GIẢI PHÁP AN TOÀN THÔNG TIN CHO DOANH NGHIỆP VIỆT NAM HIỆN NAY

THS. PHAN TRẦN ĐIỀN (*) - THS. ĐỖ THANH GIANG (**)

TÓM TẮT

Bảo mật thông tin được xem là vấn đề sống còn của doanh nghiệp trong nền kinh tế thị trường. Để nâng cao tính bảo mật cho hệ thống thông tin, doanh nghiệp cần phải tiến hành đánh giá mức độ an toàn của hệ thống thông tin (ATTT) trước khi đưa vào vận hành và cần định kỳ đánh giá lại hệ thống thông tin của doanh nghiệp trong quá trình sử dụng. Việc đánh giá này giúp cho doanh nghiệp sớm phát hiện những lỗ hổng bảo mật và ngăn chặn tin tặc (hacker) khai thác lỗ hổng bảo mật bằng phần mềm mã nguồn mở ModSecurity.(***)

Từ khóa: *đánh giá ATTT doanh nghiệp, modsecurity...*

1. Sự cần thiết phải đảm bảo an toàn thông tin doanh nghiệp hiện nay

1.1. Xuất phát từ yêu cầu của sự phát triển khoa học công nghệ trong bối cảnh hội nhập quốc tế

Ngày nay, thế giới đang bước vào cuộc cách mạng công nghiệp lần thứ tư với sự phát triển bùng nổ của những công nghệ mang tính đột phá như trí tuệ nhân tạo (AI - Artificial Intelligence), máy tính lượng tử (Quantum Computers), Internet của vạn vật (IoT - Internet of Things), công nghệ điện toán đám mây (Cloud Computing), dữ liệu nhanh (Fast Data), dữ liệu lớn (Big Data),... đã, đang và sẽ làm không gian mạng thay đổi sâu sắc cả về chất và lượng. Điều này được dự báo sẽ mang lại rất nhiều lợi ích chưa từng có cho con người. Trong bối cảnh đó, thông tin ngày càng trở thành một tài sản vô cùng quý giá đối với các chính phủ, tổ chức và đối với từng doanh nghiệp, từng cá nhân. Thông tin trở thành nhân tố hàng đầu bảo đảm sự thành công cho ai sở hữu nó. Đối với doanh nghiệp, việc ứng dụng công nghệ thông tin đã trở thành một xu hướng tất yếu trên con đường hội nhập quốc tế và thông tin trở thành một tài sản vô hình quý giá đối với từng doanh nghiệp. Công nghệ thông tin trở thành một trong những công cụ quan trọng trong sản xuất và phát triển kinh doanh. Công nghệ thông tin

(*) Giảng viên Khoa Đại Cương, Học Viện Cán Bộ
(**) Giảng viên Khoa Lý Luận Chính Trị, Học Viện Cán Bộ
(***) Là một tường lửa mức ứng dụng. Đứng trước Webserver và có khả năng xử lý traffic trước khi đưa vào Webserver. Mọi yêu cầu gửi đến Webserver từ phía client sẽ được gửi qua modsecurity

đóng vai trò vô cùng quan trọng trong khâu quảng bá, marketing sản phẩm, đồng thời cũng tạo nên ưu thế vượt trội trong việc quan hệ với các đối tác khách hàng. Việc nắm bắt và bảo mật thông tin tạo nên lợi thế lớn trong chiến lược cạnh tranh của các doanh nghiệp hiện nay.

Tuy nhiên, bên cạnh những lợi ích to lớn không thể phủ nhận được, sự phát triển của công nghệ thông tin cũng tiềm ẩn nhiều nguy cơ lớn đối với các quốc gia, tổ chức, doanh nghiệp cũng như từng cá nhân. Những thông tin quan trọng được lưu trữ ở kho dữ liệu hoặc đang trên đường truyền có thể bị đánh cắp, giả mạo hoặc làm sai lệch. Tình hình này đã và đang diễn ra trên phạm vi toàn cầu với mức độ ngày càng mãnh liệt, tập trung vào các cơ sở quốc phòng, an ninh, tài chính, ngân hàng và các lĩnh vực quan trọng khác. Chiến tranh trên mạng là cuộc chiến mới mà mỗi quốc gia, tổ chức hiện nay đều quan tâm và đề ra các biện pháp phòng ngừa, ngăn chặn . Đối với doanh nghiệp, những thông tin về khách hàng, bí mật kinh doanh, tài chính... là mục tiêu cần tìm hiểu của các đối thủ cạnh tranh. Nguồn thông tin mật này bị rò rỉ hoặc bị phá hoại không những là một sự cố có thể tác động trực tiếp đến tính phát triển bền vững và tồn tại của doanh nghiệp mà còn là một lợi thế cạnh tranh cực lớn dành cho các đối thủ sở hữu được những thông tin mật này. Tại Việt Nam, tình hình an toàn thông tin (ATTT) mạng cũng ngày càng diễn biến phức tạp với sự tăng mạnh về quy mô, số lượng, mức độ tinh vi và tính chuyên nghiệp trong các cuộc tấn công mạng, đặc biệt là tấn công mạng vào hệ thống thông tin của các doanh nghiệp lớn. Từ thực tế trên, có thể thấy, đảm bảo ATTT là việc làm cần thiết đối với mỗi doanh nghiệp trong bối cảnh hiện nay.

1.2. Xuất phát từ thực trạng ATTT của doanh nghiệp Việt Nam hiện nay

Điểm mạnh

Cơ sở pháp lý cho hoạt động đảm bảo ATTT ở Việt Nam đã hình thành và tạo thuận lợi cho việc đảm bảo ATTT của doanh nghiệp.

Trong những năm gần đây, Đảng và Nhà nước ta đã có nhiều chủ trương, chính sách về các biện pháp đẩy mạnh phát triển ứng dụng công nghệ thông tin viễn thông, gắn liền với công tác bảo đảm an toàn, an ninh thông tin sẵn sàng đối phó với các cuộc chiến tranh trên không gian mạng.

Ngày 16/9/2013, Ban Bí thư Trung ương Đảng đã ban hành Chỉ thị số 28-CT/TW về tăng cường công tác bảo đảm ATTT mạng, xác định đây là nhiệm vụ cấp bách, thường xuyên, lâu dài của cả hệ thống chính trị, là một bộ phận trọng yếu của cuộc đấu tranh bảo vệ an ninh quốc gia và giữ gìn trật tự an toàn xã hội. Chỉ thị này được quán triệt, triển khai giúp tăng cường lãnh đạo chỉ đạo, quản lý; kịp thời phát hiện, ngăn chặn xử lý những thông tin có nội dung xấu, độc hại gây tổn hại đến uy tín của Đảng, Nhà nước, chế độ, ảnh hưởng xấu đến tiến trình phát triển kinh tế, xã hội, an ninh, quốc phòng. Chủ động

phòng ngừa, hạn chế những sơ hở, thiếu sót, không để các thế lực thù địch và các đối tượng thù địch lợi dụng xâm nhập hệ thống thông tin, thu thập, chiếm đoạt bí mật nhà nước, thông tin nội bộ đe dọa đến an ninh quốc gia, lợi ích của cơ quan, tổ chức và công dân. Hành lang pháp lý trong lĩnh vực ATTT về cơ bản đang dần hoàn thiện với việc năm 2015 Quốc hội thông qua Luật An toàn thông tin mạng và các Nghị định hướng dẫn luật đã được ban hành. Ngày 27/5/2016, Chính phủ cũng đã ban hành Quyết định số 898/QĐ-TTg phê duyệt phương hướng, mục tiêu, nhiệm vụ bảo đảm ATTT mạng giai đoạn 2016-2020. Điều này thể hiện sự quan tâm sâu sắc của lãnh đạo Đảng, Nhà nước đối với công tác bảo đảm an ninh mạng trong bối cảnh tình hình hiện nay, thể hiện sự quyết tâm và đồng lòng của toàn Đảng, toàn dân đưa nước ta sớm trở thành một quốc gia mạnh về công nghệ thông tin, gắn liền với bảo vệ vững chắc quốc phòng - an ninh của đất nước. Đáng chú ý là sự ra đời của các cơ quan, tổ chức, liên minh, hiệp hội về ATTT như: Trung tâm Ứng cứu khẩn cấp máy tính (VNCERT), Hiệp hội An toàn thông tin Việt Nam (VNISA), Viện Nghiên cứu Chính sách và Phát triển Truyền thông (IPS)... Những đơn vị này đã và đang đóng góp đáng kể cho sự an toàn của internet tại Việt Nam bằng nhiều hoạt động phong phú và đa dạng: từ nghiên cứu chính sách, khảo sát thực tiễn cho đến tổ chức các hội nghị, khóa đào tạo, tập huấn về ATTT.

Điểm yếu

Hiện nay, các văn bản pháp luật có liên quan đến công tác bảo đảm ATTT còn có những vấn đề bất cập. Thực hiện các cam kết quốc tế mà Việt Nam tham gia ký kết như: Cam kết gia nhập WTO, Thỏa thuận trong khối ASEAN, của ASEAN với Nhật Bản, Trung Quốc..., Việt Nam cần có các quy định pháp lý phù hợp với thông lệ quốc tế để bảo đảm ATTT, tạo môi trường bình đẳng cho các tổ chức, doanh nghiệp hoạt động sản xuất, kinh doanh tại Việt Nam.

Quá trình đảm bảo ATTT trong doanh nghiệp Việt Nam hiện nay còn nhiều hạn chế

Theo Tổng cục Thống kê, đến tháng 07/2017, cả nước có khoảng 518.000 doanh nghiệp, năm 2018 có 131.275 doanh nghiệp đăng ký thành lập mới với tổng vốn đăng ký là 1.478,1 nghìn tỷ đồng, tăng 3,5% về số doanh nghiệp và tăng 14,1% về số vốn đăng ký so với năm 2017.[1] Tuy nhiên, doanh nghiệp vừa và nhỏ vẫn chiếm đa số trong tổng số doanh nghiệp Việt Nam. Hiện nay, việc ứng dụng công nghệ thông tin vào hoạt động sản xuất kinh doanh đang được các doanh nghiệp ngày càng quan tâm nhiều hơn. Điều này càng trở nên quan trọng hơn bao giờ hết khi mà sự phát triển và cạnh tranh giữa các doanh nghiệp ngày càng lớn, khi mà doanh nghiệp nước ngoài ngày càng nhiều trên thị trường Việt Nam.

Trong bối cảnh cuộc cách mạng công nghiệp

[1] Lê Trần "Tổng cục thống kê: Quy mô doanh nghiệp vừa và nhỏ đang ngày càng nhỏ", từ website: http://vietnamfinance.vn/tong-cuc-thong-ke-quy-mo-doanh-nghiep-vua-va-nho-dang-ngay-cang-nho-20180119145350988.htm, truy cập ngày 16/2/2019.

4.0 diễn ra ngày càng mạnh mẽ, các doanh nghiệp Việt Nam buộc phải có sự chuẩn bị và chuyển mình mạnh mẽ trong việc ứng dụng công nghệ thông tin nhằm nâng cao năng lực cạnh tranh, gia tăng lợi nhuận và mang đến nhiều hơn các dịch vụ gia trị gia tăng cho khách hàng. Tuy nhiên, chính quá trình chuyển đổi kỹ thuật số này lại đang khiến doanh nghiệp nhanh chóng trở thành mục tiêu của các cuộc tấn công mạng. Tình hình mất ATTT gây ra các tổn thất cho doanh nghiệp thậm chí gây ra tác động xấu đến nền kinh tế, chính trị, xã hội.

Theo Báo cáo tổng hợp kết quả điều tra của Hiệp hội ATTT Việt Nam (VNISA) cho thấy, chỉ số ATTT cho các doanh nghiệp Việt Nam hiện nay còn thấp.

Năm 2017, chỉ số ATTT của doanh nghiệp Việt Nam là 54,2%. Chỉ số này thấp hơn so với chỉ số ATTT nói chung năm 2016, đặc biệt là các doanh nghiệp nhỏ và vừa có chỉ số rất thấp. Cũng theo kết quả công bố của VNISA, chỉ số ATTT mạng VNISA Index năm 2018 là 45,6%, chỉ ở mức trung bình.[2]

Nếu tách riêng, chỉ số ATTT cho khối doanh nghiệp trong ngành ngân hàng tài chính là 59,9%, cao hơn mức trung bình của toàn khối doanh nghiệp. Các chỉ số ATTT thành phần của khối ngân hàng tài chính đều cao hơn chỉ số ATTT thành phần của khối doanh nghiệp nói chung, đặc biệt cao hơn hẳn về mình độ nhận thức, đào tạo bồi dưỡng về ATTT (59,9 so với 51,3); tổ chứ quản lý nhân lực đảm bảo ATTT mạng (49,5 s với 43,2); chính sách pháp lý (70,5 so với 60,9 biện pháp kỹ thuật (60,5 so với 53,7) và biệ pháp quản lý (73,3 so với 63,9).[3]

Đối với các doanh nghiệp vừa và nh (DNVVN), chỉ số ATTT mạng năm 2018 củ nhóm doanh nghiệp này đã được cải thiện, tăn từ mức 31,1% của năm 2017 lên đạt 39,9% trong năm nay. Tuy nhiên, nếu so với chỉ số ATTT củ toàn bộ doanh nghiệp Việt Nam thì chỉ số ATT của các DNVVN thấp hơn nhiều. Nếu tính theo vùng miền, chỉ số ATTT của các DNVVN miề Bắc là cao nhất, năm 2017 đạt 38,4%. Chỉ số ATTT của các DNVVN khu vực miền Nam và miền Trung lần lượt là 22,3% và 36,4%. Còn ch số ATTT cho toàn bộ DNVVN Việt Nam năm 2017 là 31,1%.[4]

Tại buổi Diễn tập quốc tế, APCERT cho biết chỉ trong hai tháng đầu năm 2018, đã có 1.50 sự cố tấn công mạng vào Việt Nam dưới ba hình thức: tiến công thay đổi giao diện (Deface), tấn công cài mã độc (Malware) và tấn công lừa đảo (Phishing). Cũng theo các số liệu mà đơn v này có được, Việt Nam lần lượt xếp ở vị trí thứ tư và thứ năm trong danh sách top 10 quốc gi bị kiểm soát bởi mạng máy tính "ma" và top 1 quốc gia bị tấn công DDos (tấn công từ chố dịch vụ). Trước đó, báo cáo chỉ số an ninh mạng toàn cầu (GCI) năm 2017 của Liên minh Viễ

[2], [3], [4] Ban cơ yếu chính phủ ATTT: "Đánh giá Chỉ số ATTT năm 2017 cho các doanh nghiệp Việt Nam", từ website:http // antoanthongtin.vn/Detail.aspx?NewsID=334e656d-d43b-4873-8195-aa15cb747c7d&CatID=e1999c9a-5eeb-418c-9ea8-ae4c5e850d0c, truy cập ngày 16/2/2019

thông quốc tế (ITU) chỉ xếp hạng Việt Nam ở vị trí 100 (giảm 25 bậc so với báo cáo thường niên năm 2016).[5]

Theo Cục ATTT, đến tháng 04 năm 2018 có ít nhất 60 trang web đặt tại Việt Nam bị lợi dụng để thực hiện tấn công Phishing hàng tuần.[6] Qua theo dõi, trích xuất thông tin từ hệ thống kỹ thuật thời gian qua, Cục ATTT nhận thấy trên không gian mạng đang tồn tại nhiều trang web Việt Nam (bao gồm cả những trang web sử dụng dịch vụ máy chủ nước ngoài) bị tấn công lợi dụng để thực hiện các hành vi gây mất ATTT như: phát tán thư rác; tấn công từ chối dịch vụ; cài đặt và phát tán các loại mã độc; lưu trữ các mã khai thác điểm yếu lỗ hổng một cách tự động (như lỗ hổng trên trình duyệt hay các thành phần mở rộng của trình duyệt mà người dùng sử dụng...).

Trong bối cảnh đó, có rất nhiều doanh nghiệp vẫn chưa thấy được vấn đề về an toàn cho hệ thống thông tin doanh nghiệp của mình và chưa có biện pháp phù hợp để bảo đảm ATTT của doanh nghiệp.

3. Giải pháp an toàn thông tin

Thực trạng trên cho thấy, vấn đề bảo mật trong doanh nghiệp ngày càng trở nên thiết yếu, đòi hỏi các doanh nghiệp Việt Nam phải có cách tiếp cận chủ động hơn trong việc đối phó với các mối đe dọa có thể xảy ra bất cứ lúc nào. Để bảo đảm ATTT cho hệ thống thông tin, các doanh nghiệp cần phải thực hiện nhiều giải pháp khác nhau. Tuy nhiên, trước tiên doanh nghiệp cần phải đánh giá mức độ ATTT của hệ thống thông tin trước khi đưa vào sử dụng và định kỳ kiểm tra để có biện pháp khắc phục các lỗ hổng bảo mật. Dựa trên tiêu chuẩn Open Web Application Security Project (OWASP)[7] và giải pháp bảo vệ hệ thống thông tin cho doanh nghiệp bằng phần mềm ModSecurity, tác giả trình bày các bước đánh giá ATTT cho hệ thống thông tin của doanh nghiệp.

3.1. Đánh giá ATTT theo tiêu chuẩn OWASP

Hiện nay, có rất nhiều chuẩn đánh giá mức độ ATTT cho hệ thống thông tin doanh nghiệp như: OWASP (Open Web Application Security Project), COBIT (Control objective for Information and Related Techniques, SANS, PCI/DSS (The Payment Card Industry Data Security Standard), (ISO/IEC27001) International Organization for Standardization and International Electrotechnical Commission. Bài viết này trình bày các bước đánh giá mức độ ATTT cho hệ thống thông tin doanh nghiệp theo chuẩn OWASP, đây là chuẩn mở của cộng đồng mạng thế giới nhằm giúp các doanh nghiệp vừa và nhỏ có thể chuẩn hóa ứng dụng chạy trên nền tảng Web, bảo đảm quá trình vận hành một cách an toàn trước nguy cơ

[5] Cục An toàn thông tin – Bộ thông và Truyền thông. Bản tin An toàn thông tin tháng 04 năm 2018

[6] Cục An toàn thông tin – Bộ thông và Truyền thông: Bản tin An toàn thông tin tháng 04 năm 2018.

[7] OWASP (Open Web Application Security Project) là 1 dự án mở về bảo mật ứng dụng web, dự án là sự cố gắng chung của cộng đồng với mục đích giúp các doanh nghiệp có thể phát triển, mua và bảo trì các ứng dụng web một cách an toàn

bị tấn công. Bên cạnh đó, còn cung cấp tài liệu về kiểm tra bảo mật ứng dụng, sách về lập trình an toàn, các bài viết về kiểm định mã nguồn, một số công cụ để đánh giá mức độ ATTT của Web hoàn toàn miễn phí.

Sau đây là các bước đánh giá mức độ ATTT của hệ thống thông tin theo tiêu chuẩn OWASP:

Bước 1: Thu thập thông tin tổng quát hệ thống

Tìm hiểu tất cả các tính năng có nguy cơ xảy ra lỗi: có thể kiểm tra tính năng của tất cả các ứng dụng web có khả năng phát sinh ra lỗi trong mã nguồn.

Thu thập những nội dung bị lỗi hoặc bị ẩn đi. Có thể sử dụng một số công cụ như Burp Suite. Sử dụng các công cụ phổ biến (các công cụ về tìm kiếm) và kiểm tra các nội dung thường được lưu trong hệ thống: robots.txt, sitemap.xml, .DS_Store, phpinfo.php, info.php, php.php, test.php, test.aspx, phpinfo.php, info.php, php.php, test.php, test.aspx. Với mục tiêu tìm kiếm những đường dẫn, những thông tin về hệ thống dành riêng cho người quản trị.

Sử dụng kỹ thuật fingerprinting để xâm nhập thử hệ thống và xem hệ thống webserver đang hoạt động trên phiên bản nào.

Tìm hiểu công nghệ được áp dụng cho các trang web: chẳng hạn với ứng dụng web chạy trên nền tảng công nghệ PHP hoặc trên nền tảng Java, ASP.NET thì có hướng kiểm tra và khai thác khác nhau.

Kiểm tra danh sách người dùng, chức năng của các quyền trong hệ thống với mục tiêu kiểm tra các tính leo thang giữa các người dùng.

Bước 2: Tấn công thử bằng các phương thức khác nhau

Để phát hiện được các lỗ hổng trong hệ thống, người kiểm định tiến hành tấn công thử hệ thống theo các phương thức khác nhau. Chẳng hạn như kiểm tra các vấn đề về xác thực mật khẩu; các vấn đề về quản lý phiên; các vấn đề về phân quyền; kiểm tra tính hợp lệ của dữ liệu; kiểm tra chức năng xử lý logic; các vấn đề mã hóa; các vấn đề về quản lý cấu hình; các vấn đề về đăng tải tập tin.

Bước 3: Xác định mức độ nghiêm trọng của lỗ hổng

Nếu trong quá trình kiểm định hệ thống mà có phát hiện lỗ hổng nghiêm trọng có thể dẫn đến việc phơi bày thông tin quan trọng của doanh nghiệp thì người đánh giá phải tiến hành thông báo ngay cho doanh nghiệp biết để có biện pháp khắc phục. Việc xác định mức độ nghiêm trọng sẽ dựa theo 10 rủi ro ứng dụng web của OWASP TOP 10 (lỗi nhúng mã; sai lầm trong kiểm tra định danh; thực thi mã script xấu; sai sót cấu hình an ninh; lưu trữ bảo mật thiếu an toàn; sai sót hạn chế truy cập; giả mạo yêu cầu; sử dụng các thành phần có lỗ hổng đã được công bố; chuyển hướng và chuyển tiếp thiếu thẩm tra).

Bước 4: Báo cáo lãnh đạo doanh nghiệp về lỗ hổng và đề xuất một số biện pháp khắc phục

Đánh giá và phát hiện lỗ hổng hệ thống chỉ là bước ban đầu của quá trình đánh giá tổng thể,

sản phẩm cuối cùng của quá trình này phải là một văn bản có nhiều thông tin dưới dạng báo cáo. Báo cáo sẽ được cung cấp cho lãnh đạo đơn vị.

Bước 5: Kết thúc quá trình đánh giá

Để kết thúc quá trình đánh giá, người kiểm định sẽ lập báo cáo tổng kết bao gồm các nội dung sau đây: mô tả sơ bộ về quá trình đánh giá; số lỗ hổng đã phát hiện và khắc phục được; số lỗ hổng đã phát hiện và chưa khắc phục được. Một số cảnh báo quan trọng; khuyến cáo và đề xuất khắc phục; tóm lại nội dung trình bày; báo cáo kỹ thuật về biện pháp khắc phục lỗi; báo cáo chi tiết về các lỗ hổng chưa được khắc phục.

Sử dụng phần mềm ModSecurity để ngăn chặn tấn công hệ thống Web cho doanh nghiệp.

ModSecurity là một chương trình phần mềm mã nguồn mở do Ivan Ristic[8] khởi nguồn. Phiên bản sau cùng của ModSecurity là một tường lửa ứng dụng (WAF) mã nguồn mở sử dụng bộ nguyên tắc để phòng chống lỗi "zero day" và một số lỗ hổng bảo mật được tìm thấy trong ứng dụng web. ModSecurity còn có thể sử dụng như một bộ lọc bảo mật, xác định các cuộc tấn công, thực hiện xác thực giá trị đầu vào hệ thống web.

ModSecurity có khả năng phát hiện những vi phạm về truy cập từ việc phân tích giao thức http. Ngoài ra, ModSecurity còn có khả năng phát hiện các chương trình thu thập thông tin, máy quét, các cuộc tấn công bằng mã độc, các truy cập có đính kèm mã độc Trojan và có khả năng bảo vệ từ xa mà không cần can thiệp vào mã nguồn hệ thống.

ModSecurity có khả năng ngăn chặn việc hacker khai thác các lỗ hổng bảo mật của hệ thống Web doanh nghiệp như: tấn công SQL Injection, thực thi mã Script xấu (XSS), ngăn cản tấn công từ chối dịch vụ DoS (Denial of Service). ModSecurity thực hiện việc ngăn chặn tấn công thông qua các Rule và không cần phải can thiệp vào mã nguồn hệ thống Web của doanh nghiệp, mã nguồn phần mềm ModSecurity được cung cấp miễn phí, phù hợp để triển khai cho các doanh nghiệp vừa và nhỏ. Sau đây là minh họa về cách triển khai các dòng lệnh trong Rule, khi hệ thống doanh nghiệp phát hiện hệ thống Web của đơn vị mình bị tấn công DoS, doanh nghiệp tiến hành cài đặt Rule để ngăn chặn cho tấn công DoS như sau [9]:

```
SecReadStateLimit 100

SecRule RESPONSE_STATUS "@streq 408"
"phase:5,id:'981051',t:none,log,pass,setvar:ip.
slow_dos_counter=+1,expirevar:ip.slow_dos_
counter=60"

SecRule IP:SLOW_DOS_COUNTER "@gt 3"
"phase:1,id:'981052',t:none,log,drop,msg:'Client
Connection Dropped due to high # of slow DoS
alerts'"
```

Khi triển khai các dòng lệnh trên, Modsecurity

[8] Magnus Mischel. *Mod Security 2.5*, Birmingham-mumbai, Published by Packt Publishing Ltd, 2009.

[9] Ryan C.Barnett: Web Application Defender's Cookbook , John Wiley & Sons Inc, The United states of America, 2013.

sẽ phân tích yêu cầu của người truy cập vào hệ thống thông tin của doanh nghiệp, nếu trong khoảng thời gian 180 giây mà người dùng đó liên tục gửi yêu cầu truy cập đến máy chủ cung cấp hệ thống thông tin của doanh nghiệp, nhưng bị báo lỗi 408 thì Rule trên sẽ được thực thi, lúc này người dùng sẽ bị ngăn chặn việc truy xuất thông tin yêu cầu, vì đây được xem là dấu hiệu của tấn công từ chối dịch vụ vào hệ thống thông tin doanh nghiệp.

4. Kết luận

Vấn đề ATTT là lĩnh vực khá mới mẻ đối với nước ta, luôn đòi hỏi nhiều kiến thức chuyên sâu trong lĩnh vực công nghệ thông tin và kinh nghiệm thực tiễn. Vì vậy, để nâng cao tính bảo mật cho hệ thống thông tin của doanh nghiệp cần phải tiến hành đánh giá mức độ ATTT cho hệ thống thông tin của doanh nghiệp. Kết quả của quá trình đánh giá, sẽ giúp cho doanh nghiệp sớm tìm ra lỗ hổng trong hệ thống thông tin. Dựa vào kết quả tìm ra các lỗ hổng, đội ngũ chuyên gia công nghệ thông tin có thể kết hợp với phần mềm ModSecurity phòng tránh việc hacker khai thác vào các lỗ hổng bảo mật, để chiếm quyền điều khiển hệ thống, đánh cắp thông tin quan trọng của doanh nghiệp.

TÀI LIỆU THAM KHẢO

1. Ban Bí thư Trung ương Đảng: *Chỉ thị số 28 CT/TW "Về tăng cường công tác bảo đảm ATTT mạng"*, 2013.

2. Thủ tướng Chính phủ: *Quyết định số 898/ QĐ-TTg về "Phê duyệt phương hướng, mục tiêu nhiệm vụ bảo đảm ATTT mạng giai đoạn 2016 2020"*, 2016.

3. VNCERT: "Các mối đe dọa tấn công từ chối dịch vụ mới - Emergence of a New DDoS Threat", từ website: http://vncert.gov.vn/baiviet php?id=45, truy cập ngày 16/2/2019.

4. Security standards council: *PCI DSS quick reference guide*, PCI SSC Security Standards 2010.

5. Ryan C.Barnett: *Web Application Defender's Cookbook* , John Wiley & Sons Inc, The United states of America, 2013.

6. Lệ Trần: "Tổng cục thống kê: Quy mô doanh nghiệp vừa và nhỏ đang ngày càng nhỏ" từ website: http://vietnamfinance.vn/tong-cuc-thong-ke-quy-mo-doanh-nghiep-vua-va-nho-dang-ngay-cang-nho-20180119145350988 htm, truy cập ngày 16/2/2019.