UBND TỈNH BẮC KẠN **VĂN PHÒNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 167 /QĐ-VP	*Bắc Kạn, ngày 10 tháng 11 năm 2023*

QUYẾT ĐỊNH
Phê duyệt Phương án ứng phó sự cố, đảm bảo an toàn thông tin đối với Hệ thống thông tin Văn phòng UBND tỉnh

CHÁNH VĂN PHÒNG ỦY BAN NHÂN DÂN TỈNH

Căn cứ Luật An ninh mạng;

Căn cứ Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng; 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;

Căn cứ 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;

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

Căn cứ Thông tư số 20/2017/TTBTTTT ngày 12/9/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố An toàn thông tin mạng trên toàn quốc;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của 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;

Căn cứ Quyết định số 22/2021/QĐ-UBND ngày 03/12/2021 của UBND tỉnh về việc ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước trên địa bàn tỉnh Bắc Kạn; Quyết định số 2601/QĐ-UBND ngày 29/12/2021 của UBND tỉnh về việc ban hành Kế hoạch ứng phó sự cố, bảo đảm an toàn, an ninh thông tin mạng trên địa bàn tỉnh Bắc Kạn giai đoạn 2022 - 2025; Công văn số 7429/UBND-VXNV ngày 07/11/2022 của Chủ tịch UBND tỉnh về việc đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng;

Căn cứ Quyết định số 136/QĐ-STTTT ngày 20/10/2021, Quyết định số 146/QĐ-STTTT ngày 08/11/2021 của Sở Thông tin và Truyền thông về việc phê duyệt cấp độ an toàn hệ thống thông tin;

Căn cứ Quyết định số 42/2022/QĐ-UBND ngày 16/11/2022 của UBND tỉnh ban hành Quy định chức năng, nhiệm vụ, quyền hạn của Văn phòng UBND tỉnh Bắc Kạn;

Căn cứ Quyết định số 87/QĐ-VP ngày 17/5/2022 của Chánh Văn phòng UBND tỉnh về ban hành Quy chế làm việc của Văn phòng UBND tỉnh Bắc Kạn;

Xét đề nghị của Giám đốc Trung tâm Công báo - Tin học, Văn phòng UBND tỉnh.

QUYẾT ĐỊNH:

Điều 1. Phê duyệt Phương án ứng phó sự cố, bảo đảm an toàn thông tin đối với các hệ thống thông tin Văn phòng UBND tỉnh *(có Phương án kèm theo)*.

Điều 2. Phương án ứng phó sự cố, bảo đảm an toàn thông tin đối với các hệ thống thông tin Văn phòng UBND tỉnh là căn cứ để Lãnh đạo Văn phòng, Trưởng các phòng, ban, đơn vị trực thuộc Văn phòng chủ động chỉ đạo, điều hành các hoạt động ứng phó sự cố, bảo đảm an toàn thông tin mạng, hạn chế thấp nhất thiệt hại do sự cố mất an toàn, an ninh thông tin gây ra đối với các hệ thống thông tin của Văn phòng.

Điều 3. Quyết định này có hiệu lực kể từ ngày ký ban hành.

Điều 4. Giám đốc Trung tâm Công báo - Tin học, Trưởng các phòng, ban, đơn vị và công chức, viên chức, người lao động thuộc Văn phòng Ủy ban nhân dân tỉnh chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- UBND tỉnh (b/c);
- Sở Thông tin và Truyền thông tỉnh (b/c);
- LĐVP;
- Lưu: VT, TTCBTH (Hiếu).

CHÁNH VĂN PHÒNG

CỘNG HÒA X.H.C.N VIỆT NAM
VĂN PHÒNG ỦY BAN NHÂN DÂN
TỈNH BẮC KẠN

Vũ Đức Chính

UBND TỈNH BẮC KẠN
VĂN PHÒNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

PHƯƠNG ÁN
Ứng phó sự cố, bảo đảm an toàn thông tin đối với Hệ thống thông tin Văn phòng UBND tỉnh

(Kèm theo Quyết định số: /QĐ-VP ngày tháng 11 năm 2023 của Văn phòng UBND tỉnh)

I. MỤC ĐÍCH, YÊU CẦU

1. Phương án này hướng dẫn việc ứng cứu sự cố hệ thống thông tin, trách nhiệm của các phòng, ban, đơn vị trực thuộc Văn phòng và công chức, viên chức, người lao động thuộc Văn phòng có liên quan đến đảm bảo an toàn, an ninh thông tin đối với hệ thống thông tin Văn phòng UBND tỉnh.

2. Thường xuyên quán triệt và thực hiện có hiệu quả phương châm chủ động thực hiện kiểm tra các mối nguy hại, rà quét lỗ hổng hệ thống thông tin trong phạm vi quản lý nhằm phòng ngừa, chủ động, ứng phó kịp thời, khắc phục khẩn trương và hiệu quả các sự cố xảy ra.

3. Nâng cao năng lực xử lý tình huống sự cố, mất an toàn thông tin của công chức, viên chức và người lao động đối với các tình huống có thể xảy ra.

4. Giáo dục, tuyên truyền, cảnh báo, hướng dẫn các biện pháp phòng, tránh sự cố hệ thống thông tin nhằm phát huy ý thức tự giác, chủ động ứng phó của công chức, viên chức và người lao động thuộc Văn phòng.

II. NHIỆM VỤ

1. Trung tâm Công báo - Tin học là đầu mối thực hiện các nhiệm vụ về an toàn, an ninh thông tin.

2. Trưởng các phòng, ban, đơn vị trực thuộc Văn phòng quán triệt, triển khai, hướng dẫn, kiểm tra, đôn đốc việc thực hiện Phương án này.

3. Thường xuyên kiểm tra, đề xuất với Lãnh đạo Văn phòng công tác bảo đảm an toàn thông tin mạng định kỳ, hằng năm hoặc theo hướng dẫn của cơ quan chuyên môn.

4. Cử công chức, viên chức tham gia hoạt động ứng cứu sự cố nhằm bảo đảm an toàn thông tin mạng khi có các lớp tập huấn do UBND tỉnh, Sở Thông tin và Truyền thông hoặc các cơ quan chuyên môn tổ chức.

III. BIỆN PHÁP THỰC HIỆN PHÒNG NGỪA SỰ CỐ HỆ THỐNG THÔNG TIN

1. Về thông tin, tuyên truyền

Trưởng các phòng, ban, đơn vị thuộc Văn phòng thông qua các cuộc họp giao ban, sinh hoạt chi bộ tăng cường công tác tuyên truyền đến công chức, viên chức và người lao động nâng cao ý thức trách nhiệm về đảm bảo an toàn thông tin; tuyên truyền các văn bản, quy định hiện hành của Trung ương của tỉnh, quy định của đơn vị về an toàn, an ninh thông tin và các tài liệu hướng dẫn chuyên môn về an toàn thông tin mạng.

2. Nhận diện các nguy cơ, sự cố, mất an toàn hệ thống thông tin

Các nguy cơ, sự cố có khả năng ảnh hưởng đến hệ thống thông tin đối với hệ thống thông tin Văn phòng như sau:

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

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

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

- Sự cố liên quan đến các thảm họa thiên tai: Bão, lụt, gió lốc, động đất, sấm sét, hỏa hoạn,...

3. Phòng chống virus máy tính, bảo mật cơ sở dữ liệu và an ninh mạng

- Bảo mật số liệu: Công chức, viên chức và người lao động có trách nhiệm bảo mật số liệu nghiệp vụ trên máy tính. Không chia sẻ thư mục, dữ liệu cá nhân trên hệ thống mạng LAN cơ quan. Việc chia sẻ dữ liệu trên mạng do kỹ thuật phụ trách công nghệ thông tin của Văn phòng thực hiện khi Lãnh đạo Văn phòng yêu cầu.

- Bảo mật truy cập: Các chương trình, phần mềm được được bàn giao cho công chức, viên chức và người lao động sử dụng phải được thiết lập mật khẩu theo quy định. Kịp thời điều chỉnh vị trí công tác cho người sử dụng (khi có sự thay đổi); xóa, vô hiệu hóa các tài khoản người dùng đã nghỉ việc, nghỉ hưu, chuyển công tác...

- Bảo mật hệ thống mạng và truyền tin: Mạng và đường truyền được áp dụng các chế độ bảo mật cần thiết, chống xâm nhập bất hợp pháp. Kỹ thuật phụ trách an toàn thông tin (ATTT), công nghệ thông tin thường xuyên theo dõi, kiểm tra phát hiện kịp thời các hoạt động xâm nhập và có biện pháp xử lý kịp thời.

- An toàn trong sử dụng: Khi không làm việc với máy vi tính trong thời gian dài, công chức, viên chức, người lao động tại các phòng, ban, đơn vị phải tắt máy tính hoặc đặt chế độ bảo vệ để đảm bảo an toàn cho dữ liệu của cá nhân.

- Phòng, chống virus: Công chức, viên chức, người lao động thuộc Văn phòng có trách nhiệm tuân thủ các biện pháp, tài liệu hướng dẫn về cảnh báo về lỗ hổng bảo, cảnh báo nguy cơ tấn công theo tài liệu hướng dẫn của cơ quan có thẩm quyền nhằm rà soát, giám sát, ngăn chặn, phòng ngừa, xử lý kịp thời hạn chế đến mức thấp nhất nguy cơ gây mất an toàn an ninh thông tin. Mọi dữ liệu từ các thiết bị lưu trữ bên ngoài (USB, ổ cứng di động, thẻ nhớ,...) đều phải được quét, diệt virus trước khi sao chép vào máy. Những máy tính phát hiện có virus phải được báo cáo ngay cho kỹ thuật phụ trách công nghệ thông tin và tách khỏi hệ thống mạng về mặt vật lý để tránh tình trạng lây nhiễm sang các máy tính khác. Không truy cập vào các trang website, đường dẫn liên kết không rõ ràng hoặc tải về các tệp (file) tài liệu từ các địa chỉ thư không nắm rõ thông tin, địa chỉ người gửi.

4. Kiểm soát việc cài đặt các phần mềm và thực hiện cơ chế sao lưu, phục hồi

- Kiểm soát chặt chẽ việc cài đặt các phần mềm mới lên các máy tính: Các phần mềm được cài đặt trên máy tính (bao gồm hệ điều hành, các phần mềm ứng dụng văn phòng, phần mềm phục vụ công việc, tiện ích khác) phải được thường xuyên theo dõi, cập nhật bản vá lỗi bảo mật của nhà phát triển, lựa chọn cài đặt các phần mềm chống, diệt virus, mã độc có bản quyền và thường xuyên cập nhật phiên bản mới, đặt lịch quét virus theo định kỳ.

- Cơ chế sao lưu, phục hồi máy tính: Công chức, viên chức, người lao động phải thực hiện việc sao lưu định kỳ cơ sở dữ liệu và các dữ liệu quan trọng khác (bao gồm dữ liệu phát sinh trong quá trình vận hành các phần mềm ứng dụng như: Các tập tin văn bản, hình ảnh,…) vào các thiết bị lưu trữ bên ngoài (USB, ổ cứng di động, thẻ nhớ,...) nhằm phục vụ cho việc phục hồi, khắc phục dữ liệu kịp thời khi có sự cố xảy ra.

5. Đảm bảo an toàn hệ thống thông tin mạng LAN cơ quan

- Về cơ sở hạ tầng: Đảm bảo việc lắp đặt thiết bị chống sét, thiết bị cảnh báo phòng chống cháy, nổ tại trụ sở để bảo vệ hệ thống, thiết bị công nghệ thông tin.

- Quản lý hệ thống mạng nội bộ: Mạng nội bộ của Văn phòng khi kết nối với mạng Internet phải thông qua thiết bị tường lửa để kiểm soát, hạn chế việc truy cập trái phép từ bên ngoài. Các máy tính trên hệ thống phải được cài đặt phần mềm diệt virus có bản quyền.

- Quản lý hệ thống mạng không dây (wifi): Khi thiết lập mạng không dây có kết nối vào mạng nội bộ phải thiết lập các thông số cần thiết như định danh, mật mã, mã hóa dữ liệu, có thay đổi mật mã định kỳ.

- Quản lý truy cập từ xa vào mạng nội bộ: Đối với việc truy cập từ xa vào mạng nội bộ phải được theo dõi, quản lý chặt chẽ, nhất là truy cập có sử dụng chức năng quản trị, phải thiết lập mật mã độ an toàn cao, thường xuyên thay đổi mật mã, hạn chế truy cập từ xa vào mạng nội bộ từ các điểm truy cập Internet công cộng.

IV. PHÂN CÔNG THỰC HIỆN

1. Trách nhiệm của Trưởng các phòng, ban, đơn vị trực thuộc Văn phòng

- Thường xuyên chỉ đạo công chức, viên chức và người lao động thực hiện nghiêm các quy định bảo đảm an toàn thông tin hệ thống mạng LAN cơ quan.

- Chủ động theo dõi, phối hợp với Trung tâm Công báo - Tin học trong công tác kiểm tra, phát hiện, xử lý kịp thời các sự cố về an toàn thông tin mạng.

2. Trách nhiệm của công chức, viên chức và người lao động thuộc Văn phòng

- Có trách nhiệm quản lý tài khoản, mật khẩu đăng nhập vào các phần mềm dùng chung được triển khai tại Văn phòng; thực hiện nghiêm các quy định về đảm bảo an toàn thông tin trong hệ thống mạng LAN. Thường xuyên thay đổi mật khẩu đủ mạnh (ít nhất 9 ký tự, có chữ hoa, chữ thường, số, ký tự đặc biệt) để đảm bảo an toàn, an ninh thông tin.

- Thực hiện tiếp nhận, xử lý, phát hành, quản lý và lưu trữ văn bản, hồ sơ điện tử trên phần mềm quản lý văn bản đúng quy định trên môi trường mạng và ký số cá nhân, đảm bảo theo đúng quy định pháp luật hiện hành. Phải sử dụng thư điện tử công vụ để gửi, nhận văn bản giữa các cơ quan nhà nước.

- Không được tự ý cài đặt phần mềm, tải trên mạng không rõ nguồn gốc, phần mềm không an toàn khi chưa có sự đồng ý của Lãnh đạo Văn phòng.

- Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm virus, nhiễm mã độc trên máy tính (máy hoạt động chậm bất thường, cảnh báo từ phần mềm diệt virus, mất dữ liệu,…), người sử dụng phải báo ngay cho kỹ thuật phụ trách công nghệ thông tin, ATTT của Văn phòng để phối hợp xử lý kịp thời tránh lây lan đến các máy tính khác.

- Kỹ thuật phụ trách công nghệ thông tin đề xuất, tham mưu các văn bản liên quan đến ký số, cấp mới, thu hồi, gia hạn chứng thư số đơn vị, cá nhân theo quy định, phải đảm bảo an toàn thông tin. Tham mưu việc sửa chữa, bảo trì, cài đặt các thiết bị, phần mềm bảo mật tại các máy tính của Văn phòng tránh nguy cơ mất an toàn, an ninh thông tin máy tính người dùng.

3. Trách nhiệm của kỹ thuật phụ trách công nghệ thông tin, ATTT của Văn phòng

- Làm đầu mối ứng cứu sự cố đối với hệ thống mạng LAN cơ quan theo đúng quy trình ứng cứu sự cố dựa trên tính chất, mức độ, phạm vi và nguyên nhân xảy ra sự cố; bảo đảm nhanh chóng, chính xác, kịp thời, an toàn và hiệu quả.

- Phối hợp với các cơ quan, đơn vị có liên quan kiểm tra, rà soát đánh giá an toàn thông tin thường xuyên, định kỳ hoặc đột xuất khi có các yếu tố quan trọng, đặc biệt thay đổi để kịp thời phát hiện các lỗ hổng đang tồn tại, các nguy cơ mất an toàn thông tin mạng.

- Thực hiện phân quyền truy cập và hướng dẫn sử dụng cho công chức, viên chức và người lao động sử dụng các phần mềm dùng chung của tỉnh đang triển khai tại Văn phòng (như Phần mềm Quản lý văn bản và điều hành - iOffice, mail công vụ, hệ thống một cửa điện tử...)*;* kịp thời điều chỉnh vị trí công tác cho người sử dụng (khi có sự thay đổi); xóa khỏi hệ thống các tài khoản người dùng đã nghỉ hưu, chuyển công tác, thôi việc...

- Chịu trách nhiệm quản lý các tài khoản quản trị được bàn giao.

- Phối hợp với Sở Thông tin và Truyền thông và các cơ quan, các đơn vị có liên quan và các phòng, ban thuộc Văn phòng thực hiện khắc phục kịp thời các lỗi phát sinh của các phần mềm (nếu có) khi có phản ánh, yêu cầu.

- Chủ động thực hiện định kỳ rà quét lỗ hổng hệ thống thông tin trong phạm vi quản lý.

- Tham mưu, phối hợp việc cử công chức, viên chức và người lao động tham dự các lớp kỹ năng bảo vệ hệ thống thông tin do Sở Thông tin và Truyền thông, các cơ quan liên quan tổ chức.

4. Phương án ứng phó sự cố an toàn hệ thống thông tin

4.1. Phương án xử lý sự cố bị nhiễm virus, mã độc

Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm virus, nhiễm mã độc trên máy tính (máy hoạt động chậm bất thường, cảnh báo từ phần mềm diệt virus, mất dữ liệu,…), công chức, viên chức và người lao động thực hiện các bước như sau:

Bước 1. Khoanh vùng cô lập sự cố

- Sau khi phát hiện sự cố, công chức, viên chức và người lao thực hiện khoanh vùng cô lập máy tính bị sự cố, như: Ngắt kết nối máy tính khỏi hệ thống thông tin mạng LAN của cơ quan (tắt máy, rút dây mạng,…).

- Báo cáo ngay lãnh đạo phòng, ban, đơn vị các dấu hiệu sự cố; đồng thời thông báo kịp thời về Trung tâm Công báo - Tin học để cử kỹ thuật phụ trách công nghệ thông tin phối hợp kiểm tra, xử lý.

Bước 2. Thu thập thông tin phục vụ phân tích sự cố:

Kỹ thuật phụ trách công nghệ thông tin Văn phòng phối hợp với công chức, người lao động tại các phòng, ban, đơn vị thuộc Văn phòng kiểm tra máy tính đang bị sự cố để nắm bắt thông tin ban đầu về sự cố.

Bước 3. Phân tích sự cố:

- Kỹ thuật phụ trách công nghệ thông tin phối hợp với công chức, viên chức và người lao động kiểm tra máy tính đang bị sự cố để phân tích nguyên nhân ban đầu về sự cố.

- Các thông tin phân tích gồm: Thời điểm mà hệ thống sử dụng lần cuối cùng; phân tích dữ liệu; kiểm tra sự thay đổi cấu hình; kiểm tra hệ thống tập tin có bị mã độc; kiểm tra tập tin Internet history và các tập tin history khác; kiểm tra Registry và tiến trình; quan sát các tập tin, tiến trình lúc khởi động.

Bước 4. Xử lý sự cố:

- Trường hợp sự cố có khả năng kiểm soát, xử lý được: Kỹ thuật phụ trách công nghệ thông tin tiến hành xử lý sự cố bao gồm các bước: Gỡ bỏ phần mềm có chứa mã độc; phân tích và kiểm tra lỗ hổng sau khi thực hiện các bản vá lỗi; khôi phục dữ liệu; thu thập các tập tin, hình ảnh, email,… bị xóa, thời gian bị xóa; tìm kiếm các tập tin không thể khôi phục; khôi phục các tập tin phù hợp.

- Trường hợp sự cố ngoài khả năng kiểm soát, xử lý được (sự cố có tính chất nghiêm trọng): Triển khai ngay các biện pháp xử lý ngăn chặn tấn công tránh lây nhiễm sự cố các máy tính khác trên hệ thống thông tin và tham mưu, báo cáo, đề nghị Sở Thông tin và Truyền thông, Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Bắc Kạn, các đơn liên quan để có các biện pháp hỗ trợ, xử lý kịp thời.

Bước 5. Tổng hợp báo cáo:

- Sau khi triển khai các giải pháp ứng cứu sự cố, kỹ thuật phụ trách công nghệ thông tin tham mưu lãnh đạo Văn phòng, tổ chức họp phân tích nguyên nhân, rút kinh nghiệm trong hoạt động xử lý sự cố và đề xuất các biện pháp ứng cứu cho các sự cố tương tự.

- Tham mưu báo cáo kết quả ứng cứu sự cố xảy ra về Sở Thông tin và Truyền thông, Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Bắc Kạn để biết, theo dõi.

Bước 6. Lưu hồ sơ:

Toàn bộ các hồ sơ trong quá trình xử lý sự cố, kỹ thuật phụ trách công nghệ thông tin lưu trữ phục vụ các hoạt động quản lý và theo dõi, kiểm tra định kỳ.

4.2. Phương án xử lý sự cố tấn thay đổi giao diện

4.2.1. Phạm vi và đối tượng áp dụng

- Website của Văn phòng http://vpubnd.backan.gov.vn/

4.2.2. Nhân lực: Bộ phận chuyên trách công nghệ thông tin, an toàn thông tin của Văn phòng phối hợp với:

a) Lực lượng ứng cứu sự cố chuyên trách của tỉnh Bắc Kạn, gồm:

- Sở Thông tin và Truyền thông Bắc Kạn.

- Đội Ứng cứu sự cố mạng, máy tính của tỉnh.

b) Lực lượng điều phối ứng cứu quốc gia VNCERT/CC

c) Lực lượng thành viên mạng lưới ứng cứu Quốc gia:

- Lực lượng ứng cứu khẩn cấp: Cụm mạng lưới ứng cứu sự cố an toàn thông tin (ATTT) mạng số 1.

- Các Trung tâm, tổ chức, chuyên gia về tấn công mạng

d) Các nhà mạng, ISP:

TT	Tên đơn vị	Thông tin liên hệ
1	VNPT Bắc Kạn	Tổ 1, Phường Phùng Chí Kiên, thành phố Bắc Kạn
2	Viettel Bắc Kạn	Tổ 10, Phường Phùng Chí Kiên, Thành phố Bắc Kạn

đ) Các đơn vị cung cấp giải pháp hệ thống

4.2.3. Công cụ hỗ trợ

- Nhóm công cụ phát hiện tấn công thay đổi giao diện: Web Monitoring (VNCS), Site 24x7, OnWebChange, WebOrion, Vesionista, Monitis,...

- Nhóm công cụ phòng chống tấn công thay đổi giao diện: Honeynet/honeypot, Website Application Firewall, IDS/IPS,...

- Nhóm công cụ hỗ trợ phân tích, điều tra và ứng cứu sự cố tấn công thay đổi giao diện: Log analysis, Code review tools, IDA Pro, Olly Dbg, FTK Imager,...

- Nhóm công cụ hỗ trợ kiểm thử xâm nhập, đánh giá an toàn website: Acunetix Web Vulnerability Scan, IBM AppScan, Burpsuite, Nessus, metasploit,...

4.2.4. Phương án xử lý

4.2.4.1 Các kịch bản tấn công:

a) Kịch bản 1: Tấn công thay đổi toàn bộ mã nguồn

- Mô tả: Kẻ tấn công có thể ghi đè hoặc chỉnh sửa tệp tin index của website sau khi đã khai thác thành công.

- Phát hiện: Kịch bản tấn công dạng này có thể phát hiện thủ công hoặc tự động sử dụng các công cụ giám sát website hay kỹ thuật đối sánh mã nguồn.

b) Kịch bản 2: Tấn công chèn mã javascript

- Mô tả: Kẻ tấn công có thể chèn các đoạn mã javascipt độc hại nhằm điều hướng người dùng khi truy cập vào trang Web hay nhập các thông tin nhạy cảm.

- Phát hiện: Kịch bản tấn công dạng này có thể bị phát hiện dựa trên đối sánh mã nguồn, lọc các thẻ đặc biệt (như <script)

c) Kịch bản 3: Tấn công thay đổi một phần giao diện

- Mô tả: Kẻ tấn công có thể chèn một số thông tin/thông báo vào giao diện website hoặc xoá/thay thế một phần giao diện website.

- Phát hiện: Kịch bản tấn công dạng này có thể bị phát hiện dựa trên đối sánh mã nguồn, tuy nhiên không hoàn toàn dựa trên cấu trúc các thẻ mà còn kiểm soát tính toàn vẹn của giao diện (nhằm phát hiện sai khác so với giao diện ban đầu).

4.2.4.2. Một số biện pháp ứng cứu sự cố tấn công thay đổi giao diện

Thông báo cho Trung tâm Công nghệ thông tin và truyền thông (đơn vị đang quản lý máy chủ Web Văn phòng), đồng thời phối hợp thực hiện các biện pháp:

- Cô lập hệ thống bị tấn công, trong một số trường hợp cần duy trì hoạt động của trang web thì sử dụng hệ thống dự phòng.

- Tạo ảnh máy chủ web liên quan tấn công để điều tra, phân tích.

- Rà soát toàn bộ mã nguồn, kiểm tra các lỗi/lỗ hổng có thể bị khai thác nhằm tấn công leo thang đặc quyền (vd SQL injection, File Upload,...)

- Xây dựng cơ chế kiểm soát ký tự đầu vào tại các form nhập liệu.

- Dò quét các tệp tin thực thi trên hệ thống, cô lập và phân tích hành vi các tệp tin này

- Kiểm tra các dịch vụ đang hoạt động trên máy chủ chứa mã nguồn của web, vô hiệu hoá các dịch vụ không cần thiết.

- Thu thập các tệp tin nhật ký liên quan tấn công (web log, firewall log, IDS/IPS log, honeynet/honeypot log,...)

- Thay đổi đường dẫn/tài khoản quản trị nếu phát sinh nghi vấn liên quan đến hoạt động đăng nhập.

4.2.4.3. Triển khai các bước ứng cứu:

Bước 1: Phát hiện lỗ hổng

- Để phát hiện nguồn gốc lỗ hổng, thực hiện xem mã nguồn của trang đã bị tấn công thay đổi giao diện. Trong trường hợp website được phân tách rõ back-end và front-end, sử dụng dev-tools tìm kiếm các request ajax, json để biết được nguồn gốc của đoạn mã được thêm vào. Trường hợp cả trang web bị thay đổi nội dung hoàn toàn, có thể liên tưởng đến việc webserver đã bị kiểm soát và thay đổi tệp hệ thống (Trường hợp 1). Trường hợp kẻ tấn công chỉ chèn một đoạn script nhỏ vào để thay đổi giao diện web (XSS), có thể liên tưởng tới việc các form lưu trữ không an toàn hoặc đối tượng tấn công lợi dụng 01 lỗ hổng mã nguồn hoặc khai thác lỗ hổng các lệnh ghi ra html không an toàn,... ngay tại nơi code XSS được chèn (Trường hợp 2).

+ Đối với trường hợp 1: Triển khai rà soát toàn bộ hệ thống, các dịch vụ đang chạy có bị out-of-date không, kiểm tra bộ mã nguồn với các hàm đọc, ghi file, thực thi mã, kiểm tra logs...

+ Đối với trường hợp 2: Triển khai kiểm tra vùng code ghi ra đoạn mã này và kiểm tra trường này trên cơ sở dữ liệu. Sau đó, ta tìm kiếm các tác vụ, tập tin có nhiệm vụ tạo mới, thay đổi trường đó, sau đó tìm ra được form nhập liệu.

Bước 2: Xử lý và khắc phục lỗ hổng

- Ngăn chặn bước đầu ảnh hưởng của tấn công thay đổi giao diện:

+ Loại bỏ các nội dung đã bị thay thế bất hợp pháp bằng nội dung hợp lệ, hoặc khôi phục lại nội dung từ bản đã sao lưu dự phòng (backup) trước đó.

+ Đảm bảo hệ thống không còn lỗ hổng.

- Khôi phục lại hệ thống (khôi phục hệ thống về trạng thái hoạt động bình thường):

+ Thay đổi tất cả các mật khẩu của hệ thống nếu hệ thống cấp quyền xác thực người dùng và nghi ngờ mật khẩu đã bị lộ.

+ Nếu hệ thống đã có bản sao dự dự phòng, triển khai khôi phục lại hệ thống như bình thường.

- Sao lưu hệ thống. Sao lưu toàn bộ thông tin, dữ liệu lưu trên web để phục vụ công tác phân tích, tìm kiếm nguyên nhân sự cố tấn công giao diện hoặc giúp

phục hội các tệp đã bị xóa.

- Xác định nguyên nhân và khắc phục triệt để sự cố:

Sau khi tìm ra được lỗ hổng, việc khắc phục lỗ hổng có thể thực hiện bằng cách:

+ Xác định điểm yếu của hệ thống mà kẻ tấn công đã lợi dụng để tấn công thay đổi giao diện.

+ Tiến hành xem xét mã nguồn và giám sát các request (yêu cầu) đối với trang web. Trường hợp trang web chỉ bị thay đổi một phần, có thể liên tưởng đến lỗ hổng XSS và tiến hành tìm vị trí mã nguồn gây ra đoạn mã không an toàn bị lợi dụng để chèn và tấn công thay đổi giao diện.

+ Trường hợp nguồn gốc tấn công do từ hệ thống khác, đề nghị cắt kết nối với hệ thống bị lợi dụng.

- Triển khai khắc phục:

+ Vá các lỗi liên quan đến ứng dụng web (phối hợp với nhà cung cấp phần mềm, hệ thống), nếu nguyên nhân lỗi do phần ứng dụng web, lỗi lập trình.

+ Nâng cấp phần mềm hệ thống, loại bỏ ứng dụng không an toàn đối với trường hợp hệ điều hành, ứng dụng bị khai thác để tấn công giao diện.

- Truy vết, xác định kẻ tấn công (qua công cụ phân tích log).

Bước 3: Tổng kết và báo cáo

Triển khai tổng kết, đánh giá nguyên nhân để phòng ngừa các sự cố tương tự trong tương lai.

4.3. Mô tả tấn công bằng phishing

Phishing là từ khóa kết hợp giữa từ fishing (câu cá) và pranks (trò đùa phạm pháp qua điện thoại). Về cơ bản, phương thức này có tính chất như "câu" thông tin của người dùng.

Tấn công Phishing là kiểu tấn công giả mạo các tổ chức uy tín như ngân hàng, website giao dịch trực tuyến hay công ty thẻ tín dụng. Kẻ tấn công giả mạo, tin tặc tìm cách lừa người dùng để đánh cắp các thông tin nhạy cảm như: Tài khoản và mật khẩu đăng nhập, mật khẩu giao dịch, thẻ tín dụng và các thông tin quý giá khác, hoặc kẻ tấn công giả mạo cũng có thể lợi dụng để cài các phần mềm độc hại vào hệ thống, thiết bị nhằm thực hiện các hành động phi pháp khác.

Các phương thức tấn công giả mạo chủ yếu gồm:

- Tấn công giả mạo bằng email, tin nhắn: Kẻ tấn công, tin tặc gửi đến những email hoặc tin nhắn giả mạo một cá nhân, cơ quan, tổ chức uy tín. Trong nội dung email, nhúng một liên kết (link), hoặc tệp đính kèm có chứa mã độc. Khi người nhận nhấn vào đường link sẽ bị điều hướng đến website không an toàn hoặc một website giả mạo và đề nghị thực hiện đăng nhập, qua đó kẻ tấn công sẽ đánh cắp các thông tin đã cung cấp trên hệ thống, hoặc khi người nhận mở tệp đính kèm có chữa phần mềm độc hại, lúc đó thiết bị sẽ bị mã hóa đòi tiền chuộc (nếu là phần mềm mã độc tống tiền), phần mềm độc hại cài cửa hậu (backdoor) để tiếp tục lợi dụng, khai thác lỗ hổng để thu thập thông tin hoặc làm bàn đạp cho các cuộc tấn công khác.

- Những email giả mạo thường rất giống với email chính chủ, chỉ khác một vài chi tiết nhỏ, khiến cho nhiều người dùng nhầm lẫn và trở thành nạn nhân của cuộc tấn công, kẻ tấn công luôn cố gắng "ngụy trang" bằng nhiều yếu tố như:

Giả mạo địa chỉ người gửi, chẳng hạn giả mạo địa chỉ sale.congtyA@gmail.com, trong khi địa chỉ email chính là sales.congtyA@gmail.com

Chèn Logo chính thức của tổ chức để tăng độ tin cậy.

Sử dụng kĩ thuật giả mạo đường link để lừa người dùng (VD: text là vietcombank.com.vn nhưng khi click vào lại điều hướng tới vietconbank.com)

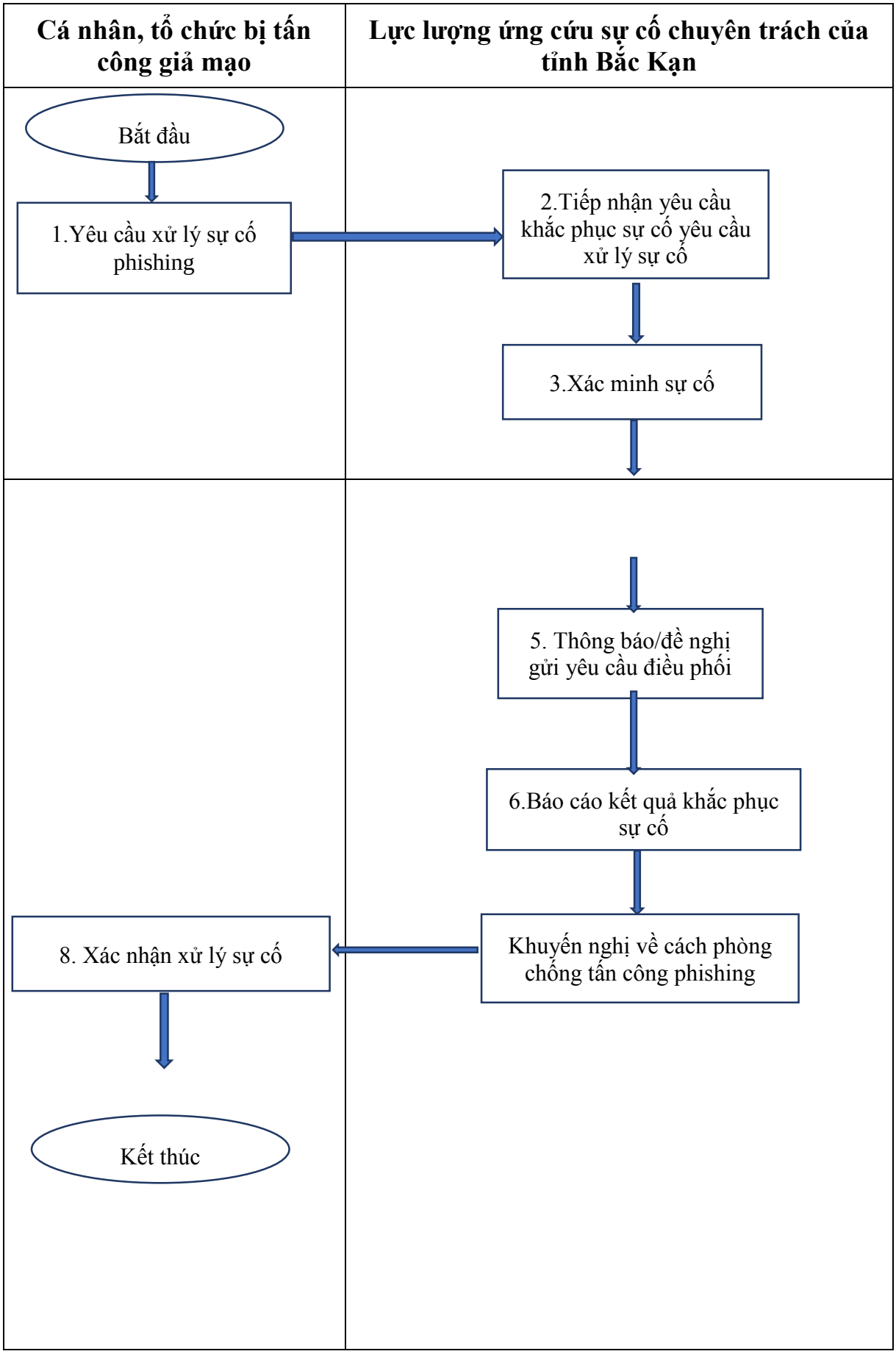
Sử dụng hình ảnh thương hiệu của các tổ chức trong email giả mạo để tăng độ tin cậy.

- Tấn công giả mạo website: Việc giả mạo website trong tấn công Phishing chỉ là làm giả một Landing page chứ không phải toàn bộ website. Trang được làm giả thường là trang đăng nhập để đánh cắp thông tin của nạn nhân. Kỹ thuật làm giả website có một số đặc điểm sau:

Thiết kế giống tới 99% so với website gốc

Đường link (url) chỉ khác 1 ký tự duy nhất. VD: reddit.com (thật) vs redit.com (giả); microsoft.com vs mircosoft.com hoặc verify-microsoft.com.

CÁC BƯỚC THỰC HIỆN XỬ LÝ SỰ CỐ



4.3.1. Các bước thực hiện xử lý sự cố

4.3.1.1. Yêu cầu xử lý sự cố phishing

Đề nghị phối hợp xử lý sự cố: Các cơ quan, tổ chức chuyên trách của tỉnh Bắc Kạn như: Sở Thông tin và Truyền thông; Đội Ứng cứu sự cố mạng, máy tính tỉnh.

4.3.1.2. Tiếp nhận yêu cầu khắc phục sự cố

Nguồn thông tin thông qua Email, điện thoại hoặc qua văn bản đến từ đại diện phía đơn vị gặp sự cố.

Thông tin tiếp nhận sự cố gồm

+ Thông tin về nguồn cung cấp sự cố như: Tên tổ chức, cá nhân, thông tin liên hệ

+ Mô tả về sự cố: Thời gian phát hiện, hiện tượng, hệ thống sự cố và nguồn tấn công (nếu có).

4.3.1.3. Xác minh sự cố

Đội Ứng cứu sự cố mạng, máy tính của tỉnh thực hiện xác minh địa chỉ (URL) phishing trong email có còn hoạt động đồng thời xác minh đích giả mạo của link phishing đang giả mạo đơn vị nào.

4.3.1.4. Kiểm tra các thông tin liên quan đến sự cố

Đội ứng cứu sự cố mạng, máy tính của tỉnh; bộ phận chuyên trách công nghệ thông tin, an toàn thông tin tiến hành xác minh tên miền phishing. Xác định địa chỉ IP và tên miền, xác định địa chỉ ISP thuộc sở hữu của nhà mạng nào. Xác định các thông tin liên hệ liên quan đến nhà mạng quản lý domain và địa chỉ IP của liên kết giả mạo.

4.3.1.5. Thông báo/đề nghị gửi lệnh điều phối

Đội ứng cứu sự cố mạng, máy tính của tỉnh; bộ phận chuyên trách công nghệ thông tin, an toàn thông tin của Văn phòng gửi yêu cầu đến các nhà mạng, ISP hoặc gửi đề nghị Trung tâm VNCERT/CC yêu cầu các nhà mạng phối hợp xử lý và bóc gỡ website giả mạo dựa trên các quyết định, nghị định được ban hành về ứng cứu sự cố an toàn thông tin mạng.

4.3.1.6. Khuyến nghị và cách phòng chống sự cố phishing:

Thông báo khuyến nghị đến các cơ quan, tổ chức đề nghị cảnh báo khi nhận được email hoặc tin nhắn có nội dung tương tự, không nhấp (click) và đường link hoặc mở các tệp đính kèm có chữa mã độc.

4.3.1.7. Báo cáo kết quả khắc phục sự cố

Bộ phận công nghệ thông tin của Văn phong, nhóm ứng cứu sự cố tiến hành lập báo cáo cho Lãnh đạo Văn phòng, đồng thời gửi Sở Thông tin và Truyền thông và các đơn vị liên quan về kết quả ứng cứu sự cố. Nội dung báo cáo gồm: dấu hiệu sự cố, quá trình xử lý, kết quả xử lý, đánh giá và khuyến nghị đưa ra.

4.3.1.8. Kết thúc.

V. TỔ CHỨC THỰC HIỆN

1. Các phòng, ban, đơn vị trực thuộc Văn phòng có trách nhiệm thực hiện Phương án, phối hợp với Trung tâm Công báo - Tin học, Phòng Hành chính tổ chức - Quản trị tài vụ trong quá trình tham gia ứng cứu sự cố an toàn thông tin khi xảy ra sự cố.

3. Thường xuyên phối hợp, thực hiện công tác đảm bảo an toàn, an ninh thông tin; rà, quét lỗ hổng hệ thống thông tin trong phạm vi quản lý theo quy định.

4. Phương án này được phổ biến đến toàn thể công chức, viên chức và người lao động thuộc Văn phòng biết để thực hiện. Trong quá trình thực hiện nếu có vướng mắc và cần sửa đổi, bổ sung, đề nghị các phòng, ban, đơn vị và cá nhân kịp thời phản ánh về Trung tâm Công báo - Tin học để tổng hợp, tham mưu, sửa đổi, bổ sung kịp thời./.