<Logo doanh nghiệp>

Số đăng ký: _____

BÁO CÁO PHÂN TÍCH RỦI RO VỀ RANSOMWARE

Stt	Nội dung phân tích	Kết quả
1.	Mục đích của Báo cáo	Hiểu bản chất của rủi ro mà Ransomware gây ra cho nạn nhân và các đặc trưng của rủi ro bao gồm cả mức độ rủi ro.
2.	Bản chất của Ransomware	Ransomware là một phần mềm độc hại (hay mã độc ('malware')). Khi nhiễm vào thiết bị lưu trữ số của nạn nhân, Ransomware mã hóa dữ liệu hoặc khóa quyền truy cập thiết bị của người dùng (là nạn nhân).
3.	Đặc trưng của rủi ro do Ransomware gây ra	Ransomware vi phạm bảo mật ATTT: - Thuộc tính bảo mật của thông tin bị tổn hại do nạn nhân bị khóa quyền truy cập thiết bị; - Thuộc tính sẵn sàng của thông tin bị tổn hại vì nạn nhân không thể truy cập (hay đọc) được thông tin do dữ liệu bị mã hóa.
4.	Mức độ rủi ro	☐ Thấp ☐ Trung bình ☒ Cao
5.	Nguồn rủi ro	Tội phạm máy tính (Hacker/ Attacker/…)
6.	Hệ quả	1) Mã độc Ransomware xâm nhập được vào thiết bị sẽ khóa tất cả các tập tin (hay mã hóa) mà nó có thể truy cập bằng thuật toán mã hóa mạnh. 2) Nạn nhân bị tống tiền: để có lại quyền truy cập thiết bị hoặc dữ liệu, người dùng phải trả cho Tội phạm máy tính một khoản tiền nhất định, gọi là tiền chuộc để được giải mã các tập tin và khôi phục toàn bộ hoạt động cho các thiết bị hoặc hệ thống CNTT bị ảnh hưởng. 3) Ransomware còn được cài đặt cùng với mã độc Trojan để có quyền kiểm soát nhiều hơn trên thiết bị bị lây nhiễm. 4) Đe dọa hủy dữ liệu nếu tiền chuộc không được giao nộp đúng hạn.
7.	Khả năng xảy ra	☐ Thấp ☐ Trung bình ☒ Cao
8.	Một số sự kiện tấn công bởi Ransomware gây ra được báo chí đưa tin	Đã có hơn 1000 sự kiện Ransomware tấn công (hay lây nhiễm) được tiết lộ công khai xảy ra từ năm 2017-2023; sau đây là một số trường hợp trong số đó: 1) Nhiều cuộc tấn công ransomware vào các thành phố của Mỹ a)Nguyên nhân sự kiện xảy ra: - Lừa nạn nhân cài đặt phần mềm máy tính (là mã độc) từ xa. - Kẻ điều hành ransomware tìm cách nhận được khoản tiền chuộc bằng cách đe dọa nạn nhân rằng thông tin bị đánh cắp sẽ bị rò rỉ trực tuyến nếu nạn nhân không đáp ứng số tiền chuộc. b) Khả năng xảy ra: Ransomware đã được sử dụng trong cuộc tấn công mạng tối 08/02/2023 c) Hệ quả: -Ngừng hoạt động mạng do các hệ thống bị ngắt kết nối với Internet. -Hộp thư thoại và các dịch vụ không khẩn cấp khác đang bị gián đoạn hoặc bị ngắt kết nối. -Thành phố Atlanta, nơi từ chối trả khoản tiền chuộc 51.000 USD, đã chi hàng triệu USD để khôi phục những hệ thống bị ảnh hưởng.

		2) Sự kiện tấn công mạng vào hệ thống đường ống dẫn nhiên liệu của Hoa Kỳ ngày 07/05/2021 a)Nguyên nhân: - Kẻ tấn công khai thác một lỗ hổng phổ biến trong ngành công nghiệp đường ống là thiếu phân đoạn mạng ("segregation in network") trong thiết kế hệ thống thu thập dữ liệu và giám sát đường ống (SCADA), - Mạng SCADA cho hệ thống đường ống thường được phân tách với mạng CNTT bằng tường lửa, tuy vậy theo thiết kế những tường lửa này vẫn trao đổi một số dữ liệu giữa các mạng. Các đường dẫn được phép này thông qua tường lửa là một cách mà phần mềm độc hại hoặc tin tặc có thể di chuyển từ mạng CNTT vào mạng SCADA. b) Khả năng xảy ra: Có thể xảy ra vì Ransomware đã được sử dụng trong cuộc tấn công mạng tối 07/05/2021. c) Hệ quả: -Ransomware khiến 45% mạng lưới cung cấp xăng ở bờ biển phía đông Mỹ bị đóng cửa. -Các mạng của Công ty Colonial Pipeline bị xâm phạm, 100GB dữ liệu bị đánh cắp và máy tính bị mã hóa bằng Ransomware. - Công ty Colonial Pipeline đã trả 4,4 triệu đô la tiền chuộc cho nhóm tấn công nhằm lấy lại dữ liệu đã bị mã hóa.
9.	Các kịch bản mà doanh nghiệp sẽ thực hiện trước và sau khi bị lây nhiễm mã độc Ransomware để đáp ứng theo A.16.1.5 [ISO 27001:2013]	1)Trước khi thiết bị nhiễm mã độc: -Không mở thư rác; -Không mở (Click vào) email lạ; -Không tải tập tin thông qua các trang web ghi vào ổ đĩa của thiết bị. 2) Sau khi thiết bị đã bị nhiễm mã độc: 2.1 Tự khắc phục: + Bước 1: Cô lập mạng và hệ thống: Bước đầu tiên là việc cách ly phần đã bị nhiễm với hệ thống để tránh virus lây lan. + Bước 2: Xác định và xóa Ransomware: tìm và xác định được phần mềm độc hại trên máy. Sau khi đã tìm được Ransomware xóa bỏ chúng thật nhanh ra khỏi thiết bị và hệ thống bị nhiễm. + Bước 3: Xóa thiết bị nhiễm Ransomware và khôi phục từ bản sao lưu: Để tránh trường hợp Ransomware còn sót lại, hãy xóa toàn bộ dữ liệu bị nhiễm mã độc và khôi phục chúng lại từ đầu qua các bản sao lưu. + Bước 4: Phân tích và giám sát hệ thống: Khi Ransomware đã bị loại bỏ hoàn toàn khỏi thiết bị và hệ thống, tìm nguyên nhân lây nhiễm Ransomware và lên kế hoạch bảo vệ phù hợp, tránh trường hợp tái nhiễm có thể xảy đến. 2.2 Nếu không thể tự khắc phục: Trả tiền chuộc cho tội phạm máy tính để được mở khóa.
10.	Các biện pháp kiểm soát ('Controls') phòng chống mã độc Ransomware để	1) Tên kiểm soát: Các biện pháp kiểm soát rủi ro nhiễm Ransomware bao gồm nhưng không giới hạn các biện pháp sau đây:

	đáp ứng theo A.12.2.1 [ISO 27001:2013]	- Sử dụng chiến lược kiểm kê tài sản dựa trên rủi ro để xác định và đánh giá về sự hiện diện của phần mềm độc hại; - Sao lưu dự phòng dữ liệu vào thiết bị lưu trữ dự phòng; - Sử dụng các dịch vụ bảo mật lưu dự phòng dữ liệu như Cloud Firewall hay Cloud Security; - Cài đặt các phần mềm anti-virus diệt Ransomware vào thiết bị tin học như BitDefender Antivirus Plus 2017, Trend Micro Antivirus+, Avast Free Antivirus 2017, Malwarebytes Anti-Ransomware Beta, Kaspersky Anti-Ransomware Tool for Business…; - Yêu cầu xác thực đa yếu tố để truy cập từ xa vào mạng công nghệ vận hành OT và mạng công nghệ thông tin IT; - Phân đoạn mạng thông tin; - Bật bộ lọc thư rác mạnh để ngăn email lừa đảo đến tay người dùng; cuối;- Lọc các email có chứa các tệp thực thi để tiếp cận người dùng cuối; - Lọc lưu lượng mạng để cấm kết nối với các địa chỉ IP độc hại đã biết. - Ngăn người dùng truy cập các trang web độc hại bằng cách triển khai danh sách chặn tên miền/ URL và/hoặc danh sách cho phép (Whitelist). - Cập nhật phần mềm, bao gồm hệ điều hành, ứng dụng và firmware trên các tài sản mạng IT một cách kịp thời. - Sử dụng hệ thống quản lý bản vá tập trung; - Sử dụng chiến lược đánh giá dựa trên rủi ro để xác định khu vực và tài sản mạng OT nào nên tham gia vào chương trình quản lý bản vá; - Hạn chế truy cập tài nguyên qua mạng, đặc biệt hạn chế giao thức truy nhập máy tính từ xa (RDP) hoặc yêu cầu xác thực đa yếu tố nếu RDP được cho là cần thiết về mặt hoạt động; - Triển khai chương trình đào tạo người dùng và các cuộc tấn công mô phỏng lừa đảo có mục tiêu nhằm tránh người dùng truy cập vào các trang web độc hại hoặc mở các tệp đính kèm độc hại; - Huấn luyện cách ứng xử thích hợp của người dùng đối với các email lừa đảo. 2) Hiệu lực của biện pháp kiểm soát: Chưa có kết quả khảo sát từ các đơn vị theo dõi ATTT trên thế giới. Ngay cả biện pháp tự khắc phục bằng dữ liệu sao lưu dự phòng thì hiệu lực không đạt 100% vì khoảng cách thời gian giữa thời điểm sao lưu và thời điểm lây nhiễm mã độc có phát sinh dữ liệu của người dùng.
11.	Mức độ phức tạp của việc phòng chống mã độc Ransomware	➢ Thấp: nếu nạn nhân dùng các biện pháp kiểm soát như bằng sao lưu dữ liệu dự phòng hoặc đã cài đặt các phần mềm anti-virus diệt Ransomware vào thiết bị tin học. ➢ Trung bình: thuê dịch vụ bảo mật bên ngoài. ➢ Cao: nếu nạn nhân không thể tự khắc phục và phải trả tiền chuộc cho tội phạm thì có nhiều trường hợp cho thấy, dù nạn nhân đã trả tiền chuộc nhưng vẫn không chắc chắn là sẽ có quyền truy cập lại được vào dữ liệu của mình.
12.	Doanh nghiệp cần kết nối với các tổ chức nào theo yêu cầu tại Nhóm A.6 Yêu cầu A.6.1 Điều	1) Sử dụng các dịch vụ ATTT của bên thứ ba như: - Dropbox Cloud - Google Cloud - Cloud Firewall hay Cloud Security của Viettel IDC - Các dịch vụ ATTT của nhà cung cấp dịch vụ khác trên thị trường

	A.6.1.3 và A.6.1.4 [ISO 27001:2013] để tìm kiếm sự hỗ trợ	- v.v. 2)Thông báo cho Chính phủ, các bên liên quan có mối quan hệ với doanh nghiệp (như cổ đông lớn, đối tác cung ứng dịch vụ CNTT cho doanh nghiệp…) khi hệ thống thông tin của doanh nghiệp bị nhiễm Ransomware.
13.	Các Yếu tố liên quan đến thời gian của cuộc tấn công do Ransomware gây ra	1)Thời gian xảy ra sự kiện/sự cố: Ransomware có thể lây nhiễm (hay tấn công) vào bất cứ lúc nào khi người dùng thiết bị: - Mở (Click vào) đường Link thư rác; - Mở (Click vào) email lạ; - Tải tập tin thông qua các trang web ghi vào ổ đĩa của thiết bị; - Cho phép người lạ cài đặt phần mềm từ xa vào thiết bị. 2)Yếu tố liên quan đến thời gian và sự biến động: - Kẻ tấn công Ransomware quy định thời gian nạn nhân phải trả tiền chuộc hoặc chấp nhận rủi ro khi dữ liệu bị tiết lộ bởi kẻ tấn công. - Thời gian phục hồi hệ thống trở lại vận hành bình thường không là vô hạn; doanh nghiệp phải phục hồi nhanh hoạt động theo áp lực của khách hàng và cổ đông.
14.	Quan điểm, định kiến và cảm nhận về rủi ro do Ransomware gây ra	Theo cách hiểu thông thường là không ai muốn bị tống tiền nên quan điểm thống nhất là: - Ransomware là mã độc nguy hiểm cho việc sử dụng thiết bị; - Phòng tránh rủi ro nhiễm mã độc Ransomware
15.	Các hạn chế kỹ thuật phòng chống Ransomware để đáp ứng theo Nhóm A.12 Yêu cầu A.12.1 Điều A.12.6.1 [ISO 27001:2013]	Các biện pháp kiểm soát chỉ được cập nhật/vá lỗi/nâng cấp sau khi biến thể Ransomware đã lây nhiễm và gây ra hệ quả cho doanh nghiệp.

(*)Chú ý: Các thông tin trong phần Phân tích rủi ro này sẽ được đưa vào kỹ thuật phân tích và đánh giá rủi ro FMECA ở Chương 7 – xem biểu mẫu dưới đây của kỹ thuật phân tích và đánh giá rủi ro FMECA

Ngày tháng năm

Họ và tên người phê duyệt báo cáo	Họ và tên người soạn báo cáo