Quy trình xử lí sự cố máy tính nhiễm virus/malware

PHÂN TÍCH RỦI RO THEO FMEA

Failure Mode and Effects Analysis (FMEA) / Failure Mode, Effects & Criticality Analysis(FMECA)

									Đánh giá lại rủi ro và cơ hội			Hành động đề nghị (Có/Không)	
stt	**Bước**	**Rủi ro tiềm ẩn**	**Nguyên nhân của rủi ro**	**Khả năng xảy ra (Xếp hạng theo thang đo)- Occ**	**Hậu quả có thể gây ra**	**Mức độ ảnh hưởng (Xếp hạng theo thang đo) - Sev**	**Số RPN1 = (5)x(7)**	**Biện pháp kiểm soát hiện hữu**	**Khả năng xảy ra (Xếp hạng theo thang đo)- Occ**	**Mức độ ảnh hưởng (Xếp hạng theo thang đo) - Sev**	**Số RPN2 = (10)x(11)**	**Duy trì BPKS hiện hữu (Có/Không)**	**Bổ sung/thay thế BPKS hoặc hành động khác (Có/Không)**
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)
1	Bước 1: Lập kế hoạch xử lýsự cố ("Plan")	Công cụ chuyên dụng dùng để xử lí sự cố bị hỏng hoặc thiếu	Phòng ATTT không trang bị dự phòng; không quản lý công cụ theo quy định	2	Kế hoạch xử lí sự cố không thể thực hiện do thiếu công cụ cần thiết	2	4	Phòng ATTT luôn mua dự phòng 2 hoặc 3 bộ công cụ	1	1	1	Có	Không
2	Bước 2: Thực hiện kế hoạch ("Do")	Một số hoạt động trong kịch bản không được thực hiện	Phần mềm, thiết bị, công cụ được sử dụng bị lỗi thời, không được cập nhật. Nhân viên làm việc cẩu thả	2	Virus/Malware chưa được cách ly hoàn toàn khỏi máy tính	2	4	Cập nhật kịch bản định kỳ. Có hình thức răn đe với những nhân viên thực hiện xử lí sự cố không tuân thủ theo quy trình	1	1	1	Có	Không
3	Bước 3: Kiểm tra kết quả lần 1 ("1st Check")	Kết quả kiểm tra có sai sót (còn virus nhưng không phát hiện được)	Xuất hiện loại mã độc mới, nâng cao có khả năng qua mặt trình phát hiện	2	Hệ thống máy tính vẫn bị malware tấn công và gây hại	2	4	Luôn cập nhật anti-virus trước khi tiến hành kiểm tra. Thực hiện kiểm tra trong sandbox để phân tích hành vi.	1	1	1	Có	Không
4	Bước 4: Tìm hỗ trợ của bên thứ ba	Không được nhận sự hỗ trợ kịp thời từ bên thứ ba	Bên thứ ba có nhiều dự án khác và đang bận	2	Hệ thống máy tính vẫn bị malware tấn công và gây hại	1	2	Có danh sách các bên thứ 3 dự phòng	1	1	1	Có	Không
5	Bước 5: Cập nhật phiên bản antivirus	Không cập nhật được phiên bản antivirus	Máy tính không đáp ứng đủ cấu hình cho phiên bản mới của anti-virus	2	Anti-virus không phát hiện được các loại mã độc mới	1	2	Xây dựng hệ thống máy tính với cấu hình mạnh, đáp ứng được cấu hình của các phần mềm antivirus mới	1	1	1	Có	Không
6	Bước 6: Quét virus / malware lần 2	Quét lần 2 không được thực hiện	Nhân viên xử lý sự cố chủ quan, nghĩ rằng không còn malware	2	Hệ thống máy tính vẫn bị malware tấn công và gây hại	2	4	Nhân viên ca sau tiếp nhận công việc xử lí sự cố và hỏi lại nhân viên ca trước đã có quét lần 2 chưa; Trưởng phòng ATTT kí xác nhận đã thực hiện bước này	1	1	1	Có	Không
7	Bước 7: Kiểm tra kết quả lần 2 ("2nd Check")	Kết quả kiểm tra có sai sót (còn virus nhưng không phát hiện được)	Xuất hiện loại mã độc mới, nâng cao có khả năng qua mặt trình phát hiện	2	Hệ thống máy tính vẫn bị malware tấn công và gây hại	2	4	Luôn cập nhật anti-virus trước khi tiến hành kiểm tra. Thực hiện kiểm tra trong sandbox để phân tích hành vi.	1	1	1	Có	Không
8	Bước 8: Kiểm tra và cải tiến ("Act")	Nhân sự không báo cáo kết quả xử lí cho trưởng phòng ATTT	Nhân sự bất mãn, làm việc thiếu trách nhiệm	2	Trưởng phòng ATTT không nắm được tình hình, khó đánh giá mức độ tin cậy hệ thống máy tính	1	2	Có hình thức răn đe với những nhân viên thực hiện xử lí sự cố không tuân thủ theo quy trình	1	1	1	Có	Không
9	Bước 9: Báo cáo kết quả xử lý	Trưởng phòng ATTT không phân công nhân sự để theo dõi hệ thống	Trưởng phòng ATTT làm việc cẩu thả	2	Hệ thống có thể bị tấn công và khó có thể ứng cứu kịp thời	1	2	Chỉ đạo và phân công được ghi thành văn bản báo cáo với cấp trên	1	1	1	Có	Không
10	Bước 10: Lưu hồ sơ	Không lưu hoặc lưu không đầy đủ hồ sơ	Thiếu giám sát, kiểm tra công việc của nhân viên; nhân viên làm việc cẩu thả…	2	Thất lạc hồ sơ, không có cơ sở khi cần kiểm tra đối chiếu	1	2	Nhân viên xử lý sự cố xong tập hợp hồ sơ chuyển cho Trưởng Phòng ATTT kiểm tra đầy đủ tài liệu trước khi lưu trữ. Thường xuyên kiểm tra, kịp thời phát hiện sai sót trong công việc lưu hồ sơ để khắc phục.	1	1	1	Có	Không