết.

1.4 Kỹ năng tuân thủ các chính sách và các quy trình:

Các thành viên của Đội UCSC cần có kỹ năng tuân thủ và hỗ trợ các chính sách, các quy trình đã ban hành của tổ chức chủ quản hoặc của Đội. Họ nên hiểu lý do và các thông tin liên quan đến việc hình thành các chính sách, quy trình đó. Để bảo đảm cho các dịch vụ phản ứng sự cố thích hợp và tin cậy, nhân viên Đội UCSC phải chuẩn bị để chấp nhận và tuân thủ các quy tắc và hướng dẫn, ngay cả khi chúng không được ghi chép đầy đủ và hoặc khi không đồng ý với chúng. Nếu nhân viên cảm thấy cần phải thay đổi thì họ được quyền đề xuất các thay đổi với cấp quản lý, cần nêu rõ những thay đổi sẽ cải thiện hoạt động của Đội và các đối tượng phục vụ như thế nào.

1.5 Kỹ năng đội – nhóm:

Nhân viên Đội UCSC phải làm việc trong môi trường làm việc nhóm và cần nhận thức rõ trách nhiệm của họ đóng góp vào mục tiêu của Đội. Họ cần phải uyển chuyển và có thể đáp ứng các thay đổi. Họ cũng cần các kỹ năng làm việc nhóm khi trao đổi với các bộ phận, đơn vị trong nội bộ của tổ chức chủ quản hoặc với các Đội UCSC khác. Nếu một nhân viên Đội UCSC không hợp tác và không hỗ trợ các thành viên khác của Đội, tinh thần của Đội sẽ bị ảnh hưởng và có thể không hài lòng trong Đội, dẫn đến mất năng suất - hiệu quả - danh tiếng hoặc mất khả năng của các nhân viên khác (một số người rời khỏi Đội vì không hài lòng với môi trường làm việc).

Khi phát triển Đội ƯCSC, cần có một hoặc nhiều thành viên trong Đội có thể đóng vai trò lãnh đạo để hỗ trợ các nhóm nhỏ hơn hoặc các đội kỹ thuật bên trong Đội ƯCSC. Cấp quản lý trung gian này quản lý các hoạt động hàng ngày của nhân viên trong các nhóm nhỏ hơn và làm việc với người quản lý của Đội về các các nội dung liên quan đến định hướng chiến lược, chính sách của Đội, về cơ sở hạ tầng, và/hoặc các hoạt động vận hành.

Đội ƯCSC là nơi khuyến khích phát huy các kỹ năng chuyên gia. Tuy nhiên, việc kết hợp giữa năng lực kỹ thuật và các kỹ năng lãnh đạo/quản lý không phải lúc nào cũng được. Một cá nhân có thể đạt được một số kỹ năng sau một thời gian kinh nghiệm hoặc được đào tạo, nhưng lãnh đạo kỹ thuật không phải là một kỹ năng luôn có sau khi một chuyên gia kỹ thuật đã tham dự khoá đào tạo lãnh đạo. Vì vậy, Đội cần thời gian để nuôi dưỡng và phát triển, hoặc tìm người phù hợp ở bên ngoài Đội. Tổ chức chủ quản có thể cần dành một khoản ngân sách cho việc tuyển dụng các vị trí lãnh đạo, kể cả người được chọn từ bên ngoài hoặc nhân viên bên trong Đội.

1.6 Kỹ năng giữ bí mật:

Bản chất công việc của Đội ƯCSC là các thành viên thường xuyên tiếp xúc với thông tin nhạy cảm và đôi khi là các thông tin có giá trị. Nhân viên của Đội phải đáng tin, tách biệt và có thể xử lý thông tin bí mật theo các hướng dẫn của Đội, theo các thoả thuận hoặc quy định của đối tượng phục vụ, và/hoặc theo các chính sách và quy trình của tổ chức chủ quản.

Khi cung cấp các giải thích hoặc phản hồi kỹ thuật, nhân viên Đội ƯCSC cần cẩn thận về sự phù hợp và tính chính xác, tránh phổ biến bất kỳ thông tin bí mật nào gây ảnh hưởng đến danh tiếng của tổ chức chủ quản, của Đội hoặc ảnh hưởng đến các hoạt động liên quan của các bên khác. Vì vậy, các thành viên của Đội phải hiểu được sự khác nhau giữa vai trò "dịch vụ khách hàng" trong việc hỗ trợ đối tượng phục vụ và nhu cầu bảo đảm thông tin được bảo vệ và được xử lý phù hợp. Nhân viên Đội ƯCSC phải luôn nhận thức được trách nhiệm của họ và không bị "đánh lạc hướng", không tiết lộ trái phép thông tin.

1.7 Biết các hạn chế, giới hạn của mình:

Nhân viên Đội ƯCSC phải khả năng thừa nhận khi bản thân đạt đến giới hạn của kiến thức hoặc chuyên môn trong một tình huống hoặc lĩnh vực nào đó, để chủ động tìm kiếm sự hỗ trợ của các thành viên khác trong Đội, của các chuyên gia khác, hoặc của cấp quản lý. Danh tiếng của Đội có thể bị ảnh hưởng nghiêm trọng nếu nhân viên cung cấp thông tin hoặc hướng dẫn không chính xác cho các bên khác.

1.8 Kỹ năng đối phó với căng thẳng:

Nhân viên Đội ƯCSC thường xuyên gặp phải các tình huống căng thẳng.

Họ cần phải có khả năng nhận biết khi đang ở trạng thái căng thẳng để các thành viên khác của Đội biết và hỗ trợ để kiểm soát, duy trì sự bình tĩnh của họ. Đặc biệt, nhân viên Đội ƯCSC cần có khả năng giữ bình tĩnh trong những tình huống căng thẳng, từ làm việc quá sức đến trả lời những người gọi hung hăng hoặc với sự cố mà tính mạng con người hoặc hạ tầng trọng yếu bị đe doạ. Danh tiếng của Đội, danh tiếng cá nhân của nhân viên sẽ được tăng cường hoặc bị ảnh hưởng tuỳ theo cách xử lý các tình huống như vậy.

1.9 Kỹ năng giải quyết vấn đề:

Nhân viên Đội ƯCSC phải đối diện với dữ liệu hàng ngày, nhiều trường hợp lượng thông tin là quá lớn. Nhân viên cần phải:

- xác định sự liên quan của dữ liệu được cấp

- nhận dạng thông tin nào là quan trọng, thiếu hoặc có thể gây hiểu nhầm hoặc không chính xác

- quyết định cách xử lý dữ liệu đó

Nếu không có các kỹ năng giải quyết vấn đề tốt, các thành viên có thể bị choáng ngợp với lượng dữ liệu liên quan đến sự cố và các nhiệm vụ khác cần xử lý. Kỹ năng giải quyết vấn đề cũng là khả năng mà nhân viên Đội ƯCSC có thể "suy nghĩ khách quan" hoặc xem xét vấn đề từ nhiều góc nhìn để xác định các thông tin hoặc dữ liêu liên quan, gồm:

- biết ai khác trong đội có thể liên lạc hoặc tiếp cận thông tin bổ sung, ý tưởng sáng tạo hoặc thêm sự hiểu biết kỹ thuật,

- nhận dạng và tìm kiếm thông tin bổ sung từ các nguồn khác,

- kiểm tra thông tin thông qua các phương pháp tiếp cận khác,

- tổng hợp thông tin để xác nhận mối quan hệ hoặc tương quan với các dữ liệu sự cố khác.

1.10 Kỹ năng quản lý thời gian:

Cùng với các kỹ năng giải quyết vấn đề, nhân viên Đội ƯCSC phải có khả năng quản lý thời gian hiệu quả. Họ có thể sẽ phải gặp cùng lúc hàng loạt các nhiệm vụ khác nhau như phân tích, phối hợp và phản ứng sự cố, thực hiện các nhiệm vụ như ưu tiên khối lượng công việc, tham dự và/hoặc chuẩn bị cho các cuộc họp, thu thập số liệu thống kê, nghiên cứu, thuyết trình, tham dự các hội nghị và có thể cung cấp các hỗ trợ kỹ thuật tại chỗ.

Dù cho Đội có các hướng dẫn xác định các tiêu chí ưu tiên, nhân viên vẫn sẽ gặp khó khi sắp xếp ưu tiên và quản lý đồng thời các trách nhiệm mà họ được giao. Để duy trì hiệu suất, nhân viên Đội ƯCSC phải cân bằng nỗ lực của mình giữa việc hoàn thành các nhiệm vụ được giao, nhận ra khi khối lượng công việc trở nên quá tải cần tìm sự giúp đỡ hoặc hướng dẫn từ cấp quản lý và tránh tình

trạng tái ưu tiên lại cho các nhiệm vụ mới phát sinh.

2. Các kỹ năng kỹ thuật: các kỹ năng kỹ thuật cơ bản của các thành viên được phân thành 2 loại: kỹ năng nền tảng kỹ thuật và kỹ năng xử lý sự cố.

Các kỹ năng nền tảng kỹ thuật yêu cầu có các hiểu biết cơ bản về các công nghệ đang được Đội ƯCSC, tổ chức chủ quản hoặc đối tượng phục vụ sử dụng, và hiểu biết về các vấn đề ảnh hưởng đến Đội và tổ chức chủ quản như là:

- Loại sự cố đang được báo cáo hoặc được cộng đồng phát hiện,

- Cách thức Đội ƯCSC hỗ trợ kỹ thuật cho tổ chức chủ quản/đối tượng phục vụ

- Các phản hồi phù hợp cho Đội

- Cấp thẩm quyền của Đội ƯCSC trong một số hoạt động cụ thể

Các kỹ năng xử lý sự cố đòi hỏi hiểu biết về kỹ thuật, các điểm ra quyết định, và các công cụ hỗ trợ (phần mềm hoặc ứng dụng) cần thiết trong các hoạt động hàng ngày của Đội.

Cuối của mỗi kỹ năng sẽ nói thêm về các kỹ năng "chuyên gia" cho kỹ năng đó. Các chuyên gia với các kỹ năng chuyên gia đó là nguồn nhân lực gia tăng giá trị mà Đội cần. Họ có thể là các thành viên cao cấp của Đội, các thành viên bổ trợ cho Đội, các nhân viên khác trong tổ chức chủ quản hoặc các chuyên gia tin cậy ở bên ngoài.

2.1 Các kỹ năng nền tảng kỹ thuật:

Các kỹ năng và kiến thức nền tảng kỹ thuật là những kỹ năng quan trọng được sử dụng trong các hoạt động hàng ngày và trong các tương tác của Đội với tổ chức chủ quản hoặc với đối tượng phục vụ. Những kỹ năng cơ bản này là cần thiết để hiểu cách cấu hình và hoạt động của các hệ thống và phần mềm, các nguy cơ/rủi ro đồng hành với các công nghệ được dùng, các cách bảo vệ, bảo mật, và/hoặc sửa chữa hệ thống.

2.1.1 Các nguyên lý an toàn:

Các thành viên của Đội ƯCSC cần phải có các hiểu biết về các nguyên lý an toàn liên quan đến sự bí mật, sự sẵn sàng, sự xác thực, sự toàn vẹn, kiểm soát truy cập, sự riêng tư, không chối bỏ, để hiểu các vấn đề tiềm ẩn có thể phát sinh nếu các biện pháp an toàn chưa được thực hiện đúng, cũng như các tác động tiềm ẩn đến các hệ thống của tổ chức chủ quản, của đối tượng phục vụ hoặc cả các hệ thống của Đội. Với các hiểu biết về các nguyên lý an toàn, thành viên Đội ƯCSC sẽ đáp ứng tốt hơn các nhu cầu của tổ chức chủ quản, của đối tượng phục vụ trong việc cấu hình bảo mật để ngăn việc lạm dụng hoặc xâm hại và cũng được chuẩn bị tốt hơn để cung cấp các hỗ trợ và hướng dẫn kỹ thuật phù hợp khi xảy ra Sự cố.

2.1.2 Lỗ hổng/điểm yếu bảo mật:

Để hiểu cách tấn công cụ thể ảnh hưởng đến các phần mềm hoặc phần cứng, nhân viên Đội ƯCSC trước tiên cần phải hiểu rõ nguyên nhân cơ bản của các lỗ hổng bị khai thác bởi các kẻ tấn công. Họ cần có khả năng nhận diện và phân loại các lỗ hổng và các tấn công tương ứng, chẳng hạn:

+ các vấn đề bảo mật vật lý

+ lỗ hổng trong thiết kế của giao thức: ví dụ tấn công ở khu vực trung gian, giả mạo

+ mã độc hại: ví dụ virút, sâu, trojan

+ thực thi các lỗ hổng: ví dụ tràn bộ đệm, cửa sổ thời gian

+ các điểm yếu trong cấu hình

+ lỗi người dùng

2.1.3 Internet:

Thành viên Đội ƯCSC phải có hiểu biết cơ bản về internet, bảo mật cho các giao thức và dịch vụ cơ bản được dùng trên mạng Internet hoặc dự đoán đượccác nguy cơ có thể xảy ra trong tương lai. Tối thiểu, các thành viên của Đội ƯCSC nên biết về lịch sử, cấu trúc của internet, và hạ tầng hỗ trợ nó.

2.1.4 Các rủi ro:

Các thành viên của Đội ƯCSC cần có hiểu biết cơ bản về phân tích các rủi ro bảo mật máy tính. Họ cần biết ảnh hưởng của các loại rủi ro khác nhau đến đối tượng phục vụ của Đội, ví dụ như tiềm ẩn các tấn công qua Internet, các vấn đề an toàn của quốc gia có liên quan đến Đội và đối tượng phục vụ, các nguy cơ vật lý, các nguy cơ tài chính, thiệt hại kinh doanh - danh tiếng hoặc sự tin cậy của khách hàng, hư hỏng hoặc mất dữ liệu. Các nhân viên mới của Đội có thể thiếu các kiến thức này và cần có hướng dẫn, chỉ bảo để đảm bảo họ hiểu các rủi ro có thể ảnh hưởng thế nào đến đối tượng phục vụ của họ, cũng như ảnh hưởng đến chính Đội ƯCSC của mình.

2.1.5 Các giao thức mạng:

Thành viên của Đội ƯCSC cần có hiểu biết về các giao thức mạng phổ biến, tối thiểu cũng phải là các giao thức được Đội và đối tượng phục vụ sử dụng. Với mỗi giao thức, họ cần hiểu về cơ bản của giao thức, các đặc tính kỹ thuật, và cách sử dụng. Ngoài ra, họ cần biết các nguy cơ và các loại tấn công phổ biến vào giao thức, cũng như biện pháp để giảm nhẹ hoặc ngăn chặn các tấn công đó.

Ví dụ, thành viên Đội ƯCSC phải thông thạo tối thiểu các giao thức như IP, TCP, UDP, ICMP, ARP và RARP. Họ cần hiểu cách mà các giao thức này hoạt động, được dùng cho mục đích nào, sự khác nhau giữa chúng, một số các điểm

yếu phổ biến, ... Ngoài ra, các thành viên trong Đội phải có hiểu biết tương tự nhau về các giao thức như TFTP, FTP, HTTTP, HTTPS, SNMP, SMTP và các giao thức khác được dùng bởi Đội hoặc các đối tượng phục vụ.

Kỹ năng chuyên gia: gồm hiểu sâu hơn các khái niệm và các nguyên lý an toàn, các kiến thức chuyên gia về cơ chế và công nghệ dẫn đến các lỗi trong các giao thức, các điểm yếu có thể bị khai thác, các phương pháp khai thác được sử dụng, và biện pháp để giảm nhẹ hoặc loại bỏ các vấn đề tiềm ẩn này. Các chuyên gia cũng cần có hiểu biết chuyên gia về các giao thức hoặc công nghệ internet bổ sung như DNSSEC, IPv6, IPSEC, các tiêu chuẩn viễn thông khác có thể thực thi hoặc giao tiếp với các mạng của đối tượng phục vụ của họ như ATM, BGP hoặc băng rộng, thoại qua internet, công nghệ không dây, các giao thức định tuyến khác, hoặc các công nghệ tích hợp mới, ... và cung cấp các hướng dẫn kỹ thuật cho các thành viên khác của Đội hoặc cho đối tượng phục vụ.

2.1.6 Các ứng dụng và dịch vụ mạng:

Các thành viên của Đội UCSC cần có hiểu biết cơ bản về các ứng dụng và dịch vụ mạng phổ biến mà Đội và đối tượng phục vụ sử dụng như DNS, NFS, SSH, ... Với mỗi ứng dụng hoặc dịch vụ, họ cần hiểu mục đích, cách hoạt động và sử dụng thông thường của nó, cấu hình bảo mật, và các loại nguy cơ hoặc các cách tấn công phổ biến nhằm vào ứng dụng hoặc dịch vụ, cũng như các biện pháp giảm nhẹ các nguy cơ.

Kỹ năng chuyên gia: hiểu biết kỹ thuật mở rộng cho các ứng dụng và các dịch vụ, cũng như các sản phẩm mới có thể tích hợp cho hệ thống thông tin của tổ chức chủ quản hoặc đối tượng phục vụ của Đội. Các chuyên gia cần cung cấp thông tin chi tiết cho các vấn đề an toàn cần được thảo luận, cần xác định hoặc giải quyết khi triển khai cho hệ thống hiện tại hoặc mới, cho các ứng dụng mới, hoặc khi thiết kế kiến trúc mạng. Ở cấp độ chuyên gia, hiểu biết phải kèm theo kinh nghiệm với cả những ứng dụng ít dùng hoặc các dịch vụ khó mà Đội hoặc tổ chức chủ quản hoặc đối tượng phục vụ có thể dùng như triển khai mới các dịch vụ không dây hoặc triển khai hạ tầng khoá công khai cho hệ thống thông tin.

2.1.7 Các vấn đề bảo mật mạng:

Các thành viên của Đợi UCSC cần có hiểu biết cơ bản về các khái niệm bảo mật mạng và có thể phát hiện các điểm yếu trong cấu hình mạng. Họ phải hiểu cơ bản các khái niệm và bảo mật vùng biên của tường lửa mạng (như thiết kế, lọc gói tin, hệ thống chuyển tiếp proxy, DMZ, ...), bảo mật bộ định tuyến, nguy cơ lộ thông tin khi truyền dữ liệu truyền qua mạng, hoặc các nguy cơ liên quan đến việc chấp nhận thông tin chưa tin cậy.

Kỹ năng chuyên gia: các chuyên gia nên có khả năng đoán trước, nhận

dạng, cô lập và mô tả các lỗ hổng mới tiềm ẩn có thể ảnh hưởng đến đối tượng phục vụ hoặc chính Đội ƯCSC do thay đổi thiết kế mạng, phần cứng hoặc phần mềm. Họ cũng có thể xác định và phát triển các công cụ hoặc các tiến trình nhằm giảm nhẹ hoặc giải quyết các điểm yếu bảo mật tiềm ẩn đó.

2.1.8 Các vấn đề bảo mật máy chủ và hệ thống:

Ngoài việc hiểu các vấn đề bảo mật ở cấp độ mạng, thành viên Đội ƯCSC cần phải hiểu các vấn đề bảo mật ở cấp độ máy chủ với nhiều loại hệ điều hành được Đội hoặc đối tượng phục vụ sử dụng như UNIX, Windows hoặc các hệ điều hành khác. Trước khi hiểu các khía cạnh bảo mật, thành viên của Đội phải có:

+ kinh nghiệm sử dụng hệ điều hành và các vấn đề bảo mật của người dùng

+ quen thuộc với việc quản lý và duy trì các hệ điều hành ở mức độ người quản trị

Với mỗi hệ điều hành, thành viên của Đội ƯCSC cần biết cách để:

+ cấu hình hệ thống một cách an toàn

+ xem xét các tập tin cấp hình để phát hiện các điểm yếu bảo mật

+ nhận dạng các phương pháp tấn công phổ biến

+ xem xét có các nỗ lực xâm nhập, thoả hiệp hệ thống hay không?

+ xem xét nếu có thoả hiệp hệ thống thì có thành công hay không?

+ xem xét các tập tin nhật ký log để xác định các bất thường

+ phân tích kết quả của các tấn công

+ quản lý các đặc quyền của hệ thống

+ bảo vệ các daemon (các dịch vụ trên Linux) của mạng

+ khôi phục sau khi bị thoả hiệp

2.1.9 Mã độc hại:

Thành viên Đội ƯCSC phải hiểu tấn công của các loại mã độc khác nhau và ảnh hưởng của chúng đến nạn nhân (thoả hiệp hệ thống, từ chối dịch vụ, mất toàn vẹn dữ liệu, ...). Mã độc có nhiều dạng khác nhau, có thể gây tấn công từ chối dịch vụ hoặc thay đổi web, hoặc mã có thể chứa các nội dung "động" để tự cấu hình các kiểu tấn công đa dạng. Thành viên Đội phải hiểu các kiểu phát tán và tấn công của mã độc như lan truyền qua các phương tiện lưu trự, qua thư điện tử, qua các các chương trình, qua các macro của Word, MIME (Multipurpose Internet Mail Extentions), qua chia sẻ tập tin ngang hàng, hoặc các vi-rút boot-sector ..., các rủi ro và hư hỏng liên quan với các tấn công như vậy, các biện pháp ngăn chặn và giảm nhẹ, các tiến trình phát hiện và gỡ bỏ, và các kỹ thuật khôi phục.

Kỹ năng chuyên gia: chuyên môn thực hiện phân tích, kiểm tra theo phương pháp hộp đen (black box, chủ yếu để xem các hành vi mà không cần phải biết trước về mã độc đó), hoặc kỹ thuật dịch ngược mã độc có liên quan đến các cuộc tấn công và tư vấn cho Đội để phản ứng hiệu quả nhất.

2.1.10 Các kỹ năng lập trình:

Một số thành viên của Đội cần có kinh nghiệm lập trình hệ thống và mạng để Đội có thể nắm được nhiều ngôn ngữ lập trình trên các hệ điều hành mà Đội và đối tượng phục vụ sử dụng. Ví dụ, Đội phải có kinh nghiệm về các ngôn ngữ C, Perl, Python, Awk, Java, shell (mọi phiên bản) và các công cụ viết kịch bản khác. Những công cụ viết kịch bản hoặc lập trình sẽ được dùng để hỗ trợ cho việc phân tích và xử lý thông tin sự cố (ví dụ viết các kịch bản khác nhau để đếm và sắp xếp các nhật ký log khác nhau, tìm kiếm trong các cơ sở dữ liệu, tìm kiếm thông tin, trích thông tin từ các nhật ký hoặc tập tin, thu thập và trộn dữ liệu).

Ngoài ra, thành viên Đội ƯCSC nên hiểu các khái niệm và kỹ thuật lập trình an toàn. Họ cần biết cách mà các điểm yếu có thể đưa vào trong mã (ví dụ qua các thực hành lập trình và thiết kế kém) và cách để tránh những lỗi này trong các công cụ hoặc sản phẩm mà họ phát triển cho Đội hoặc cho đối tượng phục vụ của họ.

Kỹ năng chuyên gia: kỹ năng chuyên môn về phát triển và lập trình phần mềm bằng nhiều ngôn ngữ. Chuyên môn của các chuyên gia sẽ hỗ trợ người phụ trách kỹ thuật, tư vấn hoặc hướng dẫn cho các thành viên khác trong Đội.

2.2 Các kỹ năng xử lý sự cố:

"Xử lý sự cố" là tập hợp các kỹ năng cần thiết liên quan đến các hoạt động hàng ngày của các thành viên Đội ƯCSC. Tuy nhiên, cần lưu ý rằng mặc dù các khái niệm cơ bản liên quan đến xử lý sự cố có thể tương tự nhau ở nhiều Đội ƯCSC, nhưng việc thực hiện, các chính sách và quy trình cụ thể của những khái niệm này sẽ khác nhau với mỗi Đội.

2.2.1 Các chính sách và quy trình nội bộ của Đội ƯCSC:

Những người xử lý sự cố của Đội ƯCSC phải được huấn luyện các chính sách và quy trình nội bộ chi phối hoạt động của đội. Mọi khía cạnh của công việc sẽ được gắn với việc tuân thủ một chính sách hoặc quy trình nào đó hoặc theo hướng dẫn của cấp quản lý. Nhân viên Đội ƯCSC cần các thông tin cơ bản này và phải nắm vững các nguyên tắc hướng dẫn, nếu không họ sẽ không hiểu được những kỹ năng và kiến thức trong khuôn khổ và ranh giới đó. Mọi thành viên của Đội ƯCSC phải có khả năng hỗ trợ các chính sách và các quy trình này, không chỉ ở cấp độ của Đội mà còn ở cấp độ của tổ chức chủ quản, hoặc thậm chí liên quan đến đối tượng mà họ phục vụ.

2.2.2 Hiểu biết, xác định các kỹ thuật xâm nhập:

Mọi thành viên xử lý sự cố của Đội ƯCSC phải có thể nhận biết các kỹ thuật xâm nhập dựa trên dấu chân (footprint) hoặc các công cụ để lại trong các kiểu tấn công khác nhau trong sự cố mà họ xử lý. Hơn nữa, họ cần biết các phương pháp phù hợp để bảo vệ chống lại các kỹ thuật tấn công đã biết và các rủi ro liên quan đến các tấn công đó.

Với dữ liệu sự cố thực tế, người xử lý sự cố phải dùng các kiến thức của họ để xác định loại tấn công, nhận biết các công cụ hoặc bộ công cụ sử dụng, các kỹ thuật, hoặc các mã độc hại đã dùng. Với mỗi loại tấn công, họ phải biết các rủi ro và ảnh hưởng liên quan, mức độ nghiêm trọng tương ứng, và các phương pháp giảm nhẹ, ngăn chặn và khôi phục.

Một kỹ năng xử lý sự cố quan trọng khác là phân tích tương quan giữa các sự cố để thông báo những gì chưa từng được biết trước đó như kỹ thuật tấn công, dấu chân, công cụ xâm nhập, phương tiện tấn công mới. Việc xác định được các hoạt động bất thường hoặc không mong muốn có thể giúp nhận diện các tấn công mới hoặc lỗ hổng tiềm ẩn để đảm bảo cho việc điều tra hoặc phân tích về sau, có thể được thực hiện bởi các thành viên cao cấp của Đội hoặc các chuyên gia khác.

Kỹ năng chuyên gia: các kỹ năng và kiến thức để có thể:

+ xác định một lỗ hổng mới

+ phân tích kỹ thuật về các công cụ và kỹ thuật xâm nhập

+ nhận biết các kỹ thuật xâm nhập mới dựa trên các dấu chân và ảnh hưởng của chúng

+ phân tích tài liệu của các chương trình để làm tham khảo cho các thành viên khác trong Đội. Công việc này cũng có thể mở rộng để cung cấp hướng dẫn giúp các nhân viên khác của Đội xác định dấu chân, các rủi ro liên quan và phương pháp phòng ngừa.

2.2.3 Giao tiếp với các nơi:

Phần lớn các giao tiếp của các thành viên xử lý sự cố của Đội ƯCSC được thực hiện trực tuyến, thường là qua thư điện tử nên yêu cầu cơ chế truyền dữ liệu sự cố phải an toàn. Vì vậy, thành viên Đội ƯCSC phải thông thạo sử dụng thư điện tử và tính năng MIME, cũng như các công cụ và các phương pháp để nhận diện liên lạc với các nơi khác và sử dụng các kỹ thuật mã hoá phù hợp.

Họ cũng cần hiểu về chức năng và cách sử dụng của các công cụ khác nhau tạo điều kiện thuận lợi cho việc xem xét và giải thích dữ liệu sự cố (các định dạng và công cụ nén tập tin, các công cụ lưu trữ như tar của UNIX hoặc WinZIP, uuencode/decode, ...). Ngoài ra, điều quan trọng là phải đảm bảo rằng các nhân viên xử lý sự cố nhận thức rõ về các kiểu phối hợp khi tương tác trong

nội bộ và ra bên ngoài như số lượng thông tin được chia sẻ và cách thức chia sẻ thông tin trong khi vẫn tuân thủ các chính sách và quy trình tiết lộ thông tin của Đội.

2.2.4 Phân tích sự cố:

Phân tích báo cáo sự cố nhằm tìm trả lời cho các câu hỏi như:

+ Ai tham gia?

+ Điều gì đã xảy ra?

+ Tấn công bắt nguồn từ đâu?

+ Khi nào (múi giờ nào)?

+ Tại sao nó xảy ra?

+ Hệ thống có lỗ hổng như thế nào hoặc tấn công đã xảy ra như thế nào?

+ Lý do tấn công là gì?

Người phân tích cần xác định những thông tin quan trọng nào bị thiếu, cần làm rõ ở đâu, hiệu quả và phạm vi hoạt động. Khi có thể, họ nên xác định các công cụ hoặc kiểu cuộc tấn công được sử dụng, mức độ truy nhập đã có được, khung giờ, thiệt hại hoặc các liên luỵ từ cuộc tấn công, các máy/các khu vực bị liên đới.

Thành viên Đội ƯCSC phải biết được tầm quan trọng của các hoạt động liên quan đến các ưu tiên của đội, cũng như xác định các phản ứng thích hợp. Hơn nữa, họ cần phân tích các báo cáo hoạt động sự cố mới để xem liệu các báo cáo này có liên quan nào đến các báo cáo khác hay không, vì dụ liên quan đến thời gian tấn công, các nhận dạng của tấn công, các lỗ hổng nào đã bị khai thác, … và để xác định xu hướng hoặc các hoạt động tương tự có thể ảnh hưởng đến đối tượng họ phục vụ.

Kỹ năng chuyên gia: phân tích sâu của các công cụ, các kịch bản và các mẫu vật khác được phát hiện trong quá trình xử lý sự cố mà các nhân viên của Đội ƯCSC chưa xác định được. Phân tích này cũng có thể gồm phân tích điều tra số hoặc thu thập dữ liệu để dùng điều tra tội phạm. Sự hỗ trợ chuyên môn này có thể yêu cầu kiểu khai thác dịch ngược và/hoặc xem xét mã nguồn.

2.2.5 Bảo quản các hồ sơ sự cố:

Dù điều này không phải là một kỹ năng như các kỹ năng khác trong phần này, nhưng đây là một phần quan trọng cần phải tích hợp vào các hoạt động của Đội ƯCSC và được mọi thành viên có trách nhiệm xử lý sự cố phải tuân theo. Để đảm bảo rằng mọi hồ sơ được bảo quản tốt, mọi thành viên xử lý sự cố của Đội phải hiểu về các kỹ thuật được dùng để bảo quản các hồ sơ báo cáo sự cố, thông tin hỗ trợ và các tập tin liên quan. Các hồ sơ sự cố phải được ghi chép đầy đủ, duy trì nhất quán để cung cấp một hình ảnh rõ ràng về tình hình hoạt động

hiện tại và những công việc vẫn còn duy trì. Giữ hồ sơ tốt là cũng là tạo điều kiện thuận lợi khi chuyển giao hoặc bàn giao giữa các thành viên trong Đội.

PHỤ LỤC 02

CÁC KỸ NĂNG KỸ THUẬT CHUYÊN SÂU CHO CÁC CHỨC DANH ĐỘI ƯCSC

(Ban hành kèm theo thông tư số /2018/TT-BTTTT ngày / /2018 của Bộ Thông tin và Truyền thông)

STT	Vị trí	Kỹ năng	Chứng chỉ	
			QT	VN
1.	Lãnh đạo Đội ƯCSC (đội trưởng, đội phó)	Người đứng đầu của Đội ƯCSC phải có nền tảng và phải có các kỹ năng kỹ thuật tốt như nhân viên dưới quyền. Các kỹ năng này bao gồm: - Phương pháp và thực hành chiến lược công nghệ thông tin, kiến trúc doanh nghiệp và kiến trúc bảo mật - Các khái niệm về bảo mật liên quan đến DNS, routing, xác thực, VPN, các dịch vụ proxy, và các kỹ thuật giảm thiểu DDoS - Có nền tảng của ISO27002, ITIL và COBIT - Đánh giá sự phù hợp của PCI, HIPAA, NIST, GLBA và SOX - Hệ điều hành Windows, UNIX và Linux - Ngôn ngữ lập trình C, C++, C#, Java và/hoặc PHP - Các giao thức tường lửa, phát hiện/chống xâm nhập - Khả năng lập trình bảo mật, hacker mũ trắng và mô hình các nguy cơ - TCP/IP, mạng máy tính, định tuyến (routing) và chuyển mạch (switching) - Định nghĩa và phát triển kiến trúc bảo mật mạng - Kiến thức về kiểm toán bảo mậtcủa các bên thứ ba và phương pháp đánh giá các rủi ro trên cloud. - Tổ chức và hoạt động của Đội	CEH CISSP CISM; ECIH	- An toàn thông tin cơ bản cho cán bộ kỹ thuật - An toàn thông tin nâng cao cho cán bộ kỹ thuật - An toàn thông tin dành cho cán bộ quản lý; - Ứng cứu sự cố an toàn thông tin

		ƯCSC - Cơ bản các phương pháp phòng chống tấn công mạng **Kỹ năng mềm** - Kỹ năng nói và truyền thông, kỹ năng về tổ chức, tư duy định hướng theo tiến trình, lập kế hoạch chiến lược và sáng tạo - Kỹ năng giao tiếp và đàm phán, cần thiết cho việc chỉ đạo một đội, cộng tác với các nhà điều hành cấp cao và xây dựng mối quan hệ với các tổ chức, đơn vị, phòng ban khác trong tổ chức hoặc tương tác với các bên ngoài của tổ chức		
2.	Chuyên viên điều phối ứng cứu Sự cố	**Kỹ năng cứng** - Am hiểu về quy định, pháp luật về an toàn thông tin, ứng cứu sự cố - Am hiểu về các quy trình ứng cứu sự cố - Có kiến thức về hệ điều hành Windows, UNIX và Linux - Am hiểu về các ngôn ngữ lập trình như: C, C++, C#, Java, ASM, PHP, PERL - Có kiến thức TCP/IP, mạng máy tính, định tuyến (routing) và chuyển mạch (switching) - Am hiểu về hệ thống phần cứng và phần mềm máy tính - Biết cài đặt, cấu hình và vá lỗi hệ điều hành - Có kỹ năng về sao lưu và phục hồi dữ liệu, - Có kiến thức về an toàn ứng dụng và bảo mật ứng dụng Web - Hiểu biết về các kiểu tấn công cơ bản và cách khắc phục	Security+: CEH; ECIH	- An toàn thông tin cơ bản cho cán bộ kỹ thuật - An toàn thông tin nâng cao cho cán bộ kỹ thuật - Ứng cứu sự cố an toàn thông tin - An toàn hạ tầng mạng - An toàn ứng dụng - Lập trình an toàn

		Kỹ năng mềm - Kỹ năng nói và truyền thông, - Kỹ năng xử lý và giải quyết vấn đề. - Kỹ năng giao tiếp và đàm phán, quan hệ với các tổ chức, đơn vị, phòng ban khác trong tổ chức hoặc tương tác với các bên ngoài của tổ chức.		
3.	Chuyên viên phân tích và ứng phó sự cố	**Kỹ năng cứng:** - Có kiến thức TCP/IP, mạng máy tính, định tuyến (routing) và chuyển mạch (switching) - Có kiến thức về hệ điều hành Windows, UNIX và Linux - Am hiểu về các ngôn ngữ lập trình như: C, C++, C#, Java, ASM, PHP, PERL - Biết cài đặt, cấu hình và vá lỗi hệ điều hành - Có kỹ năng về sao lưu và phục hồi dữ liệu, mật mã học - Có kiến thức về bảo mật ứng dụng Web - Thành thạo các phần mềm phân tích mã độc, phân tích dữ liệu mạng, phân tích logfile (Wireshark, Process_xp.exe, Procmon.exe, IDA…) - Thành thạo các ứng dụng phần mềm điều tra số (EnCase, FTK, Helix, Cellebrite, XRY, ...) - Hiểu biết về điện toán đám mây - Biết xây dựng ƯCSC	CEH; ECIH; CHFI; GCFE; GCFA; CCFE; CPT; CREA;	An toàn thông tin cho cán bộ kỹ thuật; Phân tích mã độc; Ứng cứu sự cố ATTT; Đánh giá ATTT; Điều tra số;
4.	Chuyên viên ATTT	**Kỹ năng cứng** - IDS/IPS, đánh giá thâm nhập lỗ hổng bảo mật. - Firewall và các giao thức dò/ngăn chặn xâm nhập. - DLP, antivirus, phòng chống malware.	Security+: cation CCNA:– CEH: GSEC / GCIH / GCIA: CISSP:	- An toàn thông tin cơ bản cho cán bộ kỹ thuật - An toàn thông tin

		- Mã hóa, các mô hình tấn công mới. - Hệ điều hành Window, Unix, Linux. - TCP/IP, mạng máy tính, định tuyến và chuyển mạch. - Ngôn ngữ lập trình C, C++, C#, Java hoặc PHP. - Giải pháp SIEM. - ISO 27001 / 27002, ITIL và COBIT. - PCI, HIPAA, NIST, GLBA và SOX. **Kỹ năng mềm** - Kỹ năng làm việc độc lập hoặc theo nhóm. - Cần có kỹ năng thuyết trình và giao tiếp tốt, - Có khả năng nghiên cứu, tìm hiểu, phân tích và giải quyết những vấn đề kỹ thuật phức tạp.	ECSA	nâng cao cho cán bộ kỹ thuật - Quản lý an toàn thông tin - Đánh giá an toàn thông tin - An toàn hạ tầng mạng - An toàn ứng dụng - Lập trình an toàn
5.	Chuyên viên kiểm tra, đánh giá an toàn	**Kỹ năng cứng:** - Có nền tảng của ISO 27001/27002, NIST, HIPPA, SOX, … - IDS/IPS, kiểm tra thâm nhập và lỗ hổng. - Firewall và các giao thức dò/ngăn chặn xâm nhập. - DLP, antivirus, phòng chống malware. - Hệ điều hành Window, Unix, Linux. - TCP/IP, mạng máy tính, định tuyến và chuyển mạch. - Giao thức mạng và phân tích gói tin. - Ngôn ngữ lập trình C, C++, C#, Java hoặc PHP. - Điện toán đám mây. - Các mô hình SaaS. - Giải pháp SIEM. **Kỹ năng mềm:**	CEH; CISA; CISM; CISSP; CEPT; CISSP;	- An toàn thông tin cơ bản cho cán bộ kỹ thuật - An toàn thông tin nâng cao cho cán bộ kỹ thuật - Quản lý an toàn thông tin - Đánh giá an toàn thông tin - Đánh giá và kiểm thử an toàn

		- Có khả năng làm việc nhóm và độc lập. - Có kỹ năng giao tiếp, trình bày, tổng hợp, phân tích v.v…		thông tin
6.	Chuyên viên Kiểm thử xâm nhập	**Kỹ năng cứng** - Hệ điều hành Windows, UNIX và Linux - Ngôn ngữ lập trình C, C++, C#, Java ASM, PHP, PERL - Sử dụng các công cụ đánh giá hệ thống mạng (ví dụ: Nessus, nmap, Burp, ...) - Hiểu biết về phần cứng và phần mềm máy tính; - Ứng dụng web ; - Có nền tảng của ISO 27001/27002, NIST, HIPPA, SOX, … - Sử dụng các công cụ và sản phẩm bảo mật (Fortify, AppScan, …) - Phân tích lỗ hổng và kỹ thuật dịch ngược - Sử dụng Metasploit - Các công cụ điều tra số - Các nguyên lý mật mã **Kỹ năng mềm** - Có khả năng làm việc nhóm, độc lập, chịu được áp lực cao. - Có kỹ năng giao tiếp, trình bày, tổng hợp, phân tích v.v…	CEH; CPT; CEPT; GPEN; OSCP; CREA; GCFE	- An toàn thông tin cơ bản cho cán bộ kỹ thuật - An toàn thông tin nâng cao cho cán bộ kỹ thuật - Đánh giá và kiểm thử an toàn thông tin - An toàn hạ tầng mạng - An toàn ứng dụng - Lập trình an toàn
7.	Chuyên viên Điều tra số	**Kỹ năng cứng** - Có kiến thức TCP/IP, mạng máy tính, định tuyến (routing) và chuyển mạch (switching) - Có kiến thức về hệ điều hành Windows, UNIX và Linux - Am hiểu về các ngôn ngữ lập trình như: C, C++, C#, Java, ASM, PHP,	CEH; CHFI; CCE; GCFE; GCFA; GCIH; CCFE; CPT; CREA	An toàn thông tin cơ bản cho cán bộ kỹ thuật; An toàn thông tin nâng cao cho cán bộ

		PERL - Am hiểu về hệ thống phần cứng và phần mềm máy tính - Biết cài đặt, cấu hình và vá lỗi hệ điều hành - Có kỹ năng về sao lưu và phục hồi dữ liệu, mật mã học - Có kiến thức về bảo mật ứng dụng Web - Am hiểu các ứng dụng phần mềm điều tra số (EnCase, FTK, Helix, Cellebrite, XRY, ...) - Biết về điện toán đám mây - Biết xây dựng qui trình xử lý bằng chứng **Kỹ năng mềm** - Phải có đầu óc ưa tìm hiểu và luôn luôn suy nghĩ như tội phạm để hiểu tội phạm thì mới có thể bắt được tội phạm - Có khả năng giao tiếp tốt - Có khả năng viết báo cáo, bảo vệ và diễn giải chứng cứ - Có khả năng trình bày rõ ràng, dễ hiểu kết quả chứng cứ điều tra.		kỹ thuật; Điều tra số; Phân tích mã độc; Đánh giá và kiểm thử an toàn thông tin

PHỤ LỤC 03

CHỨNG CHỈ TRONG NƯỚC VÀ QUỐC TẾ VỀ AN AN TOÀN THÔNG TIN - ỨNG CỨU SỰ CỐ

(Ban hành kèm theo thông tư số /2018/TT-BTTTT ngày / /2018 của Bộ Thông tin và Truyền thông)

1. Các chứng chỉ trong nước:

- An toàn thông tin cơ bản cho cán bộ kỹ thuật
- An toàn thông tin nâng cao cho cán bộ kỹ thuật
- An toàn thông tin cho cán bộ quản lý
- Quản lý an toàn thông tin
- Đánh giá an toàn thông tin và ứng dụng web
- Điều tra số cơ bản
- Phân tích mã độc cơ bản
- Phân tích mã độc nâng cao
- Ứng cứu sự cố an toàn thông tin
- Ứng cứu sự cố an toàn thông tin nâng cao
- An toàn hạ tầng mạng
- An toàn ứng dụng
- Lập trình an toàn
- Tổ chức và vận hành các đội ứng cứu sự cố CSIRT

2. Các chứng chỉ quốc tế:

- CISA: Certified Information Systems Auditor
- CISM: Certified Information Security Manager
- Security+: CompTIA's popular base-level security certification
- CEH: Certified Ethical Hacker
- CISSP: Certified Information Systems Security Professional
- ECSA: EC-Council Certified Security Analyst
- Security+: CompTIA's popular base-level security certification
- CISM: Certified Information Security Manager
- CPT: Certified Penetration Tester
- CEPT: Certified Expert Penetration Tester
- GSEC: GIAC Security Certifications
- GPEN: GIAC Certified Penetration Tester
- GCIH: GIAC Certified Incident Handler
- GCFE: GIAC Certified Forensic Examiner
- GCFA: GIAC Certified Forensic Analyst
- CCFE: Certified Computer Forensics Examiner
- CREA: Certified Reverse Engineering Analyst
- CHFI: Computer Hacking Forensic Investigator
- ECIH: EC-Council Certified Incident Handler

PHỤ LỤC 04

CHƯƠNG TRÌNH KHUNG ĐÀO TẠO CHỨNG CHỈ VỀ ỨNG CỨU SỰ CỐ

(Ban hành kèm theo thông tư số /2018/TT-BTTTT ngày / /2018 của Bộ Thông tin và Truyền thông)

1. An toàn thông tin cơ bản cho cán bộ kỹ thuật:

STT	NỘI DUNG
1	**Tổng quan về các vấn đề kỹ thuật**
1.1	Khái niệm cơ bản trong lĩnh vực an toàn thông tin
1.2	Công nghệ, xu hướng mới cần quan tâm trong lĩnh vực an toàn thông tin
1.3	Lỗ hổng, điểm yếu an toàn thông tin và một số kỹ thuật tấn công phổ biến
1.4	Giải pháp, công cụ bảo đảm an toàn thông tin thông dụng
1.5	Hệ thống tiêu chuẩn, quy chuẩn kỹ thuật và đạo đức nghề nghiệp an toàn thông tin
1.6	Hệ thống tổ chức quản lý về an toàn thông tin tại Việt Nam
1.7	Thực hành: Khai thác lỗ hổng, điểm yếu an toàn thông tin để tấn công, xâm nhập hệ thống.
2	**Bảo đảm an toàn hạ tầng mạng**
2.1	Quy trình xây dựng hệ thống an toàn thông tin
2.2	Thiết kế và thực thi hệ thống vành đai bảo vệ, hệ thống tường lửa, mạng riêng ảo, hệ thống giám sát, phát hiện và ngăn chặn xâm nhập trái phép
2.3	Các yêu cầu và giải pháp đảm an toàn vật lý và hệ thống dữ liệu
2.4	Yêu cầu và giải pháp giám sát đảm bảo an toàn hạ tầng mạng
2.5	Thực hành: Thiết kế mạng an toàn; thiết lập, cài đặt hệ thống tường lửa, hệ thống giám sát, phát hiện và ngăn chặn xâm nhập trái phép
3	**Bảo đảm an toàn hệ điều hành**
3.1	Thành phần bảo đảm an toàn thông tin cho hệ điều hành
3.2	Cài đặt, cấu hình, thiết lập chính sách đảm bảo an toàn cho hệ điều hành
3.3	Quản lý, vận hành an toàn hệ điều hành
3.4	Kiểm tra đánh giá an toàn thông tin cho hệ điều hành

3.5	Thực hành: Cài đặt thử nghiệm, cấu hình an toàn, kiểm tra đánh giá an toàn thông tin cho hệ điều hành máy chủ Windows và Linux.
4	**Bảo đảm an toàn ứng dụng web, thư điện tử**
4.1	Thành phần bảo đảm an toàn thông tin cho ứng dụng web, thư điện tử
4.2	Cấu hình, thiết lập chính sách và giải pháp bảo đảm an toàn cho dịch vụ web và thư điện tử
4.3	Các công cụ thiết kế và cấu hình môi trường mạng an toàn cho máy chủ web và thư điện tử
4.4	Quản lý, vận hành an toàn máy chủ web và thư điện tử
4.5	Kiểm tra, đánh giá an toàn thông tin cho ứng dụng web và thư điện tử
4.6	Thực hành: Thử nghiệm kiểm tra, đánh giá an toàn ứng dụng web/thư điện tử và áp dụng các biện pháp bảo đảm an toàn cho ứng dụng web/thư điện tử
5	**Phòng, chống phần mềm độc hại**
5.1	Khái niệm, phân loại phần mềm độc hại
5.2	Công cụ, giải pháp phát hiện và gỡ bỏ phần mềm độc hại
5.3	Thực hành: Sử dụng công cụ để rà quét và gỡ bỏ phần mềm độc hại trên máy tính, máy chủ và hệ thống
6	**Kiểm tra, đánh giá an toàn thông tin**
6.1	Xác định yêu cầu kiểm tra, đánh giá an toàn thông tin
6.2	Quy trình kiểm tra đánh giá an toàn thông tin
6.3	Công cụ, giải pháp, kỹ năng kiểm tra đánh giá an toàn thông tin
6.4	Thực hành: Xác định yêu cầu kiểm tra đánh giá an toàn thông tin cho hệ thống thông tin; thực nghiệm sử dụng công cụ để thực hành kiểm tra đánh giá an toàn thông tin.
7	**Thảo luận, kiểm tra, đánh giá kết quả**
7.1	Thảo luận, tham quan thực tế
7.2	Kiểm tra, đánh giá kết quả

2. An toàn thông tin nâng cao cho cán bộ kỹ thuật:

STT	NỘI DUNG
1	Một số kỹ năng đảm bảo an toàn thông tin cơ bản

1.1	Quản lý mật khẩu, thiết lập và quản lý dịch vụ, chia sẻ dữ liệu, quản lý người dùng, phân quyền, thiết lập Firewall hệ thống, thiết lập chính sách an ninh
1.2	Kiểm tra các dịch vụ và hệ thống
1.3	Quản lý cài đặt các phần mềm ứng dụng, các bản vá lỗi, cập nhật hệ thống, sao lưu dữ liệu, khắc phục sự cố
1.4	Kết nối Internet an toàn
1.5	Sử dụng các trình duyệt an toàn
1.6	Bảo vệ tài khoản và hộp thư cá nhân
1.7	Xử lý cảnh báo, sự cố và phản ứng sự cố thông thường bằng các công cụ và phương pháp thủ công
2	**Kỹ thuật nhận dạng và ngăn chặn tấn công**
	Nhận dạng tấn công và ngăn chặn tấn công: Active attacks (DoS, SYN, Spoofing, …); Passive attacks (scanning, sniffing, …); Password attacks; Malicious code attacks (Virus, Trojan, worm, War dialing, Dumpster Diving, Sniffer, Trojan Horses, Back doors, Worms, ...).
3	**Xác định cấu trúc Web và đảm bảo an toàn**
3.1	Hoạt động của cổng TTĐT
3.2	Mô hình các lớp trong kiến trúc Web
3.3	Vì sao phải phân chia các lớp
3.4	Các kiến trúc thường gặp
3.5	Khuyến cáo sử dụng
4	**Triển khai hệ thống phòng thủ**
4.1	Tường lửa ứng dụng Web (WAF - Web Application Firewall)
4.2	Tường lửa (Firewall)
4.3	Tổ chức mô hình mạng hợp lý
4.4	Hệ thống phát hiện xâm nhập (IDS - Intrusion Detection System)
4.5	Hệ thống ngăn chặn xâm nhập (IPS - Intrusion Prevention System)
5	**Thiết lập và cấu hình hệ thống máy chủ an toàn**
5.1	Hệ thống máy chủ Windows
5.2	Hệ thống máy chủ Linux
5.3	Máy chủ Web – IIS

5.4	Máy chủ Web - Apache HTTP
5.5	Máy chủ Web - Apache Tomcat
6	**Vận hành ứng dụng web an toàn**
6.1	Kiểm tra hoạt động web an toàn
6.2	10 lỗi phổ biến trên web và cách phòng chống
7	**Thiết đặt và cấu hình cơ sở dữ liệu an toàn**
7.1	An toàn cho cơ sở dữ liệu MS SQL
7.2	An toàn cho cơ sở dữ liệu MySQL
8	**Cài đặt các ứng dụng bảo vệ**
8.1	Anti-virus
8.2	Host Based IDS
9	**Thiết lập cơ chế sao lưu và phục hồi**
9.1	Cơ chế sao lưu
9.2	Cơ chế phục hồi
9.3	Một số hệ thống thường gặp
10	**Mạng không dây và các vấn đề an toàn thông tin**
10.1	Giới thiệu về các chuẩn trong mạng wifi cũng như các lỗ hổng có thể có trong mạng wifi
10.2	Biện pháp phòng chống tấn công vào mạng wifi
10.3	Trình diễn một số kỹ thuật tấn công vào mạng wifi
11	**Mã độc**
11.1	Định nghĩa về các loại trojan, backdoor, virus và worm
11.2	Trình diễn về mã độc
11.3	Trình diễn cách thức hoạt động của một số loại mã độc và cách thức phát hiện chúng
11.4	Biện pháp phòng tránh
12	**Các hệ thống phòng thủ**
12.1	IDS/IPS
12.2	Firewall
12.3	Honeypot
13	**Khai thác lỗ hổng**
13.1	Giới thiệu Ethical Hacking

13.2	Hacking Laws
13.3	Footprinting
13.4	Google Hacking
13.5	Scanning
13.6	Enumeration
13.7	System Hacking
13.8	Trojans and Backdoors
13.9	Virus and Worms
13.10	Sniffers
13.11	Social engineering
13.12	Phishing
13.13	Hacking Email Accounts
13.14	Denial-of-Service
13.15	Session Hijacking

3. An toàn thông tin cho cán bộ quản lý:

TT	NỘI DUNG
1	**Tổng quan về quản lý**
1.1	Sự khác nhau giữa quản lý và lãnh đạo
1.2	Nhiệm vụ trọng tâm của nhà quản lý
1.3	Vai trò của cán bộ quản lý về an toàn thông tin
1.4	Thảo luận: Các bài học, kinh nghiệm thực tiễn về quản lý an toàn thông tin
2	**Không gian mạng**
2.1	Tổng quan về không gian mạng
2.2	Sơ lược về mạng Internet
2.3	Xu hướng phát triển của không gian mạng
2.4	Các nguy cơ về an toàn thông tin trên không gian mạng
2.5	Hiện trạng và xu hướng không gian mạng tại Việt Nam
2.6	Thảo luận: Không gian mạng và các nguy cơ, thách thức mới
3	**An toàn thông tin**

3.1	Khái niệm và tính chất
3.2	Điểm yếu, lỗ hổng an toàn thông tin
3.3	Các phương thức tấn công mạng phổ biến
3.4	Thảo luận: Phân biệt một số nội dung có liên quan và hay nhầm lẫn với an toàn thông tin
4	**Quản lý nhà nước về an toàn thông tin**
4.1	Hành lang pháp lý
4.2	Hệ thống tổ chức
4.3	Hệ thống tiêu chuẩn
4.4	Tổng quan tình hình an toàn thông tin Việt Nam
4.5	Thảo luận: Đánh giá các nguy cơ về an toàn thông tin của địa phương, tổ chức chủ quản của học viên
5	**Bảo đảm an toàn thông tin**
5.1	Chủ động rà soát, chuẩn bị
5.2	Triển khai biện pháp bảo vệ
5.3	Phát hiện, cảnh báo sớm
5.4	Phản hồi và xử lý
5.5	Khắc phục sự cố
5.6	Thảo luận: Tấn công mạng nhằm vào một mục tiêu xác định
6	**Tham quan, thảo luận, kiểm tra đánh giá kết quả**
6.1	Tham quan thực tế, thảo luận các nội dung
6.2	Kiểm tra, đánh giá kết quả

4. Quản lý an toàn thông tin:

STT	NỘI DUNG
1	**Điều khiển truy cập vào các hệ thống thông tin**
1.1	Kiểm soát truy cập dữ liệu
1.2	Kiểm soát truy cập hệ thống
1.3	Xác định phương pháp quản lý kiểm soát truy cập
1.4	Thực hiện kiểm thử xâm nhập
2	Các hệ thống viễn thông và mạng
2.1	Thiết kế mạng dữ liệu

2.2	Cung cấp truy cập xa vào các mạng dữ liệu
2.3	Bảo mật mạng dữ liệu
2.4	Quản lý mạng dữ liệu
3	**Quản lý Bảo mật thông tin**
3.1	Xác định các mục tiêu quản lý bảo mật
3.2	Phân loại thông tin
3.3	Phát triển các chương trình an toàn
3.4	Quản lý rủi ro
4	**An toàn cho ứng dụng**
4.1	Thực hiện quản lý cấu hình của phần mềm
4.2	Thực thi các kiểm soát phần mềm
4.3	Bảo mật các hệ thống cơ sở dữ liệu
5	**Mã hóa**
5.1	Áp dụng mã hóa cơ bản
5.2	Chọn phương pháp mã hóa khóa đối xứng
5.3	Chọn phương pháp mã hóa khóa bất đối xứng
5.4	Xác định bảo mật cho thư điện tử
5.5	Xác định bảo mật Internet
6	**An toàn cho kiến trúc hệ thống**
6.1	Đánh giá các mô hình bảo mật
6.2	Chọn kiểu bảo mật
6.3	Cung cấp đảm bảo cho hệ thống
7	**Thực thi các hoạt động bảo mật**
7.1	Kiểm soát an toàn cho vận hành
7.2	Kiểm tra và giám sát các hệ thống
7.3	Xử lý các nguy cơ và vi phạm
8	**Đảm bảo hệ thống vận hành ổn định và kế hoạch dự phòng**
8.1	Duy trì các tiến trình hoạt động
8.2	Thực hiện phân tích các ảnh hưởng đến hoạt động
8.3	Xác định chiến lược khôi phục thảm họa
8.4	Kiểm tra kế hoạch khôi phục thảm họa

9	**Đảm bảo an toàn vật lý**
9.1	Kiểm soát ra vào
9.2	Giám sát ra vào
9.3	Thiết lập các biện pháp an toàn vật lý
9.4	Thiết kế an toàn cho các khu vực
10	**Các vấn đề pháp lý / pháp luật về an toàn thông tin**
10.1	Giải thích các luật và các quy định về tội phạm máy tính
10.2	Áp dụng vòng đời của bằng chứng
10.3	Thực hiện việc điều tra
10.4	Xác định các quy tắc ứng xử

5. Đánh giá an toàn hệ thống thông tin và ứng dụng web:

STT	NỘI DUNG
1	**Tổng quát về lập kế hoạch, phạm vi và khảo sát** *(Comprehensive Pen Test Planning, Scoping, and Recon)*
1.1	
2	**Quét sâu** *(In-Depth Scanning)*
3	**Khai thác** *(Exploitation)*
4	**Các hành động Sau khai khác** *(Post-Exploitation and Merciless Pivoting)*
5	**Tấn công sâu mật khẩu và đánh giá các ứng dụng *web*** *(In-Depth Password Attacks and Web App Pen Testing)*
6	Kiểm tra kết quả đánh giá, báo cáo, hội thảo *(Penetration Test & Capture the Flag Workshop)*

6. Điều tra số:

STT	NỘI DUNG
1	**Kỹ thuật điều tra số trên Windows và xử lý dữ liệu nâng cao**
1.1	
2	**Điều tra số trên nền tảng Windows – Phần 1: Điều tra số và phân tích Registry Windows**
3	**Điều tra số trên nền tảng Windows – Phần 2: thiết bị USB, Shell và tìm kiếm các từ khoá**
4	**Điều tra số trên nền tảng Windows – Phần 3: Email, các tác động thêm vào của người dùng và Nhật ký sự kiện**
5	**Điều tra số trên nền tảng Windows – Phần 1: Điều tra trình duyệt web – Firefox, Internet Explorer, Chrome**

7. Phân tích mã độc cơ bản:

STT	NỘI DUNG
1	**Tổng quan về phân tích mã độc**
1.1	Phân tích mã độc là gì ?
1.2	Mục đích phân tích mã độc
2	**Giới thiệu và xây dựng môi trường phân tích mã độc**
2.1	Cài đặt máy ảo (VMWare hoặc VirtualBox)
2.2	Cài đặt môi trường Windows, Linux
2.3	Cấu hình mạng giữa các môi trường
2.4	Cơ chế trao đổi tập tin giữa các môi trường
2.5	Môi trường phân tích Surface/Runtime và Static Analysis
3	**Giới thiệu và xây dựng môi trường thu thập mã độc**
3.1	Giới thiệu mô hình thu thập mã độc
3.2	Cách thức phân loại mã độc
3.3	Cách thức lữu trữ mã độc
3.4	Cách thức chia sẻ mã độc
4	**Thực hành xây dựng môi trường phân tích mã độc**
5	**Surface Analysis**
5.1	Giới thiệu Surface Analysis
5.2	Công cụ sử dụng

5.3	Thực hành Surface Analysis
6	**Runtime Analysis**
6.1	Giới thiệu Runtime Analysis
6.2	Môi trường Runtime Analysis
6.3	Công cụ sử dụng
6.4	Thực hành Runtime Analysis
7	**Kỹ thuật phân tích mã độc trong JavaScript**
7.1	Cách thức thu thập mã độc từ Website và phân tích Javascript
7.2	Giới thiệu các công cụ bổ trợ phân tích JavaScript
7.3	JavaScript deobfuscation
7.4	Thực hành JavaScript Analysis
8	**Giới thiệu ngôn ngữ Assembly**
8.1	Thực hành đọc mã Assembly
9	**Static Analysis**
9.1	Giới thiệu Static Analysis và công cụ
9.2	Giới thiệu IDAPro và các plugin (IDA python)
9.3	Thực hành Static Analysis
10	**Theo dõi và quản lý mã độc**
10.1	Báo cáo về mã độc
10.2	Cách thức chia sẻ kết quả phân tích mã độc

7. Phân tích mã độc nâng cao:

STT	NỘI DUNG
1	**Tổng quan phân tích mã độc hại (Ôn tập nội dung phân tích mã độc hại cơ bản)**
1.1	Mục đích phân tích mã độc hại
1.2	Các kỹ thuật phân tích mã độc hại
1.3	Các kiểu (loại) mã độc hiện nay
1.4	Những nguyên tắc chung khi thực hiện phân tích mã độc
1.5	Kỹ thuật phân tích mã thực thi mã độc cơ bản.
1.6	Phân tích mã độc trên Virtual Machines
1.7	Kỹ thuật phân tích hành vi mã độc cơ bản.
2	**Thực hành phân tích mã độc hại với các kỹ thuật cơ bản**
2.1	Thực hành các kỹ thuật phân tích mã thực thi mã độc cơ bản.
2.2	Thực hành các kỹ thuật phân tích hành vi mã độc cơ bản.

3	**Kỹ thuật phân tích mã thực thi mã độc nâng cao**
3.1	Tổng quan về x86 Diassembly
3.2	Giới thiệu công cụ phân tích mã độc chuyên nghiệp IDA Pro
3.3	Nhận diện các cấu trúc lệnh trong Assembly
3.4	Cách thức phân tích một chương trình trên hệ điều hành Windows
4	**Thực hành các kỹ thuật phân tích mã thực thi mã độc nâng cao**
4.1	Thực hành sử dụng công cụ IDA Pro trong phân tích mã thực thi mã độc.
4.2	Thực hành các bài tập nhận diện các cấu trúc lệnh trong ngữ Assembly
4.3	Thực hành phân tích mã thực thi của một chương trình trên hệ điều hành Windows
5	**Kỹ thuật phân tích hành vi mã độc hại nâng cao**
5.1	Các khai niệm liên quan đến debugging
5.2	Giới thiệu công cụ OllyDbg
5.3	Thực hiện Kernel Debugging với công cụ WinDbg
6	**Thực hành các kỹ thuật phân tích hành vi mã độc hại nâng cao**
6.1	Thực hành sử dụng công cụ OllyDbg trong phân tích hành vi mã độc
6.2	Thực hành phân tích hành vi mã độc nâng cao
7	**Tìm hiểu các chức năng của mã độc hại**
7.1	Giới thiệu các hành vi phổ biến của mã độc
7.2	Phân tích các cơ chế mã độc thực hiện trao đổi thông tin
7.3	Phân tích các kiểu mã hóa được sử dụng bởi mã độc hại
7.4	Nhận diện và xây dựng các Network Signatures trong phân tích mã độc hại
7.5	Thực hành phân tích các cơ chế mã độc thực hiện trao đổi thông tin
7.6	Thực hành tìm hiểu các kiểu mã hóa mã độc sử dụng
7.7	Thực hành nhận diện và xây dựng các network signatures sau khi phân tích mã độc hại
8	**Giới thiệu Anti-Reverse- Engineering**
8.1	Các cơ chế mã độc sử dụng để chống Disassembly
8.2	Các cơ chế mã độc sử dụng để chống Debugging
8.3	Các cơ chế mã độc sử dụng để chống Virtual Machine
8.4	Các Packers được mã độc sử dụng và cách thức thực hiện unpacking
8.5	Thực hành các nội dung liên quan đến việc mã độc anti

	disassembly, debugging, virtual machines
8.6	Thực hành các cách thức unpacking mã độc

9. Ứng cứu sự cố an toàn thông tin:

STT	NỘI DUNG
1	Thu thập chứng cứ
1.1	Thu thập bộ nhớ
1.2	Tạo Disk Image
1.3	Thu thập chứng cứ qua mạng
2	**Phân tích timeline**
3	**Phân tích File System**
4	**Phân tích network**
5	**Phân tích Email**
6	**Gỡ bỏ mã độc**
7	**Phân tích Memory**
8	**Kịch bản ứng cứu sự cố cho web server**

10. Ứng cứu sự cố an toàn thông tin nâng cao:

STT	NỘI DUNG
1	**Ứng cứu sự cố nâng cao và truy tìm các nguy cơ**
2	**Điều tra bộ nhớ trong ứng cứu sự cố và truy tìm các nguy cơ**
3	**Điều tra xâm nhập**
4	**Phân tích thời gian**
5	**Ứng cứu sự cố và truy tìm trong toàn tổ chức / Chống trộm dữ liệu nâng cao và Phát hiện các chống-điều tra**

11. An toàn hạ tầng mạng:

STT	NỘI DUNG
1	**Tổng quan về an toàn thông tin, an toàn hạ tầng mạng**
1.1	Tình hình an toàn thông tin tại Việt Nam, và thế giới; quy định

	chính sách về an toàn thông tin; khái quát về nguy cơ tấn công và mô hình mạng an toàn
2	**Các lỗ hổng bảo mật và kỹ thuật tấn công vào hạ tầng mạng**
2.1	Enumeration, Sniffer, Malware, Denial-of-Service…
3	**Các giải pháp bảo vệ hạ tầng mạng**
3.1	Các giải pháp giám sát, bảo vệ hạ tầng mạng, giải pháp đầu tư, thuê ngoài, sử dụng sản phẩm thương mại, sản phẩm mã nguồn mở hiệu quả…
4	**Nguyên lý xây dựng hạ tầng mạng an toàn**
4.1	Defense in depth; LAN Security, Network Devices Security, VPN; Intrusion Prevention; Network monitoring…
5.	**Nguyên tắc thiết kế hệ thống mạng an toàn**
5.1	DMZ, Firewal, IPS/IDS, Honeypot
6	**Nguyên tắc vận hành hệ thống mạng an toàn**
6.1	Rà soát, kiểm tra lỗ hổng bảo mật; cập nhật bản vá và nâng cấp hệ thống
7	**Tham quan, thảo luận, kiểm tra đánh giá kết quả**
	Tham quan thực tế, thảo luận các nội dung
	Kiểm tra, đánh giá kết quả

12. An toàn ứng dụng:

STT	NỘI DUNG
1	**Tổng quan về an toàn thông tin, an toàn ứng dụng**
1.1	Tình hình an toàn thông tin tại Việt Nam, và thế giới; quy định chính sách về an toàn thông tin; khái quát về nguy cơ tấn công ứng dụng; nguyên tắc thết kế an toàn ứng dụng, Security coding standards; Security Architecture
2	**Các lỗ hổng bảo mật và các kỹ thuật tấn công đối với ứng dụng**
2.1	Khái quát lỗ hổng ứng dụng mã nguồn mở, sản phẩm thương mại; lỗ hổng Buffer overflow; SQL injection, XSS, upload…
3	**Kiểm tra, đánh gia an toàn ứng dụng**
3.1	White box, black box, gray box; đánh gia tác động, rủi ro các lỗ hổng bảo mật ứng dụng
4	**Nguyên tắc vận hành ứng dụng an toàn**

4.1	System configuration; Design network; security patch update
5	**Tham quan, thảo luận, kiểm tra đánh giá kết quả**
5.1	Tham quan thực tế, thảo luận các nội dung
5.2	Kiểm tra, đánh giá kết quả

13. Lập trình an toàn:

STT	NỘI DUNG
1	**Tổng quan về an toàn thông tin, lập trình an toàn**
1.1	Tình hình an toàn thông tin tại Việt Nam, và thế giới; quy định chính sách về an toàn thông tin; khái quát về các lỗ hổng bảo mật và các kỹ thuật tấn công đối với ứng dụng; vận hành ứng dụng an toàn
3	**Các yêu cầu đảm bảo an toàn cho ứng dụng**
3.1	Các yêu cầu an toàn ứng dụng; Quy trình phát triển an toàn ứng dụng;
4	**Nguyên tắc thiết kế và phát triển ứng dụng an toàn**
4.1	Security coding standards; Security Architecture; input validation; Output Encoding; Authentication and password management; session management; access control; database security,
5	**Kiểm tra đánh giá lỗ hổng bảo mật ứng dụng**
5.1	White box, black box;
6	**Tham quan, thảo luận, kiểm tra đánh giá kết quả**
6.1	Tham quan thực tế, thảo luận các nội dung
6.2	Kiểm tra, đánh giá kết quả

14. Thành lập và vận hành Đội Ứng cứu Khẩn cấp:

STT	NỘI DUNG
1	**Cách thức Tổ chức**
1.1	Lên kế hoạch
1.2	Thiết lập
1.3	Đảm bảo CSIRT tồn tại và hoạt động hiệu quả

2	**Cách thức hoạt động**
2.1	Hoạt động xử lý sự cố
2.2	Cách thức xử lý, cải tiến kỹ năng
2.3	Hợp tác với các nhóm khác
3	**Vấn đề pháp lý**
3.1	Tại sao phải có luật
3.2	Một số luật hiện nay
3.3	Cách thức xây dựng luật
4	**Các dịch vụ**
4.1	Mô hình CSIRT hướng dịch vụ
4.2	Các nhóm dịch vụ và dịch vụ cơ bản
5	**Cách thức trao đổi thông tin**
5.1	Kỹ thuật mã hoá PGP
5.2	Thuật toán sinh khoá trong PGP
5.3	Ứng dụng PGP