ỦY BAN NHÂN DÂN THÀNH PHỐ HÀ NỘI	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 149 /KH-UBND	*Hà Nội, ngày 11 tháng 7 năm 2018*

KẾ HOẠCH

Triển khai "Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia" của thành phố Hà Nội

Thực hiện Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia và các Thông tư hướng dẫn của Bộ Thông tin và Truyền thông; Nghị quyết số 05/2015/NQ-HĐND ngày 01/12/2015 của HĐND Thành phố khóa XIV, tại kỳ họp thứ 14 thông qua Chương trình mục tiêu ứng dụng CNTT trong hoạt động cơ quan nhà nước thành phố Hà Nội giai đoạn 2016 - 2020, Nghị quyết số 11/2017/NQ-HĐND ngày 05/12/2017 của HĐND Thành phố khóa XV, tại kỳ họp thứ 5 về việc điều chỉnh nội dung Nghị quyết số 05/2015/NQ-HĐND ngày 01/12/2015, UBND thành phố Hà Nội ban hành Kế hoạch "Triển khai Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia" của thành phố Hà Nội như sau:

I. MỤC TIÊU

- Tổ chức xây dựng các phương án ứng cứu khẩn cấp bảo đảm an toàn cho hệ thống thông tin của Thành phố; chuẩn bị đủ nguồn nhân lực, trang thiết bị cần thiết phục vụ công tác ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng (ATTTM).

- Tăng cường công tác đánh giá, dự báo nguy cơ mất ATTTM, ứng cứu khắc phục sự cố ATTTM đối với các hệ thống thông tin của các cơ quan nhà nước thành phố Hà Nội. Chủ động phòng ngừa, ngăn chặn các hành vi làm mất ATTTM.

- Nâng cao nhận thức về ATTTM, tạo chuyển biến mạnh mẽ trong nhận thức đối với đội ngũ cán bộ, công chức trên địa bàn Thành phố.

II. NHIỆM VỤ VÀ GIẢI PHÁP

1. Nhiệm vụ

1.1. Đánh giá các nguy cơ, sự cố ATTTM

- Đánh giá hiện trạng và khả năng bảo đảm ATTTM của các hệ thống thông tin và các đối tượng cần bảo vệ thuộc phạm vi của kế hoạch. Phân loại, xác định cấp độ an toàn hệ thống thông tin.

- Đánh giá, dự báo các nguy cơ, sự cố, tấn công mạng có thể xảy ra với các hệ thống thông tin và các đối tượng cần bảo vệ.

- Đánh giá, dự báo các hậu quả, thiệt hại, tác động có thể có nếu xảy ra sự cố.

- Đánh giá hiện trạng nhân lực, trang thiết bị, phần mềm, phương tiện, công cụ phục vụ đối phó, ứng cứu, khắc phục sự cố (bao gồm của cả nhà thầu đã ký hợp đồng cung cấp dịch vụ nếu có).

1.2. Xây dựng phương án đối phó, ứng cứu, khắc phục sự cố ATTTM

a) Xác định nguyên nhân, nguồn gốc sự cố ATTTM

- Sự cố do bị tấn công mạng.

- Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật hoặc do lỗi đường điện, đường truyền, hosting...

- Sự cố do lỗi của người quản trị, vận hành hệ thống.

- Sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn...

b) Xây dựng phương án đối phó, ứng cứu, khắc phục sự cố ATTTM

- Xây dựng phương án bảo đảm an toàn hệ thống thông tin theo cấp độ phù hợp quy định pháp luật và tiêu chuẩn, quy chuẩn kỹ thuật.

- Xây dựng khung phương án và các phương án chi tiết đối phó, ứng cứu, khắc phục sự cố ATTTM trong các tình huống:

+ Tình huống sự cố do bị tấn công mạng;

+ Tình huống sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật;

+ Tình huống sự cố do lỗi của người quản trị, vận hành hệ thống;

+ Tình huống sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn v.v...

1.3. Triển khai huấn luyện, diễn tập, đào tạo, phòng ngừa sự cố, giám sát phát hiện, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố

a) Huấn luyện, diễn tập, đào tạo:

Tham gia huấn luyện, diễn tập các phương án đối phó, ứng cứu sự cố theo yêu cầu của các Bộ, ngành; tổ chức đào tạo bồi dưỡng nâng cao kỹ năng, nghiệp vụ phối hợp, ứng cứu, chống tấn công, xử lý mã độc, khắc phục sự cố ATTTM.

b) Phòng ngừa sự cố và phát hiện sớm sự cố:

- Giám sát, phát hiện sớm nguy cơ, sự cố;

- Kiểm tra, đánh giá an toàn thông tin mạng và rà quét, bóc gỡ, phân tích, xử lý mã độc;

- Phòng ngừa sự cố, quản lý rủi ro; nghiên cứu, phân tích, xác minh, cảnh báo sự cố, rủi ro ATTTM; triển khai các giải pháp phòng, chống mã độc, phần mềm độc hại;

- Xây dựng, áp dụng quy trình, quy định, tiêu chuẩn an toàn thông tin;

- Tuyên truyền, nâng cao nhận thức về nguy cơ, sự cố, tấn công mạng;.

c) Bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố:

- Mua sắm, nâng cấp, gia hạn bản quyền sử dụng trang thiết bị, phần mềm, công cụ, phương tiện phục vụ phòng ngừa, ứng cứu, khắc phục sự cố (cho đến khi Trung tâm chức năng giám sát bảo mật, an toàn thông tin thuộc Trung tâm Điều hành thông minh thành phố Hà Nội đi vào hoạt động).

- Chuẩn bị các điều kiện bảo đảm, dự phòng nhân lực, vật lực, tài chính để sẵn sàng đối phó, ứng cứu, khắc phục khi sự cố xảy ra.

- Tổ chức hoạt động của đội ứng cứu sự cố, bộ phận tác nghiệp ứng cứu sự cố (đối với Sở Thông tin và Truyền thông); thuê dịch vụ kỹ thuật đối phó, ứng cứu, khắc phục sự cố ATTTM.

- Tổ chức và tham gia các hoạt động của mạng lưới ứng cứu sự cố.

2. Giải pháp

a) Các giải pháp để thực hiện kế hoạch:

- Các Sở, ban, ngành, UBND các quận, huyện, thị xã thực hiện tốt công tác tuyên truyền, nâng cao nhận thức cho cán bộ, công chức, viên chức về công tác đảm bảo ATTTM.

- Các Sở, ban, ngành, UBND các quận, huyện, thị xã phối hợp các đơn vị tư vấn có năng lực trong lĩnh vực ATTTM tổ chức triển khai các nhiệm vụ của kế hoạch.

b) Nguồn lực và điều kiện bảo đảm thực hiện kế hoạch:

Các Sở, ban, ngành, UBND các quận, huyện, thị xã chủ động bố trí nguồn lực và điều kiện bảo đảm thực hiện các nhiệm vụ được giao.

c) Kinh phí và nguồn vốn triển khai thực hiện kế hoạch:

- Các Sở, ban, ngành, UBND các quận, huyện, thị xã chủ động bố trí kinh phí từ nguồn chi thường xuyên được giao hàng năm đảm bảo an toàn thông tin cho các hệ thống thông tin do đơn vị tự triển khai trước đây, chủ động lên kế hoạch di trú các hệ thống thông tin của đơn vị tập trung về Trung tâm Dữ liệu của Thành phố.

- Sở Thông tin và Truyền thông lập, trình UBND Thành phố phân bổ kinh phí thuộc Chương trình Ứng dụng CNTT Thành phố hàng năm để đảm bảo ATTTM đối với các hệ thống thông tin, hạ tầng kỹ thuật công nghệ thông tin dùng chung của Thành phố và triển khai phòng ngừa, ứng cứu, khắc phục sự cố ATTTM tại các Sở, ban, ngành, UBND các quận, huyện, thị xã và xã, phường, thị trấn.

III. TIẾN ĐỘ THỰC HIỆN

1. Năm 2018

- Tuyên truyền, nâng cao nhận thức cho cán bộ công chức, viên chức về công tác đảm bảo ATTTM.

- Đánh giá các nguy cơ, sự cố ATTTM đối với các hệ thống thông tin dùng chung của Thành phố tại các Sở, ban, ngành.

- Xây dựng khung phương án đối phó, ứng cứu, khắc phục sự cố ATTTM.

- Tham gia huấn luyện, diễn tập, phòng ngừa sự cố, giám sát phát hiện, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố.

- Tổ chức diễn tập ATTTM cấp Thành phố; Tổ chức và tham gia các khóa đào tạo về ATTTM do Bộ, ngành tổ chức.

2. Giai đoạn 2019 - 2020

- Đánh giá, cập nhật thông tin các nguy cơ, sự cố ATTTM đối với các hệ thống thông tin của các Sở, ban, ngành và UBND các quận, huyện, thị xã.

- Xây dựng các phương án chi tiết đối phó, ứng cứu, khắc phục sự cố ATTTM.

- Tổ chức đào tạo, bồi dưỡng và tham gia diễn tập, phòng ngừa sự cố, giám sát phát hiện, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố. Tổ chức diễn tập ATTTM cấp Thành phố (năm 2020).

IV. TỔ CHỨC THỰC HIỆN

1. Nguyên tắc, phương châm ứng cứu sự cố

- Tuân thủ các quy định pháp luật về ứng cứu sự cố An toàn thông tin mạng.

- Chủ động, kịp thời, nhanh chóng, chính xác, đồng bộ và hiệu quả.

- Phối hợp chặt chẽ, chính xác, đồng bộ và hiệu quả giữa các cơ quan tổ chức tham gia ứng cứu.

- Ứng cứu sự cố trước hết phải được thực hiện, xử lý bằng lực lượng tại chỗ và trách nhiệm chính của chủ quản hệ thống thông tin.

- Tuân thủ các điều kiện, nguyên tắc ưu tiên về duy trì hoạt động của hệ thống thông tin theo quy định.

- Thông tin trao đổi trong mạng lưới phải được kiểm tra, xác thực đối tượng trước khi thực hiện các bước tác nghiệp tiếp theo.

- Bảo đảm bí mật thông tin biết được khi tham gia, thực hiện các hoạt động ứng cứu sự cố theo yêu cầu của Cơ quan điều phối quốc gia hoặc cơ quan tổ chức, cá nhân gặp sự cố.

2. Các lực lượng tham gia ứng cứu sự cố

a) Lực lượng ứng cứu sự cố ATTTM quốc gia:

Các đơn vị được quy định tại Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia.

b) Lực lượng ứng cứu sự cố ATTTM thành phố Hà Nội:

- Ban Chỉ đạo Ứng dụng Công nghệ thông tin thành phố Hà Nội.

- Sở Thông tin và Truyền thông (Đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng Thành phố).

- Đội Ứng cứu xử lý sự cố ATTTM thành phố Hà Nội (trực thuộc Sở Thông tin và Truyền thông).

- Các Sở, ban, ngành và UBND các quận, huyện, thị xã.

c) Lực lượng phối hợp ứng cứu sự cố ATTTM thành phố Hà Nội:

- Trung tâm Công nghệ thông tin và Giám sát an ninh mạng, Cục Cơ yếu Đảng - Chính quyền - Ban Cơ yếu Chính phủ.

- Bộ Tư lệnh tác chiến không gian mạng (Bộ Tư lệnh 86) - Bộ Quốc phòng.

- Các doanh nghiệp hoạt động trong lĩnh vực an toàn thông tin.

3. Chức năng, nhiệm vụ, trách nhiệm và cơ chế, quy trình phối hợp giữa các cơ quan, đơn vị

3.1. Chức năng, nhiệm vụ, trách nhiệm

a) Ban Chỉ đạo Ứng dụng Công nghệ thông tin thành phố Hà Nội:

Chỉ đạo công tác điều phối, ứng cứu sự cố đối với các cơ quan nhà nước của Thành phố; chỉ đạo các cơ quan, đơn vị trực thuộc phối hợp, tuân thủ yêu cầu của Cơ quan điều phối quốc gia trong điều phối, ứng cứu sự cố.

b) Sở Thông tin và Truyền thông (Đơn vị chuyên trách về ứng cứu sự cố ATTTM Thành phố):

- Thành lập Đội ứng cứu sự cố và tổ chức hoạt động ứng cứu sự cố trong lĩnh vực, địa bàn, phạm vi mình quản lý.

- Tham gia hoạt động ứng cứu khẩn cấp bảo đảm ATTTM quốc gia khi có yêu cầu từ Bộ Thông tin và Truyền thông hoặc Trung tâm VNCERT.

c) Đội Ứng cứu xử lý sự cố ATTTM thành phố Hà Nội (trực thuộc Sở Thông tin và Truyền thông):

- Sử dụng các biện pháp nghiệp vụ, trang thiết bị, phương tiện kỹ thuật và các biện pháp khác theo chức năng nhiệm vụ được giao và tuân thủ quy định pháp luật.

- Đề nghị cơ quan, tổ chức, cá nhân cung cấp thông tin, tài liệu, thiết bị khi có căn cứ xác định liên quan đến sự cố nhằm phục vụ hoạt động ứng cứu.

- Kiểm tra hệ thống thông tin của cơ quan, tổ chức, cá nhân khi có căn cứ xác định liên quan đến sự cố nhằm phục vụ hoạt động ứng cứu.

- Báo cáo Sở Thông tin và Truyền thông đề nghị cơ quan, tổ chức, doanh nghiệp viễn thông, Internet liên quan phối hợp thực hiện các công việc cần thiết cho hoạt động ứng cứu, khắc phục sự cố.

d) Các Sở, ban, ngành, UBND các quận, huyện, thị xã và xã, phường, thị trấn thuộc thành phố Hà Nội (Đơn vị quản lý, vận hành hệ thống thông tin) khi phát hiện hoặc nhận được thông báo sự cố đối với hệ thống thông tin do đơn vị mình quản lý, phải thực hiện:

- Ghi nhận, tiếp nhận thông báo, báo cáo sự cố và tập hợp các thông tin liên quan theo đúng quy trình.

- Phản hồi cho tổ chức, cá nhân gửi thông báo, báo cáo ban đầu ngay sau khi nhận được để xác nhận về việc đã nhận được thông báo, báo cáo sự cố.

- Chủ trì, phối hợp đơn vị cung cấp dịch vụ ATTTM (trong trường hợp đã ký hợp đồng thuê đơn vị cung cấp dịch vụ ATTTM) và Sở Thông tin và Truyền thông (thông qua Đội Ứng cứu xử lý sự cố ATTTM thành phố Hà Nội) tiến hành phân tích, xác minh, đánh giá tình hình, sơ bộ phân loại sự cố và triển khai ngay các hoạt động ứng cứu sự cố và báo cáo theo quy định.

- Báo cáo về sự cố, diễn biến tình hình ứng cứu sự cố, đề xuất hỗ trợ ứng cứu sự cố hoặc nâng cấp nghiêm trọng của sự cố (khi cần) cho chủ quản hệ thống thông tin, Cơ quan điều phối quốc gia và Sở Thông tin và Truyền thông.

e) Lực lượng phối hợp ứng cứu sự cố ATTTM thành phố Hà Nội:

- Trung tâm Công nghệ thông tin và Giám sát an ninh mạng, Cục Cơ yếu Đảng - Chính quyền - Ban Cơ yếu Chính phủ thực hiện chức năng, nhiệm vụ, trách nhiệm do Chính phủ giao và các nội dung đã ký kết với UBND thành phố Hà Nội tại Thỏa thuận phối hợp số 01/BCYCP-UBND ngày 13/4/2016 về Chương trình phối hợp thực hiện nhiệm vụ bảo mật, xác thực và giám sát an toàn thông tin đối với hệ thống ứng dụng CNTT của thành phố Hà Nội và các kế hoạch triển khai đã ký kết với Sở Thông tin và Truyền thông hàng năm.

- Lực lượng ứng cứu sự cố ATTTM quốc gia, Bộ Tư lệnh tác chiến không gian mạng (Bộ Tư lệnh 86) - Bộ Quốc phòng và các doanh nghiệp hoạt động trong lĩnh vực an toàn thông tin: Thực hiện tư vấn và tham gia phối hợp ứng cứu sự cố ATTTM thành phố Hà Nội khi có yêu cầu.

3.2. Cơ chế, quy trình phối hợp giữa các cơ quan, đơn vị

a) Bộ phận chuyên trách công nghệ thông tin (hoặc cá nhân được giao nhiệm vụ chuyên trách công nghệ thông tin) thuộc đơn vị quản lý, vận hành hệ thống thông tin khi phát hiện sự cố hoặc được thông báo sự cố phải báo cáo sự cố tới cơ quan chủ quản, Sở Thông tin và Truyền thông (thông qua Đội Ứng cứu xử lý sự cố an toàn thông tin mạng thành phố Hà Nội) chậm nhất 5 ngày kể từ khi phát hiện sự cố:

- Báo cáo sự cố ATTTM thực hiện theo quy định tại Điều 9 Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc.

- Đối với sự cố ATTTM nghiêm trọng (quy định tại Điều 9 Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ), thực hiện báo cáo theo quy định tại Điều 11 Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ.

b) Sở Thông tin và Truyền thông (Đội Ứng cứu xử lý sự cố an toàn thông tin mạng thành phố Hà Nội) khi phát hiện sự cố hoặc nhận được thông báo, báo cáo sự cố ATTTM phải thực hiện:

- Tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố ATTTM theo quy định tại Điều 10 Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông hoặc Điều 12 Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ (đối với sự cố ATTTM nghiêm trọng).

- Thực hiện quy trình ứng cứu sự cố ATTTM theo quy định tại Điều 11 Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông hoặc Điều 14 Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ (đối với sự cố ATTTM nghiêm trọng).

UBND Thành phố yêu cầu các Sở, ban, ngành và UBND các quận, huyện, thị xã nghiêm túc triển khai thực hiện Kế hoạch; định kỳ hàng Quý báo cáo gửi Sở Thông tin và Truyền thông tổng hợp, báo cáo UBND Thành phố./.

Nơi nhận:
- Bộ Thông tin và Truyền thông;
- Thường trực Thành ủy;
- Chủ tịch UBND Thành phố;
- Thường trực HĐND Thành phố;
- Các Phó Chủ tịch UBND Thành phố;
- Ban Cơ yếu Chính phủ,
  Bộ Tư lệnh 86 - Bộ Quốc phòng;
- Cục ATTT, VNCERT - Bộ TT&TT;
- Các Sở, ban, ngành;
- UBND các quận, huyện, thị xã;
- Lưu: VT, KGVX.

24651 (130)

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Nguyễn Đức Chung