HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Nguyễn Thị Hạnh

NGHIÊN CỨU CÁC PHƯƠNG THỨC TẤN CÔNG HỆ THỐNG EMAIL VÀ CÁC GIẢI PHÁP PHÒNG CHỐNG ANTI-SPAM

Chuyên ngành: HỆ THỐNG THÔNG TIN

Mã số: 8.48.01.04

TÓM TẮT LUẬN VĂN THẠC SĨ

HÀ NỘI - 2019

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: **PGS.TS. TRẦN QUANG ANH**

Phản biện 1:

Phản biện 2:

Luận văn sẽ được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông

Vào lúc: … ngày … tháng … năm 2019

Có thể tìm hiểu luận văn tại:

- Thư viện của Học viện Công nghệ Bưu chính Viễn thông

LỜI MỞ ĐẦU

1. Lý do chọn đề tài

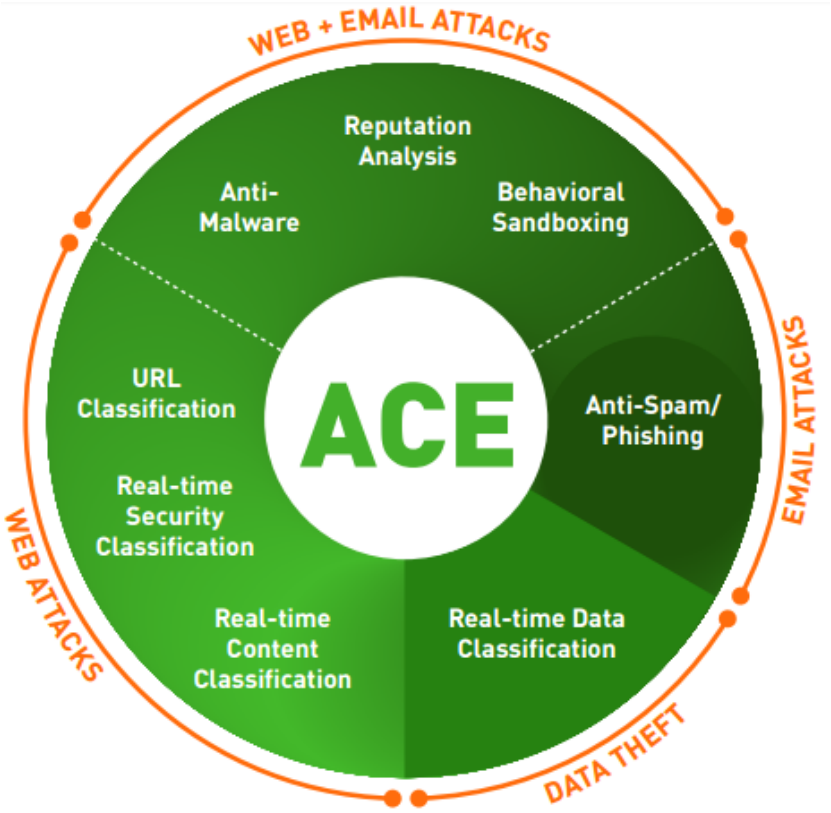
Ngày nay với sự phát triển bùng nổ của công nghệ thông tin, hầu hết các thông tin của các tổ chức, cá nhân đều được lưu trữ trên hệ thống máy tính và trao đổi với nhau từ mọi vị trí địa lý. Cùng với sự phát triển của tổ chức là những đòi hỏi ngày càng cao của môi trường hoạt động cần phải chia sẻ thông tin của mình cho nhiều đối tượng khác nhau qua mạng. Việc mất mát, rò rỉ thông tin sẽ có thể ảnh hưởng nghiêm trọng đến tài nguyên thông tin, tài chính, danh tiếng của tổ chức, cá nhân.

Các phương thức tấn công thông qua mạng ngày càng tinh vi, phức tạp có thể dẫn đến mất mát thông tin, thậm chí có thể làm sụp đổ hoàn toàn hệ thống thông tin của tổ chức. Vì vậy an toàn thông tin là nhiệm vụ quan trọng, nặng nề và khó đoán trước đối với các hệ thống thông tin.

Email là một trong các nguồn chính gây rủi ro về an toàn thông tin. Bên cạnh vấn đề thư rác, virus, có khá nhiều tấn công lừa đảo thực hiện qua Email, và Email chính là mục tiêu hàng đầu của các cuộc tấn công có chủ đích (APT). Các rủi ro về mất mát dữ liệu nhạy cảm do tấn công lừa đảo, malware, và do người dùng cố ý hoặc vô ý được diễn ra một phần không nhỏ là qua Email.

- 84% các Email là thư rác (spam)
- 89% các Email không mong muốn chứa đường link tới Email độc hại
- 9% rò rỉ dữ liệu nhạy cảm xảy ra qua Email

Do đó cần phân tích các mối đe doạ theo thời gian thực tại Email Gateway, cung cấp báo cáo nâng cao để đánh giá, điều tra các sự kiện đối với hệ thống Email.



Hình 1: Sử dụng ACE phân tích các nguy hại theo thời gian thực

2. Mục đích nghiên cứu:

Trong nhiều năm trước, khi Internet bắt đầu phát triển mạnh mẽ trên khắp thế giới, các Email đã truyền tải thông tin dưới dạng dữ liệu ngày càng phức tạp. Tổng lượng tổ chức và người truy cập và sử dụng Email đã tăng lên nhanh chóng.

Hệ thống Email là thành phần thiết yếu trong mọi cơ quan, tổ chức và đem lại khả năng xử lý thông tin, truyền tải thông tin, là tài sản rất quan trọng nhưng hệ thống thông tin cũng chứa rất nhiều điểm yếu và rủi do. Do Email được phát triển với tốc độ rất nhanh để đáp ứng nhiều yêu cầu của người dùng ngày càng tăng, các loại dịch vụ hoặc thông tin quảng cáo có chứa mã độc mới được thêm vào ngày càng nhiều, điều này làm cho Email không được kiểm tra kỹ trước khi phát hành và bên trong chúng chứa rất nhiều lỗ hổng có thể dễ dàng bị lợi dụng. Thêm vào đó là việc phát triển của hệ thống Email, cũng như sự phân tán của hệ thống thông tin, làm cho người dùng truy cập thông tin dễ dàng hơn và tin tặc cũng có nhiều mục tiêu tấn công dễ dàng hơn.

Với việc phân tích các phương thức tấn công qua Email, đề tài mà tác giả quan tâm và nghiên cứu sẽ đưa ra cách nhận diện một tấn công từ bên ngoài hoặc bên trong đối với hệ thống Email. Từ đó phân tích các mối nguy hại, các phương thức tấn công và mức độ ảnh hưởng để đưa ra các phương pháp ngăn chặn, phòng chống, khắc phục và bảo vệ hệ thống Email một cách hiệu quả.

- ***Bảo vệ tài nguyên của hệ thống***

Các hệ thống máy tính lưu giữ rất nhiều thông tin cần truyền tải trên mạng và tài nguyên đó cần được bảo vệ. Trong một tổ chức, những thông tin và tài nguyên này có thể là dữ liệu kế toán, thông tin nguồn nhân lực, thông tin quản lý, bán hàng, nghiên cứu, sáng chế, phân phối, thông tin về tổ chức và thông tin về các hệ thống nghiên cứu. Đối với rất nhiều tổ chức, toàn bộ dữ liệu quan trọng của họ thường được lưu trong một cơ sở dữ liệu và được quản lý và sử dụng bởi các chương trình phần mềm. Các tấn công vào hệ thống thông tin có thể được thực hiện qua Email và xuất phát từ những đối thủ của tổ chức hoặc cá nhân do đó, các phương pháp để bảo đảm an toàn cho những thông tin này có thể rất phức tạp và nhạy cảm. Các tấn công có thể xuất phát từ nhiều nguồn khác nhau, cả từ bên trong và bên ngoài tổ chức. Hậu quả mà những tấn công thành công để lại sẽ rất nghiêm trọng và gây tổn thất rất lớn đến từng cá nhân và tổ chức.

- ***Bảo đảm tính riêng tư***

Các hệ thống Email lưu giữ và truyền tải rất nhiều thông tin cần được giữ bí mật và chính xác. Những thông tin này bao gồm: Số thẻ bảo hiểm xã hội, số thẻ ngân hàng, số thẻ tín dụng, thông tin về gia đình,…Những thông tin riêng tư là yêu cầu rất quan trọng mà các ngân hàng, các công ty tín dụng, các công ty đầu tư và các hãng khác cần phải đảm bảo để gửi đi các tài liệu thông tin chi tiết về cách họ sử dụng và chia sẻ thông tin về khách hàng. Các hãng này có những quy định bắt buộc để bảo đảm những thông tin được bí mật và bắt buộc phải thực hiện những quy định đó để bảo đảm tính riêng tư. Hậu quả nghiêm trọng sẽ xảy ra nếu một kẻ giả mạo truy nhập được những Email và đánh cắp các thông tin cá nhân. Do đó bảo vệ Email cũng là một phương pháp để bảo đảm tính riêng tư của cá nhân và tổ chức.

3. Đối tượng và phạm vi nghiên cứu

- Với việc xác định đối tượng nghiên cứu chính là phân tích các phương thức tấn công qua Email, đề tài sẽ đưa ra cách nhận diện một tấn công từ bên ngoài hoặc bên trong đối với hệ thống Email. Từ đó phân tích các mối nguy hại, các phương thức tấn công và mức độ ảnh hưởng để đưa ra các phương pháp ngăn chặn, phòng chống, khắc phục và bảo vệ hệ thống Email một cách hiệu quả.
- Phạm vi nghiên cứu: Nghiên cứu đối với các phương pháp tấn công Email
- Luận văn được xây dựng trên cơ sở kế thừa kết quả khảo sát thực tế và các tài liệu.

4. Phương pháp nghiên cứu:

Luận văn này dự kiến tổ chức thực hiện nghiên cứu, đề xuất các phương pháp phòng chống tấn công Email và các yếu tố liên quan mật thiết đến việc xây dựng, vận hành hệ thống.

Nghiên cứu thực hiện thông qua phương pháp lý thuyết: các phương thức tấn công hệ thống Email, luồng gửi nhận dữ liệu, các thuật toán mã hóa, các phương pháp lọc gói tin,…

Nghiên cứu bằng phương pháp thực tiễn: từ việc phân tích dữ liệu gửi và nhận, thu thập các mẫu và phân tích cách phòng chống tại Ngân hàng Hàng Hải Việt Nam (MSB).

5. Kết cấu luận án

Luận án gồm 3 chương được kết cấu như sau:

- Chương 1: Giới thiệu về thư điện tử, thư rác và các hình thức tấn công thư điện tử.
- Chương 2: Các phương pháp phòng chống tấn công thư điện tử
- Chương 3: Triển khai thử nghiệm, đề xuất áp dụng phương pháp phòng chống tấn công anti spam email cho hệ thống email tại ngân hàng hàng hải việt nam

CHƯƠNG I. GIỚI THIỆU VỀ THƯ ĐIỆN TỬ, THƯ RÁC VÀ CÁC HÌNH THỨC TẤN CÔNG THƯ ĐIỆN TỬ

1.1 Tìm hiểu về thư điện tử (Email) và thư rác (Spam Email)

1.1.1. Tìm hiểu về thư điện tử (Email)

1.1.1.1 Định nghĩa thư điện tử (Email)

Email (là từ ghép viết tắt của Electronic Mail – Thư điện tử) là một dạng tin nhắn/ thông điệp được gửi đi từ một người dùng máy tính đến một hoặc nhiều người nhận qua mạng.

Thông điệp được lưu trữ trong Email có thể tồn tại ở dạng văn bản (text), hình ảnh, âm thanh, video dưới dạng tệp tin đính kèm..

1.1.1.2 Phân loại các loại Email hiện nay

Đối với hệ thống Email hiện nay có 2 loại Email là Email Server và Email miễn phí.

- Email server
- Email miễn phí
- So sánh hai dịch vụ Email Server và Email miễn phí

Nhằm nghiên cứu tổng thể các phương thức tấn công hệ thống Email cũng như chủ động phân tích luồng dữ liệu gửi nhận trong hệ thống, luận văn tập trung nghiên cứu dịch vụ Email Server.

1.1.2. Tìm hiểu về thư rác (Spam Email)

1.1.2.1 Định nghĩa thư rác (Spam Email)

Spam Email: là việc gửi hàng loạt Email chứa nội dung không liên quan hoặc vô bổ đến nhiều người nhận. Spam Email thường chứa các loại quảng cáo được gửi một cách vô tội vạ từ một địa chỉ không xác định đến nơi nhận là một danh sách rất dài gửi từ các cá nhân hay các nhóm người. Chất lượng của loại thư này thường thấp, đôi khi là một sự lừa đảo để tìm cách thu thập tin tức cá nhân hoặc từ đó xâm nhập vào hệ thống mạng.

1.1.2.2 Các đặc điểm thư rác (Spam Email)

- Spam Email được gửi đi một cách tự động
- Spam Email được gửi đến những địa chỉ ngẫu nhiên trên một diện rộng
- Spam Email dùng chương trình tự động dò tìm địa chỉ Email trên mạng Internet, các trang chủ, Newsgroup, Chat room…
- Spam Email dùng chương trình đoán tên tự động
- Nội dung của Spam Email thường là những nội dung bất hợp pháp, gây phiền hà cho người dùng
- Địa chỉ của người gửi thư rác thường là những địa chỉ trá hình

1.1.2.3 Các kỹ thuật tạo ra một Spam Email

- Kỹ thuật che giấu hoặc chuyển hướng nội dung, liên kết
- Tấn công trang web.
- Văn bản ẩn hoặc nhồi nhét từ khóa
- Tên miền trỏ hướng
- Spam thuần túy
- Cung cấp DNS động và máy chủ lưu trữ gây ra spam
- Nội dung nghèo nàn có ít hoặc không có giá trị
- Liên kết bất thường từ trang web

1.2 Các hình thức tấn công Email

1.2.1 Một số hình thức tấn công Email

- Lừa đảo qua tổ chức danh tiếng
- Email thỏa thuận từ doanh nghiệp:
- Email tống tiền:
- Email có chứa phần mềm độc hại:

1.2.2 Kiến trúc của thư điện tử dạng lừa đảo tấn công

1.3 Hiện trạng về các tấn công Email hiện nay

1.3.1 Tình hình tấn công Email trên thế giới

1.3.2 Tình hình tấn công Email tại Việt Nam

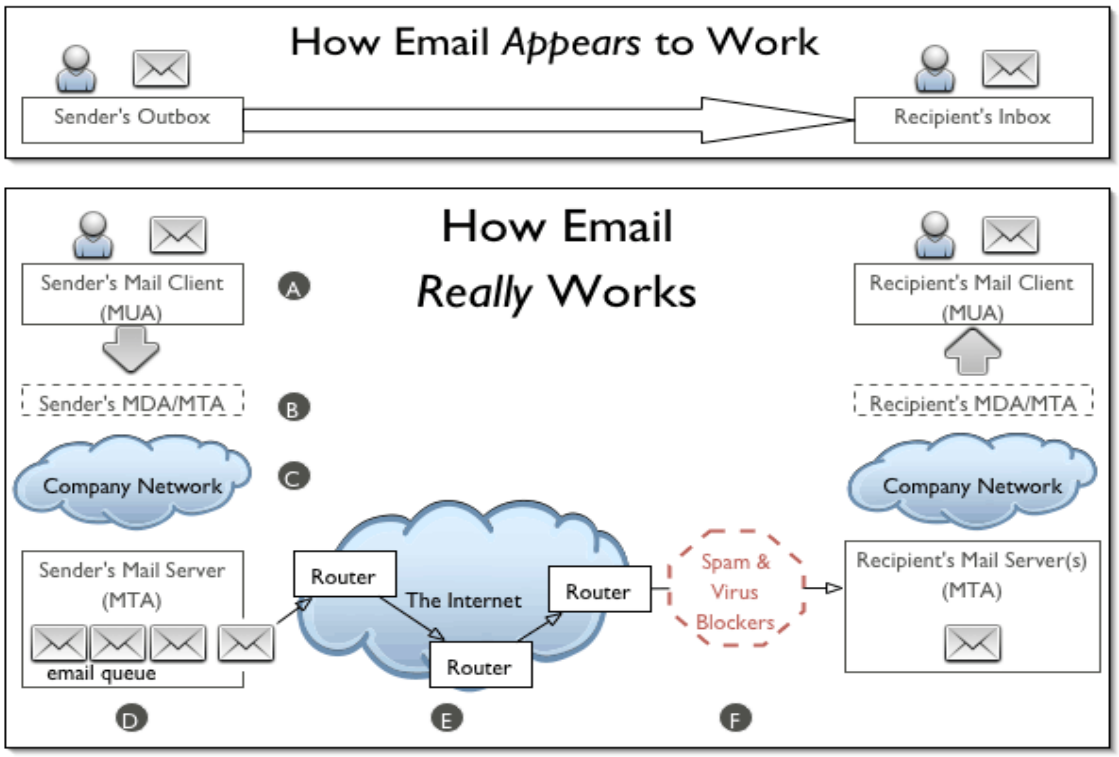
Kết luận chương:

Chương 1 của luận văn đã giới thiệu tổng quan hệ thống thư điện tử, thư rác, trong đó nêu rõ các khái niệm, đặc điểm, kiến trúc của thư điện tử, thư rác. Chương 1 cũng đưa ra các hình thức tấn công Email cũng như hiện trạng về các tấn công thư điện tử hiện nay. Từ đó, đưa ra một khái quát chung nhất vấn đề mà luận văn đề cập đến.

CHƯƠNG II: CÁC PHƯƠNG PHÁP PHÒNG CHỐNG TẤN CÔNG THƯ ĐIỆN TỬ

2.1. Các phương pháp phòng chống tấn công đối với Hệ thống Email.

Một hệ thống Email bao gồm những thành phần sau:



Hình 2.1: Những thành phần của hệ thống Email

Theo sơ đồ trên thì hệ thống Email bao gồm các thành phần sau: ứng dụng Mail Client, ứng dụng Mail Server, đường truyền Internet.

Vậy để bảo vệ một hệ thống Email hoàn chỉnh, các thành phần cần xây dựng các phương pháp để bảo vệ các hệ thống trên.

2.1.1 Các phương pháp bảo vệ đối với ứng dụng Mail Client

Bảo vệ ứng dụng Mail Client chính là bảo vệ người dùng tránh được các tấn công lừa đảo từ Email. Để thực hiện được điều đó, người dùng cần thực hiện các phương pháp sau:

- Kiểm tra virus và phần mềm độc hại (viruses and malware):
- Chọn mật khẩu mạnh và không trùng với trang khác
- Nên có ít nhất khoảng 2 tài khoản Email
- Đăng ký xác minh 2 bước
- Chú ý Phishing lừa đảo
- Xem xét các link đính kèm Email
- Không mở file đính kèm khi không xác định rõ người gửi
- Hạn chế kết nối WiFi công cộng

2.1.2 Các phương pháp bảo vệ đối với hệ thống ứng dụng Mail Server

Để đảm bảo tính toàn vẹn, an toàn và xác thực đối với hệ thống ứng dụng Mail Server cần đáp ứng các yêu cầu sau:

2.1.2.1 Kiểm tra dữ liệu đầu vào (Input Data Validation)

2.1.2.2 Xác thực và quản lý mật khẩu (Authentication and Password Management)

2.1.2.3 Ủy quyền (Authorization)

2.1.2.4 Bảo vệ dữ liệu nhạy cảm (Sensitive Data Protection)

2.1.2.5 Quản lý phiên làm việc (Session Management)

2.1.2.6 Mã hóa (Cryptographic Practices)

2.1.2.7 Kiểm soát và ghi log (Auditing and Logging).

2.1.2.8 Quản lý tập tin và tài nguyên (File and Resource Management)

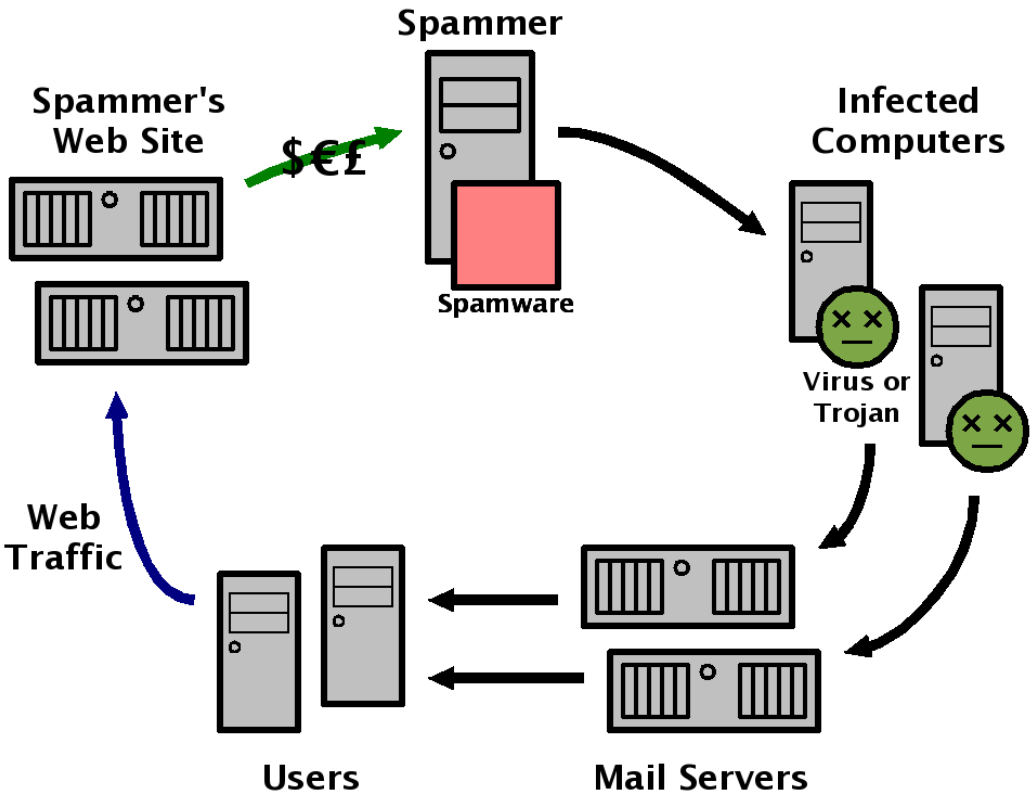
2.1.2.9 Cấu hình hệ thống đảm bảo an toàn (Systerm Configuraiton)

2.1.2.10 An ninh cho các ứng dụng Email trên di động

2.1.3 Bảo vệ đường truyền, kết nối (Communication Security)

2.2. Các phương pháp điển hình phòng chống tấn công AntiSpam Email

2.2.1 Cơ chế hoạt động của Spam Email



Hình 2.2: Cơ chế hoạt động của Spam Email

Quá trình thực hiện của một Spammer như sau:

Bước 1: Spammer’s web site trả tiền cho các người phán tán Spammer

Bước 2: Spammer gửi spam với các đường dẫn, virus đến các máy tính thông qua đường truyền Internet

Bước 3: Các Email spam được gửi đến Mail Servers của cá nhân hoặc tổ chức.

Bước 4: Các Email Spam được gửi từ Mail Server gửi đến mail của các cá nhân

Bước 5: sau khi các các nhân nhận được Mail Spam để nhập các thông tin cá nhân, khi đó các thông tin sẽ được gửi về Spammer’s Website.

2.2.2 Các phương pháp lọc Spam Email

Tất cả những công cụ lọc có giá trị ngày nay thường sử dụng một trong số những phương pháp hoặc kết hợp của các phương pháp sau:

2.2.2.1 ***Phương pháp lọc theo từ khóa***

2.2.2.2 Phương pháp lọc Bayesian

2.2.2.3 Phương pháp lọc SpamAssassin

2.2.2.4 Phương pháp dùng danh sách trắng/đen

2.2.2.5 Phương pháp lọc thư rác dùng chuỗi hỏi đáp

2.2.2.6 Phương pháp lọc dựa vào vị trí của các bộ lọc

2.2.2.7 Phương pháp lọc dựa trên xác nhận danh tính của người gửi

2.2.2.8 Phương pháp lọc thư rác mới dựa trên mạng Xã hội

Kết luận chương:

Chương 2 đã khái quát về các phương pháp phòng chống tấn công hệ thống Email, chi tiết phương pháp áp dụng cho từng thành phần hệ thống: mail client, mail server, đường truyền Internet. Đồng thời chương tập trung nghiên cứu phương pháp phòng chống tấn công Antispam để làm cơ sở tiền đề đưa ra giải pháp cụ thể nhằm phòng chống tấn công trong hoạt động của Ngân hàng tại Chương 3

CHƯƠNG III: TRIỂN KHAI THỬ NGHIỆM, ĐỀ XUẤT ÁP DỤNG PHƯƠNG PHÁP PHÒNG CHỐNG TẤN CÔNG ANTI SPAM EMAIL CHO HỆ THỐNG EMAIL TẠI NGÂN HÀNG HÀNG HẢI VIỆT NAM

3.1. Hiện trạng tấn công Spam Email tại ngân hàng Hàng Hải Việt Nam (MSB)

Ngân hàng MSB là ngân hàng TMCP đầu tiên ra đời (năm 1991) với sự đa dạng các sản phẩm dịch vụ tài chính ngân hàng với trên 1,8 triệu khách hàng cá nhân, gần 45.000 khách hàng doanh nghiệp và nhiều đối tác.

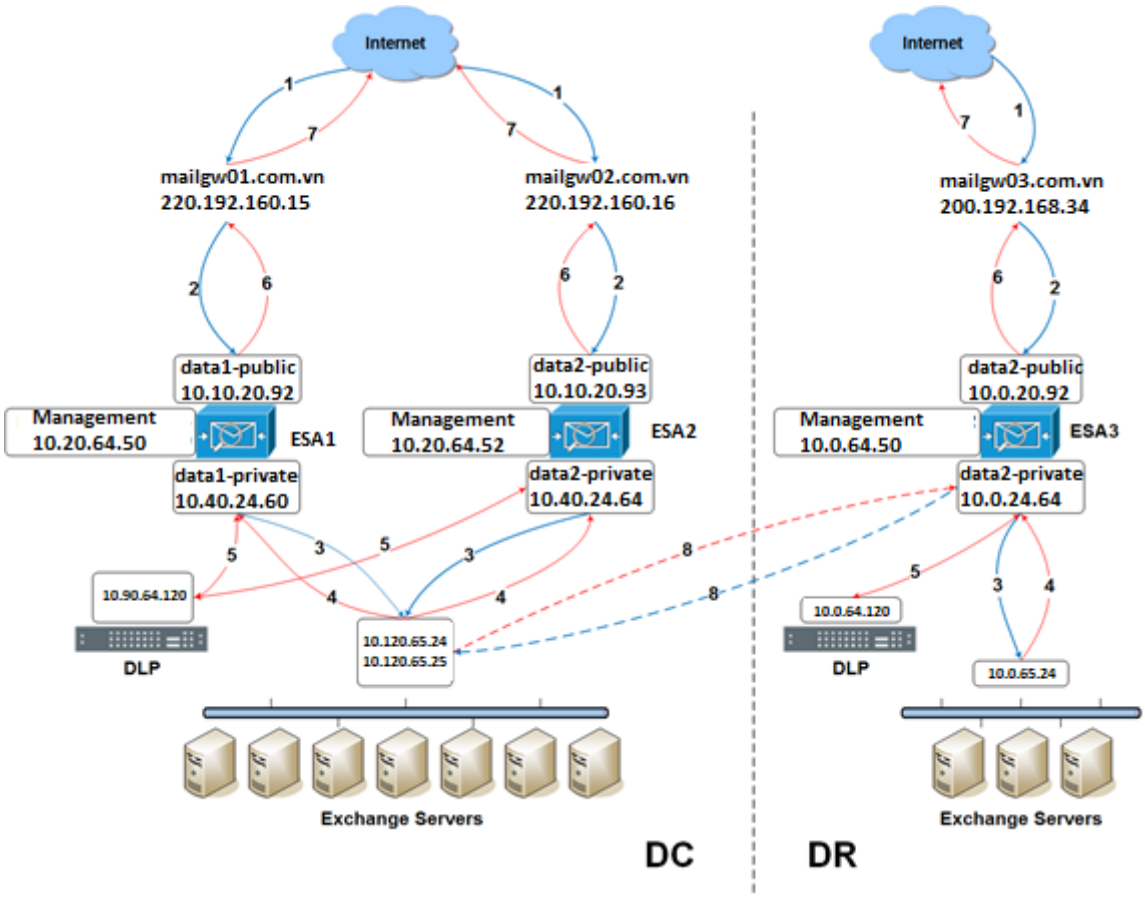
Xây dựng hệ thống phòng chống tấn công Email nhằm đáp ứng khả năng phân tích các mối đe doạ theo thời gian thực tại Email Gateway, cung cấp báo cáo nâng cao để đánh giá, điều tra các sự kiện đối với hệ thống Email, phát hiện và ngăn chặn các mối đe dọa, các tấn công để bảo vệ hệ thống Email tại Ngân hàng Hàng Hải Việt Nam (MSB).

Xây dựng phương án chống tấn công hệ thống Email đáp ứng các yêu cầu như sau:

- Hệ thống Email Security Gateway được thiết kế chạy theo mô hình 2N+1 (1 thiết bị hoạt động tại DC, 1 thiết bị hoạt động tại DR).
- Hệ thống đang đáp ứng cho số lượng: 7.000 người dùng MSB và các tài khoản dịch vụ với các tính năng lọc thư rác, lọc virus, lọc nội dung.
- Hệ thống đang tích hợp với McAfee Network Data Loss Prevention để chặn các Email không được phép gửi ra ngoài; tích hợp với hệ thống Qradar SIEM đẩy các sự kiện an ninh tập trung.
- Hiên trạng lọc Email tại MSB như sau:
  - Lượng mail lớn nhất: 320.000 Emails/ngày;
  - Lượng mail trung bình: 100.000 Emails/ngày

3.2. Phân tích luồng gửi và nhận Email tại ngân hàng Hàng Hải Việt Nam (MSB)

3.2.1 *Sơ đồ luồng dữ liệu gửi và nhận Email*



Hình 3.3: Sơ đồ luồng dữ liệu gửi và nhận Email tại ngân hàng

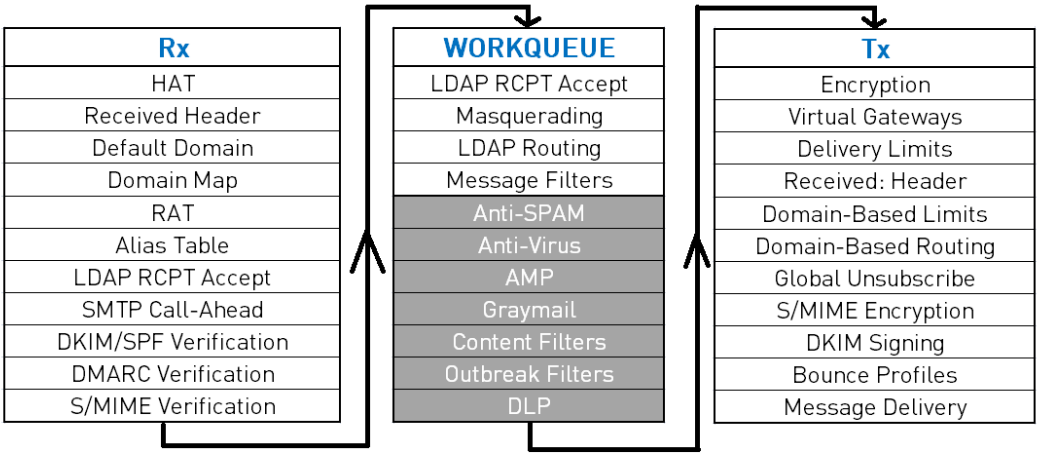
3.2.2 Cơ chế hoạt động đề xuất đối với luồng dữ liệu gửi và nhận Email

Đối với mỗi Email nhận được, ESA thực hiện xử lý theo 3 luồng (3 giai đoạn) tuần tự của một tiến trình được gọi là Email pipeline trên thiết bị, gồm có:

Receipt: thiết bị kiểm tra các thông tin ở mức SMTP connection với host ở đầu gửi mail và thực hiện giới hạn, kiểm soát theo chính sách

Work queue: sau khi trải qua giai đoạn Receipt, thiết bị tiếp tục kiểm soát tập trung vào các thông tin của nội dung bức thư.

Deliver: sau khi đã vượt qua giai đoạn Work queue, thiết bị chuẩn bị khởi tạo phiên kết nối với host ở đầu nhận mail. Tại bước này thiết bị cũng tiếp tục thực hiện các thao tác thay đổi, kiểm soát Email theo chính sách



Hình 3.4: Trình tự xử lý luồng Email

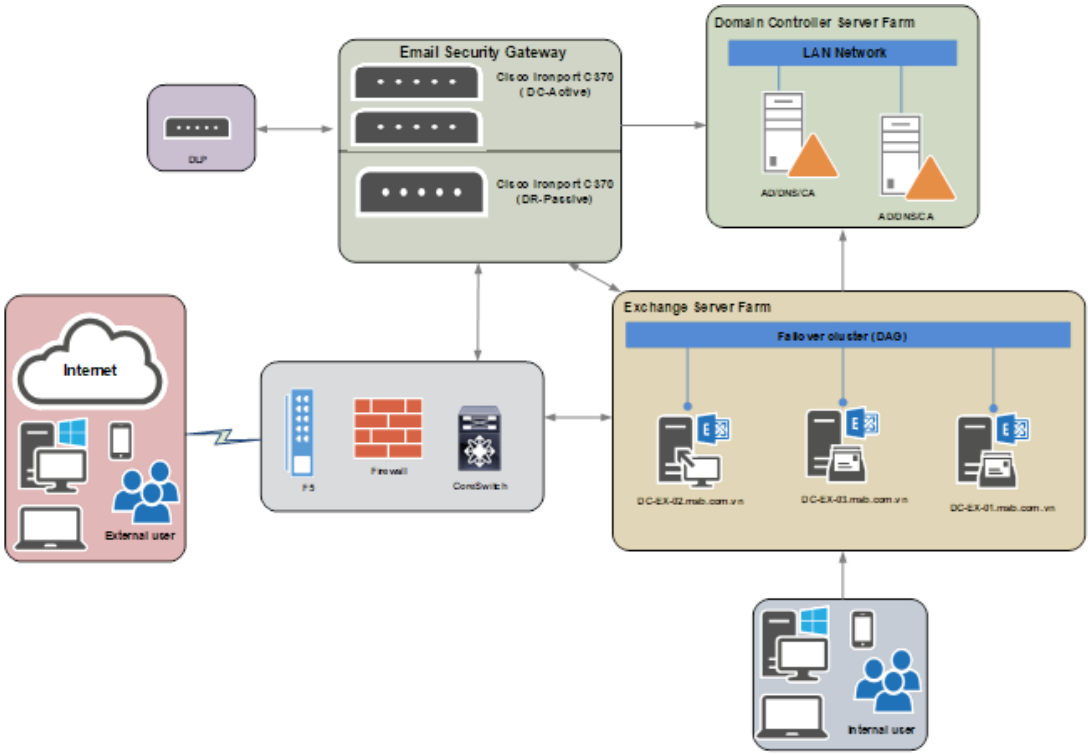
a. Trình tự xử lý của luồng Receipt

b. Trình tự xử lý Work queue

c. Trình tự xử lý của luồng Delivery

3.2.3 Đề xuất triển khai thực giải pháp

Để đáp ứng các yêu cầu trên, MSB thực hiện triển khai hệ thống Email Security Gateway với giải pháp Cisco Ironport C390 Appliance với mô hình kết nối như sau:



Hình 3.8: Mô hình triển khai giải pháp

Kết quả sau khi thực hiện

Sau khi thực hiện giải pháp, hệ thống đã ngăn chặn được thư rác, virus, các tấn công lừa đảo thực hiện qua Email, và Email chính là mục tiêu hàng đầu của các cuộc tấn công có chủ đích (APT)

Kết luận chương:

Dựa trên cơ sở lý thuyết về thư điện tử, thư rác tại Chương 1 và các phân tích về phương pháp phòng chống tấn công thư điện tử, chương 3 đã phân tích chi tiết hiện trạng, nhu cầu thực tế tại ngân hàng, phân tích luồng gửi và nhận email để từ đó lựa chọn phương án thực hiện triển khai tại Ngân hàng Hàng hải Việt Nam (MSB)

KẾT LUẬN

Luận văn đã hệ thống hóa một số vấn đề lý thuyết về thư rác, các hướng tiếp cận trong vấn đề lọc thư rác trước đây đồng thời trình bày một số khái niệm và đặc điểm về quá trình xâm nhập và lừa đảo thông qua thư rác. Đồng thời đề xuất một giải

pháp đặc trưng có thể thực hiện phát hiện, ngăn chặn và theo dõi quá trình tấn công an ninh thông tin qua Email.

- Kết quả chính đạt được của luận văn:
  - Tìm hiểu về các tấn công Email
  - Nghiên cứu và phân tích luồng dữ liệu;
  - Phân tích quá trình hoạt động từ đó ngăn chặn được các rủi ro
  - Đề xuất được giải pháp lựa chọn đặc trưng tốt nhất đảm bảo hiệu quả, hiệu suất của hệ thống
  - Tiến hành thực nghiệm và đánh giá, so sánh các kết quả.
- Hướng phát triển tiếp theo của nghiên cứu:

Mở rộng nhiều hướng tiếp cận phân tích mã độc và các phương thức tấn công mới. Thực hiện phân tích dựa trên kinh nghiệm từ đó phối hợp với các giải pháp mới để cập nhật những xu hướng tấn công mới nhất. Đảm bảo an ninh, an toàn cho hệ thống và bảo vệ thông tin của người sử dụng.