Hệ thống giám sát, cảnh báo nguy cơ mất an toàn thông tin mạng

PGS.TS Hoàng Đăng Hải
Học viện Công nghệ Bưu chính Viễn thông

Trong bối cảnh chuyển đổi số diễn ra toàn diện trên nhiều ngành, nhiều lĩnh vực, việc đảm bảo an toàn thông tin (ATTT) trở thành nhiệm vụ vô cùng cấp thiết. Hiểu được tầm quan trọng này, nhóm nghiên cứu thuộc Học viện Công nghệ Bưu chính Viễn thông đã đề xuất và được Bộ Khoa học và Công nghệ (KH&CN) phê duyệt thực hiện đề tài "Nghiên cứu, xây dựng hệ thống giám sát, đánh giá cấp độ an toàn, cảnh báo nguy cơ mất ATTT mạng cho các trang tin/cổng thông tin điện tử (TTĐT)", mã số KC.01.08/16-20*, nhằm đảm bảo an toàn và tạo điều kiện phát triển bền vững Chính phủ điện tử (CPĐT) cũng như dịch vụ trên các cổng TTĐT.

Mở đầu

Cổng TTĐT là cốt lõi của CPĐT, là thành phần không thể thiếu trong hoạt động của mọi cơ quan, tổ chức, doanh nghiệp. Do cung cấp thông tin cho mọi đối tượng trong xã hội, cổng TTĐT luôn là một mục tiêu tấn công hấp dẫn của tin tặc. Trong quá trình hoạt động, các trang/cổng TTĐT luôn tồn tại các lỗ hổng bảo mật. Kẻ tấn công sẽ tìm cách khai thác các lỗ hổng này để thực hiện tấn công. Sẽ không thể phát hiện được kịp thời các lỗ hổng bảo mật và nguy cơ tấn công nếu không có một hệ thống giám sát và đánh giá ATTT cho các trang tin/cổng TTĐT theo thời gian thực.

Thực hiện đề tài "Nghiên cứu, xây dựng hệ thống giám sát, đánh giá cấp độ an toàn, cảnh báo nguy cơ mất ATTT mạng cho các trang tin/cổng TTĐT", nhóm nghiên cứu thuộc Học viện Công nghệ Bưu chính Viễn thông đã xây dựng giải pháp thu thập dữ liệu từ các máy chủ cài đặt trang tin/cổng TTĐT tại các cơ quan cấp tỉnh/cấp bộ để theo dõi, phân tích, phát hiện và cảnh báo nguy cơ mất an toàn, hỗ trợ tìm kiếm chứng cứ, truy xuất nguồn gốc các sự cố đã được phát hiện của trang tin/cổng TTĐT theo thời gian thực. Đồng thời, nhóm nghiên cứu xây dựng giải pháp đánh giá cấp độ bảo đảm an toàn cho các trang tin/cổng TTĐT theo tiêu chuẩn đánh giá ATTT đã được công bố.

Những sản phẩm chính của đề tài

Sau 5 năm triển khai thực hiện đề tài, nhóm nghiên cứu đã xây dựng được hệ thống giám sát, đánh giá cấp độ an toàn, cảnh báo nguy cơ mất ATTT, bao gồm phần mềm Agent được cài đặt tại máy chủ của các đơn vị phối hợp và phần mềm trung tâm đặt tại Học viện Công nghệ Bưu chính Viễn thông.

Phần mềm Agent cài đặt tại máy chủ

Lõi của phần mềm Agent bao gồm các cấu trúc Script thu thập dữ liệu từ các nguồn chính gồm: nhật ký truy cập (Access Log), nhật ký lỗi (Error Log), nhật ký tường lửa (Firewall Log), nhật ký DNS (DNS Log), nhật ký sự kiện (Event Log), dữ liệu hoạt động của máy chủ (Performance). Các Script được phát triển bằng ngôn ngữ Python (phiên bản Python từ 2.7 trở lên), được biên dịch và có thể chạy trên cả Windows và Linux.

Các chức năng chính của phần mềm Agent bao gồm: thu thập dữ liệu từ các máy chủ (Windows, Linux) vận hành trang tin/cổng TTĐT theo thời gian thực; thu thập ít nhất 3 chuẩn định dạng dữ liệu IIS, Apache, Nginx (dữ liệu trạng thái máy chủ Web, Web log, Syslog, Access log, Error log); tiền xử lý và chuẩn hóa định dạng dữ liệu từ ít nhất 3 định dạng (IIS, Apache, Nginx), sau đó truyền có bảo mật về trung tâm giám sát. Mỗi Agent có thể giám sát ít nhất 10 trang tin.

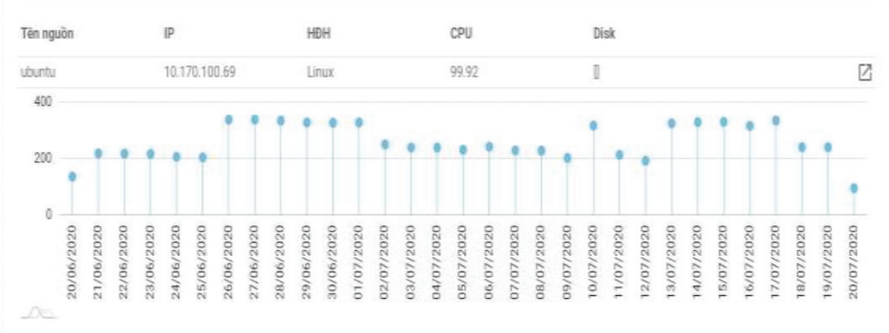
Phần mềm hệ thống trung tâm

Dữ liệu thu thập được từ các Agent được truyền về trung tâm giám sát theo kênh truyền bảo mật TLS. Tại đó, phần mềm hệ thống trung tâm đảm nhận việc xử lý, phân tích, đánh giá thông tin gửi về.

Phần mềm hệ thống trung tâm bao gồm các phân hệ chính sau: theo dõi, phân tích, phát hiện nguy cơ sự cố theo thời gian thực; giám sát từ xa không dùng Agent; hỗ trợ quản lý, giám sát từ xa từ thiết bị di động; hỗ trợ đánh giá cấp độ an toàn theo tiêu chuẩn.

Các chức năng chính của phần mềm hệ thống trung tâm bao gồm: thu thập dữ liệu từ tối thiểu 500

*Thuộc Chương trình "Nghiên cứu công nghệ và phát triển sản phẩm công nghệ thông tin phục vụ Chính phủ điện tử", mã số KC.01/16-20.



Theo dõi lượng bản tin sự kiện gửi bởi từng Agent theo thời gian thực về trung tâm giám sát.

trang tin/cổng TTĐT dựa trên các phần mềm Agent; theo dõi, phân tích và phát hiện nguy cơ sự cố ATTT tại các trang tin/cổng TTĐT theo thời gian thực, năng lực xử lý tối thiểu 10.000 sự kiện/giây; hỗ trợ công tác đánh giá ATTT cho các trang tin/cổng TTĐT theo bộ tiêu chuẩn quốc gia TCVN 8709; tạo lập báo cáo, thống kê trạng thái hoạt động của máy chủ Web; phát hiện và cảnh báo nguy cơ suy giảm chất lượng hoạt động của tối thiểu 500 trang tin/cổng TTĐT.

Hệ thống đã và đang được thử nghiệm tại các trang tin/cổng TTĐT của Cục Công nghệ thông tin (Bộ Công an), Cục Công nghệ thông tin (Bộ Y tế), Sở Thông tin và Truyền thông TP Hồ Chí Minh, Sở Thông tin và Truyền thông tỉnh Quảng Bình. Phần mềm Agent được cài đặt tại các máy chủ vận hành trang tin/cổng TTĐT tại các địa điểm nêu trên để thực hiện thu thập dữ liệu truyền về hệ thống trung tâm. Phần mềm hệ thống trung tâm đặt tại Học viện Công nghệ Bưu chính Viễn thông. Ngoài ra, nhóm đề tài cũng đã thiết lập một số máy chủ Web tại Hà Nội phục vụ cho việc thử nghiệm.

Hiệu quả đạt được

Sự thành công của hệ thống đã mang lại hiệu quả lớn về mặt KH&CN. Phần mềm Agent thu thập dữ liệu máy chủ và trang tin/cổng TTĐT với cơ chế thu thập dữ liệu đa dạng, nhiều tính năng, chạy được trên đa nền tảng hệ điều hành Windows và Linux, có thể thu thập được nhiều loại dữ liệu và truyền có bảo mật về trung tâm theo thời gian thực, có thể tự khởi tạo khi gặp lỗi, có tính năng thiết lập cấu hình từ xa.

Phần mềm hệ thống trung tâm có chức năng hỗ trợ giám sát từ xa, không cần cài đặt Agent tại các máy chủ Web. Hệ thống có thể theo dõi, giám sát trạng thái hoạt động của máy chủ Web, phát hiện và cảnh báo suy giảm chất lượng hoạt động của trang tin/cổng TTĐT. Ngoài ra, hệ thống có thể phát hiện nhanh thay đổi nội dung, phát hiện mã độc và rà soát lỗ hổng bảo mật của trang tin/cổng TTĐT.

Sản phẩm do cán bộ kỹ thuật Việt Nam làm chủ công nghệ, chỉ dựa một phần trên mã nguồn mở để phát triển nên có khả năng cạnh tranh về giá và ưu thế trong vận hành, khai thác, bảo dưỡng, hỗ trợ kỹ thuật và bảo đảm an ninh. Do thiết kế theo kiến trúc mô đun nên cũng có thể tách hệ thống thành 3 phân hệ một cách linh hoạt, đáp ứng nhu cầu ứng dụng của các cơ quan, tổ chức: *Thứ nhất,* phần mềm Agent và phân hệ giám sát trung tâm có thể chuyển giao ứng dụng cho các cơ quan bộ/ngành, các doanh nghiệp hoặc cơ quan tổ chức khác có nhu cầu giám sát các trang tin/cổng TTĐT quản lý. Hệ thống cho phép theo dõi, giám sát hoạt động của các trang tin/cổng TTĐT cần giám sát và cảnh báo nguy cơ sự cố, nguy cơ suy giảm chất lượng hoạt động. Đặc biệt, hệ thống còn cho phép giám sát 24/7 qua các thiết bị di động. *Thứ hai,* phân hệ giám sát không dùng Agent có thể chuyển giao ứng dụng cho các doanh nghiệp, các đơn vị cung cấp dịch vụ theo dõi, giám sát an toàn trang tin/cổng TTĐT cho các cơ quan tổ chức. Ưu điểm của phân hệ là không cần cài đặt Agent tại trang tin/cổng TTĐT cần giám sát, phần mềm gọn nhẹ và khá hiệu quả. *Thứ ba,* phân hệ đánh giá cấp độ an toàn có thể chuyển giao ứng dụng cho các đơn vị cung cấp dịch vụ kiểm thử, đánh giá ATTT. Phân hệ cũng có thể áp dụng cho các cơ quan, tổ chức, doanh nghiệp muốn thường xuyên kiểm tra mức độ áp dụng các biện pháp bảo đảm an toàn trang tin/cổng TTĐT định kỳ theo các chu kỳ bảo dưỡng, nâng cấp hệ thống thông tin.

Trang tin/cổng TTĐT là một phần không thể thiếu trong hệ thống thông tin của CPĐT. Bảo đảm ATTT cho trang tin/cổng TTĐT là yêu cầu thiết yếu cho phát triển CPĐT. Bên cạnh đó, kết quả nghiên cứu của đề tài còn có những đóng góp nhất định vào sự phát triển KH&CN trong lĩnh vực ATTT tại Việt Nam, góp phần đào tạo, bồi dưỡng nguồn nhân lực trình độ cao về ATTT, nâng cao chất lượng đào tạo ATTT tại các cơ sở đào tạo như Học viện Công nghệ Bưu chính Viễn thông ✍