CỤC AN TOÀN THÔNG TIN
AUTHORITY OF INFORMATION SECURITY

NCSC VN
National Cyber Security Center

VNCERT/CC

CẨM NANG

PHÒNG CHỐNG, GIẢM THIỂU RỦI RO TỪ TẤN CÔNG

RANSOMWARE

Tháng 4 năm 2024

NCSC.VN National Cyber Security Center

CỤC AN TOÀN THÔNG TIN
AUTHORITY OF INFORMATION SECURITY

VNCERT/CC

CẨM NANG PHÒNG CHỐNG , GIẢM THIỂU RỦI RO TỪ TẤN CÔNG RANSOMWARE

Qua theo dõi, giám sát hoạt động tấn công mạng thời gian qua, Cục An toàn thông tin (Bộ TT&TT) nhận thấy đang 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, gây thiệt hại về tài sản, ảnh hưởng đến danh tiếng, và gián đoạn hoạt động kinh doanh đối với các đơn vị gặp sự cố gây ra bởi Ransomware.

Cuộc tấn công Ransomware hiện nay thường được bắt đầu từ một điểm yếu bảo mật của cơ quan, tổ chức, kẻ tấn công xâm nhập hệ thống, duy trì sự hiện diện, mở rộng phạm vi xâm nhập, và kiểm soát hạ tầng công nghệ thông tin của tổ chức, làm tê liệt hệ thống, nhằm bắt buộc các tổ chức nạn nhân thực hiện hành vi tống tiền mà kẻ tấn công hướng tới.

Cục An toàn thông tin đã xây dựng Cẩm nang về một số biện pháp phòng chống, giảm thiểu rủi ro từ tấn công Ransomware cho các cơ quan, tổ chức, doanh nghiệp, hướng đến mục tiêu bảo đảm an toàn không gian mạng quốc gia, gồm các nội dung chính:

- Xây dựng kế hoạch **sao lưu, phục hồi dữ liệu** đối với hệ thống, thông tin quan trọng.
- Triển khai các biện pháp **xác thực mạnh** cho các tài khoản truy cập hệ thống.
- Chủ động tìm kiếm dấu hiệu tấn công, rà quét mã độc, yêu cầu đơn vị chuyên trách xử lý các mã độc.
- Giám sát liên tục để phát hiện sớm các hành vi xâm nhập, đặc biệt giám sát các truy cập đến **vCenter, ESXI, Domain Control-**
- **Rà quét, cập nhật** bản vá lỗ hổng an toàn thông tin trên các thiết bị, phần mềm, ứng dụng.
- **Xây dựng kế hoạch** ứng phó sự cố để kịp thời phản ứng với sự cố Ransomware.
- Áp dụng các **nguyên tắc đặc quyền** tối thiểu cho các hệ thống.
- **Hạn chế** việc sử dụng **dịch vụ** điều khiển máy tính **từ xa**.
- Thực hiện **phân vùng** mạng chặt chẽ.

1. Xây dựng kế hoạch sao lưu, phục hồi dữ liệu với hệ thống, thông tin quan trọng

Mục tiêu của các cuộc tấn công sử dụng Ransomware là cố gắng ngăn chặn việc khôi phục dữ liệu sau khi bị mã hóa, kẻ tấn công thường tìm và thu thập thông tin xác thực được lưu trữ trong hệ thống, sử dụng những thông tin xác thực đó để truy cập vào các giải pháp sao lưu, phục hồi, từ đó xóa hoặc mã hóa các bản sao lưu đó.

Chúng tôi khuyến nghị thực hiện việc sao lưu **"offline"**, không để các bản sao lưu đặt trong môi trường kết nối với hạ tầng mạng.

Thực hiện sao lưu **thường xuyên** và đảm bảo dữ liệu của các bản sao lưu được đầy đủ, từ đó 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.

Thực hiện quy tắc dự phòng 3-2-1:

Có **03** bản sao lưu dự phòng trên các phương tiện lưu trữ khác nhau giúp hệ thống có khả năng chống lại các rủi ro về ransomware cao hơn.

Lưu trữ ít nhất trên **02** loại phương tiện khác nhau: có thể lưu trữ lên cloud, NAS, SAN,...

01 bản được lưu giữ "offline".

Kiểm tra bản sao lưu:

- Kiểm tra tính toàn vẹn của tất cả các bản sao lưu, đảm bảo rằng các bản sao lưu không có lỗi khi tiến hành khôi phục.

- Kiểm tra, tính toán lượng băng thông và tài nguyên cần thiết để khôi phục nhiều hệ thống đồng thời.

Trường hợp dữ liệu được lưu trữ, sử dụng trên hệ thống là dữ liệu cá nhân, được quy định tại điều 3, Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân, các cơ quan, tổ chức phải thực hiện các phương pháp bảo đảm an toàn cho dữ liệu cá nhân: Thực hiện mã hoá, ẩn danh các dữ liệu cá nhân; Đảm bảo tính bí mật, toàn vẹn của dữ liệu trong quá trình hệ thống và dịch vụ xử lý dữ liệu; Phục hồi tính sẵn sàng và quyền truy cập tới dữ liệu cá nhân một cách kịp thời khi xảy ra sự cố; Kiểm tra, đánh giá định kỳ tính hiệu quả của các phương án bảo vệ dữ liệu cá nhân.

2. Triển khai các biện pháp xác thực mạnh cho các tài khoản truy cập hệ thống

Các cuộc tấn công sử dụng Ransomware thường sử dụng các tài khoản bị đánh cắp, bị lộ lọt trên mạng internet để truy cập các dịch vụ, máy chủ nội bộ. Từ đó kẻ tấn công sử dụng các phương pháp khác nhau như: man-in-the-middle, brute-force, dump bộ nhớ... để tìm kiếm và chiếm quyền các tài khoản có quyền quản trị, quyền truy cập vào tài nguyên quan trọng.

Việc triển khai xác thực mạnh, giúp hệ thống có thể an toàn hơn trước các rủi ro bị lộ lọt tài khoản, góp phần đảm bảo hệ thống được an toàn.

TRIỂN KHAI XÁC THỰC MẠNH CHO HỆ THỐNG

- Thiết lập chính sách mật khẩu an toàn cho tất cả các tài khoản quản trị, tài khoản truy cập hệ thống quan trọng.

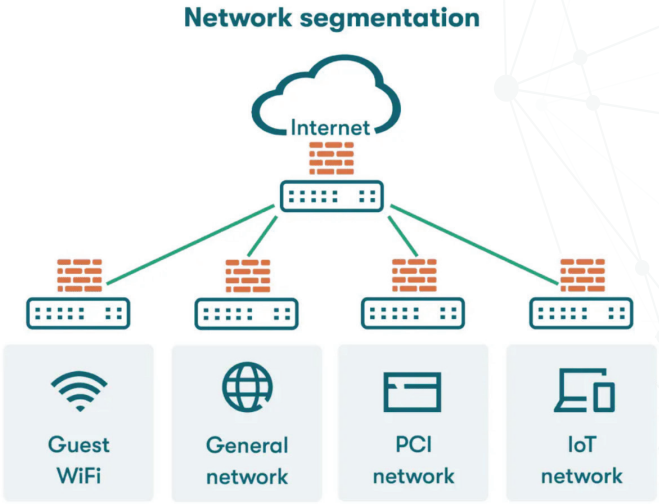
- Triển khai xác thực đa yếu tố **MFA** cho tất cả các dịch vụ nếu có thể, đặc biệt đối với **Email, VPN, vCenter, ESXI**, tài khoản truy cập dữ liệu, và các tài khoản truy cập vào các hệ thống quan trọng.

3. Thực hiện phân vùng truy cập mạng chặt chẽ

Những kẻ tấn công thường thường bắt đầu xâm nhập thông qua các máy trạm của người dùng, qua các vùng mạng DMZ, các máy chủ mở dịch vụ ra Internet. Sau khi đã có quyền truy cập nội bộ, kẻ tấn công tìm cách mở rộng, leo thang xâm nhập vào các máy chủ, hệ thống quan trọng của tổ chức.

Thực hiện phân vùng truy cập mạng đến các tài nguyên một cách chặt chẽ giúp hạn chế việc truy cập trái phép giữa các phân vùng, giữa các máy tính với nhau, ngăn chặn rủi ro lây lan thông qua mạng nội bộ.

- Thực hiện phân vùng mạng, tách biệt phân vùng của các tài nguyên quan trọng như: vCenter, ESXI, Domain Controller... với các phân vùng khác như DMZ, CSDL...
- Thực hiện phân vùng mạng giữa vùng mạng quản trị với vùng mạng người dùng thường, phân vùng mạng riêng cho các phòng ban...
- Tắt những tính năng SSH, Telnet trên các máy chủ ESXI, chặn quyền truy cập SMB từ Internet bằng cách chặn cổng TCP 445 nếu không sử dụng.
- 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 các truy cập đến vùng mạng quan trọng: vCenter, ESXI, DC. Có thể cấu hình chỉ cho phép truy cập vật lý vào vCenter, ESXI trong trường hợp cần thiết.



Các đối tượng tấn công Ransomware thường nhắm mục tiêu vào các máy chủ vCenter, ESXI, Domain Controller, khi chiếm được quyền điều khiển các máy chủ này kẻ tấn công có thể thực hiện tấn công trên phạm vi lớn.

4. Áp dụng nguyên tắc đặc quyền tối thiểu cho các hệ thống

Việc áp dụng nguyên tắc đặc quyền tối thiểu, đặc biệt đối với các hệ thống quan trọng, giúp giảm khả năng bị tấn công, hạn chế lây lan mã độc, dễ dàng phát hiện các bất thường, các hành vi cố gắng xâm nhập hệ thống.

- Không sử dụng tài khoản truy cập administrator/root cho các hoạt động thường xuyên. Tạo người dùng, nhóm và vai trò để thực hiện nhiệm vụ quản trị tài nguyên cụ thể.
- Hạn chế quyền truy cập vào vCenter, ESXI, DC. Có thể cấu hình chỉ cho phép truy cập theo whitelist.
- Vô hiệu hoá các tính năng không cần thiết, hạn chế việc cài đặt các phần mềm trên DC vì chúng có thể được tận dụng để tấn công vào hệ thống.
- Đánh giá định kỳ các tài khoản quản trị và đặc quyền, giúp giảm nguy cơ "leo thang đặc quyền", lỗ hổng này thường xảy ra khi các bộ phận tổ chức lại hoặc các cá nhân thay đổi vai trò mà hệ thống giữ lại các đặc quyền mà họ không cần nữa.
- Sử dụng các đặc quyền có giới hạn thời gian.

5. Rà quét, cập nhật bản vá lỗ hổng ATTT trên các thiết bị, phần mềm, ứng dụng

- Kẻ tấn công thường sử dụng lỗ hổng của các dịch vụ mở công khai trên internet để xâm nhập vào hệ thống, từ đó leo thang đặc quyền, khai thác sâu vào bên trong các hệ thống quan trọng.

- Thực hiện rà quét lỗ hổng thường xuyên để xác định và cập nhật bản vá lỗ hổng, đặc biệt là các lỗ hổng trên các thiết bị mở công khai trên Internet giúp hạn chế bề mặt tấn công, chủ động kiểm soát được các rủi ro.

  - 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 bản vá cho VPN, tường lửa...

  - Đảm bảo rằng tất cả các trình ảo hóa và cơ sở hạ tầng CNTT liên quan: vCenter, ESXI, DC đều được cập nhật đầy đủ bản vá mới nhất.

  - Định kỳ rà quét để kịp thời phát hiện ra các lỗ hổng mới.

  - 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.

6. Hạn chế sử dụng các dịch vụ điều khiển máy tính từ xa

Những kẻ tấn công có thể sử dụng các tài khoản bị đánh cắp, bị lộ lọt như tài khoản VPN, RDP... hoặc các dịch vụ điều khiển máy tính từ xa để xâm nhập vào vùng mạng của hệ thống. Cần hạn chế việc sử dụng các dịch vụ điều khiển, truy cập mạng từ xa để tránh các rủi ro tấn công:

Hạn chế sử dụng RDP và các dịch vụ máy tính từ xa khác như Teamview, Anydesk...

Rà soát toàn bộ các tài khoản đang được kết nối từ xa thông qua VPN, xóa các tài khoản không sử dụng.

Giới hạn quyền truy cập từ VPN đến các tài nguyên, chỉ cho phép truy cập vào các tài nguyên theo đúng mục đích.

Triển khai MFA trên tất cả các kết nối VPN để tăng tính bảo mật. Nếu MFA không được triển khai, hãy yêu cầu nhân viên làm việc từ xa sử dụng mật khẩu từ 15 ký tự trở lên.

7. Giám sát liên tục phát hiện sớm các hành vi xâm nhập

Việc thực hiện chủ động giám sát giúp phát hiện sớm được các vấn đề rủi ro, các dấu hiệu tấn công trong mạng, đặc biệt giám sát các truy cập đến vCenter, ESXI, Domain Controller.

- Đảm bảo rằng hệ thống IDS/IPS hoạt động đúng và dữ liệu được quản lý tập trung.
- Cấu hình các công cụ gửi các cảnh báo về các dấu hiệu xâm nhập mức mạng.
- Cấu hình cảnh báo các hành vi cố gắng truy cập, đăng nhập thành công/ không thành công vào các hạ tầng quan trọng vCenter, ESXI, Domain Controller, VPN...
- Cấu hình cảnh báo về các kết nối từ mạng nội bộ đến các máy chủ C&C để kịp thời phát hiện các rủi ro trong hệ thống.
- Cập nhật liên tục các chỉ báo về mã độc, tấn công mạng (Indicators of Compromise) để phát hiện các rủi ro trong hệ thống.
- Cấu hình cảnh báo về các thay đổi trên các hệ thống quan trọng vCenter, ESXI, Domain Controller... do kẻ tấn công thường cố gắng chiếm quyền điều khiển vCenter, ESXI, Domain Controller để có thể tối đa các ảnh hưởng đến hệ thống.
- Thực thi chính sách khóa tài khoản đăng nhập vào các hệ thống sau một số lần đăng nhập thất bại nhất định.

8. Chủ động tìm kiếm dấu hiệu tấn công, rà quét mã độc, yêu cầu đơn vị chuyên trách xử lý

Rà quét mã độc là một phần quan trọng trong chiến lược bảo mật để phát hiện và loại bỏ các phần mềm độc hại khỏi hệ thống. Bằng cách thực hiện rà quét mã độc một cách định kỳ và toàn diện, điều đó có thể giữ cho hệ thống an toàn khỏi các mối đe dọa tiềm ẩn của phần mềm độc hại.

- Thực hiện rà quét mã độc bằng giải pháp rà quét mã độc hiện có
- Yêu cầu đơn vị chuyên trách ATTT thực hiện xử lý các mã độc phát hiện ra.
- Kiểm tra tất cả các cảnh báo về dấu hiệu về mã độc trên máy chủ.
- Rà soát đầy đủ các cảnh báo trên hệ thống SIEM/SOC trong thời gian gần đây, yêu cầu đơn vị vận hành điều tra đầy đủ theo các cảnh báo.
- Thường xuyên cập nhật các chỉ báo về các mã độc APT

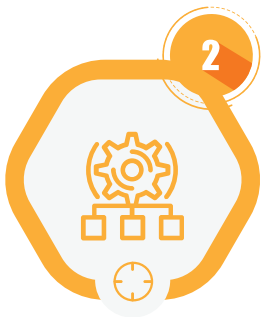
9. Xây dựng kế hoạch ứng phó sự cố để kịp thời phản ứng với Ransomware

Xây dựng kế hoạch ứng phó sự cố là một phần quan trọng trong việc đảm bảo khả năng bảo vệ và khôi phục hệ thống khi gặp phải các sự cố bảo mật, bao gồm cả các cuộc tấn công Ransomware. Bằng cách xây dựng và thực hiện một kế hoạch ứng phó sự cố một cách đầy đủ sẽ giúp tổ chức giảm thiểu rủi ro và tăng cường khả năng ứng phó khi gặp phải các sự cố bảo mật.

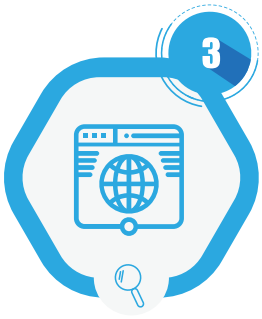
XÂY DỰNG KẾ HOẠCH ỨNG PHÓ SỰ CỐ

- Xác định rõ vai trò và trách nhiệm của mỗi thành viên trong tổ chức khi có sự cố xảy ra, bao gồm cả các người quản lý, nhân viên IT, bộ phận bảo mật.
- Đảm bảo có đủ các tài nguyên cần thiết để ứng phó với sự cố, bao gồm cả con người, công cụ, và phần mềm, hạ tầng cung cấp và sẵn sàng sử dụng khi cần thiết.
- Thử nghiệm các phương án phục hồi, khôi phục hệ thống để kiểm tra tính sẵn sàng của con người, của hạ tầng, của dữ liệu.

Xây dựng kế hoạch tổng quan



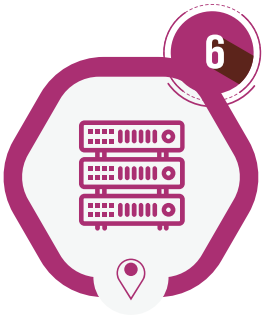
Cập nhật tài liệu từng giai đoạn



Chuẩn bị các kế hoạch truyền thông

Lập danh sách các công việc cần làm

Thường xuyên đào tạo ATTT cho nhân viên



Giám sát các hệ thống sau sự cố

Một số chỉ dẫn giúp khôi phục hệ thống sau khi phát hiện tấn công Ransomware

Xác định hệ thống nào bị ảnh hưởng và **cô lập** mạng hệ thống ngay lập tức.

- Nếu một số hệ thống hoặc phân vùng mạng bị ảnh hưởng, hãy thực hiện cô lập mạng ngay lập tức bằng cách chặn các kết nối ra vào các hệ thống, vùng mạng này
- Nếu không thể chặn các kết nối, hãy cô lập bằng cách rút cáp mạng để cô lập hệ thống

Phân loại các hệ thống bị ảnh hưởng để tiến hành khôi phục.

- Phục hồi hệ thống ở vùng mạng tách biệt
- Ưu tiên phục hồi các hệ thống quan trọng
- Đảm bảo rằng hệ điều hành máy chủ phục hồi an toàn, không bị xâm nhập, không chứa mã độc
- Khôi phục dữ liệu lên một hệ thống an toàn
- Xác định các tệp cần khôi phục

Liên hệ ngay cơ quan chuyên trách về ATTT để được hỗ trợ.

- **Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC)**, điện thoại **024.3640.4421** hoặc số điện thoại trực đường dây nóng ứng cứu sự cố **086.9100.317**, thư điện tử: **ir@vncert.vn**
- **Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC)**, điện thoại: **024.32091.616** hoặc số điện thoại trực đường dây nóng hỗ trợ giám sát, cảnh báo sớm **096.1405.333**, thư điện tử: **ais@mic.gov.vn**

Một số chỉ dẫn giúp khôi phục hệ thống sau khi phát hiện tấn công Ransomware

Thu thập lại các dấu hiệu, bằng chứng tấn công.

- Thực hiện thu thập các dữ liệu log từ các máy chủ, các hệ thống bảo vệ
- Thu thập các mẫu mã độc phát hiện trong hệ thống

Xác định mẫu Ransomware.

- Phân tích mẫu dữ liệu bị mã hóa để xác định mẫu Ransomware bị ảnh hưởng
- Trao đổi với các cơ quan chức năng để tìm kiếm bộ giải mã nếu có (một số loại Ransomware đã được phân tích và có các bộ giải mã được công bố)

Xác định phạm vi bị ảnh hưởng.

- Xác định về các dữ liệu bị ảnh hưởng, khả năng dữ liệu bị đánh cắp
- Xác định danh sách các tài khoản bị ảnh hưởng: của người dùng tổ chức và khách hàng

CỤC AN TOÀN THÔNG TIN
AUTHORITY OF INFORMATION SECURITY

NCSC VN
National Cyber Security Center

VNCERT/CC

Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC)

khonggianmang.vn

ais@mic.gov.vn

024.32091.616 - 096.1405.333

Tầng 16, 115 Trần Duy Hưng, Cầu Giấy, Hà Nội

Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC)

vncert.vn

ir@vncert.vn

024.3640.4421 - 086.9100.317

Tầng 5, 115 Trần Duy Hưng, Cầu Giấy, Hà Nội