|  |  |
| --- | --- |
| **ỦY BAN NHÂN DÂNTỈNH HÀ TĨNH**Số: /KH-UBND | CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAMĐộc lập - Tự do - Hạnh phúc*Hà Tĩnh, ngày tháng 10 năm 2019* |

**DỰ THẢO**

**KẾ HOẠCH**

**Ứng phó sự cố an toàn thông tin mạng năm 2020**

*(Thực hiện theo Phụ lục II, kèm theo Quyết định số 05/2017/QĐ-TTg)*

**I. Các quy định chung**

**1. Phạm vi và đối tượng của kế hoạch**

Kế hoạch này để ứng phó sự cố, bảo đảm an toàn thông tin mạng đối với các hệ thống thông tin của tỉnh,áp dụng cho các sở, ban, ngành, đoàn thể cấp tỉnh; UBND các huyện, thành phố, thị xã; các cơ quan, đơn vị, doanh nghiệp có liên quan. Hệ thống thông tin chuyên ngành của Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh do Bộ Công an, Bộ Quốc phòng quản lý không thuộc phạm vi điều chỉnh của Kế hoạch này.

**2. Xác định sự cố an toàn thông tin và nguyên tắc, phương châm ứng phó sự cố**

2.1. Xác định sự cố an toàn thông tin

a) Hệ thống thông tin bị sự cố là hệ thống thông tin cấp độ 4 (được quy định tại Điều 10 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ) và chủ quản hệ thống thông tin thuộc thẩm quyền quản lý UBND tỉnh.

b) Phân nhóm sự cố an toàn thông tin (ATTT) mạng đáp ứng các tiêu chí sau:

- Hệ thống thông tin bị sự cố là hệ thống thông tin cấp độ 4 và bị một trong số các sự cố sau:

+ Hệ thống thông tin bị gián đoạn dịch vụ.

+ Dữ liệu tuyệt mật hoặc bí mật nhà nước có khả năng bị tiết lộ.

+ Dữ liệu quan trọng của hệ thống không bảo đảm tính toàn vẹn và không có khả năng khôi phục được.

+ Hệ thống bị mất quyền điều khiển.

+ Sự cố có khả năng xảy ra trên diện rộng hoặc gây ra các ảnh hưởng dây chuyền, làm tổn hại cho các hệ thống thông tin cấp độ 4 hoặc cấp độ liên quan khác.

- Chủ quản hệ thống thông tin không đủ khả năng tự kiểm soát, xử lý được sự cố.

 2.2. Nguyên tắc, phương châm ứng phó sự cố

 - Tuân thủ các quy định pháp luật về điều phối, ứng cứu sự cố ATTT mạng;

- Chủ động, kịp thời, nhanh chóng, nghiêm ngặt và kỷ luật;

- Phối hợp chặt chẽ, chính xác, đồng bộ và hiệu quả giữa các cơ quan, tổ chức, doanh nghiệp;

- Thông tin được trao đổi, cung cấp trong quá trình điều phối, ứng cứu sự cố phải được bảo đảm bí mật theo yêu cầu của cơ quan, tổ chức, cá nhân gặp sự cố hoặc của Cơ quan điều phối quốc gia trừ khi sự cố xảy ra có liên quan tới nhiều đối tượng người dùng khác mà Cơ quan điều phối quốc gia có yêu cầu cảnh báo, nhắc nhở.

- Công tác ứng phó sự cố ATTT mạng phải tuân thủ theo Quy trình tổng thể hệ thống phương án ứng cứu sự cố ATTT mạng quy định tại Phụ lục I kèm theo Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ (sau đây gọi là Quyết định 05) và các văn bản quy định khác có liên quan.

**3. Các lực lượng tham gia ứng phó sự cố**

- Ban Chỉ đạo CNTT tỉnh (kiêm nhiệm Ban Chỉ đạo ứng cứu khẩn cấp sự cố an toàn thông tin mạng);

- Các sở, ban, ngành, đoàn thể cấp tỉnh; UBND các huyện, thị xã, thành phố và các đơn vị, doanh nghiệp có liên quan;

- Sở Thông tin và Truyền thông;

- Đội ứng cứu sự cố ATTT mạng của tỉnh;

- Trung tâm CNTT và Truyền thông Hà Tĩnh;

- Đơn vị chủ quản; đơn vị quản lý, vận hành hệ thống thông tin;

- Trong trường hợp cần thiết, mời các cơ quan Trung ương có chức năng cùng tham gia.

**4. Chức năng, nhiệm vụ, trách nhiệm và cơ chế, quy trình phối hợp giữa các lực lượng tham gia ứng phó sự cố**

4.1. Ban Chỉ đạo xây dựng Chính quyền điện tử tỉnh: Đảm nhiệm chức năng Ban Chỉ đạo ứng cứu khẩn cấp sự cố an toàn thông tin mạng trong phạm vi địa bàn tỉnh (sau đây gọi là Ban Chỉ đạo Ứng cứu khẩn cấp sự cố của tỉnh). Ban Chỉ đạo Ứng cứu khẩn cấp sự cố của tỉnh có trách nhiệm và quyền hạn được quy định tại Khoản 2, Điều 5 Quyết định 05.

4.2. Sở Thông tin và Truyền thông:

Là cơ quan thường trực của Ban Chỉ đạo ứng cứu khẩn cấp sự cố ATTT tỉnh; chỉ đạo đơn vị chuyên trách ứng cứu sự cố ATTT mạng của tỉnh thực hiện đầy đủ, kịp thời các chức năng, nhiệm vụ theo Quyết định 05 và các nhiệm vụ khác khi xảy ra sự cố.

4.3. Đội ứng cứu sự cố ATTT mạng của tỉnh:

- Tham gia hoạt động ứng cứu khẩn cấp bảo đảm ATTT mạng quốc gia khi có yêu cầu từ Bộ Thông tin và Truyền thông hoặc các bộ, ngành có liên quan và theo Quy chế hoạt động của Đội;

- Hàng năm, tổ chức tập huấn nghiệp vụ cho thành viên của Đội để nâng cao trình độ, khả năng ứng phó sự cố ATTT mạng;

- Tham mưu Sở Thông tin và Truyền thông trình UBND tỉnh khen thưởng những cá nhân, tập thể có thành tích kịp thời phát hiện và khắc phục sự cố, đồng thời xử lý nghiêm các cá nhân, tập thể gây ra sự cố.

4.4. Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh:

Phối hợp với Sở Thông tin và Truyền thông, Trung tâm CNTT và Truyền thông tỉnh kiểm tra, xử lý các vi phạm về ATTT mạng theo quy định; ứng cứu các sự cố về ATTT xảy ra trên địa bàn tỉnh và những hệ thống thông tin dùng chung được triển khai tại Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh không do Bộ Công an, Bộ Quốc phòng quản lý.

4.5. Trung tâm CNTT và Truyền thông là đơn vị chuyên trách kỹ thuật ATTT mạng của tỉnh:

- Phối hợp với Đội ứng cứu sự cố ATTT mạng của tỉnh trong hoạt động ứng cứu khẩn cấp bảo đảm ATTT mạng của tỉnh.

- Thực hiện nhiệm vụ Thường trực Đội ứng cứu sự cố ATTT mạng của tỉnh theo Quy ché hoạt động của Đội.

4.7. Các sở, ban, ngành; UBND các huyện, thị xã, thành phố; đơn vị chủ quản; đơn vị quản lý, vận hành hệ thống thông tin:

Các cơ quan, đơn vị có trách nhiệm cử cán bộ, công chức phụ trách ATTT tham gia Đội ứng cứu sự cố ATTT của tỉnh. Phối hợp với đơn vị chuyên trách ứng cứu sự cố ATTT mạng của tỉnh trong công tác ứng phó, xử lý các sự cố ATTT.

4.8. Các doanh nghiệp cung ứng dịch vụ:

- Doanh nghiệp cung ứng dịch vụ viễn thông trên địa bàn tỉnh: Theo chức năng, nhiệm vụ, thẩm quyền của mình, phối hợp Sở Thông tin và Truyền thông trong việc cung cấp thông tin thuê bao, khách hàng liên quan tới sự cố (IP thuê bao, máy chủ, nhật ký dịch vụ phân giải tên miền DNS,... trong phạm vi quản lý của doanh nghiệp);

- Doanh nghiệp cung cấp, xây dựng các hệ thống thông tin: Tích cực phối hợp với đơn vị chủ quản; đơn vị quản lý, vận hành, Sở Thông tin và Truyền thông trong công tác ứng phó, xử lý các sự cố ATTT liên quan hệ thống thông tin do mình xây dựng hoặc cung cấp.

**II. Đánh giá các nguy cơ, sự cố ATTT mạng**

*(Chi tiết trong Phụ lục I kèm theo)*

**III. Phương án đối phó, ứng cứu đối với một số tình huống sự cố cụ thể**

*(Chi tiết trong Phụ lục II kèm theo).*

**IV. Triển khai hoạt động thường trực, điều phối, xử lý, ứng cứu sự cố**

1. Báo cáo sự cố ATTT mạng: Triển khai các hoạt động thuộc trách nhiệm của các cơ quan, đơn vị liên quan theo quy định tại Điều 11Quyết định 05.

2. Tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố ATTT mạng: Triển khai các hoạt động thuộc trách nhiệm của các cơ quan, đơn vị liên quan theo quy định tại Điều 12 Quyết định 05.

3. Quy trình ứng cứu sự cố ATTT mạng thông thường: Triển khai theo quy định tại Điều 13 Quyết định 05.

4. Quy trình ứng cứu sự cố ATTT mạng quan trọng: Triển khai theo quy định tại Điều 14 Quyết định 05.

5. Dự phòng kinh phí, nhân lực, vật lực thường trực sẵn sàng ứng cứu sự cố; triển khai điều hành phối hợp tổ chức ứng cứu và thực hiện ứng cứu, xử lý, ngăn chặn, khắc phục sự cố khi có sự cố xảy ra.

**V. Triển khai 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**

Xây dựng các nội dung, nhiệm vụ cụ thể cần triển khai nhằm phòng ngừa sự cố, giám sát phát hiện, huấn luyện, diễn tập, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố trên địa bàn tỉnh, bao gồm:

1. Triển khai các chương trình huấn luyện, diễn tập:

- Huấn luyện, diễn tập các phương án đối phó, ứng cứu sự cố tương ứng với các kịch bản, tình huống sự cố cụ thể tại Phần III của Kế hoạch này.

- Huấn luyện, diễn tập nâng cao kỹ năng, nghiệp vụ phối hợp, ứng cứu, chống tấn công, xử lý mã độc, khắc phục sự cố.

2. Các nội dung, nhiệm vụ nhằm phòng ngừa sự cố và phát hiện sớm sự cố:

- Thực hiện nghiêm túc công tác giám sát, phát hiện sớm nguy cơ, sự cố.

- Kiểm tra, đánh giá ATTT 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 ATTT mạng, phần mềm độc hại.

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

3. Các nội dung, nhiệm vụ nhằm bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố:

- Mua sắm, nâng cấp, gia hạn bản quyền trang thiết bị, phần mềm, công cụ, phương tiện phục vụ ứng cứu, khắc phục sự cố.

- 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.

- Tham gia các hoạt động của mạng lưới ứng cứu sự cố.

- Tổ chức hoạt động của đội ứng cứu sự cố, bộ phận tác nghiệp ứng cứu sự cố; thuê dịch vụ kỹ thuật và tổ chức, duy trì đội chuyên gia ứng cứu sự cố.

**VI. Các giải pháp đảm bảo, tổ chức triển khai kế hoạch và kinh phí**

**1. Các giải pháp thực hiện Kế hoạch**

Các cơ quan, đơn vị căn cứ quy định tại Quyết định 05, các văn bản khác quy định về bảo đảm ATTT mạng và phương án ứng cứu sự cố của Kế hoạch này để triển khai các nhiệm vụ được giao.

**2. Nguồn lực và điều kiện bảo đảm thực hiện Kế hoạch**

Ưu tiên bố trí nguồn lực và điều kiện để bảo đảm thực hiện các nội dung của Kế hoạch này, cũng như các nội dung liên quan đến bảo đảm ATTT mạng khác.

**3. Kinh phí và nguồn vốn triển khai thực hiện Kế hoạch**

- Kinh phí thực hiện các hoạt động ứng cứu sự cố ATTT mạng trên địa bàn tỉnh được bố trí trong dự toán chi ngân sách nhà nước của tỉnh (nguồn chi sự nghiệp CNTT) và giao Sở Thông tin và Truyền thông quản lý, sử dụng, thanh quyết toán theo quy định.

- Các sở, ban, ngành cấp tỉnh; UBND cấp huyện chủ động bố trí kinh phí bảo đảm cho hoạt động ứng phó sự cố ATTT mạng trong phạm vi quản lý của mình.

**VII. Tổ chức thực hiện**

**1. Sở Thông tin và Truyền thông**

- Chủ trì, hương dẫn, kiểm tra việc tổ chức triển khai thực hiện Kế hoạch.

- Định kỳ 6 tháng một lần tổng hợp báo cáo UBND tỉnh, đề xuất điều chỉnh các nội dung khi cần thiết.

- Phối hợp với các ngành liên quan tham mưu cho UBND tỉnh thu hút nguồn lực và các nguồn hỗ trợ từ Trung ương để thực hiện thành công Kế hoạch.

**2. Sở Kế hoạch và Đầu tư, Sở Tài chính**

Sở Kế hoạch và Đầu tư, Sở Tài chính phối hợp Sở Thông tin và Truyền thông tham mưu UBND tỉnh bố trí kinh phí cho các dự án, kế hoạch bảo đảm ATTT mạng nói chung và kế hoạch ứng phó sự cố ATTT mạng trên địa bàn tỉnh; kinh phí thường xuyên, hàng năm cho nhiệm vụ làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về ATTT mạng trên địa bàn tỉnh.

**3. Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh**

- Tăng cường công tác nắm tình hình, kịp thời tham mưu cho UBND tỉnh về các chủ trương, giải pháp và phối hợp chặt chẽ với các cơ quan, đơn vị liên quan trong công tác bảo đảm an ninh, ATTT mạng.

- Chủ trì phối hợp với các đơn vị liên quan triển khai các giải pháp đảm bảo an ninh thông tin; phát hiện, đấu tranh, ngăn chặn mọi âm mưu, thủ đoạn hoạt động sử dụng không gian mạng của các thế lực thù địch, tội phạm mạng nhằm xâm phạm an ninh quốc gia, trật tự an toàn xã hội và gây mất ATTT mạng. Điều tra, xử lý kịp thời các vi phạm về an ninh, ATTT mạng.

- Hỗ trợ các cơ quan, đơn vị đánh giá nguy cơ mất ATTT mạng khi có yêu cầu.

**4. Trách nhiệm của các cơ quan, đơn vị**

- Thực hiện các nhiệm vụ thuộc trách nhiệm theo quy định tại các Điều 11, Điều 12, Điều 13, Điều 14 và các nội dung liên quan khác của Quyết định 05 và các nội dung tại Kế hoạch.

- Quan tâm, chú trọng đến công tác bảo đảm ATTT cho hệ thống thông tin tại cơ quan, đơn vị.

- Chủ động bố trí kinh phí trang bị phần mềm chống virus, thiết bị tường lửa cho hệ thống máy tính, hệ thống mạng, hệ thống thông tin tại cơ quan, đơn vị.

- Phối hợp với Sở Thông tin và Truyền thông và các đơn vị liên quan thực hiện công tác ứng phó sự cố ATTT mạng trên địa bàn tỉnh.

**5. Trách nhiệm của các doanh nghiệp cung cấp dịch vụ**

5.1. Doanh nghiệp cung ứng dịch vụ viễn thôngtrên địa bàn tỉnh:

- Tổ chức nâng cấp, mở rộng, bảo đảm hạ tầng viễn thông hoạt động ổn định, thông suốt phục vụ các hệ thống thông tin của cơ quan nhà nước trên địa bàn tỉnh hoạt động hiệu quả.

- Giám sát đầy đủ, thường xuyên hệ thống đường truyền viễn thông nhằm phát hiện và ngăn chặn, xử lý kịp thời các nguy cơ gây mất ATTT trên môi trường mạng.

5.2. Doanh nghiệp cung cấp, xây dựng các hệ thống thông tin: Thường xuyên rà soát, kiểm tra nhằm phát hiện và khắc phục các lỗi của các hệ thống thông tin do mình cung cấp, xây dựng.

Trong quá trình thực hiện Kế hoạch nếu có vấn đề vướng mắc, phát sinh, các cơ quan, đơn vị phản ánh kịp thời về Sở Thông tin và Truyền thông để tổng hợp, báo cáo UBND tỉnh điều chỉnh, bổ sung./.

|  |  |
| --- | --- |
| ***Nơi nhận:***- Bộ Thông tin và Truyền thông;- Chủ tịch, các PCT UBND tỉnh;- BCĐ CNTT tỉnh, BCĐ CNTT cơ quan Đảng;- Các sở, ban, ngành, đoàn thể cấp tỉnh;- UBND các huyện, thành phố, thị xã;- Chánh, Phó VP UBND tỉnh;- Cổng TTĐT tỉnh, Trung tâm CB-TH;- Lưu: VT, VX1. | **TM. ỦY BAN NHÂN DÂN** **KT. CHỦ TỊCH****PHÓ CHỦ TỊCH****Đặng Quốc Vinh** |

**Phụ lục I**

**Đánh giá các nguy cơ, sự cố ATTT mạng**

*(Kèm theo kế hoạch số /KH-UBND ngày /10/2019 của UBND tỉnh)*

**1. Hiện trạng và khả năng bảo đảm an toàn thông tin mạng của các hệ thống thông tin**

1.1. Tình hình an toàn thông tin trên địa bàn tỉnh:

Trong thời gian qua, diễn biến ATTT tại Hà Tĩnh có chiều hướng gia tăng phức tạp, nhưng chưa có các sự cố nghiêm trọng xảy ra. Một số vụ tấn công được cảnh báo và ghi nhận bao gồm:

Trong năm 2018, đơn vị thường trực đã cảnh báo và hỗ trợ xử lý tới 167 lượt cảnh báo tới các đơn vị, cảnh báo về tấn công thay đổi giao diện, mã độc GandCrab 5.2, mã độc lây nhiễm qua phần mềmWinrar; cảnh báo các tài khoản của một số phần mềm dùng chung đang sử dụng mật khẩu đơn giản. Phối hợp, hỗ trợ xử lý Website bị tấn công thay đổi giao diện tại Hội Liên hiệp phụ nữ tỉnh; Rà quét lỗ hổng bảo mật 13 Cổng/trang thông tin điện tử các cơ quan nhà nước cấp huyện, 10 trang thông tin điện cấp xã. Kết quả, các Cổng/trang thông tin điện tử của các đơn vị đang tồn tại nhiều lỗ hổng bảo mật ở mức nghiêm trọng dễ bị tin tặc lợi dụng tấn công.

1.2. Khả năng bảo đảm an toàn thông tin mạng của các hệ thống thông tin:

Hệ thống mạng của các cơ quan, đơn vị trên địa bàn tỉnh chưa được cấu hình đúng chuẩn, nhiều đơn vị chưa có hệ thống tường lửa, nên nguy cơ bị nhiễm mã độc cao; Hệ thống phần mềm lõi để xây dựng các cổng/trang thông tin điện tử các đơn vị chưa được nâng cấp kịp thời, trình độ lập trình chưa cao nên còn tồn lại nhiều lỗ hổng dễ bị khai thác, tấn công, chèn mã độc. Xu hướng sử dụng các thiết bị thông minh, việc tham gia vào các trang mạng xã hội, sử dụng các hệ thống Email miễn phí có địa chỉ máy chủ đặt tại nước ngoài cũng là một trong các nguy cơ lớn mất an toàn, an ninh thông tin, dễ bị tin tặc lợi dụng để trung gian tấn công vào hệ thống thông tin của các đơn vị.

**2. Dự báo các nguy cơ, sự cố ATTT đối với các hệ thống thông tin trên địa bàn trong thời gian tới**

- Từ tình hình an ninh, ATTT của trong nước và thế giới, diễn biến ATTT là rất khó lường, các mã độc lây lan và ăn cắp thông tin trên địa bàn thường diễn ra và hoạt động mạnh vào các ngày có tính chất đặc biệt (như: các ngày trước, trong và sau bầu cử hoặc các sự kiện lớn). Dạng tấn công mã hóa dữ liệu đòi tiền chuộc, ăn cắp dữ liệu cá nhân, tài khoản thông qua các thiết bị thông minh, hệ thống mạng xã hội được đẩy mạnh.

- Đánh cắp thông tin cá nhân: Hiện nay, việc đánh cắp dữ liệu nhằm vào các doanh nghiệp, nhà hàng, khách sạn… sử dụng các máy tính tiền ngày càng gia tăng và nguy cơ người dùng bị đánh cắp thông tin là rất lớn. Ngoài ra, việc thanh toán bằng các phương tiện di động đang phát triển cũng tạo thêm kênh để tin tặc tấn công. Nguy cơ đánh cắp dữ liệu y tế khi các bệnh viện, công ty bảo hiểm và các dịch vụ y tế công cộng khác sử dụng các hệ thống trực tuyến.

**3. Đánh giá, dự báo các hậu quả, tác động khi xảy ra sự cố**

Khi xảy ra sự cố ATTT, các hệ thống thông tin của cơ quan nhà nước bị tấn công sẽ dẫn đến nhiều hậu quả, tác động:

- Các dữ liệu, hồ sơ, tài liệu quan trọng bị đánh cắp, gây nguy cơ lộ lọt bí mật nhà nước;

- Bị chiếm quyền điều khiển, thay đổi giao diện, chỉnh sửa nội dung của các hệ thống thông tin làm ảnh hưởng xấu đến văn hóa, chính trị và trật tự xã hội;

- Bị đình trệ, tê liệt hoạt động của hệ thống Cổng/trang thông tin điện tử của các cơ quan nhà nước, các hệ thống thông tin quan trọng khác của tỉnh; nguy cơ gây rối loạn các giao dịch xử lý thủ tục hành chính trên hệ thống dịch vụ công trực tuyến mức độ cao và hoạt động vận hành của các hệ thống thông tin,…

**4. Đánh giá về hiện trạng trang thiết bị, nhân lực, vật lực phục vụ đối phó, ứng cứu, khắc phục sự cố**

- Các Cổng/Trang thông tin điện tử, hệ thống mạng thông tin của các cơ quan nhà nước trong tỉnh chưa đáp ứng theo tiêu chuẩn thống nhất; các hệ thống thông tin, phần mềm, thiết bị phần cứng chưa được nâng cấp thường xuyên, việc cập nhật, vá các lỗ hổng bảo mật chưa được khắc phục, trong đó có những lỗ hổng bảo mật ở mức rất nguy hiểm.

- Hệ thống dự phòng chưa đồng bộ, khi xảy ra tấn công hoặc bị lỗi phần cứng thường khó khăn trong khắc phục. Hệ thống máy chủ đặt tại nhà cung cấp dịch vụ không có “tường lửa” bảo vệ hoặc có nhưng không đủ mạnh.

- Hà Tĩnh đã có Ban Chỉ đạo ứng cứu khẩn cấp sự cố an toàn thông tin mạng (do Ban Chỉ đạo xây dựng Chính quyền điện tử tỉnh kiêm nhiệm), Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh, Đơn vị chuyên trách ứng cứu sự cố ATTT mạng (Sở Thông tin và Truyền thông) và Đơn vị chuyên trách về đảm bảo kỹ thuật an toàn thông tin mạng của tỉnh (Trung tâm CNTT và Truyền thông tỉnh). Đây là các tổ chức có trách nhiệm trong việc điều phối đối phó, ứng cứu, khắc phục sự cố về ATTT trên địa bàn tỉnh.

- Ngoài ra, hệ thống đội ngũ cán bộ chuyên trách CNTT của các cơ quan nhà nước trên địa bàn tỉnh đã được hình thành, chuẩn hóa. Tuy nhiên, chưa được quan tâm, bồi dưỡng thường xuyên về ATTT nên nhiều lúc chưa đáp ứng được yêu cầu công việc./.

**Phụ lục II**

**Phương án đối phó, ứng cứu đối với một số tình huống sự cố cụ thể**

*(Kèm theo Kế hoạch số /KH-UBND ngày /10/2019 của UBND tỉnh)*

**1. Phân tích và thông báo sự cố**

1.1. Tiếp nhận, xác định sự cố:

Đơn vị vận hành hệ thống thông tin chủ trì, phối hợp với Trung tâm CNTT và Truyền thông (Đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng tỉnh Hà Tĩnh) và các cơ quan, tổ chức liên quan tiếp nhận, phân tích các cảnh báo, dấu hiệu sự cố từ các nguồn bên trong và bên ngoài (cảnh báo sự cố: Công văn, email. điện thoại, website, facebook, mạng xã hội...; phát hiện sự cố thông qua kiểm tra, rà soát, đánh giá). Khi xác định được sự cố đã xảy ra, cần tổ chức ghi nhận, thu thập chứng cứ, xác định nguồn gốc sự cốnhằm áp dụng phương án đối phó, ứng cứu, khắc phục sự cố phù hợp:

- 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, v.v...

1.2. Triển khai các bước ưu tiên ứng cứu ban đầu:

Sau khi đã xác định sự cố xảy ra, đơn vị vận hành hệ thống thông tin triển khai các bước ưu tiên ban đầu để xử lý sự cố theo phương án, kế hoạch ứng phó sự cố đã được cấp thẩm quyền phê duyệt/xác nhận hoặc theo tư vấn, hướng dẫn của Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh và Trung tâm CNTT và Truyền thông.

Đội ứng cứu sự cố phải kịp thời phân tích và xác định tình hình sự cố để xác định phạm vi ảnh hưởng. Những phân tích ban đầu sẽ cung cấp thông tin cho các hoạt động tiếp theo.

1.3. Thông báo, báo cáo sự cố:

Sau khi triển khai các bước ưu tiên ứng cứu ban đầu, đơn vị vận hành hệ thống thông tin tổ chức thông báo, báo cáo sự cố đến các tổ chức, cá nhân liên quan bên trong và bên ngoài cơ quan, tổ chức theo quy định. Cụ thể:

- Thông báo sự cố tới cơ quan chủ quản Đội ứng cứu sự cố chậm nhất 3 ngày kể từ khi phát hiện sự cố; trường hợp xác định sự cố có thể vượt khả năng xử lý, đơn vị vận hành hệ thống thông tin phải báo cáo ban đầu sự cố bằng văn bản về Trung tâm CNTT và Truyền thông.

- Hình thức thông báo sự cố: Bằng công văn, fax, thư điện tử, nhắn tin đa phương tiện, phần mềm gửi nhận văn bản, phần mềm điều hành tác nghiệp, hoặc thông qua hệ thống kỹ thuật báo sự cố ATTT mạng của cơ quan điều phối cấp tỉnh.

- Hình thức báo cáo sự cố: Bằng văn bản giấy hoặc văn bản điện tử.

**2. Ngăn chặn, xử lý sự cố**

2.1. Chọn phương án:

Đơn vị vận hành hệ thống phối hợp với Đội ứng cứu sự cố và các đơn vị liên quan báo cáo, đề xuất cơ quan chủ quản hệ thống thông tin, Ban Chỉ đạo ứng cứu khẩn cấp sự cố an toàn thông tin mạng của tỉnh, Đội ứng cứu sự cố phê duyệt phương án, chiến lược ngăn chặn và xử lý sự cố và đề nghị hỗ trợ từ Cơ quan điều phối quốc gia nếu cần thiết.

Đơn vị vận hành hệ thống phối hợp với Đội ứng cứu sự cố, Trung tâm CNTT và Truyền thông và các đơn vị liên quan tiến hành:

- Phân loại sự cố:

+ Sự cố về tấn công từ chối dịch vụ;

+ Sự cố về tấn công giả mạo;

+ Sự cố về tấn công sử dụng mã độc;

+ Sự cố về tấn công truy cập trái phép, chiếm quyền điều khiển;

+ Sự cố về tấn công thay đổi giao diện;

+ Sự cố về tấn công mã hóa phần mềm, dữ liệu, thiết bị;

+ Sự cố về tấn công phá hoại thông tin, dữ liệu, phần mềm;

+ Sự cố về tấn công nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu;

+ Sự cố về tấn công tổng hợp sử dụng kết hợp nhiều hình thức;

+ Sự cố về các hình thức tấn công mạng khác.

- Báo cáo lãnh đạo đơn vị: Chỉ đạo xử lý và phân công trách nhiệm xử lý.

- Thu thập thông tin để phục vụ phân tích sự cố:

+ Thông tin về đầu mối liên hệ;

+ Thu thập thông tin hệ thống;

+ Thu thập chức năng của hệ thống;

+ Thu thập cấu hình của hệ thống (OS, Servise, version, network...);

+ Thu thập chứng cứ;

+ Thu thập bộ nhớ;

+ Thu thập trạng thái network và các kết nối;

+ Thu thập các tiến trình đang chạy;

+ Thu thập hard drive media;

+ Thu thập log file;

+ Thu thập các cổng đang mở của hệ thống.

- Phân tích sự cố:

+ Phân tích dòng thời gian;

+ Thời gian bị sửa đổi, truy cập, tạo hoặc thay đổi.

+ Thời gian thực hiện các cập nhật lớn đối với hệ thống;

+ Thời điểm mà hệ thống sử dụng lần cuối cùng;

+ Phân tích dữ liệu ...

- Xử lý sự cố:

+ Gỡ bỏ sự cố;

+ Xác định và gỡ bỏ các backdoors;

+ Phân tích và kiểm tra lỗ hổng sau khi thực hiện các bản vá lỗi;

+ Khôi phục;

+ Phân tích và kiểm tra lỗ hổng sau khi thực hiện các bản vá lỗi;

+ Khôi phục dữ liệu;

+ Thu thập các tệp tin, hình ảnh, email,... bị xóa, thời gian bị xóa;

+ Tìm kiếm các tệp tin không thể khôi phục;

+ Khôi phục các tệp tin phù hợp.

- Tổng hợp báo cáo Lãnh đạo đơn vị và Trung tâm CNTT và Truyền thông:

+ Báo cáo kết quả phân tích sự cố: Mô tả chi tiết các bước quan trọng khi thực hiện xử lý sự cố;

+ Tổng hợp báo cáo gửi lãnh đạo cơ quan, tổ chức và các bên liên quan đến sự cố;

+ Rút kinh nghiệm và ứng dụng cho các sự cố tương tự.

2.2. Triển khai thu thập chứng cứ:

Trên cơ sở phương án, nguồn lực đã được phê duyệt, đơn vị được giao hoặc Đội ứng cứu sự cố tổ chức thu thập chứng cứ, phạm vi, đối tượng bị ảnh hưởng,...

2.3. Xác định nguồn gốc tấn công:

Đơn vị được giao hoặc Đội ứng cứu sự cố triển khai phân tích, xác định nguồn gốc tấn công để ngăn chặn, giảm thiểu tác động, thiệt hại đến hệ thống thông tin.

**3. Khắc phục, gỡ bỏ và khôi phục**

3.1. Khắc phục, gỡ bỏ sự cố:

Sau khi đã triển khai ngăn chặn sự cố, phải tiến hành tiêu diệt các mã độc, phần mềm độc hại, khắc phục các điểm yếu ATTT của hệ thống (xây dựng lại hệ thống, thay thế các tệp tin bị lỗi, cài đặt các bản vá lỗi, thay đổi mật khẩu và rà soát các chính sách ATTT).

3.2. Khôi phục:

Đơn vị vận hành hệ thống triển khai các hoạt động khôi phục hệ thống, dữ liệu và kết nối (phải khôi phục từ các bản sao lưu hệ thống “sạch”); cấu hình hệ thống an toàn; bổ sung các thiết bị, phần cứng, phần mềm bảo đảm ATTT cho hệ thống thông tin và kiểm tra thử toàn bộ hệ thống sau khi khắc phục sự cố.

Trong quá trình ứng cứu sự cố, đơn vị vận hành hệ thống phải chủ trì, phối hợp với các cơ quan, đơn vị liên quan xây dựng và duy trì thực hiện các báo cáo ứng cứu sự cố gồm:

+ Báo cáo ban đầu;

+ Báo cáo diễn biến tình hình;

+ Báo cáo phương án ứng cứu cụ thể;

+ Báo cáo xin ý kiến chỉ đạo, chỉ huy;

+ Báo cáo đề nghị hỗ trợ, phối hợp;

+ Báo cáo kết thúc ứng phó sự cố.

**4. Tổng kết, đánh giá**

4.1. Tổng kết, đúc rút kinh nghiệm:

Đơn vị vận hành hệ thống bị sự cố phối hợp với Đội ứng cứu sự cố và Trung tâm CNTT và Truyền thông triển khai tổng hợp tất cả các thông tin, báo cáo, phân tích có liên quan đến sự cố, công tác triển khai phương án ứng cứu khẩn cấp bảo đảm ATTT mạng, báo cáo Ban Chỉ đạo ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh; tổ chức phân tích nguyên nhân, rút kinh nghiệm trong hoạt động xử lý sự cố và đề xuất các biện pháp bổ sung nhằm phòng ngừa, ứng cứu đối với các sự cố tương tự trong tương lai...

4.2. Xây dựng báo cáo kết thúc ứng phó sự cố:

Đơn vị vận hành hệ thống thông tin bị sự cố, Đội ứng cứu sự cố, Trung tâm CNTT và Truyền thông chịu trách nhiệm chủ trì ứng cứu sự cố triển khai tổng hợp và xây dựng báo cáo kết thúc ứng phó sự cố, trong đó trình bày chi tiết quá trình xử lý sự cố, tóm tắt tổng quát về tình hình sự cố và đề xuất cách thức triển khai điều phối, ứng cứu sự cố nhằm xử lý nhanh, giảm nhẹ rủi ro và thiệt hại đối với sự cố tương tự.

Sau khi kết thúc ứng cứu sự cố, trong vòng 10 ngày đơn vị vận hành hệ thống thông tin, đơn vị được giao chủ trì ứng cứu hệ thống thông tin bị sự cố phải xây dựng báo cáo kết thúc ứng phó sự cố, gửi về Đội ứng cứu sự cố, Trung tâm CNTT và Truyền thông./.