UBND TỈNH KHÁNH HÒA **SỞ THÔNG TIN VÀ TRUYỀN THÔNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số:1312 /STTTT-TTCNTT&DVHCCTT V/v hướng dẫn một số biện pháp phòng chống, giảm thiểu rủi ro từ tấn công tấn công mã hóa tống tiền (ransomware)	*Khánh Hòa, ngày 26 tháng 4 năm 2024*

Kính gửi:

- Các cơ quan tham mưu, giúp việc Tỉnh ủy;
- Các huyện, thị, thành ủy và Đảng ủy trực thuộc;
- Các cơ quan Mặt trận, đoàn thể tỉnh;
- Các Sở, ban, ngành;
- Các đơn vị sự nghiệp trực thuộc UBND tỉnh;
- Các cơ quan ngành dọc Trung ương;
- UBND các huyện, thị xã, thành phố;
- UBND các xã, phường, thị trấn;
- Các doanh nghiệp nhà nước thuộc tỉnh.

Qua theo dõi, giám sát hoạt động tấn công mạng thời gian qua, Cục An toàn thông tin (Bộ Thông tin và Truyền thông) đã cảnh báo việc xuất hiện các chiến dịch tấn công mã hóa tống tiền (ransomware) nhằm vào các cơ quan, tổ chức, doanh nghiệp tại Việt Nam, đặc biệt là các tổ chức hoạt động trong lĩnh vực quan trọng như: tài chính, ngân hàng, năng lượng, viễn thông. Hiện nay, đã có nhiều cơ quan, tổ chức, doanh nghiệp bị tấn công mạng, gây thiệt hại về tài sản, ảnh hưởng đến uy tín và làm gián đoạn hoạt động của các hệ thống thông tin.

Nhằm triển khai các phương án phòng chống, giảm thiểu rủi ro từ t tấn công mã hóa tống tiền (ransomware), Sở Thông tin và Truyền thông hướng dẫn các cơ quan, đơn vị, địa phương một số biện pháp phòng chống, giảm thiểu rủi ro từ tấn công ransomware liên quan đến công tác thiết lập hệ thống mạng nội bộ, quản lý tài khoản truy cập, khai thác hệ thống thông tin dùng chung, cụ thể như sau:

1. Thiết lập phân vùng truy cập mạng

- Thiết lập vùng mạng không dây, mạng công cộng phục vụ người dân, doanh nghiệp, khách hàng đến cơ quan liên hệ công tác,… tách biệt hoàn toàn về mặt vật lý với hệ thống mạng nội bộ của cơ quan phục vụ tác nghiệp, hoạt động công vụ.

- Thực hiện phân vùng mạng giữa vùng mạng quản trị với vùng mạng người dùng thường, phân vùng mạng riêng cho các phòng ban.

- Trang bị các thiết bị chuyển mạch, thiết bị định tuyến, thiết bị bảo mật có băng thông vật lý tại các cổng giao tiếp tối thiểu 01Gbps, tương thích giao thức IPv6.

- Sử dụng tường lửa để kiểm soát truy cập giữa các vùng, các máy chủ, áp dụng nguyên lý tối thiểu hóa truy cập. Kiểm soát chặt chẽ, hạn chế quyền truy cập đến vùng mạng quan trọng.

Các tính năng tối thiểu trên thiết bị tường lửa cần đảm bảo:

+ Tương thích với giải pháp kết nối mạng SD-WAN, các chức năng định tuyến, kiểm soát truy cập, giám sát truy cập.

+ Phòng chống tấn công DDoS, IDS/IPS, Web/App Control, Web Threat Protection, Advanced Threat Protection.

- Xây dựng phương án theo dõi, giám sát an toàn thông tin cho hệ thống mạng nội bộ. Thiết lập chính sách ngăn chặn kết nối đến danh sách các địa chỉ do Cục an toàn thông tin, Trung tâm Giám sát an toàn không gian mạng quốc gia NCSC, Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT) khuyến nghị.

2. Trang bị bản quyền phần mềm

- Trang bị bản quyền bản quyền hệ điều hành, bản quyền phần mềm soạn thảo văn bản *(ví dụ: Microsoft Windows 10, Microsoft Office 2017 trở lên)*, bản quyền phần mềm phòng chống mã độc (antivirus), bản quyền phần mềm ứng dụng... cho các máy tính làm việc tại cơ quan, đơn vị, địa phương.

- Xem xét ưu tiên trang bị cho các máy tính có kết nối, truy cập sử dụng và khai thác dữ liệu từ những hệ thống thông tin dùng chung của tỉnh.

- Đối với hệ thống máy chủ, trang bị bản quyền hệ điều hành, cơ sở dữ liệu tùy thuộc vào loại mã nguồn của dịch vụ ứng dụng và dữ liệu đang sử dụng *(ví dụ: Microsoft Windows Server 2019, Microsoft SQL Server 2019 trở lên)*.

- Triển khai mô hình máy chủ ảo hóa như Hyper-V, VMWare.

Đối với phần mềm phòng chống mã độc (antivirus), các cơ quan, đơn vị, địa phương cần lưu ý sử dụng sản phẩm từ các hãng phần mềm bảo mật uy tín, đáp ứng yêu cầu kỹ thuật tối thiểu theo Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng, chống phần mềm độc hại, Công văn số 2290/BTTTT-CATTT ngày 17/7/2018 của Bộ Thông tin và Truyền thông về việc hướng dẫn kết nối, chia sẻ thông tin về mã độc giữa các hệ thống kỹ thuật.

3. Thực hiện sao lưu định kỳ dữ liệu

Tùy theo mức độ quan trọng và khối lượng dữ liệu phát sinh, thực hiện sao lưu dữ liệu định kỳ (hàng tháng, hàng tuần, hàng ngày), đảm bảo dữ liệu của các bản sao lưu được đầy đủ và tách biệt với hệ trống mạng đang sử dụng nhằm hạn

chế, giảm thiểu ảnh hưởng của việc mất dữ liệu (khi bị mã hóa) và đẩy nhanh quá trình khôi phục khi có sự cố theo các phương pháp sau:

- Sao lưu tại chỗ: Phương pháp lưu trữ dữ liệu sử dụng các thiết bị lưu trữ cục bộ để sao lưu dữ liệu trên máy tính. Một số thiết bị thường được sử dụng: USB, ổ cứng ngoài… cho đến các thiết bị chuyên dụng như NAS, SAN. Tuy nhiên cần lưu ý dữ liệu trong các ổ lưu trữ này hoàn toàn có thể bị ảnh hưởng nếu kết nối vào máy tính đã bị nhiễm mã độc Ransomware. Do vậy, phải đảm bảo máy tính chưa bị nhiễm mã độc trước khi sao lưu hoặc khởi động máy tính từ ổ đĩa khởi động ngoài (USB Boot) khi thực hiện sao lưu để đảm bảo an toàn. Thực hiện việc sao lưu "offline", không để các bản sao lưu đặt trong môi trường kết nối với hạ tầng mạng.

- Sao lưu sử dụng dịch vụ lưu trữ: Phương pháp sao lưu đám mây hay còn gọi là Online Backup - sao lưu trực tuyến, là một phương án sao lưu dữ liệu qua mạng đến một hệ thống sao lưu dữ liệu bên ngoài cơ quan, đơn vị.

Một số khuyến nghị về trang thiết bị, phần mềm sao lưu dữ liệu:

- Thiết bị sao lưu lớp 1: Thiết bị sao lưu dữ liệu (NAS, SAN…) có dung lượng cho phép lưu trữ tối thiểu 07 ngày đối với toàn bộ dữ liệu của hệ thống.

- Thiết bị sao lưu lớp 2: Thiết bị sao lưu dữ liệu (NAS, SAN…), triển khai phương án cô lập về mặt vật lý sau khi hoàn tất phiên sao lưu.

- Trang bị phần mềm sao lưu dữ liệu chuyên dụng để thiết lập, lựa chọn các yêu cầu sao lưu dữ liệu khác nhau tùy theo mục đích sử dụng.

- Xây dựng phương án thuê dịch vụ công nghệ thông tin phục vụ việc sao lưu dữ liệu dự phòng thảm họa (mã độc, thiên tai…).

4. Phòng ngừa để hạn chế tối đa khả năng bị nhiễm mã độc

- Thiết lập quyền người sử dụng không ở chế độ quản trị hệ thống (admin) và thiết lập các cấu hình bảo vệ tập tin không cho xóa, sửa các tập tin dữ liệu quan trọng một cách tự động. Ngăn chặn thực thi ứng dụng từ các thư mục chứa dữ liệu.

- Thường xuyên sử dụng phần mềm diệt mã độc, virus kiểm tra máy tính, ổ lưu trữ để phát hiện sớm nếu xuất hiện mã độc trên thiết bị.

- Yêu cầu người sử dụng chú ý cảnh giác với các tập tin đính kèm, các đường dẫn (link) được gửi đến qua thư điện tử hoặc tin nhắn, hạn chế tối đa việc truy cập vào các đường dẫn này vì đối tượng tấn công có thể đánh cắp hoặc giả mạo thư điện tử của người gửi phát tán các kết nối chứa mã độc.

- Sử dụng phần mềm diệt mã độc, virus kiểm tra các tập tin được gửi qua thư điện tử, tải từ trên mạng về trước khi kích hoạt. Nếu không cần thiết hoặc không rõ nguồn gốc thì không kích hoạt các tập tin này; tắt chế độ tự động mở, chạy các tập tin (autoruns) đính kèm theo thư điện tử.

- Cập nhật các phần mềm, hệ điều hành lên phiên bản mới nhất hiện có, ưu tiên vá lỗi kịp thời cho các máy chủ kết nối Internet cung cấp dịch vụ ra Internet.

- Cập nhật đầy đủ bản vá mới nhất tất cả các trình ảo hóa và cơ sở hạ tầng CNTT liên quan.

- Thường xuyên cập nhật thông tin về các lỗ hổng mới được phát hiện, công bố, đảm bảo bản vá lỗ hổng được tải từ nguồn tin cậy.

- Thường xuyên, liên tục sử dụng các Nền tảng về an toàn thông tin do Cục An toàn thông tin (Bộ Thông tin và Truyền thông) phát triển, cung cấp để hỗ trợ các cơ quan, tổ chức, doanh nghiệp: Nền tảng Điều phối xử lý sự cố an toàn thông tin mạng quốc gia (IRLab): https://irlab.vn/ để được hướng dẫn, nhận các cảnh báo sớm và hỗ trợ xử lý sớm nguy cơ, sự cố; Nền tảng Hỗ trợ điều tra số (DFLab): https://df.irlab.vn/ 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.

5. Tuân thủ các quy định về đảm bảo an toàn thông tin

- Để đảm bảo an toàn thông tin và bảo mật dữ liệu khi tham gia hoạt động trên môi trường mạng, đề nghị các cơ quan, đơn vị, địa phương thực hiện xây dựng và phê duyệt Hồ sơ đề xuất cấp độ an toàn hệ thống thông tin đối với các hệ thông thông tin do cơ quan, đơn vị, địa phương vận hành.

- Đối với các hệ thống thông tin đã được phê duyệt Hồ sơ đề xuất cấp độ, đề nghị cơ quan, đơn vị, địa phương triển khai đầy đủ các phương án đảm bảo an toàn thông tin đã được thuyết minh và phê duyệt.

- Thường xuyên, định kỳ thực hiện việc đánh giá an toàn thông tin hệ thống mạng nội bộ.

- Xây dựng phương án, quy chế quản lý và sử dụng tài khoản, thiết bị khai thác sử dụng các hệ thống thông tin dùng chung.

- Tập huấn, đào tạo nhận thức an ninh mạng cho cán bộ, công chức, viên chức và thường xuyên rà soát các quy trình, chính sách an ninh của cơ quan, để đảm bảo vận hành đúng cách và hiệu quả, tránh gây ra những lỗ hổng bảo mật.

6. Xử lý khi phát hiện bị lây nhiễm mã độc

Khi mã độc Ransomware lây nhiễm vào máy tính, mã độc sẽ tiến hành mã hóa các tập tin dữ liệu trong một khoảng thời gian, đồng thời khóa máy tính của người dùng để người dùng không can thiệp tắt các tiến trình đang chạy. Do đó, việc phản ứng nhanh chóng khi phát hiện ra sự cố có thể giúp giảm thiểu thiệt hại cho các dữ liệu chứa trên máy bị nhiễm và tăng khả năng khôi phục các dữ liệu đã bị mã hóa.

Cụ thể, đối với các máy tính cá nhân khi phát hiện có dấu hiệu bị nhiễm mã độc Ransomware cần phải nhanh chóng thực hiện các thao tác sau:

- Nhanh chóng tắt máy tính bằng cách ngắt nguồn điện (không sử dụng chức năng shutdown của Hệ điều hành Windows). Cách ly máy tính ra khỏi mạng nội bộ nhằm ngăn ngừa trường hợp có thể lây nhiễm sang các máy tính khác trong hệ thống.

- Báo cáo sự cố ngay lập tức cho bộ phận an ninh thông tin cơ quan để có phản ứng nhanh chóng.

- Không được khởi động lại máy tính theo cách thông thường mà phải khởi động lại máy tính từ Hệ điều hành sạch (từ đĩa CD hoặc từ USB), hoặc tháo ổ cứng ra để kết nối vào máy tính sạch khác, khuyến cáo sử dụng các Hệ điều hành Linux. Sau đó thực hiện kiểm tra các tập tin dữ liệu và sao lưu các dữ liệu chưa bị mã hóa.

Sau khi xử lý khắc phục, phục hồi dữ liệu từ bản sao lưu đã tạo trước khi bị tấn công.

Trên đây là một số nội dung hướng dẫn phương án phòng chống, giảm thiểu rủi ro từ tấn công mã hóa tống tiền (ransomware), Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị, địa phương nghiên cứu triển khai, thực hiện và phổ biến đến các cơ quan, đơn vị, doanh nghiệp thuộc phạm vi quản lý để thực hiện.

Quá trình triển khai nếu có vướng mắc, khó khăn đề nghị cơ quan, đơn vị, địa phương liên hệ Trung tâm Công nghệ thông tin và Dịch vụ hành chính công trực tuyến, Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ *(gặp ông Phan Quang Vinh; điện thoại 0258.3899888)*.

Trân trọng./.

Nơi nhận:
- Như trên (VBĐT);
- UBND tỉnh (VBĐT, để b/c);
- Lưu: VT, TTCNTT&DVHCCTT (PV).

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

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

Nguyễn Văn Hiền