HỆ THỐNG ĐÁNH GIÁ, QUẢN LÝ RỦI RO VÀ HỖ TRỢ XỬ LÝ SỰ CỐ AN TOÀN THÔNG TIN TRONG CHÍNH PHỦ ĐIỆN TỬ

MẶC DÙ DỊCH COVID-19 KÉO DÀI LÀM CẢN TRỞ QUÁ TRÌNH THỬ NGHIỆM SẢN PHẨM, NHƯNG PGS.TS. NGUYỄN NGỌC HÓA VÀ NHÓM NGHIÊN CỨU KHOA CÔNG NGHỆ THÔNG TIN (TRƯỜNG ĐẠI HỌC CÔNG NGHỆ, ĐHQGHN) VẪN HOÀN THÀNH ĐỀ TÀI "NGHIÊN CỨU, XÂY DỰNG HỆ THỐNG ĐÁNH GIÁ, QUẢN LÝ RỦI RO VÀ HỖ TRỢ XỬ LÝ SỰ CỐ AN TOÀN THÔNG TIN TRONG CHÍNH PHỦ ĐIỆN TỬ", VỚI HAI GIẢI PHÁP UET.SRA VÀ UET.SIR PHỤC VỤ CÔNG TÁC ĐẢM BẢO AN TOÀN THÔNG TIN TRONG CHÍNH PHỦ ĐIỆN TỬ.

☞**TUYẾT NGA**

Xuất phát từ thực tiễn nào mà PGS cùng với nhóm nghiên cứu thực hiện đề tài "Nghiên cứu, xây dựng hệ thống đánh giá, quản lý rủi ro và hỗ trợ xử lý sự cố an toàn thông tin trong Chính phủ điện tử"?

Việc đảm bảo an toàn thông tin (ATTT) cho các hệ thống trong Chính phủ điện tử (CPĐT) là một trong những bài toán lớn, luôn được Chính phủ, các bộ/ngành quan tâm hiện nay. Từ đó, đặt ra vấn đề cần phải có công cụ, hệ thống hỗ trợ cho công tác đánh giá, quản lý rủi ro và xử lý sự cố ATTT trong CPĐT. Hiện cũng đã có một số những sản phẩm thương mại từ những hãng lớn như Nessus, Nexposes, Fireeyes, IBM,... phục vụ giải quyết những yêu cầu chuyên biệt trong vấn đề đó. Tuy nhiên, các sản phẩm này cũng có những hạn chế khi triển khai trong các bộ/ngành do những nguyên nhân chưa phù hợp với quy trình nghiệp vụ thực tế, chưa thể đánh giá được mức độ đảm bảo ATTT của bản thân các engines trong các hệ thống đó, ...

Chính vì thế, Bộ Khoa học và công nghệ đã đặt hàng nhóm nghiên cứu để hình thành được nhiệm vụ nghiên cứu với mục tiêu làm chủ được công nghệ và quy trình, từ đó xây dựng được hệ thống phục vụ hoạt động đánh giá, quản lý rủi ro và hỗ trợ xử lý sự cố ATTT trong các hệ thống thông tin tại các cơ quan nhà nước. Nhiệm vụ này thuộc đề tài KC.01.19/16-20 và nhóm nghiên cứu bắt đầu triển khai vào tháng 1/2019.

Quan trọng là, hệ thống được xây dựng cũng phải tuân thủ quy trình đánh giá, quản lý rủi ro và hỗ trợ xử lý sự cố ATTT trong CPĐT Việt Nam, phù hợp với tiêu chuẩn quốc gia và quốc tế về ATTT.

Kết quả của đề tài nghiên cứu đã giải quyết những vấn đề nào về ATTT trong CPĐT hiện nay?

Sau hai năm triển khai, hai sản phẩm của đề tài được đánh giá, thử nghiệm thực tế theo các yêu cầu nghiệp vụ tại Bộ Tài nguyên và môi trường, minh chứng được khả năng áp dụng, triển khai thực tế và góp phần nâng cao công tác đảm bảo ATTT trong các bộ/ngành của CPĐT.

Trong đề tài, nhóm nghiên cứu đã đưa ra hai giải pháp tương ứng với hai bài toán chính cần giải quyết trong đảm bảo ATTT của CPĐT, cụ thể:

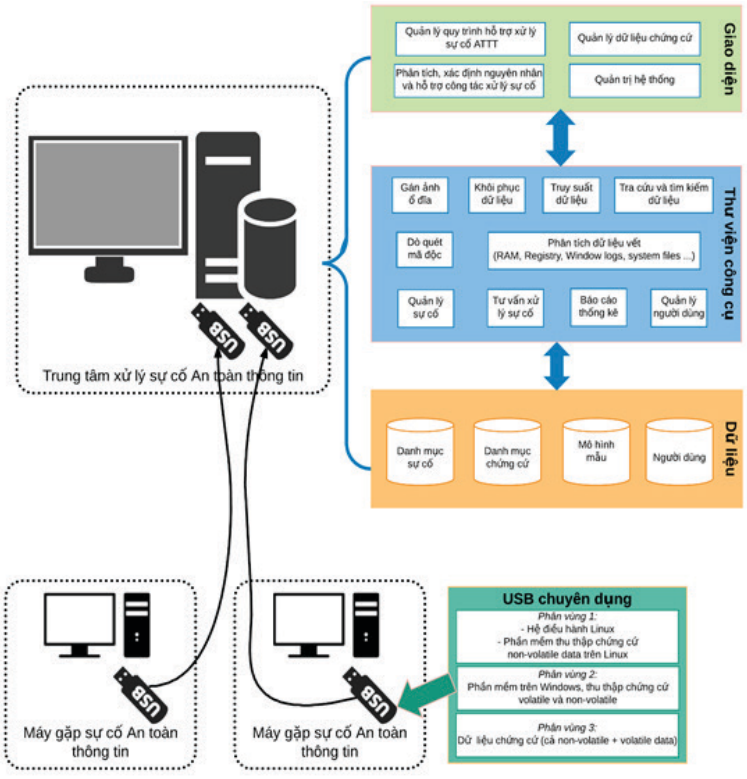
Thứ nhất là, giải pháp có thể chủ động xác định sớm được những nguy cơ dẫn đến những rủi ro mất ATTT trong các hệ thống thông tin của cơ quan nhà

nước. Bao gồm: quy trình đánh giá, quản lý rủi ro ATTT với sự kết hợp của ISO/IEC 27005-2018, NIST SP800-39 và NIST SP800-53r4; hệ thống UET.SRA cho phép thực hiện được các nghiệp vụ đánh giá, quản lý rủi ro ATTT theo quy trình đề xuất (bao gồm cả chức năng dò quét sâu lỗ hổng hệ thống, các website, bản vá chưa áp dụng, chính sách không tuân thủ, dò quét mã nguồn ứng dụng Web, đánh giá tổng thể theo CVSS/OWASP, xây dựng phương án xử lý rủi ro theo NIST SP800-53r4).

Thứ hai là, giải pháp hỗ trợ xử lý sự cố mất ATTT để nhóm chuyên gia kỹ thuật có thêm những thông tin cụ thể dẫn đến sự cố, gợi ý phương án xử lý sự cố. Bao gồm: quy trình hỗ trợ xử lý sự cố ATTT theo chuẩn ISO/IEC 27035-2016 và NIST SP800-61r1; hệ thống UET.SIR với USB chuyên dụng chứa công cụ thu thập được những dữ liệu chứng cứ sự cố ATTT quan trọng, cung cấp các chức năng để phân tích dữ liệu sự cố (dò quét mã độc, phân tích theo kiểu xếp chồng, so khác, ...).

Đối với đề tài này, PGS và nhóm nghiên cứu có tâm đắc đối với các giải pháp hoặc sản phẩm nào?

Đối với lĩnh vực đảm bảo ATTT trong CPĐT, hiện nay chưa



Kiến trúc tổng thể hệ thống hỗ trợ xử lý sự cố ATTT UET.SIR

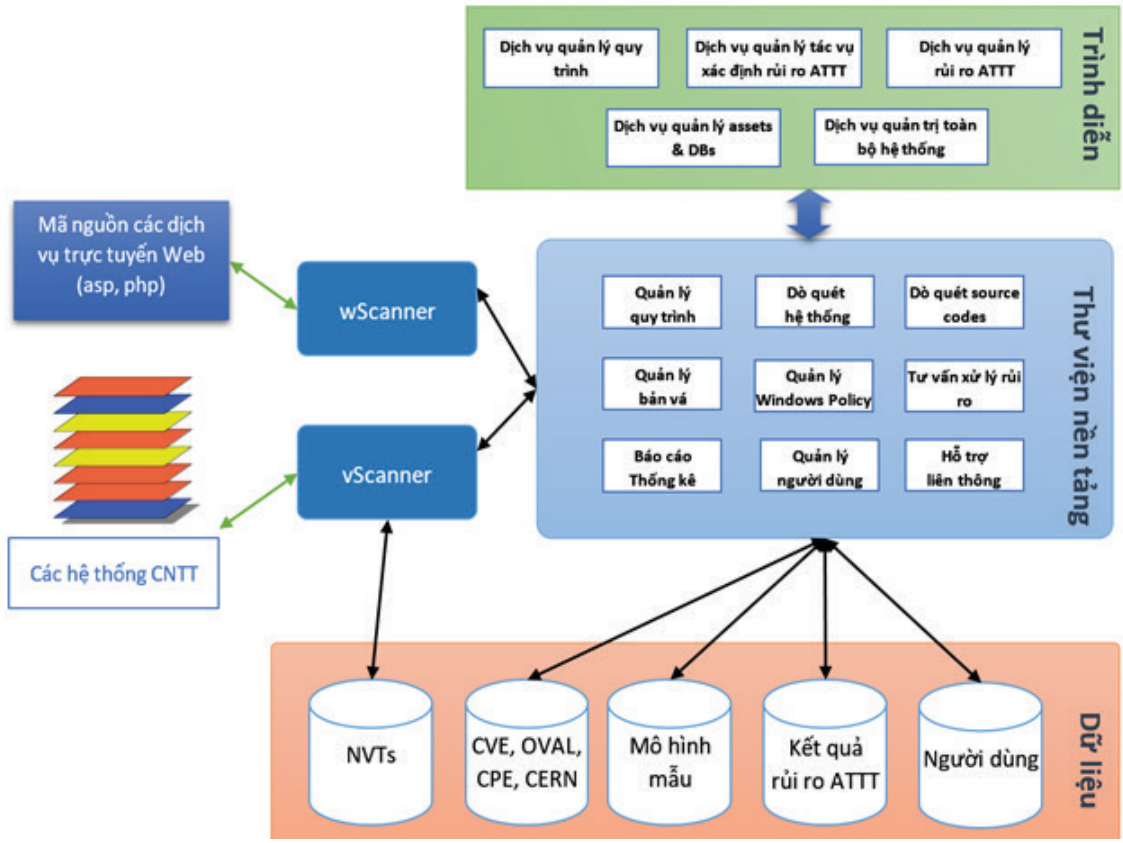
có đề tài cũng như sản phẩm có mục tiêu, định hướng giống như hai sản phẩm của nhóm nghiên cứu đã xây dựng. Hai hệ thống UET.SRA và UET.SIR đều có thể được xem như những hệ thống đầu tiên ở Việt Nam hỗ trợ các hoạt động đánh giá, quản lý và xử lý sự cố ATTT theo chuẩn quốc tế và Việt Nam.

Trong quá trình thực hiện đề tài, nhóm cũng đã chú trọng, nghiên cứu chuyên sâu nhiều vấn đề, đặc biệt là ứng dụng những phương pháp học máy hiện đại trong các bài toán đảm bảo ATTT. Từ đó, nhóm đã được chấp nhận đơn 02 sáng chế liên quan đến việc phát hiện các đoạn mã độc trong phân tích mã nguồn ứng dụng Web. Các kết quả khoa học của nhóm cũng đã được công bố trên 03 bài báo và 02 bài kỷ yếu hội thảo đều trong chỉ mục Scopus/WoS.

Đối với sản phẩm ứng dụng, hệ thống UET.SRA là hệ thống đánh giá, quản lý rủi ro ATTT tương đối toàn diện; tuân thủ theo chuẩn quốc tế và trong nước; có thể đánh giá được rủi ro ATTT đối với cả hệ thống phần mềm, hạ tầng mạng; mã nguồn ứng dụng Web; có chức năng xây dựng phương án xử lý rủi ro ATTT theo chuẩn quốc tế, ... Đối với hệ thống UET. SIR, đây cũng là hệ thống xử lý sự cố ATTT từ pha thu thập dữ liệu chứng cứ sự cố ATTT đến pha phân tích, gợi ý và xây dựng phương án xử lý sự cố ATTT.

Hiện nay, hai hệ thống này được triển khai thực tế tại hai đơn vị, gồm Trung tâm máy tính (Trường ĐH Công nghệ), Cục Công nghệ thông tin và Dữ liệu tài nguyên Môi trường (Bộ Tài nguyên và môi trường). Các kết quả triển khai bước đầu tại Bộ Tài nguyên và môi trường đã minh chứng được hiệu quả cũng như hỗ trợ rất lớn cho công tác đánh giá rủi ro và xử lý sự cố ATTT tại các đơn vị của Bộ này.

Ngoài ra, hiện nay có một số đơn vị như Văn phòng Trung ương Đảng, Văn phòng Chính phủ... đã liên hệ với Trường và nhóm nghiên cứu để đề nghị chuyển



Kiến trúc tổng thể hệ thống đánh giá, quản lý rủi ro ATTT UET.SRA

giao kết quả nghiên cứu hai hệ thống giải pháp nêu trên trong thời gian tới.

Với những ảnh hưởng của dịch Covid-19, nhóm nghiên cứu đã khắc phục những khó khăn như thế nào?

26 tháng thực hiện đề tài cũng là một thách thức rất lớn với nhóm nghiên cứu. Bởi vì, đề tài KC.01.19/16-20 được các thành viên Hội đồng đánh giá là đề tài phức tạp về nội dung nghiên cứu và khối lượng công việc rất lớn. Hơn nữa, đây là lần đầu tiên nhóm nghiên cứu thực hiện đề tài cấp quốc gia, nên áp lực về kết quả của đề tài cũng không nhỏ.

Nhưng với sự gắn kết chặt chẽ trong nghiên cứu, cùng sự quan tâm của lãnh đạo Nhà trường và các đơn vị quản lý, phối hợp như Bộ Khoa học và Công nghệ, Bộ Tài nguyên và môi trường,... nhóm nghiên cứu đã hoàn thành toàn bộ nội dung nghiên cứu cũng như đạt được các mục tiêu đặt ra.

Khoảng thời gian dịch Covid-19 diễn biến phức tạp cũng là một trở ngại lớn cho nhóm và trở thành nguyên nhân dẫn đến quá trình thử nghiệm sản phẩm kéo dài thêm 02 tháng. Tuy nhiên, nghiên cứu khoa học trở thành cầu nối nhóm nghiên cứu Trường ĐH Công nghệ đến với các đơn vị và nhóm nghiên cứu khác, để tập trung toàn bộ nguồn lực ở những giai đoạn nước rút hoàn thành hai giải pháp UET.SRA và UET.SIR.

Thời gian tới, nhóm nghiên cứu có tiếp tục triển khai hướng nghiên cứu mới đối với đề tài này không?

Hai sản phẩm chính của đề tài là hệ thống UET.SRA và UET.SIR vẫn được nhóm nghiên cứu tiếp tục hoàn thiện, cập nhật các mẫu dò quét lỗ hổng, bổ sung thêm các chức năng khác, ... Đặc biệt, dựa trên các đề nghị chuyển giao từ các bộ/ngành, chúng tôi sẽ tiếp tục phối hợp cùng với các đơn vị đang sử dụng hệ thống để tuỳ biến, hoàn thiện hai hệ thống giải pháp UET.SRA và UET.SIR theo các yêu cầu cụ thể của các bộ/ngành đó.

Cảm ơn PGS về cuộc trò chuyện!