UBND TỈNH QUẢNG NGÃI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 1467 /STTTT-BCVT&CNTT

V/v triển khai thực hiện một số giải pháp tăng cường bảo đảm an toàn hệ thống thông tin trên địa bàn tỉnh

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

Quảng Ngãi, ngày 09 tháng 7 năm 2024

Kính gửi:
- Ủy ban MTTQ Việt Nam tỉnh;
- Văn phòng: Tỉnh ủy, Đoàn ĐBQH&HĐND, UBND tỉnh;
- Các sở, ban, ngành; Hội, đoàn thể tỉnh;
- UBND các huyện, thị xã, thành phố;
- Báo Quảng Ngãi; Đài Phát thanh và Truyền hình tỉnh;
- UBND các xã, phường, thị trấn;
- Trường Đại học Phạm Văn Đồng, Trường Cao đẳng Đặng Thùy Trâm, Trường Cao đẳng Việt Nam - Hàn Quốc.

Thực hiện chỉ đạo của UBND tỉnh tại Công văn số 3446/UBND-KGVX ngày 01/7/2024 về việc triển khai thực hiện một số giải pháp tăng cường bảo đảm an toàn hệ thống thông tin trên địa bàn tỉnh *(triển khai Công văn số 2517/BTTTT-CATTT ngày 27/6/2024 của Bộ Thông tin và Truyền thông về việc hướng dẫn một số giải pháp tăng cường đảm bảo an toàn hệ thống thông tin)*. Để tăng cường hiệu quả công tác bảo đảm an toàn thông tin và phục hồi nhanh hoạt động sau sự cố, bên cạnh việc triển khai đầy đủ các quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ, Sở Thông tin và Truyền thông kính đề nghị Thủ trưởng các cơ quan, đơn vị và địa phương triển khai thực hiện một số giải pháp tăng cường bảo đảm an toàn hệ thống thông tin như sau:

1. Định kỳ thực hiện sao lưu dữ liệu ngoại tuyến "offline". Với chiến lược sao lưu dữ liệu theo nguyên tắc 3-2-1: có ít nhất 03 bản sao dữ liệu, lưu trữ bản sao trên 02 phương tiện lưu trữ khác nhau, với 01 bản sao lưu ngoại tuyến "offline" (sử dụng các thiết bị: USB/ổ cứng di động/NAS/Tape, …). Dữ liệu sao lưu offline phải được tách biệt hoàn toàn, không kết nối mạng, cô lập để phòng chống tấn công leo thang vào hệ thống lưu trữ.

2. Triển khai giải pháp để sẵn sàng phục hồi nhanh hoạt động của hệ thống thông tin khi gặp sự cố, đưa hoạt động của hệ thống thông tin trở lại bình thường trong vòng 24 tiếng hoặc theo yêu cầu nghiệp vụ.

3. Triển khai các giải pháp, đặc biệt là giải pháp giám sát an toàn thông tin, để ngăn ngừa, kịp thời phát hiện sớm nguy cơ tấn công mạng đối với cả 3 giai đoạn: (1) xâm nhập vào hệ thống; (2) nằm gián điệp trong hệ thống; (3) khởi tạo quá trình phá hoại hệ thống.

4. Phân tách, kiểm soát truy cập giữa các phân vùng mạng. Đồng thời thực hiện chuyển đổi, nâng cấp các ứng dụng, giao thức, kết nối lạc hậu, không còn

được hỗ trợ kỹ thuật sang phương án sử dụng các nền tảng, ứng dụng để giảm thiểu nguy cơ tấn công mạng leo thang đặc quyền.

5. Tăng cường giám sát, quản lý các tài khoản quan trọng, tài khoản quản trị để phòng ngừa, giảm thiểu thiệt hại trong trường hợp kẻ tấn công có được tài khoản quản trị.

6. Rà soát, khắc phục và không để xảy ra các lỗi cơ bản dẫn đến mất an toàn hệ thống thông tin.

(Hướng dẫn chi tiết xem tại Phụ lục kèm theo)

Trong trường hợp cần hỗ trợ và điều phối xử lý, ứng cứu sự cố an toàn thông tin mạng, đề nghị các đơn vị kịp thời thông báo về Sở Thông tin và Truyền thông để có các biện pháp hỗ trợ, xử lý kịp thời.

Thông tin liên hệ:

- Bà Phạm Thị Ngọc Yến, Phó Giám đốc - Trung tâm Công nghệ thông tin và Truyền thông, Sở Thông tin và Truyền thông; Số điện thoại: 0906835511; Email: ptnyen-stttt@quangngai.gov.vn.

- Ông Nguyễn Công Nguyên, Chuyên viên Phòng Bưu chính - Viễn thông và Công nghệ thông tin, Sở Thông tin và Truyền thông; Số điện thoại: 0914559068; Email: ncnguyen-stttt@quangngai.gov.vn.

Đề nghị các cơ quan, đơn vị và địa phương quan tâm triển khai thực hiện./.

Nơi nhận:
- Như trên;
- UBND tỉnh (báo cáo);
- Sở TT&TT: GĐ, PGĐ;
- Trung tâm CNTT&TT (biết thực hiện);
- Lưu: VT, BCVT&CNTT.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH QUẢNG NGÃI

Trần Thanh Trường

Phụ lục

HƯỚNG DẪN MỘT SỐ GIẢI PHÁP TĂNG CƯỜNG BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN VÀ PHỤC HỒI NHANH HOẠT ĐỘNG SAU SỰ CỐ AN TOÀN THÔNG TIN MẠNG

(Kèm theo Công văn số / STTTT-BCVT&CNTT ngày /7/2024 của Sở Thông tin và Truyền thông)

I. ĐỊNH KỲ THỰC HIỆN SAO LƯU DỮ LIỆU NGOẠI TUYẾN "OFFLINE", CÔ LẬP (ISOLATE/AIR GAP). VỚI CHIẾN LƯỢC SAO LƯU DỮ LIỆU THEO NGUYÊN TẮC 3-2-1: CÓ 03 BA BẢN SAO DỮ LIỆU, LƯU TRỮ TRÊN 02 PHƯƠNG TIỆN LƯU TRỮ KHÁC NHAU, VỚI 01 BẢN SAO LƯU NGOẠI TUYẾN "OFFLINE"

1. Với chiến lược sao lưu dữ liệu theo nguyên tắc 3-2-1: có ít nhất 03 bản sao dữ liệu, lưu trữ bản sao trên 02 phương tiện lưu trữ khác nhau, với 01 bản sao lưu ngoại tuyến "offline":

- Có ít nhất 3 bản sao dữ liệu: Cần có ít nhất ba bản sao của dữ liệu, bao gồm dữ liệu gốc và hai bản sao lưu.

- Sao lưu trên 02 phương tiện khác nhau: Lưu trữ các bản sao này trên ít nhất hai phương tiện lưu trữ khác nhau (ví dụ: ổ cứng nội bộ, ổ cứng ngoài, băng từ, dịch vụ đám mây (Cloud)).

- Bản sao lưu ngoại tuyến (offline): Giữ ít nhất một bản sao lưu ngoại tuyến, không kết nối với Internet để tránh các mối đe dọa từ phần mềm độc hại và ransomware trên môi trường mạng.

2. Bản sao lưu ngoại tuyến được triển khai bằng một trong các giải pháp sau:

- Sao lưu bằng các thiết bị: USB/ổ cứng di động/NAS/Tape,…sau khi kết thúc phiên sao lưu, các thiết bị lưu trữ phải được tách rời khỏi hệ thống và không kết nối Internet;

- Có giải pháp cô lập dữ liệu sao lưu đặt các bản sao lưu ngoại tuyến ở một địa điểm an toàn và cách biệt để đảm bảo rằng chúng không thể bị truy cập hoặc tấn công qua mạng.

3. Với mỗi hệ thống khác nhau, với mỗi lượng dữ liệu lưu trữ của từng hệ thống, tổ chức có thể lựa chọn phương án sao lưu ở *mức tập tin (File)*, hoặc *mức máy ảo (Virtual machine)* (nếu có). Đối với mỗi mức sao lưu, quy trình khôi phục hệ thống cũng sẽ khác nhau, các cơ quan, đơn vị cần xây dựng phương án phù hợp theo nhu cầu khôi phục của cơ quan, đơn vị.

II. TRIỂN KHAI GIẢI PHÁP ĐỂ SẴN SÀNG PHỤC HỒI NHANH HỆ THỐNG THÔNG TIN KHI GẶP SỰ CỐ, ĐƯA HOẠT ĐỘNG TRỞ LẠI BÌNH THƯỜNG TRONG VÒNG 24 TIẾNG HOẶC THEO YÊU CẦU NGHIỆP VỤ

1. Rà soát, xây dựng và thực hiện kế hoạch khôi phục hệ thống, ứng phó sự cố an toàn thông tin (ATTT) mạng, bảo đảm:

- Có kế hoạch khôi phục cho từng loại dữ liệu quan trọng và từng hệ thống thông tin (HTTT);

- Có quy trình xử lý, khắc phục và sớm đưa hệ thống hoạt động trở lại bình thường trong vòng 24 giờ.

2. Tham gia, tổ chức các cuộc diễn tập phương án ứng cứu, khắc phục sự cố, phục hồi dữ liệu, khôi phục lại hoạt động bình thường của HTTT với các tình huống phổ biến, tấn công ransomware từ đó xác định tính khả thi của kế hoạch ứng phó sự cố.

3. Cấu hình triển khai các hệ thống dự phòng:

- Cấu hình hệ thống dự phòng: Triển khai hệ thống chuyển đổi dự phòng (Failover) để tự động chuyển đổi sang hệ thống dự phòng khi hệ thống chính gặp sự cố.

- Đồng bộ hóa dữ liệu: Đảm bảo dữ liệu giữa hệ thống chính và hệ thống dự phòng được đồng bộ liên tục.

4. Có nhiều phương pháp khác nhau để phục hồi nhanh chóng hệ thống như: Hot site, Warm site, Cold site, Cloud site:

- Hot Site: bao gồm các hệ thống dự phòng đang hoạt động và ở trạng thái gần như sẵn sàng tiếp nhận khối lượng công việc thay cho hệ thống chính. Các hệ thống tại một Hot site có thể đã có phần mềm ứng dụng và phần mềm quản lý cơ sở dữ liệu đã được cài đặt và hoạt động, các ứng dụng, phần mềm có thể được cập nhật vá lỗi như các hệ thống trong trung tâm xử lý chính.

- Warm Site: bao gồm các hệ thống xử lý thay thế, các hệ thống ở trạng thái sẵn sàng thấp hơn các hệ thống khôi phục Hot site. Ví dụ: mặc dù cùng một phiên bản hệ điều hành có thể đang chạy trên hệ thống Warm site, nhưng nó có thể chưa được cập nhật liên tục như các hệ thống chính.

- Cold Site: bao gồm các hệ thống xử lý thay thế với mức độ sẵn sàng cho các hệ thống có yêu cầu phục hồi thấp. Thông thường, có rất ít hoặc không có thiết bị ở Cold site. Khi xảy ra thảm họa hoặc sự có có tính gián đoạn cao, thời gian ngừng hoạt động dự kiến sẽ vượt quá 7 đến 14 ngày.

- Cloud Site: là phương án sử dụng dịch vụ lưu trữ Cloud làm điểm khôi phục hệ thống. Phương pháp này sẽ tính phí sử dụng máy chủ và thiết bị khi sử dụng. Do đó, chi phí cho phương án này vừa phải nhưng vẫn có thể đáp ứng các yêu cầu về thời gian, tính linh hoạt,...

III. TRIỂN KHAI CÁC GIẢI PHÁP, ĐẶC BIỆT LÀ GIẢI PHÁP GIÁM SÁT AN TOÀN THÔNG TIN, ĐỂ NGĂN NGỪA, KỊP THỜI PHÁT HIỆN SỚM NGUY CƠ TẤN CÔNG MẠNG ĐỐI VỚI CẢ 3 GIAI ĐOẠN: (1) XÂM NHẬP VÀO HỆ THỐNG; (2) NẰM GIÁN ĐIỆP TRONG HỆ THỐNG; (3) KHỞI TẠO QUÁ TRÌNH PHÁ HOẠI HỆ THỐNG

1. Thực hiện triển khai, duy trì kết nối các hệ thống thông tin về hệ thống Giám sát, điều hành an toàn, an ninh mạng tập trung (SOC) tại Trung tâm dữ

liệu tỉnh Quảng Ngãi để kịp thời phát hiện các dấu hiệu bất thường trên hệ thống thông tin tại các cơ quan, đơn vị. Các đơn vị chưa chia sẻ dữ liệu với hệ thống Giám sát, điều hành an toàn, an ninh tập trung (SOC), vui lòng có văn bản đề nghị Sở Thông tin và Truyền thông tỉnh Quảng Ngãi để kết nối, chia sẻ *(Hệ thống giám sát tập trung của tỉnh hiện có thể kết nối với các hệ thống thông tin có thiết bị tường lửa như: sophos, fortigate, pfsense,...và các dòng thiết bị tường lửa có chức năng Log setting).*

2. Thực hiện cài đặt, duy trì kết nối với Hệ thống phòng chống mã độc tập trung BKAV Endpoint AI tại Trung tâm dữ liệu tỉnh Quảng Ngãi; cài đặt BKAV Endpoint AI hoặc một số phần mềm phòng, chống mã độc khác *(Ưu tiên phần mềm có bản quyền, có thể kết nối, chia sẽ về Trung tâm giám sát an toàn không gian mạng quốc gia - NCSC)* trên toàn bộ các thiết bị máy chủ, máy trạm tại các cơ quan, đơn vị nhằm loại bỏ các mã độc tiềm ẩn trong hệ thống.

3. Định kỳ tổ chức, thực hiện kiểm tra, đánh giá lỗ hổng bảo mật để phát hiện sớm nguy cơ hệ thống bị xâm nhập và khắc phục kịp thời các điểm yếu đang tồn tại trên HTTT theo quy định của pháp luật, cụ thể: HTTT cấp độ 1, 2: tối thiểu 01 lần/02 năm; HTTT cấp độ 3, 4: tối thiểu 01 lần/01 năm; HTTT cấp độ 5: tối thiểu 01 lần/6 tháng.

4. Thực hiện săn lùng mối nguy hại (Threat hunting) tối thiểu 06 tháng/lần để phát hiện sớm dấu hiệu hệ thống thông tin đã bị thâm nhập, cài cắm mã độc,… giảm "thời gian trú ngụ của kẻ tấn công" bên trong HTTT.

5. Phát hiện máy chủ, máy trạm có dấu hiệu bất thường về mất an toàn thông tin, cần liên hệ với Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh để phối hợp ứng phó, khắc phục, xử lý sự cố.

IV. PHÂN TÁCH, KIỂM SOÁT TRUY CẬP GIỮA CÁC VÙNG MẠNG VÀ CHUYỂN ĐỔI, NÂNG CẤP CÁC ỨNG DỤNG, GIAO THỨC, KẾT NỐI LẠC HẬU, KHÔNG CÒN ĐƯỢC HỖ TRỢ KỸ THUẬT SANG PHƯƠNG ÁN SỬ DỤNG CÁC NỀN TẢNG, ỨNG DỤNG ĐỂ GIẢM THIỂU NGUY CƠ TẤN CÔNG MẠNG LEO THANG

1. Rà soát, phân vùng mạng các HTTT phù hợp theo cấp độ và có các giải pháp phòng chống xâm nhập mạng giữa các vùng mạng, đặc biệt giải pháp để ngăn ngừa nguy cơ bị tấn công leo thang từ người dùng nội bộ/người dùng cuối.

a) Rà soát, điều chỉnh thiết kế mô hình mạng để bảo bảo đảm hệ thống thông tin được phân vùng tối thiểu theo cấp độ *(Tham khảo các yêu cầu phân vùng mạng theo cấp độ tại Thông tư số 12/2022/TT-BTTTT của 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)* , với các vùng tối thiểu:

- Vùng mạng biên (outside zone): được thiết lập để cung cấp các kết nối hệ thống ra bên ngoài Internet và các mạng khác. Vùng mạng này bao gồm các cặp Core Switch, Firewall, được thiết lập để cung cấp các kết nối hệ thống ra bên ngoài Internet và các mạng khác.

- Vùng DMZ (demilitarized zone): Vùng mạng được thiết lập để đặt các máy chủ công cộng, cho phép truy cập trực tiếp từ các mạng bên ngoài và mạng Internet (thiết bị VPN, các máy chủ ứng dụng, dịch vụ Web, Email,… phục vụ người dùng từ bên ngoài Internet).

- Vùng máy chủ nội bộ (internal server zone): Vùng mạng bao gồm các máy chủ web, ứng dụng, AD, File Server,… phục vụ cho người dùng trong nội bộ.

- Vùng quản trị (management zone): Vùng mạng được thiết lập để đặt các máy chủ, máy quản trị và các thiết bị chuyên dụng khác phục vụ việc quản lý, vận hành và giám sát hệ thống (bao gồm các máy chủ vật lý, switch, router, thiết bị lưu trữ, máy chủ quản trị phần mềm diệt virus tập trung, máy chủ quản trị hệ thống máy ảo, máy chủ giải pháp sao lưu dữ liệu, máy chủ giám sát ATTT tập trung,…).

- Vùng máy chủ cơ sở dữ liệu (database server zone): Vùng mạng được thiết lập để đặt các máy chủ cơ sở dữ liệu. Vùng này bao gồm các máy chủ chứa cơ sở dữ liệu (CSDL) của các ứng dụng trong hệ thống ví dụ như: MySQL, Oracle, MSSQL,….

- Vùng mạng nội bộ (LAN - local area network): Vùng mạng này được thiết lập để cung cấp kết nối mạng cho các máy trạm và các thiết bị đầu cuối và các thiết bị khác của người sử dụng vào hệ thống. Vùng mạng này có thể chia nhỏ thành vùng mạng theo phòng ban hoặc theo chức năng, nhiệm vụ,…

- Vùng mạng không dây (nếu có): Vùng mạng không dây cần được tách riêng, độc lập với các vùng mạng khác: Bao gồm các Access point và Wifi Controller để quản lý các Access point.

- Vùng hệ thống dự phòng: Vùng mạng này bao gồm các máy chủ vật lý, thiết bị tối thiểu để phục vụ khôi phục hệ thống khi xảy ra sự cố. Vùng hệ thống dự phòng phải được tách biệt hoàn toàn với hệ thống chính về mặt logic: ngắt kết nối vật lý, hoặc được cô lập/cách lý (isolate) bằng các thiết bị kiểm soát truy cập.

b) Rà soát, cấu hình thiết lập các giải pháp để đảm bảo phòng chống xâm nhập giữa các phân vùng mạng, nhất là phòng chống leo thang giữa phân vùng mạng nội bộ (LAN) vào các phân vùng mạng khác.

2. Phân loại các thiết bị lạc hậu, không còn được hỗ trợ kỹ thuật hoặc có quyền truy cập trực tiếp đến hệ thống để giảm thiểu nguy cơ tấn công mạng leo thang từ phía người dùng.

Thực hiện loại bỏ các máy trạm có hệ điều hành windows thấp như: Windows 8, Windows 7, Windows XP,… các phiên bản này đã ngừng hỗ trợ bởi Microsoft, do đó bị ảnh hưởng bởi nhiều lỗ hổng từ mức cao đến nghiêm trọng như chiếm quyền điều khiển từ xa, leo thang đặc quyền, từ chối dịch vụ. Cài mới hoặc nâng cấp lên hệ điều hành mới nhất như Windows 10, Windows

11 để đảm bảo cập nhật các phần mềm bảo mật mới nhất của Microsoft về các tính năng bảo mật, các lỗ hổng.

V. TĂNG CƯỜNG GIÁM SÁT, QUẢN LÝ CÁC TÀI KHOẢN QUAN TRỌNG, TÀI KHOẢN QUẢN TRỊ HỆ THỐNG ĐỂ PHÒNG NGỪA HACKER CHIẾM QUYỀN, CÓ TÀI KHOẢN QUẢN TRỊ

1. Rà soát, tổng hợp và phân loại các tài khoản quan trọng, tài khoản quản trị hệ thống có nguy cơ bị tin tặc khai thác, chiếm quyền điều khiển hệ thống. Triển khai xác thực 2 lớp đối với tất cả tài khoản quản trị trên các hệ thống, ứng dụng quan trọng.

- Thống kê, rà soát và đánh giá lại việc phân quyền hệ thống theo Ma trận phân quyền truy cập (Access Control Matrix) và loại các điểm yếu, bất cập trong việc phân quyền quản lý, truy cập hệ thống.

- Phân vùng, thiết kế hệ thống để đảm bảo các tài khoản quản trị của hệ thống độc lập với các vùng mạng khác

2. Triển khai giải pháp quản lý tài khoản đặc quyền (PIM/PAM)

- Đối với các HTTT cấp độ 4 và cấp độ 5: Triển khai giải pháp quản lý tài khoản đặc quyền (PIM/PAM) đối tất cả 100% các hệ thống thông tin theo quy định.

- Đối với các HTTT cấp độ 3: Rà soát, đánh giá mức độ quan trọng và nguy cơ chiếm quyền điều khiển các tài khoản quản trị, từ đó đề xuất triển khai giải pháp quản lý tài khoản đặc quyền (PIM/PAM) phù hợp.

VI. RÀ SOÁT, KHẮC PHỤC CÁC LỖI CƠ BẢN CÓ NGUY CƠ GÂY MẤT AN TOÀN HỆ THỐNG THÔNG TIN THUỘC PHẠM VI QUẢN LÝ

1. Tổ chức triển khai rà soát, kịp thời khắc phục các lỗi trong quản lý, vận hành hệ thống thông tin và bảo đảm an toàn, an ninh mạng cho hệ thống thông tin như:

- Hệ thống sao lưu dự phòng online, cùng vùng mạng với hệ thống đang hoạt động.

- Sử dụng cùng thông tin đăng nhập (tài khoản và mật khẩu) cho nhiều hệ thống, thiết bị, quan trọng. Sử dụng mật khật khẩu mặt định, dễ đoán và không thay đổi định kỳ. Các thông tin đăng nhập được lưu trữ trên các trình duyệt như Google Chrome, Mozilla Firefox, Microsoft Edge, Cốc cốc,…

- Không cài đặt các phần mềm phòng phần mềm phòng chống mã độc trên thiết bị máy trạm.

- Không phân tách các phân vùng mạng với nhau vùng mạng LAN, WiFi, Camera cùng chung một phân vùng mạng.

- Các máy trạm sử dụng hệ điều hành thấp: Windows XP, Windows 7, Windows 8,…

- Kiểm soát truy cập từ đối tác, giữa các bộ phận chuyên môn trên các thiết bị tường lửa lỏng lẻo, không theo đúng nghiệp vụ chuyên môn.

- Không tuân thủ việc cập nhật các bản vá bảo mật theo khuyến nghị từ cơ quan chức năng, từ nhà cung cấp giải pháp, sản phẩm.

- Quản trị hệ thống sử dụng phần mềm bẻ khóa (phần mềm crack), dẫn đến việc nhiễm các dòng mã độc, cài cửa hậu (backdoor) hoặc đánh cắp mật khẩu.

2. Triển khai rà soát, khắc phục các lỗi cơ bản.

- Thực hiện đổi các mật khẩu quản trị trên các hệ thống thông tin quan trọng, và thực hiện đổi mật khẩu định kì theo các chu kì tiếp theo. Tăng cường giám sát, quản lý các tài khoản quan trọng, tài khoản quản trị để phòng ngừa, giảm bớt thiệt hại trong trường hợp kẻ tấn công có được tài khoản quản trị.

- Rà soát và đóng toàn bộ các kết nối cổng quản trị, cổng cơ sở dữ liệu (SSH, RDP, DB, ...) qua giao diện Internet đồng thời triển khai thực hiện qua kết nối an toàn (VPN, PAM, jump, xác thực đa yếu tố MFA,..). Rà soát và tiến hành khóa/ngắt các giao thức (protocol), dịch vụ (services) không sử dụng. Các hệ thống thông tin cấp độ 2 trở lên bắt buộc phải triển khai xác thực đa yếu tố.

- Rà soát cấp phát IP public, thực hiện ngắt các máy chủ (server), dịch vụ (services) có IP public nhưng không qua hệ thống Tường lửa (Firewall).

- Thực hiện rà soát các tài khoản VPN (Nếu có) có kết nối từ xa tới hệ thống thông tin đang được cấp phát, tiến hành ngắt đối với các tài khoản không sử dụng hoặc sử dụng sai mục đích.

- Chủ động thực hiện rà soát các lỗi lộ lọt mật khẩu, tài khoản người dùng trên các nền tảng chia sẻ dữ liệu tội phạm mạng (threat intelligent platform).

- Sử dụng có hiệu quả Nền tảng Điều phối xử lý sự cố an toàn thông tin mạng quốc gia (IRLab.vn) để được hướng dẫn, nhận các cảnh báo sớm và hỗ trợ xử lý sớm nguy cơ, sự cố. Sử dụng Nền tảng Hỗ trợ điều tra số (DFLab) trong trường hợp phù hợp để tổ chức ứng cứu sự cố và được sự hỗ trợ từ cơ quan nhà nước, các chuyên gia đầu ngành về an toàn thông tin./.
