HƯỚNG DẪN 06 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 /BTTTT-CATTT ngày tháng năm 2024 của Bộ 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".

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". Dữ liệu sao lưu offline phải được tách biệt hoàn toàn, không kết nối mạng hoặc được cô lập (isolate/air gap) để phòng chống tấn công leo thang vào hệ thống lưu trữ.

Bản sao lưu ngoại tuyến được triển khai bằng một trong các giải pháp sau để phòng chống tấn công theo thang vào hệ thống sao lưu, như sau:

+ Sao lưu bằng Tape/USB/Ổ cứng di động,…sau khi kết thúc phiên sao lưu, các thiết bị lưu trữ được tách rời khỏi hệ thống, không kết nối mạng;

+ Có giải pháp cô lập (isolate/airgap), khi kết thúc phiên sao lưu dữ liệu, giải pháp này cho phép cô lập/ngắt kết nối lôgíc của hệ thống sao lưu.

Triển khai chiến lược sao lưu và phục hồi dữ liệu, đảm bảo các yêu cầu đặt ra phù hợp với thực tế. Đồng thời xây dựng quy trình các bước sao lưu và phục hồi dữ liệu tương ứng với từng loại dữ liệu và hệ thống thông tin (HTTT).

Để xây dựng phương án sao lưu dữ liệu hệ thống, tổ chức cần dựa trên một số tiêu chí để xác định được mục tiêu khôi phục mà tổ chức mong muốn. Các tiêu chí để xác định mục tiêu khôi phục có thể là: Recovery Time Objective - RTO, Recovery Point Objective - RPO…

Recovery Time Objective - RTO: là thời gian khôi phục hệ thống mà tổ chức mong muốn: RTO có thể vài tiếng hoặc cũng có thể kéo dài vài ngày.

Recovery Point Objective - RPO: là khoảng thời gian mà dữ liệu có thể bị mất không thể khôi phục mà tổ chức có thể chấp nhận được.

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, hoặc mức máy ảo. 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.

Đối với sao lưu mức máy ảo, các dữ liệu sao lưu sẽ rất lớn. Khuyến nghị nên sử dụng các thiết bị sao lưu có tốc độ đọc ghi cao để đảm bảo tốc độc đọc ghi dữ liệu trong suốt quá trình sao lưu và khôi phục dữ liệu.

Dữ liệu sao lưu tối thiểu như sau: cấu hình của hệ thống và các phần mềm, ứng dụng; log file; dữ liệu quan trọng của hệ thống;.... Căn cứ yêu cầu thực tế của HTTT và nhu cầu, năng lực của tổ chức để thực hiện sao lưu theo kỳ, đối tượng dữ liệu sao lưu,... nhằm đảm bảo đủ điều kiện để có thể nhanh chóng khôi phục hoạt động của hệ thống nếu xảy ra tấn công mạng.

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

Căn cứ vào mục tiêu RPO, RTO… của tổ chức, từ đó triển khai giải pháp phục hồi hoạt động của hệ thống thông tin một cách phù hợp. Cụ thể:

- Rà soát, cập nhật Kế hoạch ứng phó sự cố ATTT mạng, bảo đảm:

+ Có kế hoạch khôi phục cho từng loại dữ liệu và từng HTTT;

+ Có quy trình xử lý, khắc phục và sớm đưa hệ thống hoạt động trở lại **bình thường trong vòng 24 giờ**, hoặc theo RTO tương ứng từng loại dữ liệu, HTTT.

- Tổ chức 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.

- Xây dựng và tổ chức triển khai ứng phó xử lý khủng hoảng truyền thông trong trường hợp xảy ra sự cố, giảm thiểu tác động và thiệt hại.

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,...

So sánh giữa các điểm phục hồi Cold, Warm, Hot, Cloud và một số đặc điểm của từng phương pháp.

	Cold	**Warm**	**Hot**	**Cloud (IaaS)**
Phần cứng	Mua sắm khi có sự cố	Đã sẵn sàng	Đã sẵn sàng và đã chạy	Sẵn sàng
Phần mềm	Cài đặt khi sự cố	Đã cài đặt	Đã cài đặt và đã chạy	Tùy mong muốn
Dữ liệu	Phục hồi khi có sự cố	Phục hồi khi có sự cố	Dữ liệu đồng bộ liên tục	Phục hồi khi có sự cố
Kết nối	Bắt đầu thiết lập khi sự cố	Sẵn sàng để hoạt động	Đã hoạt động	Đã hoạt động
Chi phí	Thấp nhất	Vừa phải	Cao nhất	Vừa phải

So sánh chi tiết các phương pháp Cold, Warm, Hot và Cloud

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. Triển khai giải pháp giám sát điều hành an toàn thông tin mạng (SOC), bảo đảm 100% các HTTT cấp độ 3 được giám sát an toàn thông tin tập trung, kịp thời phát hiện các dấu hiệu bất thường trên hệ thống.

Các giải pháp SOC cần có tính năng cho phép theo dõi, phát hiện các sự kiện bất thường (nhất là mã độc) trong cả 03 giai đoạn: (1) xâm nhập vào hệ thống; (2) nằm gián điệp trong hệ thống; (3) khởi tạo quá trình phá hoại hệ thống.

Đặc biệt, giải pháp SOC cần kịp thời phát hiện sớm khi kẻ tấn công (mã độc) khởi tạo quá trình phá hoại hệ thống, từ đó thực hiện các biện pháp cô lập, xử lý nhằm ngăn chặn lây lan, tấn công leo thang.

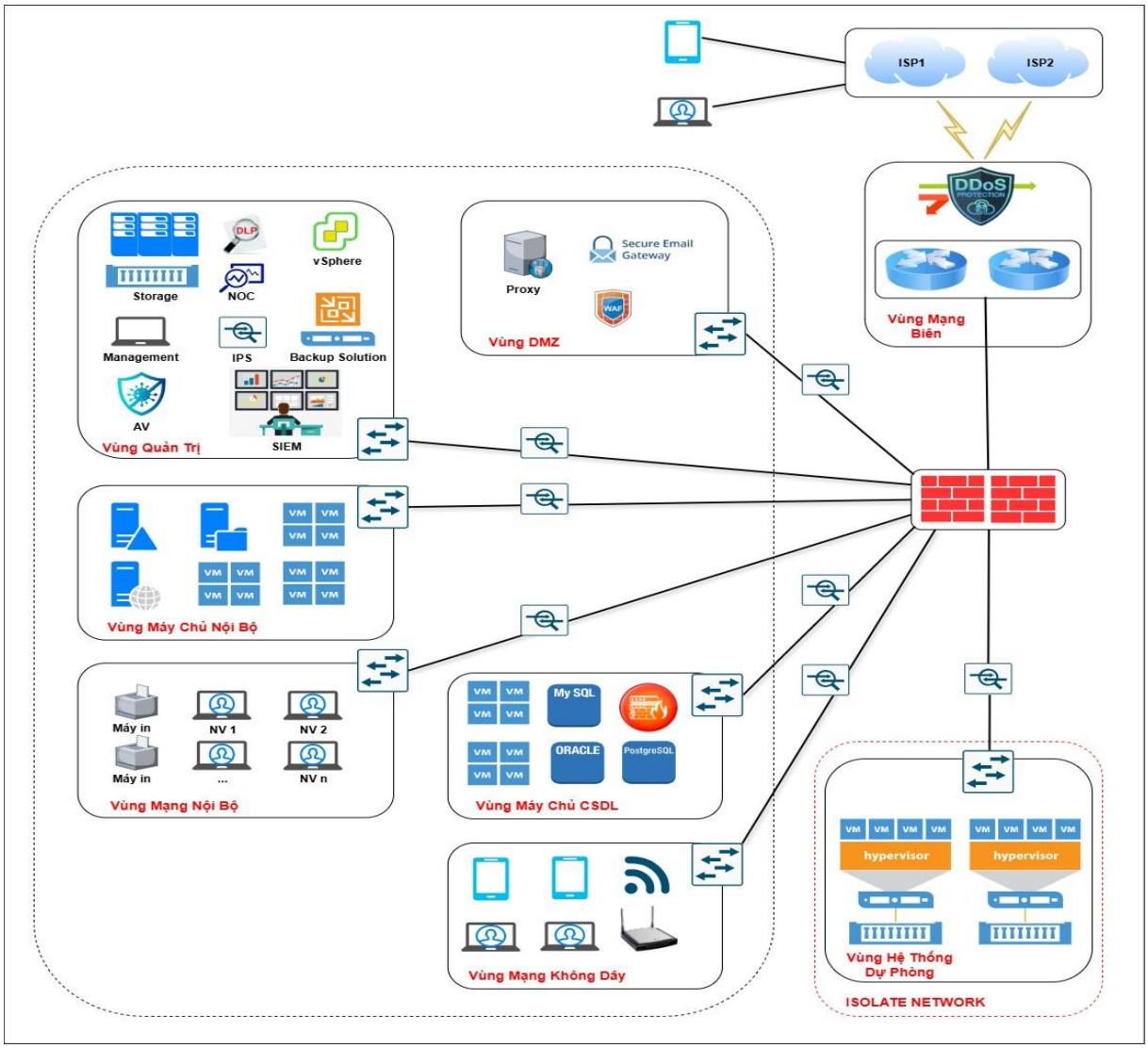
2. Định kỳ thực hiện kiểm tra, đánh giá lỗ hổng bảo mật để phát hiện sớm nguy cơ hệ thống bị xâm nhập và khắc phục kịp thời các điểm yếu đang tồn tại trên HTTT theo quy định của pháp luật, cụ thể: HTTT cấp độ 1, 2: tối thiểu 01 lần/02 năm; HTTT cấp độ 3, 4: tối thiểu 01 lần/01 năm; HTTT cấp độ 5: tối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

01 lần/06 tháng.

3. Thực hiện săn lùng mối nguy hại (threat hunting), đặc biệt là sau khi phát hiện có hoạt động tấn công mạng thành công vào hệ thống, 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.

4. Triển khai giải pháp phòng chống mã độc tập trung, đặc biệt là cài đặt giải pháp Chống phần mềm mã độc (AV), Phát hiện và phản hồi các mối nguy hại tại điểm cuối (EDR) tối thiểu trên tất cả các máy chủ, máy quản trị (hỗ trợ cài đặt).

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 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, với các vùng tương ứng:

- Vùng mạng biên (outside zone)

Vùng mạng 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 chạy HA với nhau, 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, cập nhật giải pháp để đảm bảo phòng chống xâm nhập giữa các vùng mạng, nhất là phòng chống leo thang giữa Vùng mạng nội bộ (LAN) vào các vùng mạng khác.

2. Phân loại các ứng dụng và phần mềm, giao thức, kết nối lạc hậu, không còn được hỗ trợ kỹ thuật hoặc có quyền truy cập trực tiếp đến hệ thống sang phương án sử dụng các ứng dụng (app/web based) để giảm thiểu nguy cơ tấn công mạng leo thang từ phía người dùng.

a) Thống kê các ứng dụng, phần mềm do người dùng tại Vùng mạng nội bộ (LAN) có quyền truy cập trực tiếp vào các vùng mạng quan trọng như: Vùng máy chủ nội bộ, Vùng máy chủ cơ sở dữ liệu, …

b) Rà soát, điều chỉnh, nâng cấp, cập nhật các ứng dụng và thiết lập chế độ phân quyền người dùng, phân quyền truy cập hệ thống để hạn chế nguy cơ tấn công leo thang khi tin tặc chiếm quyền được máy tính người dùng có thể tấn công leo thang vào các vùng mạng quan trọng trong tổ chức.

3. Tổ chức rà soát, quản lý phân quyền ứng dụng để triển khai giải pháp quản lý tài khoản đặc quyền (PIM/PAM) cho các tài khoản quan trọng.

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.

a) 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.

b) 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)

a) 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.

b) 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 cơ bản trong quản lý, vận hành và bảo đảm an toàn, an ninh mạng cho hệ thống thông tin như:

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

(2) Không thay đổi mật khẩu tài khoản quản trị, tài khoản quan trọng định kỳ hoặc thu hồi quyền đối với tài khoản khi người quản trị nghỉ việc.

(3) Để các máy chủ quan trọng, máy chủ quản trị kết nối trực tiếp với Internet nhưng không được bảo vệ hoặc mở dịch vụ không cần thiết.

(4) Các máy chủ, máy quản trị được cài các phần mềm AV, EDR nhưng khi kẻ tấn công vô hiệu hóa các tính năng này, hệ thống không phát hiện được.

(5) Sử dụng cùng thông tin đăng nhập (tài khoản và mật khẩu) cho nhiều hệ thống, thiết bị, quan trọng. Thông tin đăng nhập được lưu trữ trên các máy tính quản trị và các máy chủ không được mã hóa.

(6) 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.

(7) 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.

(8) Phân quyền tài khoản người dùng đối với hệ thống, ứng dụng không hợp lý, chưa tuân thủ nguyên tắc đặc quyền tối thiểu, cho phép kẻ tấn công dễ dàng có được quyền cao nhất khi khai thác lỗ hổng bảo mật.

(9) 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 quản trị.

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

a) Thực hiện đổi ngay 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.

b) 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 cấp độ 2 trở lên bắt buộc phải triển khai xác thực đa yếu tố.

c) Rà soát cấp phát IP public, thực hiện ngắt các server dịch vụ có IP public nhưng không qua hệ thống Firewall

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

đ) 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).

Cục An toàn thông tin (Bộ Thông tin và Truyền thông) sẽ công bố và cập nhật danh sách các lỗi cơ bản trên website https://ais.gov.vn.