UBND TỈNH GIA LAI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

Số: 1638/STTTT-BCVT
V/v tăng cường công tác đảm bảo thông tin liên lạc, an ninh trật tự trong dịp Tết Dương lịch và Tết Nguyên đán Canh Tý 2020

Gia Lai, ngày 20 tháng 12 năm 2020

Kính gửi:
- Các sở, ban, ngành cấp tỉnh;
- Các cơ quan báo chí địa phương, Văn phòng đại diện, phóng viên thường trú trên địa bàn tỉnh;
- Ủy ban nhân dân các huyện, thị xã, thành phố;
- Trung tâm Công nghệ thông tin và Truyền thông;
- Các doanh nghiệp Bưu chính, Viễn thông trên địa bàn tỉnh.

Thực hiện ý kiến chỉ đạo của Ủy ban nhân dân tỉnh Gia Lai tại Công văn số 2789/UBND-NC ngày 06/12/2019 về việc tăng cường bảo đảm ANTT trong dịp Tết Dương lịch và Tết Nguyên đán Canh Tý 2020,

Để tăng cường công tác đảm bảo an toàn thông tin, an ninh trật tự trước, trong và sau Tết Dương lịch và Tết Nguyên đán Canh Tý 2020; phòng ngừa và có phương án đối phó khi có tình huống xảy ra, Sở Thông tin và Truyền thông (TT&TT) đề nghị các đơn vị, địa phương trên địa bàn tỉnh thực hiện một số nội dung sau:

1. Các sở, ban, ngành; UBND các huyện, thị xã, thành phố:

- Đẩy mạnh công tác tuyên truyền nâng cao nhận thức cho cán bộ, công chức, viên chức về công tác bảo đảm an toàn thông tin mạng, cảnh giác với những nguy cơ mất an toàn thông tin trong việc sử dụng máy tính từ môi trường mạng, Internet; cảnh giác với các hoạt động lừa đảo thông qua hàng loạt trang web giả mạo mạng xã hội, các tin nhắn, cơ sở cung cấp dịch vụ lớn, các chương trình khuyến mại, trúng thưởng, tặng quà tri ân để thu thập thông tin cá nhân, các tài khoản ngân hàng, thẻ tín dụng... của người sử dụng.

- Kiểm tra, bảo trì hệ thống máy tính, hệ thống mạng nội bộ tại các đơn vị, địa phương kịp thời loại bỏ việc lây nhiễm virus, mã độc ra khỏi hệ thống để nhằm hạn chế tối đa xảy ra sự cố mất an toàn, an ninh thông tin; tiến hành cập nhật phần mềm chống virus, sao lưu dữ liệu định kỳ trên thiết bị, phần mềm bảo mật mật tại các cơ quan, đơn vị.

- Tăng cường công tác quản trị, theo dõi hệ thống cổng/trang thông tin điện tử của đơn vị, địa phương; kiểm tra, thiết lập các hệ thống tường lửa và thiết bị phát hiện/phòng chống xâm nhập để bảo vệ, chống tấn công trái phép vào hệ thống mạng nội bộ; chú trọng công tác an toàn thông tin đối với các tài khoản quản trị, đăng tải thông tin trên hệ thống cổng/trang thông tin điện tử. Chủ động triển khai các giải pháp đảm bảo an toàn và an ninh thông tin trong các hoạt động ứng dụng

công nghệ thông tin tại đơn vị, địa phương mình; tổ chức phòng ngừa, đấu tranh, ngăn chặn các hành vi lợi dụng mạng thông tin, các trang thông tin điện tử cá nhân, đặc biệt là mạng xã hội để tuyên truyền, xuyên tạc đường lối, chủ trương, chính sách của Đảng và pháp luật của Nhà nước, xâm phạm đến an ninh quốc gia và trật tự an toàn xã hội.

- Hệ thống mạng máy tính tại các đơn vị, địa phương phải đảm bảo các điều kiện kỹ thuật cho công tác trao đổi, thông tin, liên lạc và chỉ đạo điều hành; không để xảy ra sự cố nào về an toàn, an ninh thông tin mạng trong dịp Tết Dương lịch và Tết Nguyên đán Canh Tý 2020.

- Có phương án phòng chống xử lý tấn công mạng, tấn công vào các ứng dụng công nghệ thông tin như hệ thống thư điện tử công vụ, hệ thống quản lý văn bản và điều hành, một cửa điện tử…;

- Các cơ quan, đơn vị có thể tham khảo các tài liệu:

+ Hướng dẫn bảo đảm an toàn thông tin cho hệ thống thư điện tử của cơ quan, tổ chức Nhà nước và Cổng/trang thông tin điện tử được công bố tại Công văn số 430/BTTTT-CATTT ngày 09/02/2015 và Công văn 2132/BTTTT-VNCERT ngày 18/7/2011 của các đơn vị thuộc Bộ TT&TT.

+ Cảnh báo và hướng dẫn phòng tránh nguy cơ bị tấn công lừa đảo thông qua các trang web giả mạo được công bố tại Công văn số 29/CATTT-TTTV ngày 18/01/2018 của Cục An toàn thông tin – Bộ TT&TT.

(Bản sao Công văn số 430/BTTTT-CATTT, Công văn 2132/BTTTT-VNCERT và Công văn số 29/CATTT-TTTV được đăng tải kèm theo Công văn này tại địa chỉ website:stttt.gialai.gov.vn/Mục văn bản/Văn bản Sở TTTT/Bưu chính – Viễn thông)

2. Các cơ quan báo chí địa phương, Văn phòng đại diện, phóng viên thường trú trên địa bàn tỉnh:

Thông tin, tuyên truyền chủ trương, chính sách của Đảng, pháp luật của Nhà nước về bảo đảm trật tự xã hội trên địa bàn tỉnh; Tăng cường thông tin, tuyên truyền âm mưu, thủ đoạn chống phá của các thế lực thù địch, bọn phản động; Chủ động tuyên truyền phổ biến, giáo dục pháp luật về an ninh, trật tự, thủ đoạn hoạt động của các loại tội phạm, cảnh báo nguy cơ cháy nổ, tai nạn giao thông, an toàn vệ sinh thực phẩm và các biện pháp phòng tránh, thoát nạn, cứu người… để cán bộ và nhân dân biết, phòng ngừa, ngăn chặn; Thông tin, tuyên truyền, nhân rộng các điển hình tiên tiến trong phòng chống tội phạm, các tệ nạn xã hội để động viên, khích lệ phong trào.

3. Trung tâm Công nghệ thông tin và Truyền thông (thuộc Sở Thông tin và Truyền thông):

Tăng cường các biện pháp nhằm đảm bảo Trung tâm tích hợp dữ liệu của tỉnh vận hành tốt, cổng thông tin điện tử, trang thông tin điện tử của các đơn vị thuộc hệ thống chính trị hoạt động ổn định, liên tục để phục vụ tốt nhiệm vụ đưa các thông tin tuyên truyền, phổ biến pháp luật. Đảm bảo an toàn, bảo mật các hệ thống thư điện tử công vụ của tỉnh, hệ thống quản lý văn bản và điều hành...

4. Công an tỉnh:

Đề nghị Công an tỉnh chủ trì, phối hợp với các cơ quan chức năng, UBND các huyện, thị xã, thành phố tăng cường công tác thanh tra, kiểm tra và có biện pháp xử lý nghiêm các tổ chức, cá nhân lợi dụng mạng lưới và các dịch vụ viễn thông, Internet để cung cấp các nội dung trái pháp luật, các nội dung phản động, xuyên tạc gây mất uy tín của Đảng, Nhà nước trước, trong và sau Tết Dương lịch và Tết Nguyên đán Canh Tý 2020. Chỉ đạo Công an các huyện, thị xã, thành phố phối hợp với phòng Văn hóa và Thông tin thực hiện tốt công tác quản lý Internet, quản lý SIM thuê bao di động trên địa bàn.

5. Các doanh nghiệp bưu chính, viễn thông trên địa bàn tỉnh:

- Tổ chức, triển khai thực hiện các phương án đảm bảo an toàn mạng lưới và an ninh thông tin, bảo đảm tuyệt đối an toàn thông tin liên lạc phục vụ các cơ quan Đảng, Nhà nước, chính quyền địa phương các cấp; Tăng cường các trạm thu phát sóng thông tin di động lưu động để đáp ứng tối đa các nhu cầu thông tin liên lạc tăng cao trong dịp Tết Dương lịch và Tết Nguyên đán Canh Tý 2020 của nhân dân (*Chú ý:* Lưu lượng thuê bao tăng cao những địa điểm tập trung đông người có thuê bao di động sử dụng tại các khu vui chơi, giải trí như: Quảng Trường Đại đoàn kết; Công viên Đồng Xanh; Công viên Diên Hồng; Khu du lịch về nguồn…).

- Phối hợp với lực lượng Công an và Quân sự tại các địa phương triển khai phương án, kế hoạch bảo vệ an toàn mạng lưới và công trình bưu chính, viễn thông.

- Phối hợp chẽ với các cơ quan Nhà nước có thẩm quyền phát hiện và ngăn chặn kịp thời những hành vi lợi dụng mạng lưới và dịch vụ bưu chính, viễn thông, Internet để gửi và phát tán những thông tin gây mất an ninh chính trị, trật tự an toàn xã hội trước, trong và sau dịp Tết Dương lịch và Tết Nguyên đán Canh Tý 2020.

- Có phương án đảm bảo các thiết bị dự phòng hoạt động tốt để ứng cứu kịp thời khi có sự cố về mạng; chỉ đạo tổ ứng cứu thông tin sẵn sàng, phối hợp chặt chẽ, hỗ trợ lẫn nhau với các doanh nghiệp Bưu chính, Viễn thông trên địa bàn; Tăng cường lực lượng tuần tra cáp quang, các trạm vi ba; phối hợp với các địa phương bảo vệ trạm thu, phát sóng thông tin di động.

- Tăng cường việc kiểm tra, khai thác các dịch vụ bưu chính; tổ chức kiểm soát chặt chẽ, ưu tiên và đảm bảo tuyệt đối an toàn việc tiếp nhận, chuyển phát các loại bưu phẩm, ấn phẩm, công điện của cơ quan Đảng, Nhà nước, lực lượng vũ trang; đề cao cảnh giác, kịp thời phát hiện, ngăn chặn các hành vi lợi dụng mạng lưới bưu chính, chuyển phát để vận chuyển, phát tán hàng cấm, hàng lậu và các ấn phẩm có nội dung kích động lôi kéo các phần tử xấu chống đối chính quyền.

- Tăng cường kiểm tra công tác bảo đảm an toàn mạng lưới và phòng chống cháy, nổ, đặc biệt tại các trung tâm chuyển mạch, các tuyến truyền dẫn, đầu mối khai thác và vận chuyển bưu chính phát hành báo chí, các điểm trực tiếp giao dịch.

- Tuyên truyền, hướng dẫn cho các chủ đại lý, khách hàng sử dụng dịch vụ bưu chính, viễn thông và Inernet nắm vững và thực hiện nghiêm các quy định của

Nhà nước về bảo đảm an toàn, an ninh thông tin. Tăng cường kiểm tra giám sát hoạt động của các đại lý dịch vụ viễn thông và Internet theo hợp đồng đã ký kết.

- Phân công trực lãnh đạo đơn vị, tăng cường trực điều hành, trực ứng cứu thông tin, xử lý kịp thời các sự cố nhằm đáp ứng tốt nhất các nhu cầu thông tin trước, trong và sau Tết Dương lịch và Tết Nguyên đán Canh Tý 2020**.**

Trường hợp đột xuất các đơn vị, địa phương và các doanh nghiệp Bưu chính, Viễn thông cần thông báo về Sở TT&TT qua các số máy:

- Giám đốc Sở: 0913.421376 (Đ/c Nguyễn Ngọc Hùng);

- Phó Giám đốc Sở: 0932.532789 (Đ/c Lê Thị Thu Hương);

- Phó Giám đốc Sở: 0904.422662 (Đ/c Đặng Quang Khanh).

Đề nghị các sở, ban, ngành; UBND các huyện, thị xã, thành phố và các đơn vị liên quan trên địa bàn tỉnh triển khai thực hiện./.

Nơi nhận:
- Như trên;
- UBND tỉnh (báo cáo);
- Lưu: VT, VP, TTra Sở, P.TTBCXB, P.CNTT, P.BCVT.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH GIA LAI

Sở Thông tin và Truyền thông
Tỉnh Gia Lai
20.12.2019 16:30:47 +07:00

Lê Thị Thu Hương

BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập - Tự do - Hạnh phúc

Số: 430/BTTTT-CATTT
V/v hướng dẫn bảo đảm ATTT cho hệ thống thư điện tử của cơ quan, tổ chức nhà nước

Hà Nội, ngày 09 tháng 02 năm 2015

Kính gửi:
- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương;
- Các tập đoàn kinh tế, tổng công ty Nhà nước.

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 20/4/2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

Căn cứ Nghị định số 72/2013/NĐ-CP ngày 15/7/2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng;

Căn cứ Thông tư số 22/2013/TT-BTTTT ngày 23/12/2013 của Bộ trưởng Bộ Thông tin và Truyền thông ban hành Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan, tổ chức nhà nước,

Bộ Thông tin và Truyền thông công bố Tài liệu hướng dẫn bảo đảm an toàn thông tin cho hệ thống thư điện tử của cơ quan, tổ chức nhà nước. Tài liệu này hướng dẫn các điều kiện cơ bản, quy trình, yêu cầu tối thiểu về cấu hình và hoạt động của máy chủ thư điện tử nhằm phòng, chống các hoạt động nguy hại đến hệ thống thư điện tử của cơ quan, tổ chức nhà nước.

Bản mềm tài liệu hướng dẫn có thể được tải về từ cổng thông tin điện tử của Bộ Thông tin và Truyền thông tại địa chỉ: http://www.mic.gov.vn.

Trong quá trình thực hiện, nếu có điều gì vướng mắc, đề nghị các cơ quan, tổ chức phản ánh về Bộ Thông tin và Truyền thông (Cục An toàn thông tin) để được hướng dẫn giải quyết./.

Nơi nhận:
- Như trên;
- Bộ trưởng và các Thứ trưởng;
- Cổng Thông tin điện tử Chính phủ;
- Đơn vị chuyên trách về CNTT của các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ (qua thư điện tử);
- Đơn vị chuyên trách về CNTT của Văn phòng Trung ương Đảng, Văn phòng Chủ tịch nước, Văn phòng Quốc hội, Tòa án nhân dân tối cao, Viện kiểm sát nhân dân tối cao, Kiểm toán Nhà nước;
- Đơn vị chuyên trách về CNTT của Cơ quan Trung ương của các đoàn thể;
- Sở TT&TT các tỉnh, thành phố trực thuộc Trung ương (qua thư điện tử);
- Cổng thông tin điện tử Bộ TT&TT;
- Lưu: VT, CATTT.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Nguyễn Minh Hồng

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

TÀI LIỆU HƯỚNG DẪN
BẢO ĐẢM AN TOÀN THÔNG TIN CHO HỆ THỐNG THƯ ĐIỆN TỬ CỦA CƠ QUAN, TỔ CHỨC NHÀ NƯỚC

*(Kèm theo Công văn số **430**/BTTTT-CATTT ngày 09 tháng 02 năm 2015 của Bộ Thông tin và Truyền thông)*

Hà Nội, 2015

MỤC LỤC

THUẬT NGỮ CHUYÊN MÔN 2
CHƯƠNG 1. PHẠM VI, ĐỐI TƯỢNG ÁP DỤNG 3
1.1. Phạm vi áp dụng 3
1.2. Đối tượng áp dụng 3
CHƯƠNG 2. MÔI TRƯỜNG HỆ THỐNG THƯ ĐIỆN TỬ 3
2.1. Phần mềm hệ điều hành 3
2.1.1. Lựa chọn hệ điều hành 3
2.1.2. Cài đặt và cấu hình hệ điều hành 4
2.1.3. Cấu hình xác thực người dùng trên hệ điều hành 5
2.1.4. Các thành phần bảo vệ khác 5
2.1.5. Kiểm thử định kỳ mức độ bảo mật của máy chủ 5
2.2. Phần mềm máy chủ thư điện tử 6
2.2.1. Cài đặt phần mềm máy chủ thư điện tử 6
2.2.2. Cấu hình phần mềm máy chủ thư điện tử 6
2.3. Hệ thống, thiết bị mạng 7
2.3.1. Vị trí đặt máy chủ thư điện tử trên mô hình mạng 7
2.3.2. Thiết bị tường lửa 7
2.3.3. Hệ thống phát hiện và phòng chống xâm nhập 9
2.3.4. Thiết bị chuyển mạch 10
CHƯƠNG 3. PHÒNG, CHỐNG LỢI DỤNG, GIẢ MẠO THƯ ĐIỆN TỬ 10
3.1. Phòng, chống mã độc và virus. 10
3.1.1. Thực hiện dò quét trên tường lửa trước máy chủ thư điện tử 10
3.1.2. Thực hiện dò quét ngay trên máy chủ thư điện tử 10
3.2. Phòng, chống thư rác và thông tin độc hại 10
3.3. Phòng, chống thư giả mạo 11
3.3.1. Đối với thư điện tử giả mạo gửi từ bên ngoài vào tổ chức 11
3.3.2. Đối với thư điện tử giả mạo gửi nội bộ trong tổ chức 11
3.3.3. Xác thực mail relay trong việc gửi/nhận thư điện tử 11
3.3.4. Phòng, chống giả mạo các thông số thư điện tử 12
3.3.5. Sử dụng chữ ký số đối với người dùng cuối 12
3.4. Phòng, chống tấn công dò quét mật khẩu 12
CHƯƠNG 4. QUẢN TRỊ MÁY CHỦ THƯ ĐIỆN TỬ 12
4.1. Lưu nhật ký 12
4.1.1. Yêu cầu chung 12
4.1.2. Các thông tin tối thiểu cần lưu lại 13
4.2. Sao lưu và phục hồi 13
4.2.1. Các hình thức sao lưu 14
4.2.2. Quy trình khôi phục khi bị sự cố 14
4.3. Kiểm thử, đánh giá máy chủ thư điện tử 15
4.3.1. Công cụ quét các nguy cơ mất an toàn 15
4.3.2. Kiểm thử bảo mật 15
4.4. Quản trị từ xa 15
PHỤ LỤC: DANH SÁCH NHIỆM VỤ BẢO ĐẢM AN TOÀN THÔNG TIN 16

THUẬT NGỮ CHUYÊN MÔN

Trong tài liệu này, những thuật ngữ chuyên môn tiếng Việt và tiếng Anh được tham chiếu như sau:

STT	TIẾNG VIỆT	TIẾNG ANH
1	Đánh giá bảo mật	Pennetration test
2	Làm cứng	Hardening
3	Tệp tin nhật ký	Log file
4	Lưu nhật ký	Logging
5	Sao lưu toàn phần	Full backup
6	Sao lưu bổ sung	Incremental backup
7	Sao lưu khi có khác biệt	Differential backup
8	Mào đầu của gói tin	Packet header
9	Bản vá	Patch hoặc Bug fix
10	Thư điện tử lừa đảo	Phishing email
11	Lỗi bảo mật	Vulnerability
12	Lưu lượng mạng	Network traffic
13	Danh sách đen	Blacklist
14	Lớp Mạng	Network layer
15	Lớp Giao vận	Transport layer
16	Lớp Ứng dụng	Application layer
17	Hệ thống phát hiện xâm nhập	IDS
18	Hệ thống ngăn ngừa xâm nhập	IPS
19	Thiết bị chuyển mạch	Network switch
20	Khu vực cách ly	DMZ
21	Cơ sở dữ liệu định danh	Alias database
22	Quản trị từ xa	Remotely administering

CHƯƠNG 1
PHẠM VI, ĐỐI TƯỢNG ÁP DỤNG

1.1. Phạm vi áp dụng

a) Tài liệu này hướng dẫn các điều kiện cơ bản, cách thức, quy trình thực hiện, hướng dẫn áp dụng các yêu cầu tối thiểu về cấu hình và hoạt động của máy chủ thư điện tử nhằm bảo đảm an toàn thông tin và phòng tránh các hoạt động nguy hại đến hệ thống thư điện tử của các cơ quan, tổ chức nhà nước.

b) Cơ quan, tổ chức chịu trách nhiệm xây dựng hệ thống thư điện tử cho các cơ quan, tổ chức nhà nước dựa trên hướng dẫn này để tăng cường bảo đảm an toàn thông tin.

1.2. Đối tượng áp dụng

a) Tài liệu này áp dụng đối với các cơ quan, tổ chức, cá nhân có liên quan đến việc thiết kế, xây dựng, quản lý, vận hành các hệ thống thư điện tử cho các cơ quan, tổ chức nhà nước.

b) Khuyến khích các doanh nghiệp, tổ chức khác áp dụng hướng dẫn này.

CHƯƠNG 2
MÔI TRƯỜNG HỆ THỐNG THƯ ĐIỆN TỬ

Yêu cầu kỹ thuật về bảo đảm an toàn thông tin cho môi trường hệ thống thư điện tử được diễn giải như sau:

2.1. Phần mềm hệ điều hành

2.1.1. Lựa chọn hệ điều hành

Trước khi thực hiện việc cài đặt môi trường cho hệ thống thư điện tử, cơ quan, tổ chức cần xem xét theo nhu cầu hoạt động của mình để lựa chọn hệ điều hành phù hợp. Việc lựa chọn hệ điều hành cho máy chủ thư điện tử cần tuân theo một số yêu cầu sau:

a) Xác định mục đích hoạt động và các dịch vụ sẽ được sử dụng trên máy chủ thư điện tử để triển khai sử dụng các dịch vụ thư điện tử như SMTP, POP, IMAP,... Tuy nhiên, trong tình hình hiện tại, các máy chủ thư điện tử được khuyến cáo sử dụng các dịch vụ dựa trên giao thức bảo mật như HTTPS, SMTPS, POPS, IMAPS với giao thức TLS. Việc sử dụng giao thức SSL có thể được áp dụng khi

các bản cập nhật của giao thức SSL đã vá các lỗi bảo mật của các phiên bản SSLv1, SSLv2, SSLv3.

b) Xác định tính chất của các người dùng để phân loại và tạo ra các nhóm người dùng thích hợp với đặc tính của hệ điều hành.

c) Hệ điều hành được chọn cần có các tính năng:

- Có khả năng từ chối các truy cập đến các thông tin quan trọng trên hệ thống.

- Có khả năng loại bỏ hoặc vô hiệu quá các dịch vụ mạng đi kèm hệ điều hành nhưng không cần thiết.

- Có khả năng ghi nhật ký các hoạt động cần thiết trên máy chủ để phát hiện các xâm nhập và hành động cố gắng xâm nhập.

- Được hỗ trợ thường xuyên từ đơn vị phát triển, có các hoạt động cập nhật các bản vá và nâng cấp phần mềm định kỳ.

d) Tổ chức cần xem xét đến khả năng đào tạo nhân lực trong việc quản trị và điều hành hệ điều hành sắp được chọn lựa.

2.1.2. Cài đặt và cấu hình hệ điều hành

Việc cài đặt và cấu hình hệ điều hành sử dụng cho máy chủ thư điện tử cần đáp ứng các yêu cầu:

a) Vá các lỗi và nâng cấp hệ điều hành: Các bản cài của hệ điều hành không phải bao giờ cũng là phiên bản mới nhất. Do đó, sau khi tiến hành cài đặt, quản trị viên cần cập nhật các bản vá bảo mật cũng như nâng cấp hệ điều hành. Việc nâng cấp này đồng thời cũng được áp dụng cho các phần mềm khác được cài đặt trên máy chủ. Lưu ý rằng cần cân nhắc sử dụng các phiên bản ổn định (stable) hơn là các phiên bản vẫn đang trong các giai đoạn phát triển và thử nghiệm.

b) Loại bỏ hoặc vô hiệu hoá các dịch vụ và phần mềm không cần thiết: Máy chủ thư điện tử nên được đặt trên một máy chủ riêng và hoạt động cho chỉ một mục đích. Vì vậy, các dịch vụ và các phần mềm khác cần được loại bỏ hoặc vô hiệu hoá. Chỉ các phần mềm cần thiết cho sự hoạt động của máy chủ thư điện tử mới được kích hoạt và sử dụng trên máy chủ thư điện tử. Các dịch vụ thông thường có thể cần được vô hiệu hoá gồm:

- Dịch vụ NETBIOS

- Dịch vụ chia sẻ tệp tin và máy in

- Dịch vụ NFS

- Dịch vụ Telnet

- Dịch vụ FTP

- Dịch vụ Hệ thống thông tin mạng (NIS - Network Information System)

- Các bộ cài ngôn ngữ và thư viện không cần thiết

- Các công cụ phát triển và gỡ rối (debug) có sẵn trên hệ thống

- Các công cụ quản lý mạng không cần thiết

Cần lưu ý rằng việc loại bỏ được khuyến cáo ưu tiên hơn việc vô hiệu hoá vì thông qua việc tấn công, kẻ tấn công có thể thay đổi cấu hình và kích hoạt lại các dịch vụ và phần mềm không cần thiết này dẫn đến việc máy chủ phải đối mặt với rủi ro trong tương lai.

c) Các tài khoản trên hệ thống cần bị vô hiệu hoá trong một thời gian nhất định khi có nhiều lượt xác thực không thành công xảy ra.

2.1.3. Cấu hình xác thực người dùng trên hệ điều hành

Số lượng các tài khoản trên máy chủ cần được giới hạn và chỉ được cấp cho những cán bộ cần thiết phục vụ cho công tác quản trị, cụ thể:

a) Loại bỏ hoặc vô hiệu hoá các tài khoản và nhóm mặc định không cần thiết trên hệ thống.

b) Vô hiệu hoá các tài khoản không hoạt động và không cần thiết.

c) Tạo, cấp phát tài khoản cần dựa trên kế hoạch triển khai.

d) Phân cấp và phân quyền hợp lý các tài khoản người dùng vào các nhóm phù hợp với tính chất công việc của từng người.

2.1.4. Các thành phần bảo vệ khác

Cơ quan, tổ chức có thể xem xét việc sử dụng thêm các thành phần và công nghệ để hỗ trợ cho tính bảo mật của máy chủ thư điện tử như sử dụng thẻ thông minh (smart card), xác thực sinh trắc học (biometric) hoặc mật khẩu sử dụng một lần (one-time password).

2.1.5. Kiểm thử định kỳ mức độ bảo mật của máy chủ

Cơ quan, tổ chức cần có kế hoạch kiểm tra định kỳ độ bảo mật và an toàn của hệ điều hành để chắc chắn rằng các giải pháp bảo mật đang áp dụng vẫn phù

hợp. Các phương thức kiểm tra có thể áp dụng như dò quét lỗ hổng hoặc tiến hành đánh giá bảo mật (pennetration test).

2.2. Phần mềm máy chủ thư điện tử

2.2.1. Cài đặt phần mềm máy chủ thư điện tử

Sau khi chắc chắn rằng hệ điều hành đã được cài đặt đúng theo các quy trình bảo mật, người quản trị cần thực hiện cài đặt phần mềm máy chủ thư điện tử theo các nguyên tắc sau:

a) Cần cài đặt máy chủ thư điện tử trên máy chủ ảo hoặc vật lý riêng, không sử dụng chung với các dịch vụ khác như web, cơ sở dữ liệu,...

b) Tuỳ thuộc vào nhu cầu sử dụng của từng đơn vị để xác định ứng dụng thư điện tử nào sẽ được cài.

c) Sau khi cài đặt cần thực hiện ngay việc cập nhật các bản vá bảo mật và nâng cấp từ nhà cung cấp.

d) Sử dụng một phân vùng hoặc ổ cứng vật lý riêng để lưu trữ thư điện tử. Cơ quan, tổ chức có thể xem xét triển khai hệ thống lưu trữ như SAN (Storage Aera Networking) phù hợp với thực tế từng đơn vị.

đ) Tháo gỡ hoặc vô hiệu hoá các dịch vụ đi kèm của máy chủ thư điện tử không cần thiết như các dịch vụ truyền tải tệp tin (FTP), quản trị từ xa,...

e) Xoá bỏ các thành phần kèm theo không cần thiết từ đơn vị phát triển như tài liệu hướng dẫn, bản dùng thử các ứng dụng khác ...

g) Cấu hình các thông tin của máy chủ trên tất cả giao thức như SMTP, POP, IMAP hay các dịch vụ khác đảm bảo rằng máy chủ không đưa lên các thông tin về tên ứng dụng thư điện tử hay hệ điều hành và phiên bản đang sử dụng.

h) Vô hiệu hoá các lệnh nguy hiểm và không cần thiết như VRFY hay EXPN

2.2.2. Cấu hình phần mềm máy chủ thư điện tử

Việc vận hành máy chủ thư điện tử cần tuân thủ một số quy tắc sau nhằm giảm thiểu các rủi ro từ các tấn công về sau:

a) Giới hạn quyền truy cập của phần mềm máy chủ thư điện tử đến các tài nguyên khác hệ thống, đặc biệt là các tài nguyên như:

- Các tệp tin cấu hình của hệ thống.

- Các tệp tin chứa thông tin đăng nhập, phân quyền cũng như khoá mật mã.

- Tệp tin nhật ký của máy chủ.

b) Cần chắc chắn rằng các tệp tin nhật ký của máy chủ thư điện tử được lưu tại phân vùng với dung lượng phù hợp cho hoạt động lâu dài.

c) Hạn chế kích thước của tệp tin đính kèm phù hợp với dung lượng ổ cứng đang sử dụng của máy chủ thư điện tử.

d) Hạn chế các loại tệp tin có thể được đính kèm theo thư điện tử để đảm bảo các tệp thực thi và tệp có nguy cơ mất an toàn cao không được gửi đi trên hệ thống.

đ) Giới hạn tốc độ gửi thư điện tử của từng tài khoản phù hợp với nhu cầu của tổ chức. Ví dụ: có thể giới hạn cho phép gửi không quá 5 thư điện tử trong vòng 1 phút và giới hạn số lượng người được gửi cùng lúc thông qua chức năng CC, BCC.

2.3. Hệ thống, thiết bị mạng

2.3.1. Vị trí đặt máy chủ thư điện tử trên mô hình mạng

a) Máy chủ thư điện tử thường được đặt trong mạng nội bộ và được bảo vệ bởi mail gateway hoặc tường lửa để đảm bảo an toàn và tiện dụng cho người dùng nội bộ.

b) Mail gateway đóng vai trò trung gian, giúp máy chủ thư điện tử giao tiếp với Internet, mail gateway chỉ cài đặt những chức năng cơ bản, thiết yếu nhất nên dễ dàng để làm cứng và nâng cao bảo mật hơn máy chủ thư điện tử. Tất cả thư điện tử và liên lạc phải đi qua mail gateway trước khi được chuyển tới máy chủ mail để xử lý. Mail gateway sẽ làm cho các cuộc tấn công vào máy chủ thư điện tử khó khả thi hơn, sử dụng mail gateway trong khu vực cách ly (DMZ) sẽ tăng mức độ an toàn hơn cho máy chủ thư điện tử.

2.3.2. Thiết bị tường lửa

a) Một tường lửa để bảo vệ hệ thống thư điện tử cần được cấu hình để chặn tất cả truy cập tới máy chủ thư điện tử từ Internet trừ các cổng cần thiết như cổng TCP 443 (HTTPS), 25 (SMTP), 110 (POP), 143 (IMAP), 465 (SMTPS), 389 (LDAP), 636 (Secure LDAP), 993 (Secure IMAP) và 995 (Secure POP). Tường lửa là vị trí phòng thủ đầu tiên trong mạng nội bộ cho máy chủ thư điện tử. Tuy nhiên, để đảm bảo an toàn, các tổ chức cần triển khai nhiều lớp bảo vệ khác nhau cho hệ thống thư điện tử, đảm bảo hệ thống thư điện tử không bị phụ thuộc vào một bộ định tuyến, tường lửa hay một cấu phần nào đó của hệ thống mạng để ngăn chặn tấn công. Mặt khác, tường lửa cần được cấu hình để chặn các dịch vụ không được mã hoá trên các cổng 25,110,143,398 ngay khi các dịch vụ có hỗ trợ mã hoá đã được triển khai trên các cổng mới. Ngoài ra, LDAP là dịch vụ không cần thiết

phải công khai trên Internet, việc sử dụng LDAP hay LDAPS cần giới hạn các địa chỉ IP có thể truy cập.

b) Một tường lửa tối thiểu cần có khả năng ngăn chặn ở các lớp Mạng và lớp Giao vận (trong mô hình OSI), với mức ngăn chặn này, tường lửa có thể lọc theo các thông tin sau: Địa chỉ IP nguồn; Địa chỉ IP đích; Kiểu dữ liệu truyền tải; cổng TCP/UDP và trạng thái, không thể ngăn chặn các cuộc tấn công ở lớp ứng dụng (chặn lọc theo nội dung). Khuyến khích sử dụng tường lửa có khả năng lọc ở lớp ứng dụng.

c) Để tăng cường bảo mật cho hệ thống thư điện tử bằng tường lửa, phần mềm tường lửa cần đảm bảo được cập nhật các bản vá mới nhất, có khả năng và được cấu hình để hỗ trợ các nội dung sau:

- Kiểm soát tất cả lưu lượng mạng giữa máy chủ thư điện tử và Internet

- Chặn tất cả các lưu lượng mạng đến máy chủ thư điện tử trừ các cổng cần thiết nhất

- Chặn các địa chỉ IP hoặc dải IP mà hệ thống IDS/IPS báo về trong thời gian vận hành

- Chặn tất cả các IP hoặc dải IP tại danh sách đen mà các tổ chức uy tín đã thống kê và công bố định kỳ

- Cảnh báo cho quản trị mạng hoặc quản trị hệ thống thư điện tử về các hành động đáng ngờ

- Có khả năng chặn lọc theo nội dung

- Có khả năng dò quét mã độc

- Có khả năng phòng chống các cuộc tấn công từ chối dịch vụ

- Có khả năng ngăn chặn các hành động bất thường được phát hiện trong quá trình hoạt động của hệ thống

- Lưu vết các sự kiện quan trọng với các thông tin chi tiết: thời gian, địa chỉ IP nguồn và đích, giao thức, tên sự kiện,...

d) Ngoài hệ thống tường lửa chung bảo vệ trong mạng, tường lửa tích hợp trong hệ điều hành vẫn cần được kích hoạt và duy trì. Các tường lửa này cần đặt các luật chỉ cho phép những giao dịch vào/ra cần thiết, phục vụ cho dịch vụ thư điện tử và các dịch vụ hỗ trợ liên quan.

2.3.3. Hệ thống phát hiện và phòng chống xâm nhập

a) Hệ thống phát hiện xâm nhập (IDS) là một hệ thống nhằm phát hiện các hành động tấn công vào một mạng. Mục đích của IDS là phát hiện các hành động phá hoại đối với vấn đề bảo mật hệ thống, hoặc những hành động trong tiến trình tấn công như tìm hiểu, quét các cổng. Một tính năng chính của hệ thống này là cung cấp thông tin nhận biết về những hành động không bình thường và đưa ra các báo cảnh báo cho quản trị viên mạng để khóa các kết nối đang tấn công này.

b) Hệ thống ngăn ngừa xâm nhập (IPS) là hệ thống theo dõi, ngăn ngừa kịp thời các hoạt động xâm nhập không mong muốn. Chức năng chính của IPS là xác định các hoạt động nguy hại, lưu giữ các thông tin này. Sau đó kết hợp với tường lửa để dừng ngay các hoạt động này, và cuối cùng đưa ra các báo cáo chi tiết về các hoạt động xâm nhập trái phép trên.

c) Hệ thống IPS được xem là trường hợp mở rộng của hệ thống IDS, cách thức hoạt động cũng như đặc điểm của hai hệ thống này tương tự nhau. Điểm khác nhau duy nhất là hệ thống IPS ngoài khả năng theo dõi, giám sát thì còn có chức năng ngăn chặn kịp thời các hoạt động nguy hại đối với hệ thống. Hệ thống IPS sử dụng tập luật tương tự như hệ thống IDS.

d) Các hệ thống IDS/IPS cần được cấu hình để tối thiểu đáp ứng các khả năng sau:

- Theo dõi toàn bộ lưu lượng mạng đi và đến máy chủ thư điện tử

- Theo dõi sự thay đổi của các tập tin quan trọng trên máy chủ thư điện tử

- Theo dõi tài nguyên hệ thống trên máy chủ thư điện tử

- Chặn (kết hợp thông qua tường lửa) các địa chỉ IP hoặc dải IP được xác định đang tấn công vào hệ thống mạng

- Thông báo tới các bộ phận liên quan (quản trị mạng, quản trị hệ thống, quản trị máy chủ thư điện tử,...) về các hành động khả nghi

- Phát hiện các hành động dò quét và dấu hiệu nghi ngờ tấn công

- Lưu sự kiện liên quan với đầy đủ thông tin

- Lưu mào đầu của các gói tin liên quan tới các hành động khả nghi để phục vụ phân tích nếu xảy ra sự cố

- Cập nhật dấu hiệu nhận biết định kỳ (hàng ngày tới hàng tuần)

2.3.4. Thiết bị chuyển mạch

Thiết bị chuyển mạch cần được cấu hình ở chế độ bảo đảm an toàn thông tin cao nhất để chống lại các hình thức tấn công vào ARP (Address Resolution Protocol) và cấu hình để có thể gửi toàn bộ lưu lượng mạng về thiết bị IPS (nếu có) để phân tích và phòng chống các cuộc tấn công.

CHƯƠNG 3
PHÒNG, CHỐNG LỢI DỤNG, GIẢ MẠO THƯ ĐIỆN TỬ

3.1. Phòng, chống mã độc và virus.

Thư điện tử là một trong những phương tiện phổ biến để phát tán mã độc và virus trong thời gian gần đây. Các thư điện tử nguy hại cho người dùng cần được đánh dấu và thông báo rõ ràng đến người dùng thông qua tiêu đề, phân loại thư điện tử hoặc các phương thức khác. Do đó, máy chủ thư điện tử cần được triển khai các phương án phát hiện, phòng tránh và cảnh báo virus/mã độc gửi đến người dùng như:

3.1.1. Thực hiện dò quét trên tường lửa trước máy chủ thư điện tử

Việc dò quét virus trên tường lửa là cách phổ biến để phát hiện mã độc trước khi nó vào hệ thống. Đồng thời, tường lửa cũng có khả năng kiểm tra cả thư điện tử gửi đến và gửi đi từ máy chủ. Tuy nhiên, việc triển khai tường lửa có khả năng này cần phù hợp với tình hình và chi phí thực tế của đơn vị. Ngoài ra, các cơ quan tổ chức có thể xem xét thực hiện việc dò quét trên thiết bị mail gateway nếu có đảm bảo phù hợp năng lực quản trị và thực tế của từng đơn vị.

3.1.2. Thực hiện dò quét ngay trên máy chủ thư điện tử

Đây là lựa chọn phù hợp và có khả năng phát hiện việc mã độc được gửi trong nội bộ đơn vị. Việc dò quét mã độc trên máy chủ thư điện tử đồng thời cũng có khả năng dò quét trên cả các thư điện tử gửi đi và gửi đến máy chủ. Hầu hết các phần mềm máy chủ thư điện tử đều được phát triển sẵn công cụ hỗ trợ dò quét virus kèm theo. Vì vậy, quản trị viên có thể kích hoạt chức năng này và tiến hành cập nhật cơ sở dữ liệu cho việc phát hiện virus/mã độc.

3.2. Phòng, chống thư rác và thông tin độc hại

Hệ thống thư điện tử cần có khả năng phòng tránh được các nguy cơ về thư rác và các thư điện tử có nội dung độc hại cũng như thư điện tử lừa đảo. Do đó, các máy chủ thư điện tử cần được cài đặt và kích hoạt chức năng chặn lọc theo nội

dung, theo địa chỉ gửi và các thông số khác của thư điện tử. Ngoài ra, máy chủ thư điện tử cần cung cấp khả năng cập nhật các thông tin cho bộ lọc định kỳ và đột xuất tuỳ theo tình hình thực tế của đơn vị. Đối với các trường hợp phát hiện thư điện tử chứa mã độc hay giả mạo, các cơ quan, tổ chức có thể gửi mẫu thư giả mạo, thư chứa mã độc về Trung tâm VNCERT để được hỗ trợ ngăn chặn. Thông tin tiếp nhận được phổ biến tại website của Trung tâm VNCERT (http://vncert.vn) hoặc qua địa chỉ email antoanthudientu@report.vncert.vn.

3.3. Phòng, chống thư giả mạo

Máy chủ thư điện tử cần có cơ chế phát hiện và chặn các thư điện tử giả mạo (là các thư điện tử giả mạo địa chỉ gửi đi để đánh lừa người nhận) gây hại cho người dùng. Các thư điện tử giả mạo cần được phân loại và thông báo đến người dùng tương tự như đối với thư điện tử chứa virus và mã độc. Thư điện tử giả mạo có thể được gửi từ hai nguồn: gửi từ ngoài vào tổ chức và từ trong tổ chức đến người nhận nội bộ. Các biện pháp phát hiện và phòng chống bao gồm:

3.3.1. Đối với thư điện tử giả mạo gửi từ bên ngoài vào tổ chức

a) Sử dụng DKIM (DomainKeys Identified Mail): DKIM là phương thức sử dụng mã khoá công khai trên thư điện tử dựa trên thông tin về tên miền giúp người nhận xác định được rằng một thư điện tử được gửi đi từ đúng tên miền trên địa chỉ MAIL FROM. Hầu hết các phần mềm máy chủ thư điện tử hiện tại đều hỗ trợ việc xác thực sử dụng DKIM để phát hiện giả mạo là các thư điện tử không mang thông tin xác thực DKIM hợp lệ khi gửi đến tổ chức.

b) Sử dụng SPF (Sender Policy Framework): SPF cho phép chỉ định những địa chỉ IP được phép gửi thư điện tử từ một tên miền xác định. Do đó, máy chủ thư điện tử có thể dựa trên địa chỉ IP của thư điện tử để phát hiện việc giả mạo và thực hiện chặn lọc.

3.3.2. Đối với thư điện tử giả mạo gửi nội bộ trong tổ chức

Để phòng, chống thư điện tử giả mạo gửi từ tài khoản thư điện tử nội bộ đến một tài khoản thư điện tử khác cùng tổ chức, máy chủ thư điện tử cần được cấu hình bắt buộc người dùng thực hiện xác thực trước khi gửi thư điện tử bằng giao thức SMTP hay SMTPS.

3.3.3. Xác thực mail relay trong việc gửi/nhận thư điện tử

Người quản trị cần cấu hình để yêu cầu người dùng thực hiện xác thực trước khi gửi thư điện tử relay. Lưu ý rằng việc xác thực này bao gồm cả xác thực qua các lệnh của máy chủ thư điện tử như SMTP AUTH. Đây là một cấu hình thông

thường không được đặt sẵn trên các máy chủ thư điện tử nên người quản trị cần lưu ý để tránh bỏ xót dẫn đến việc máy chủ bị lợi dụng về sau.

3.3.4. Phòng, chống giả mạo các thông số thư điện tử

Người quản trị cần chắc chắn rằng người dùng không có khả năng giả mạo các thông số quan trọng của thư điện tử, đặc biệt là các trường MAIL FROM, RETURN TO. Việc ngăn chặn này cần được thực hiện ngay cả đối với các người dùng đã xác thực trên hệ thống.

3.3.5. Sử dụng chữ ký số đối với người dùng cuối

Cơ quan, tổ chức có thể nghiên cứu và triển khai việc cấp phát chữ ký số tới từng người sử dụng để phòng, chống thư giả mạo. Việc triển khai cần phù hợp với tình hình thực tế của từng đơn vị.

3.4. Phòng, chống tấn công dò quét mật khẩu

Các mật khẩu sử dụng trên hệ thống cần đảm bảo các yêu cầu sau:

a) Độ dài: các mật khẩu phải có độ dài ít nhất là 8 ký tự

b) Độ phức tạp: các mật khẩu phải chứa cả ký tự in hoa và ký tự in thường và ít nhất có một ký tự đặc biệt và chữ số

c) Thời gian hiệu lực: các mật khẩu phải được thay định kỳ 120 ngày một lần, với các tài khoản cấp cao cần thay đổi mật khẩu cứ 30 ngày một lần.

d) Dùng lại mật khẩu: mật khẩu thay mới không được trùng với mật khẩu cũ.

đ) Quản lý: người quản trị hệ thống thư điện tử được phép đổi hay khởi tạo lại mật khẩu phải được xác thực và có quy trình quản lý cho việc yêu cầu đổi hay khởi tạo lại mật khẩu.

CHƯƠNG 4
QUẢN TRỊ MÁY CHỦ THƯ ĐIỆN TỬ

4.1. Lưu nhật ký

Lưu nhật ký là chức năng đặc biệt quan trọng trong quản lý, vận hành hệ thống thư điện tử. Việc lựa chọn các thông tin tối thiểu để lưu trữ cần phù hợp cho việc dò tìm lỗi, cảnh báo kịp thời tới người quản trị và phục vụ công tác điều tra, phục hồi khi có sự cố xảy ra.

4.1.1. Yêu cầu chung

Cần đảm bảo đủ không gian lưu trữ để sao lưu nhật ký; Các bản lưu nhật ký cần được sao lưu định kỳ phục vụ công tác phân tích sau này. Khuyến khích sao

lưu các bản nhật ký trên hệ thống tách rời với máy chủ thư điện tử, sao lưu nhật ký tập trung. Thời gian lưu nhật ký cần phù hợp với năng lực lưu trữ của hệ thống, nhưng ít nhất cần lưu trữ nhật ký trong 3-6 tháng để phục vụ công tác điều tra và phân tích khi xảy ra sự cố.

4.1.2. Các thông tin tối thiểu cần lưu lại

a) Liên quan tới mạng nội bộ:

- Các lỗi về thiết lập cấp phát địa chỉ IP
- Các vấn đề liên quan tới cấu hình của hệ thống phân giải (ví dụ: DNS, NIS)
- Lỗi cấu hình máy chủ thư điện tử
- Thông tin tài nguyên hệ thống máy chủ (dung lượng lưu trữ, bộ nhớ, CPU)
- Cơ sở dữ liệu các định danh

b) Liên quan tới kết nối:

- Thông tin về đăng nhập sai (cả đăng nhập thành công nếu còn dung lượng lưu trữ)
- Sự cố về bảo mật
- Sự cố về mạng
- Lỗi giao thức kết nối
- Kết nối quá thời gian cho phép
- Kết nối bị từ chối
- Thông tin về lệnh VRFY và EXPN

c) Liên quan tới thư điện tử:

- Các thư điện tử gửi theo sự cho phép của người dùng (Send on behalf of/Send as)
- Địa chỉ không tồn tại
- Thống kê về số lượng thư điện tử
- Các thư điện tử lỗi bị trả về
- Các thư điện tử bị trì hoãn

4.2. Sao lưu và phục hồi

Sao lưu là một trong những chức năng và nhiệm vụ quan trọng của người quản trị hệ thống thư điện tử để bảo đảm tính nguyên vẹn của dữ liệu trên máy chủ

thư điện tử. Người quản trị hệ thống thư điện tử cần có kế hoạch và thực hiện công tác sao lưu thường xuyên và trước các đợt nâng cấp, chỉnh sửa hệ thống.

4.2.1. Các hình thức sao lưu

Có 03 hình thức sao lưu, bao gồm: sao lưu toàn phần, sao lưu bổ sung và sao lưu khi có khác biệt. Sao lưu toàn phần bao gồm hệ điều hành, ứng dụng và dữ liệu chứa trong máy chủ thư điện tử. Sao lưu toàn phần cho phép dễ dàng phục hồi toàn bộ hệ thống về trạng thái tại thời điểm sao lưu tuy nhiên việc sao lưu này đòi hỏi thời gian và dung lượng sao lưu lớn. Sao lưu bổ sung giảm các ảnh hưởng này bằng cách chỉ sao lưu phần dữ liệu có thay đổi so với trước đó (có thể từ bản sao lưu toàn phần hoặc bản sao lưu bổ sung trước đó). Sao lưu khi có sự khác biệt gần giống với sao lưu bổ sung, nó sẽ sao lưu toàn bộ dữ liệu có sự thay đổi kể từ bản sao lưu toàn phần gần nhất. Phương án này sẽ tăng dung lượng sao lưu khi thời gian sao lưu khi có sự khác biệt cách xa với thời điểm sao lưu toàn phần.

4.2.2. Quy trình khôi phục khi bị sự cố

Khôi phục máy chủ thư điện tử sau khi bị mất an toàn cần đảm bảo tuân thủ theo quy trình do tổ chức xây dựng, có thể tham khảo các bước như sau:

a) Bước 1: Báo cáo sự cố tới bộ phận chức năng của tổ chức chịu trách nhiệm về xử lý sự cố máy tính

b) Bước 2: Cách ly máy chủ bị sự cố để không bị lây lan hoặc bị đánh cắp thông tin

c) Bước 3: Kiểm tra các máy chủ khác để đảm bảo không bị tương tự

d) Bước 4: Phân tích nhật ký, các thông tin liên quan để tìm ra nguyên nhân và thủ phạm tấn công

đ) Bước 5: Khôi phục hệ thống từ bản sao lưu: Cần đảm bảo máy chủ được cài phiên bản hệ điều hành "sạch" trước khi khôi phục lại từ bản sao lưu; tắt các dịch vụ không cần thiết; Cập nhật các bản vá mới nhất; Thay đổi toàn bộ mật khẩu; Cấu hình lại các yếu tố bảo mật của hệ thống mạng để bổ sung thêm lớp bảo vệ và cảnh báo.

e) Bước 6: Kiểm tra máy chủ để đảm bảo an toàn

g) Bước 7: Kết nối máy chủ vào mạng

h) Bước 8: Theo dõi hệ thống và mạng về các dấu hiệu kẻ tấn công cố gắng truy nhập vào hệ thống hoặc mạng

i) Bước 9: Viết báo cáo toàn bộ sự cố và quá trình khôi phục để rút kinh nghiệm

4.3. Kiểm thử, đánh giá máy chủ thư điện tử

Kiểm thử an toàn thông tin cho hệ thống máy chủ thư điện tử cần được thực hiện định kỳ để phát hiện những nguy cơ tiềm ẩn mất an toàn thông tin. Có một số kỹ thuật để kiểm thử các máy chủ thư điện tử nhưng phổ biến nhất là:

4.3.1. Công cụ quét các nguy cơ mất an toàn

Sử dụng phần mềm tự động để nhận biết các nguy cơ tiềm ẩn hoặc cấu hình sau của máy chủ thư điện tử. Công cụ này sẽ sử dụng cơ sở dữ liệu lớn các nguy cơ mất an toàn để đánh giá hệ điều hành và các ứng dụng trên máy chủ thư điện tử. Thông thường đây là những lỗi phổ biến, những lỗ hổng mới phải chờ cập nhật từ các nhà sản xuất, do vậy đây không phải là một phương pháp tuyệt đối để phát hiện các nguy cơ mất an toàn.

4.3.2. Kiểm thử bảo mật

Đây là một phương pháp kiểm thử bằng cách dùng các công cụ, kỹ thuật phổ biến, kẻ tấn công hay sử dụng để kiểm tra máy chủ thư điện tử. Khuyến khích các cơ quan, tổ chức thực hiện phương pháp này, tuy nhiên cần đảm bảo các biện pháp sao lưu dự phòng trước khi tiến hành và cần được tiến hành bởi cá nhân, tổ chức chuyên nghiệp để tránh sai sót không đáng có.

4.4. Quản trị từ xa

Để bảo đảm an toàn cho hệ thống thư điện tử, khuyến cáo các cơ quan, tổ chức vô hiệu chức năng quản trị từ xa. Trong trường hợp thực sự cần thiết, cần kích hoạt chức năng này để quản lý hệ thống thư điện tử thì cần đảm bảo các yếu tố sau:

- Sử dụng các biện pháp kỹ thuật đủ mạnh khi xác thực truy cập (ví dụ: mã khóa công khai, đăng nhập 2 bước, mật khẩu sử dụng một lần,...)
- Giới hạn truy cập theo địa chỉ IP
- Sử dụng giao thức truyền tải mã hóa (SSL/TLS) cho cả mật khẩu và dữ liệu
- Giới hạn quyền quản lý đối với tài khoản quản trị từ xa
- Không cho phép quản lý từ xa thông qua Internet, trừ khi đã có đầy đủ các biện pháp đảm bảo an toàn như thiết lập VPN
- Khi kích hoạt chức năng quản trị từ xa, cần thay đổi hết toàn bộ mật khẩu mặc định (nếu có)
- Không thiết lập chia sẻ file/thư mục giữa máy chủ thư điện tử và mạng nội bộ và ngược lại.

PHỤ LỤC:

DANH SÁCH NHIỆM VỤ BẢO ĐẢM AN TOÀN THÔNG TIN CHO HỆ THỐNG THƯ ĐIỆN TỬ

A. Mức độ 1 - Danh mục các nhiệm vụ bảo đảm an toàn thông tin tối thiểu

STT	Nội dung cần thực hiện	Tham chiếu
1	Triển khai các giao thức bảo mật HTTPS, SMTPS, POP3S, IMAPS thay thế các dịch vụ HTTP, SMTP, POP3, IMAP	2.1.1.a
2	Nâng cấp và cập nhật các bản vá bảo mật mới nhất cho hệ thống. Cần thử nghiệm việc nâng cấp trên hệ thống dự phòng trước để tránh xung đột sau khi nâng cấp	2.1.2.a
3	Cấu hình từ chối truy cập vào tài khoản mail và các tài khoản hệ thống khi vượt quá 5 lần xác thực thất bại	2.1.2.c
4	Sửa chữa các hiển thị thông tin trên các dịch vụ đang hoạt động	2.2.1.g
5	Chặn các cổng dịch vụ không cần thiết trên máy chủ thư điện tử	2.3.2.a
6	Triển khai DKIM hoặc SPF	3.3.1
7	Kích hoạt yêu cầu xác thực SMTP	3.3.2
8	Chỉ cho phép mail relay cho các tài khoản đã xác thực	3.3.3

B. Mức độ 2 - Danh mục các nhiệm vụ bảo đảm an toàn thông tin nâng cao

Các nhiệm vụ dưới đây cần được xem xét thực hiện phù hợp với tình hình thực tế tại từng đơn vị.

STT	Nội dung cần thực hiện	Tham chiếu
Phần mềm hệ điều hành		
1	Loại bỏ hoặc vô hiệu hoá các tài khoản và nhóm mặc định không hoạt động trên hệ điều hành và ứng dụng máy chủ thư điện tử	2.1.3
2	Loại bỏ hoặc vô hiệu hoá các dịch vụ không cần thiết đi kèm hệ điều hành	2.1.2.b
3	Cấu hình máy chủ thư điện tử hoạt động với tài khoản hệ	2.1.3.d

	thống được phân quyền phù hợp. Không sử dụng tài khoản root hay administrator cho các tiến trình lắng nghe kết nối và ứng dụng máy chủ thư điện tử	
Phần mềm máy chủ thư điện tử		
4	Triển khai máy chủ thư điện tử trên máy chủ riêng	2.2.1.a
5	Loại bỏ hoặc vô hiệu hoá các dịch vụ không cần thiết đi kèm ứng dụng máy chủ thư điện tử	2.2.1.đ
6	Lưu trữ thư điện tử và tệp nhật ký trên phân vùng hoặc ổ đĩa cứng vật lý riêng	2.2.1.d 2.2.2.b
7	Vô hiệu hoá các lệnh VRFY và EXPN của giao thức SMTP	2.2.1.h
8	Cấu hình ứng dụng thư điện tử có thể ghi log file nhưng không thể đọc những log file này	2.2.2.a
9	Cấu hình ứng dụng thư điện tử chỉ có thể ghi nội dung file trên các thư mục cần thiết mà không có quyền ghi nội dung file ngoài các thư mục này	2.2.2.a
10	Giới hạn sự truy cập của máy chủ thư điện tử vào các dữ liệu quan trọng trên hệ thống	2.2.2.a
11	Giới hạn các loại tệp được đính kèm trên thư điện tử	2.2.2.
12	Giới hạn số lượng thư điện tử có thể được gửi đi trong một khoảng thời gian nhất định	2.2.2.
13	Giới hạn số lượng người nhận có thể gửi cùng lúc bằng chức năng CC, BCC	2.2.2.đ
Hệ thống, thiết bị mạng		
14	Máy chủ email được đặt ở trong mạng nội bộ và được bảo vệ bởi mail gateway và/hoặc tường lửa hoặc máy chủ email được đặt trong khu vực cách lý (DMZ)	2.3.1.a
15	Cấu hình tường lửa	2.3.2.a
16	Máy chủ email được bảo vệ bởi tường lửa ở lớp ứng dụng	2.3.2.b
17	Tường lửa quản lý toàn bộ traffic giữa mạng Internet và máy chủ email	2.3.2.c

18	Tường lửa có khả năng chặn tất cả các lưu lượng mạng vào máy chủ email trừ các cổng cần thiết để hoạt động	2.3.2.c
19	Tường lửa có khả năng chặn các địa chỉ IP hoặc dải địa chỉ IP mà IDS/IPS cảnh báo tấn công hệ thống mạng	2.3.2.c
20	Tường lửa có khả năng chặn "danh sách đen" được phát hiện bởi các tổ chức bảo mật uy tín	2.3.2.c
21	Tường lửa có khả năng cảnh báo quản trị mạng hoặc quản trị hệ thống email về các hành động khả nghi tấn công	2.3.2.c
22	Tường lửa có khả năng chặn lọc theo nội dung và quét mã độc	2.3.2.c
23	Tường lửa được cấu hình để có thể chống các cuộc tấn công từ chối dịch vụ	2.3.2.c
24	Tường lửa có lưu nhật ký các sự kiện quan trọng	2.3.2.c
25	IDS/IPS được cấu hình để theo dõi toàn bộ traffic đi và đến máy chủ email	2.3.3.d
26	IDS/IPS được cấu hình để theo dõi sự thay đổi của các tệp tin quan trọng trên máy chủ email	2.3.3.d
27	IDS/IPS được cấu hình để theo dõi tài nguyên hệ thống trên máy chủ email	2.3.3.d
28	IDS/IPS có khả năng chặn (thông qua firewall) các địa chỉ IP hoặc dải địa chỉ IP được xác định là tấn công vào hệ thống mạng	2.3.3.d
29	IDS/IPS có khả năng gửi thông báo tới bộ phận liên quan về các sự kiện khả nghi	2.3.3.d
30	IDS/IPS được cấu hình để lưu sự kiện khả nghi và lưu mào đầu các gói tin liên quan tới sự kiện đó	2.3.3.d
31	IDS/IPS được cập nhật các dấu hiệu tấn công mới nhất theo định kỳ (hàng ngày đến hàng tuần)	2.3.3.d
32	Thiết bị chuyển mạch được cấu hình để chống tấn công bằng hình thức ARP	2.3.4

33	Thiết bị chuyển mạch được cấu hình để chuyển toàn bộ traffic tới IDS/IPS	2.3.4
Phòng, chống lợi dụng, giả mạo thư điện tử		
34	Cài đặt thành phần dò quét virus/mã độc. Cập nhật cơ sở dữ liệu của các thành phần dò quét virus/mã độc này và đặt chế độ hoạt động liên tục (real time).	3.1
35	Cập nhật nội dung cho các bộ chặn lọc thư điện tử spam/phishing và nội dung xấu	3.2
36	Ngăn chặn việc giả mạo các thông số quan trọng của thư điện tử ngay cả khi người dùng đã được xác thực	3.3.4
37	Triển khai chính sách mật khẩu mạnh	3.4
Lưu nhật ký		
38	Phân tích các bản nhật ký định kỳ để phát hiện sự cố	4.1
39	Sử dụng công cụ phân tích nhật ký tự động	4.1
40	Lưu nhật ký các lỗi cấu hình máy chủ thư điện tử	4.1.2.a
41	Lưu nhật ký về các thông tin tài nguyên hệ thống máy chủ (dung lượng lưu trữ, bộ nhớ, CPU)	4.1.2.a
42	Lưu nhật ký về cơ sở dữ liệu các định danh	4.1.2.a
43	Lưu các sự cố về bảo mật	4.1.2.b
44	Lưu các sự cố về mạng	4.1.2.b
45	Lưu lỗi giao thức kết nối	4.1.2.b
46	Lưu kết nối quá thời gian cho phép	4.1.2.b
47	Lưu kết nối bị từ chối	4.1.2.b
48	Lưu thông tin về lệnh VRFY và EXPN	4.1.2.b
49	Lưu các sự kiện liên quan đến việc gửi thư điện tử theo sự cho phép của người dùng (Send on behalf of/Send as)	4.1.2.c
50	Lưu thông tin về các email gửi tới/từ địa chỉ không tồn tại	4.1.2.c

51	Lưu thống kê về số lượng email đã gửi/nhận hàng ngày	4.1.2.c
52	Lưu các email bị trả về	4.1.2.c
53	Lưu các email bị trì hoãn gửi	4.1.2.c
Sao lưu và phục hồi		
54	Lưu các bản lưu nhật ký theo nội quy của cơ quan, tổ chức	4.2
55	Giả lập tình huống bị tấn công để diễn tập phục hồi hệ thống theo quy trình	4.2
56	Sao lưu máy chủ email theo hình thức toàn bộ hàng tuần và hàng tháng	4.2.1
57	Lưu trữ ngoại tuyến các bản sao lưu theo định kỳ	4.2.1
58	Sao lưu máy chủ email theo hình thức bổ sung hoặc khi có khác biệt hàng ngày và hàng tuần	4.2.1
59	Có quy chế và quy trình về sao lưu/phục hồi máy chủ email	4.2.2
Kiểm thử, đánh giá máy chủ thư điện tử		
60	Định kỳ quét lỗi bảo mật cho máy chủ thư điện tử và mạng tối thiểu 6 tháng/lần	4.3
61	Cập nhật dữ liệu cho công cụ quét lỗi bảo mật trước khi kiểm thử	4.3.1
62	Tự triển khai hoặc thuê công ty bảo mật thực hiện kiểm thử thâm nhập cho máy chủ email và mạng	4.3.2
63	Định kỳ rà soát, kiểm tra nhật ký hoạt động trên máy chủ thư điện tử	4.3
Quản trị từ xa		
64	Áp dụng các biện pháp kỹ thuật cho xác thực đăng nhập	4.4
65	Giới hạn nguồn truy cập từ xa thông qua địa chỉ IP hoặc cấu hình mạng/máy	4.4
66	Sử dụng các giao thức bảo mật để truyền tải mật khẩu và dữ liệu	4.4
67	Giới hạn quản lý đối với các tài khoản quản trị từ xa	4.4

68	Thay đổi tài khoản hoặc mật khẩu mặc định cho hệ điều hành và toàn bộ ứng dụng trên máy chủ email	4.4
69	Chỉ cho phép quản trị từ xa ngoài mạng nội bộ khi có VPN	4.4
70	Không cho phép chia sẻ file/thư mục giữa máy chủ thư điện tử và máy trong mạng nội bộ	4.4

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 2132/BTTTT-VNCERT

V/v Hướng dẫn đảm bảo an toàn thông tin cho các Cổng/Trang thông tin điện tử

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc Lập - Tự Do - Hạnh Phúc

Hà Nội, ngày 18 tháng 7 năm 2011

Kính gửi:
- Các Bộ, cơ quan ngang Bộ, cơ quan trực thuộc Chính phủ;
- UBND các tỉnh, thành phố trực thuộc Trung ương.

Thực hiện chỉ đạo của Thủ tướng Chính phủ về việc đảm bảo an toàn thông tin cho các cổng thông tin điện tử, đồng thời để thống nhất về nội dung và phương pháp quản lý an toàn thông tin theo yêu cầu của Nghị định của Chính phủ số 43/2011/NĐ-CP ngày 13/6/2011, Bộ Thông tin và Truyền thông hướng dẫn các cơ quan nhà nước triển khai áp dụng tài liệu "Hướng dẫn một số biện pháp kỹ thuật cơ bản đảm bảo an toàn cho cổng/trang thông tin điện tử". Tài liệu này bao gồm một số biện pháp kỹ thuật thiết yếu nhất nhằm đảm bảo xây dựng và vận hành an toàn các cổng/trang thông tin điện tử và được trình bày trong văn bản gửi kèm theo công văn này.

Trong quá trình triển khai thực hiện, mọi góp ý và đề xuất xin đề nghị Quý cơ quan phản ánh về Bộ Thông tin và Truyền thông, Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT).

Xin trân trọng cám ơn./.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Nguyễn Minh Hồng

Nơi nhận:
- Như trên;
- Phó TTg CP Nguyễn Thiện Nhân (để b/c);
- Bộ TT&TT: Bộ trưởng và các Thứ trưởng, các cơ quan đơn vị thuộc Bộ;
- Văn phòng TW Đảng;
- Văn phòng Quốc hội;
- Văn phòng Chính phủ;
- Cơ quan TW các đoàn thể;
- Toà án nhân dân tối cao;
- Viện kiểm sát nhân dân tối cao;
- Kiểm toán nhà nước;
- Ban chỉ đạo quốc gia về CNTT;
- Ban chỉ đạo CNTT các cơ quan Đảng;
- Đơn vị chuyên trách CNTT các Bộ, cơ quan ngang Bộ, cơ quan chính phủ;
- Sở TT&TT các tỉnh, TP thuộc TW;
- Các tập đoàn kinh tế NN;
- Lưu VT, VNCERT.

HƯỚNG DẪN
MỘT SỐ BIỆN PHÁP KỸ THUẬT CƠ BẢN ĐẢM BẢO AN TOÀN CHO CỔNG/TRANG THÔNG TIN ĐIỆN TỬ

(Kèm theo công văn số 2432/BTTTT-VNCERT ngày 18 /7/2011 của Bộ Thông tin và Truyền thông)

1. PHẠM VI VÀ ĐỐI TƯỢNG ÁP DỤNG

1.1. Phạm vi áp dụng

Tài liệu hướng dẫn này được xây dựng nhằm mục đích cung cấp những kiến thức và chỉ dẫn kỹ thuật cơ bản về việc đảm bảo an toàn thông tin (ATTT) đối với hệ thống phần cứng và phần mềm thuộc cổng/trang thông tin điện tử (TTĐT), các yêu cầu thiết lập hệ thống phòng thủ và bảo vệ, qua đó giúp các đơn vị quản lý cổng/trang TTĐT có thể đánh giá mức độ ATTT và lựa chọn giải pháp phù hợp nhằm xây dựng một cổng/trang TTĐT an toàn.

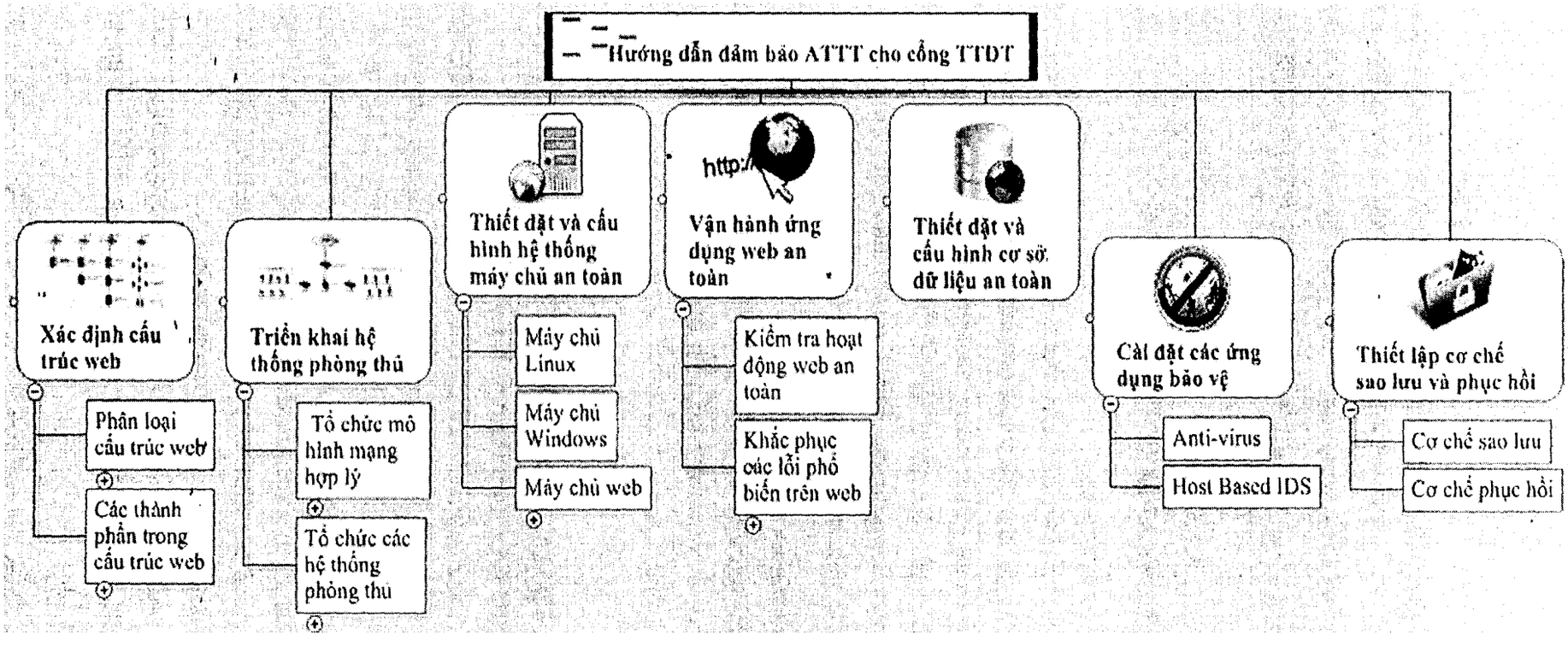
1.2. Đối tượng áp dụng

Các cổng/trang TTĐT của các cơ quan nhà nước và các doanh nghiệp được khuyến cáo tổ chức thực hiện áp dụng tối đa các biện pháp này trong điều kiện cụ thể cho phép.

2. TỔNG QUAN VỀ CÁC BIỆN PHÁP KỸ THUẬT CƠ BẢN ĐẢM BẢO ATTT CHO CỔNG/TRANG TTĐT

Một ứng dụng web nói chung hay cổng/trang TTĐT nói riêng khi triển khai được trên mạng Internet ngoài yếu tố mã nguồn ứng dụng web, còn có những thành phần khác như: máy chủ phục vụ web, hệ quản trị cơ sở dữ liệu,... Do vậy, một cổng/trang TTĐT an toàn đòi hỏi bản thân mã nguồn của cổng phải được lập trình an toàn, tránh các lỗi bảo mật xảy ra trên ứng dụng web và các thành phần bổ trợ như máy chủ phục vụ web và hệ quản trị cơ sở dữ liệu cho ứng dụng đó cũng phải đảm bảo an toàn.

Các biện pháp đảm bảo ATTT cho cổng/trang TTĐT cần được triển khai cho toàn bộ các thành phần của cổng/trang TTĐT, bao gồm các nội dung sau (xem hình 1):



Hình 1. Nội dung đảm bảo ATTT cho cổng/trang TTĐT

- **Xác định cấu trúc web**: giúp người quản trị xác định được mô hình thiết kế web của đơn vị, qua đó có biện pháp tổ chức mô hình web hợp lý, tránh được các khả năng tấn công leo thang đặc quyền.

- **Triển khai hệ thống phòng thủ**: gồm hai nội dung chính là tổ chức mô hình mạng hợp lý và tổ chức các hệ thống phòng thủ, giúp người quản trị có cách nhìn tổng quan về toàn bộ mô hình mạng của cổng/trang TTĐT của mình, qua đó tổ chức mô hình mạng hợp lý cũng như thiết đặt các hệ thống phòng thủ quan trọng như tường lửa (firewall), thiết bị phát hiện/phòng, chống xâm nhập (IDS/IPS), tường lửa mức ứng dụng web (WAF-web application firewall).

- **Thiết đặt và cấu hình hệ thống máy chủ an toàn**: đây là một phần rất quan trọng trong việc đảm bảo vận hành một cổng/trang TTĐT an toàn. Nội dung này giúp người quản trị cấu hình hệ thống máy chủ một cách hợp lý, giảm thiểu khả năng bị tin tặc tấn công vào máy chủ làm ảnh hưởng đến hoạt động của cổng/trang TTĐT.

- **Vận hành ứng dụng web an toàn**: trình bày các nội dung cơ bản cần thực hiện để vận hành một ứng dụng web an toàn. Người quản trị có thể tham khảo phần Phụ lục I "Mười lỗi ATTT phổ biến trên cổng/trang TTĐT" để qua đó nhận diện nguy cơ mắc lỗi của cổng/trang TTĐT tại đơn vị, có biện pháp khắc phục hợp lý hoặc sửa đổi mã nguồn web để loại bỏ các nguy cơ nói trên.

- **Thiết đặt và cấu hình cơ sở dữ liệu an toàn**: đây cũng là một phần rất quan trọng trong việc vận hành một cổng/trang TTĐT. Cơ sở dữ liệu là nơi lưu trữ toàn bộ dữ liệu quan trọng của cổng/trang TTĐT, vì vậy thường bị tin tặc tìm cách tấn công và khai thác. Nội dung này giúp người quản trị hiểu yêu cầu thiết đặt hợp lý cho cơ sở dữ liệu, tránh các lỗi có thể dẫn đến khả năng bị tấn công.

- **Cài đặt các ứng dụng bảo vệ**: ngoài việc khắc phục lỗi cho các thành phần của một cổng/trang TTĐT, nội dung này sẽ trình bày việc cài đặt các ứng dụng bảo vệ như hệ thống chống virus (Anti-Virus) hay hệ thống phát hiện xâm nhập máy tính (Host Based IDS) nhằm bảo vệ cổng/trang TTĐT một cách chủ động và tổng quát.

- **Thiết lập cơ chế sao lưu và phục hồi**: Việc thiết lập cơ chế sao lưu thường xuyên cho hệ thống nhằm giúp lưu lại các tình trạng khi hệ thống hoạt động ổn định. Các bản sao lưu này sẽ được sử dụng trong trường hợp kiểm tra lỗi hệ thống hoặc phục hồi hệ thống ở trạng thái trước khi bị tấn công trong trường hợp lỗi không thể khắc phục hay sửa chữa.

- **Một số biện pháp kỹ thuật chống tấn công từ chối dịch vụ**: đây là nội dung cuối cùng trong tài liệu này nhằm cung cấp định hướng nâng cao năng lực chống tấn công từ chối dịch vụ DoS và DDoS cho các cổng/trang TTĐT.

3. NỘI DUNG CÁC BIỆN PHÁP KỸ THUẬT CƠ BẢN ĐẢM BẢO ATTT

3.1. Xác định cấu trúc của web

Một ứng dụng web khi triển khai, về cơ bản sẽ có 3 lớp như sau: lớp trình diễn, lớp ứng dụng và lớp cơ sở dữ liệu.

Lớp trình diễn (Web Server) là nơi mà máy chủ cài đặt có tác dụng phục vụ các yêu cầu về Web hay nói cách khác, lớp trình diễn là máy chủ phục vụ web (có thể là: IIS Server, Apache HTTP Server, Apache Tomcat Server,...).

Lớp ứng dụng (Web Application) là nơi các kịch bản hay mã nguồn phát triển ra ứng dụng web thực thi (có thể là: ASP.NET, PHP, JSP, Perl, Python,...).

Lớp cơ sở dữ liệu (Database Server) là nơi mà ứng dụng web lưu trữ và thao tác với dữ liệu (thường dựa trên nền các hệ quản trị cơ sở dữ liệu (CSDL) như: Oracle, SQL Server, MySQL,...).

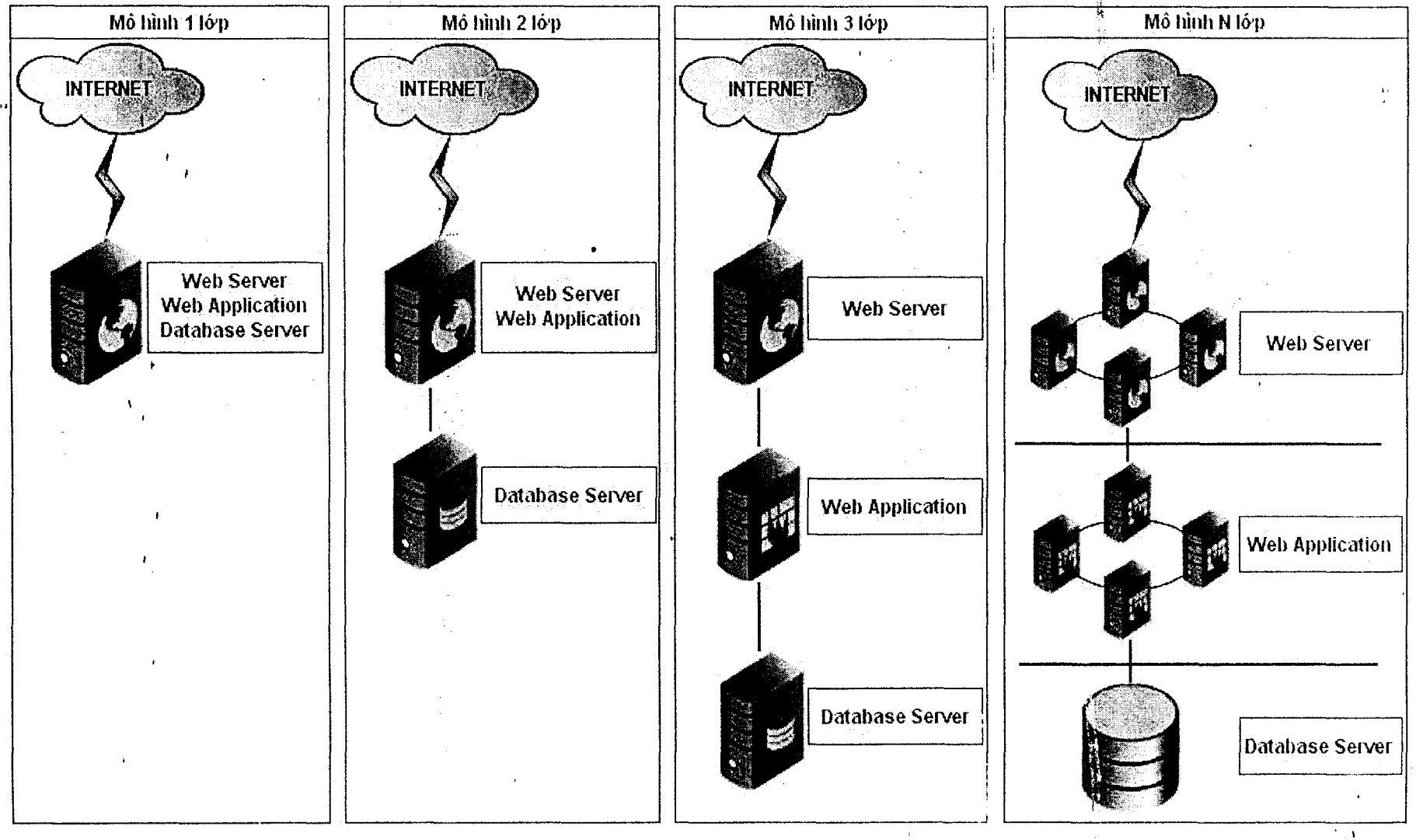
Việc hoạch định tốt các lớp trong cấu trúc web không những giúp người quản trị dễ vận hành mà còn chủ động trong phòng, chống các nguy cơ tấn công từ tin tặc. Một số cách bố trí lớp thường gặp trong thực tế như trên hình vẽ 2.

Mỗi lớp nên khởi tạo một cơ chế phòng thủ riêng cho mình để chống lại những hành động không được phép và không nên "tin tưởng" những lớp khác để tránh tình trạng tấn công leo thang. Một số kịch bản thông dụng:

- Lớp trình diễn có thể áp đặt cơ chế điều khiển truy cập trên một tài nguyên. Ví dụ khi lập chính sách truy cập một tài nguyên nào đó trên hệ thống, chẳng hạn như thư mục */admin*, có thể cài đặt cấu hình lớp trình diễn yêu cầu xác thực với quyền quản trị (administrator). Điều này sẽ hạn chế ảnh hưởng từ lớp ứng dụng có thể sử dụng nhiều kịch bản để truy cập đến tài nguyên trên.

- Lớp cơ sở dữ liệu có thể cung cấp các tài khoản khác nhau với những quyền hành động khác nhau. Ví dụ như với nhóm người sử dụng có tên tài khoản chưa được chứng thực thì thiết đặt quyền thấp nhất là chỉ có thể đọc, còn các thao tác ghi, thay đổi, thực thi là không được phép. Nếu tài khoản được chứng thực thì cũng chỉ được ghi, thay đổi, thực thi trên CSDL đã được chỉ định và chỉ có tác dụng trong phạm vi CSDL đã được cấu hình từ trước.

- Các lớp khác nhau không nên cho phép truy cập đọc hoặc ghi bởi lớp khác. Ví dụ: lớp trình diễn không có khả năng truy cập đến tập tin vật lý được sử dụng lưu trữ dữ liệu tại lớp CSDL mà chỉ có khả năng truy cập dữ liệu này thông qua các truy vấn với các tài khoản phù hợp (truy cập ở cấp độ ứng dụng). Các dịch vụ giao tiếp giữa các lớp trên cấp độ mạng cũng nên được lọc để chỉ cho phép các dịch vụ cần thiết được thực thi. Ví dụ: chỉ cho phép kết nối đến hệ quản trị cơ sở dữ liệu SQL Server trên cổng TCP 1433, còn các cổng khác thì phải được lọc hoặc không cho phép.



Hình 2. Các mô hình triển khai cổng/trang TTĐT

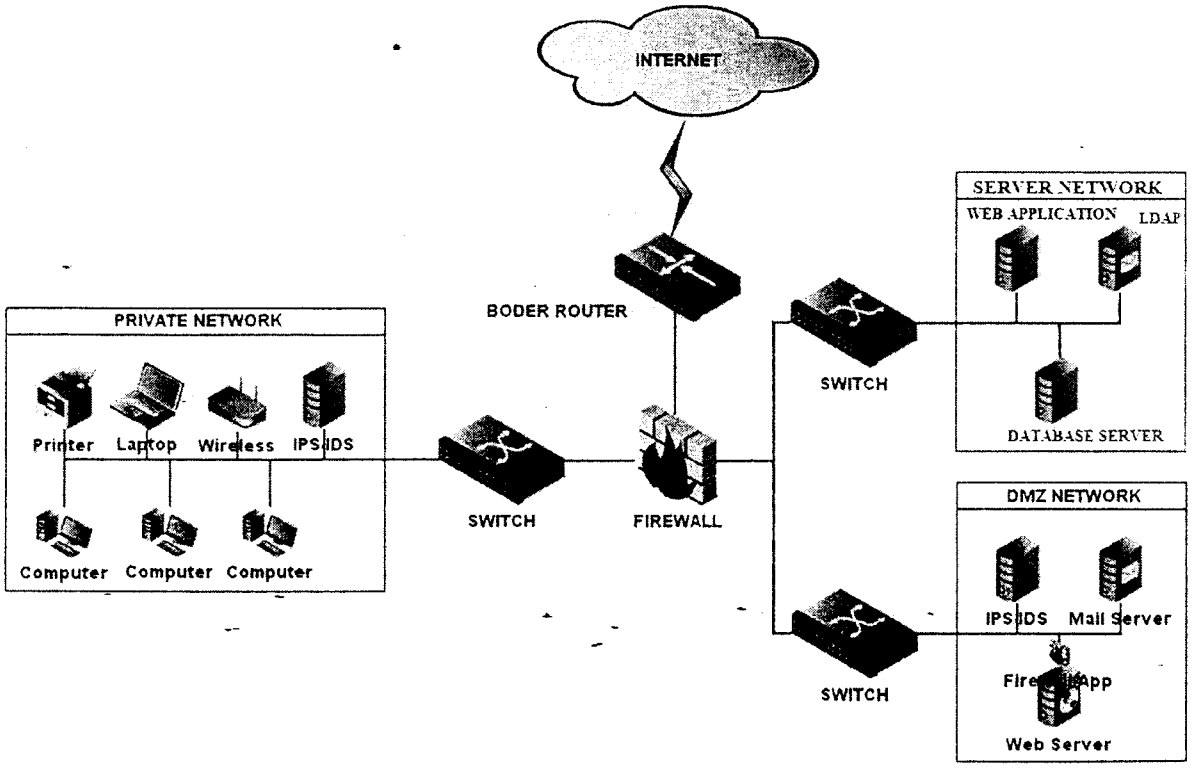
Việc phân tích các mô hình trên cho thấy, nếu giữa các lớp không có sự tách biệt rõ ràng thì khi một lớp bị tin tặc tấn công và chiếm quyền kiểm soát có thể dẫn đến các lớp khác cũng bị ảnh hưởng theo. Ví dụ trường hợp tất cả ứng dụng web, cơ sở dữ liệu đều được đặt trên máy chủ phục vụ web thì khi tin tặc tấn công vào máy chủ phục vụ web có thể dẫn đến mã nguồn và cơ sở dữ liệu của ứng dụng đó bị xâm phạm. Do vậy, khi triển khai thực tiễn nên thiết kế tách biệt độc lập theo mô hình 3 lớp để tránh tình trạng một lớp bị tấn công và chiếm quyền kiểm soát dẫn đến các lớp khác bị ảnh hưởng. Việc phân loại độc lập 3 lớp như trên sẽ tạo điều kiện thuận lợi cho việc vận hành, bảo trì hệ thống cũng như dễ dàng áp dụng các biện pháp bảo vệ đối với mỗi lớp riêng biệt.

Trong trường hợp có khó khăn, hạn chế về nguồn lực xây dựng cổng/trang TTĐT thì vẫn nên áp dụng tối thiểu mô hình hai lớp với lớp cơ sở dữ liệu được tách biệt độc lập.

3.2. Triển khai hệ thống phòng thủ

3.2.1. Tổ chức mô hình mạng hợp lý

Việc tổ chức mô hình mạng hợp lý có ảnh hưởng lớn đến sự an toàn cho các cổng/trang TTĐT. Đây là cơ sở đầu tiên cho việc xây dựng các hệ thống phòng thủ và bảo vệ. Ngoài ra, việc tổ chức mô hình mạng hợp lý có thể hạn chế được các tấn công từ bên trong và bên ngoài một cách hiệu quả.



Hình 3. Mô hình mạng tổng quan

Trong một mô hình mạng hợp lý cần phải phân biệt rõ ràng giữa các vùng mạng theo chức năng và thiết lập các chính sách an toàn thông tin riêng cho từng vùng mạng theo yêu cầu thực tế:

- Vùng mạng Internet (hay Untrusted Network): còn gọi là mạng ngoài.
- Vùng mạng DMZ Network: Đặt các máy chủ cung cấp dịch vụ trực tiếp ra mạng Internet như web server, mail server, FTP Server, v.v...
- Vùng mạng Server Network (hay Server Farm): Đặt các máy chủ không trực tiếp cung cấp dịch vụ cho mạng Internet.
- Vùng mạng Private Network: Đặt các thiết bị mạng, máy trạm và máy chủ thuộc mạng nội bộ của đơn vị.

Một số khuyến cáo khi tổ chức mô hình mạng:

- Nên đặt các máy chủ web, máy chủ thư điện tử (mail server), v.v... cung cấp dịch vụ ra mạng Internet trong vùng mạng DMZ, nhằm tránh các tấn công mạng nội bộ hoặc gây ảnh hưởng tới an toàn mạng nội bộ nếu các máy chủ này bị cướp quyền điều khiển. Chú ý không đặt máy chủ web, mail server hoặc các máy chủ chỉ cung cấp dịch vụ cho nội bộ cơ quan trong vùng mạng này.
- Các máy chủ không trực tiếp cung cấp dịch vụ ra mạng ngoài như máy chủ ứng dụng, máy chủ cơ sở dữ liệu, máy chủ xác thực v.v... nên đặt trong vùng mạng server network để tránh các tấn công trực diện từ Internet và từ mạng nội bộ. Đối với các hệ thống thông tin yêu cầu có mức bảo mật cao, hoặc có nhiều cụm máy chủ khác nhau có thể chia vùng server network thành các vùng nhỏ hơn độc lập để nâng cao tính bảo mật.
- Nên thiết lập các hệ thống phòng thủ như tường lửa (firewall) và thiết bị phát hiện/phòng chống xâm nhập (IDS/IPS) để bảo vệ hệ thống, chống tấn công và xâm nhập trái phép. Khuyến cáo đặt firewall và IDS/IPS ở các vị trí như sau: đặt firewall giữa đường nối mạng Internet với các vùng mạng khác nhằm hạn chế các tấn công từ mạng từ bên ngoài vào; đặt firewall giữa các vùng mạng nội bộ và mạng DMZ nhằm hạn chế các tấn công giữa các vùng đó; đặt IDS/IPS tại vùng cần theo dõi và bảo vệ.
- Nên đặt một Router ngoài cùng (Router biên) trước khi kết nối đến nhà cung cấp dịch vụ internet (ISP) để lọc một số lưu lượng không mong muốn và chặn những gói tin đến từ những địa chỉ IP không hợp lệ.

3.2.2. Tổ chức các hệ thống phòng thủ

3.2.2.1. Firewall (Tường lửa)

Firewall là một thiết bị phần cứng hoặc một phần mềm hoạt động trong một môi trường máy tính nối mạng nhằm ngăn chặn những lưu lượng bị cấm bởi

chính sách an ninh của một cá nhân hay một tổ chức. Mục đích của việc sử dụng Firewall là:

- Bảo vệ hệ thống khi bị tấn công.
- Lọc các kết nối dựa trên chính sách truy cập nội dung.
- Áp đặt các chính sách truy cập đối với người dùng hoặc nhóm người dùng.
- Ghi lại nhật ký để hỗ trợ phát hiện xâm nhập và điều tra sự cố.

Cần thiết lập luật cho Firewall từ chối tất cả các kết nối từ bên trong Web Server ra ngoài Internet ngoại trừ các kết nối đã được thiết lập – tức là chỉ từ chối tất cả các gói tin TCP khi xuất hiện cờ SYN. Điều này sẽ ngăn chặn việc nếu như tin tặc có khả năng chạy các kịch bản mã độc trên Web Server thì cũng không thể cho các mã độc nối ngược từ Web Server trở về máy tính của tin tặc.

Tuy nhiên, hạn chế của Firewall là có thể làm chậm quá trình kết nối và trong một số trường hợp đối với một số người có hiểu biết thì có thể vượt qua được Firewall. Vì thế cần chú trọng đến việc bảo vệ hệ thống theo chiều sâu.

3.2.2.2. IDS/IPS (Thiết bị phát hiện/phòng, chống xâm nhập)

Các thiết bị IDS có tính năng phát hiện dấu hiệu các xâm nhập trái phép, còn các thiết bị IPS có tính năng phát hiện và ngăn chặn việc xâm nhập trái phép của tin tặc vào hệ thống. Như các thiết bị mạng, IDS/IPS cũng có thể bị tấn công và chiếm quyền kiểm soát và do đó bị vô hiệu hóa bởi tin tặc. Vì vậy cần thiết đảm bảo thực hiện một số tiêu chí khi triển khai và vận hành, gồm:

- Xác định công nghệ IDS/IPS đã, đang hoặc dự định triển khai.
- Xác định các thành phần của IDS/IPS.
- Thiết đặt và cấu hình an toàn cho IDS/IPS.
- Xác định vị trí hợp lý để đặt IDS/IPS.
- Có cơ chế xây dựng, tổ chức, quản lý hệ thống luật (rule).
- Hạn chế thấp nhất các tình huống cảnh báo nhầm (false positive) hoặc không cảnh báo khi có xâm nhập (false negative).

3.2.2.3. WAF (Tường lửa ứng dụng web)

Một WAF thường là một phần mềm, hay một thành phần nhúng được cài ngay trên máy chủ phục vụ web. Đôi khi WAF cũng được cung cấp như một thiết bị phần cứng có cài đặt sẵn phần mềm bên trong. WAF hoạt động bằng cách sử dụng một bộ lọc với các "luật" được định nghĩa trước hoặc do người dùng thêm vào để giám sát các dữ liệu trao đổi với ứng dụng web thông qua giao thức HTTP. Những quy tắc này có thể giúp phát hiện và chặn các truy vấn nhằm tấn công vào các lỗi phổ biến như Cross-site Scripting (XSS), SQL Injection, OS command Injection, Path Travesal,... cũng như một số lỗi khác

được nêu trong danh mục "OWASP Top 10" (http://en.wikipedia.org/wiki/Application_firewall)

Các dữ liệu đi vào hoặc đi ra khỏi ứng dụng web sẽ được WAF kiểm tra so sánh với các dấu hiệu được định nghĩa sẵn và quyết định cho phép dữ liệu đi qua hay chặn các dữ liệu đó lại. Đây là một quá trình lọc mà các thiết bị tường lửa lớp dưới không thực hiện được. Việc triển khai WAF sẽ phần nào hạn chế được các sai sót của người lập trình ứng dụng web. Các WAF nên được cài đặt giữa mỗi lớp trong kiến trúc web.

Xem thông tin tham khảo về các WAF tại Phụ lục II.

3.3. Thiết đặt và cấu hình hệ thống máy chủ an toàn

Để vận hành một máy chủ an toàn, việc cần lưu ý đầu tiên là luôn cập nhật phiên bản và bản vá mới nhất cho hệ thống. Ngoài ra, với mỗi loại máy chủ khác nhau sẽ có những biện pháp thiết đặt và cấu hình cụ thể để đảm bảo vận hành an toàn.

3.3.1. Hệ thống máy chủ Linux

- Đối với hệ thống cài đặt mới thì phải đảm bảo một số yêu cầu sau:
  + Khả năng hỗ trợ từ các bản phân phối (thông tin vá lỗi, thời gian cập nhật, nâng cấp, kênh thông tin hỗ trợ kỹ thuật).
  + Khả năng tương thích với các sản phẩm của bên thứ 3 (tương thích giữa nhân hệ điều hành với các ứng dụng, cho phép mở rộng module).
  + Khả năng vận hành và sử dụng hệ thống của người quản trị (thói quen, kỹ năng sử dụng, tính tiện dụng).
- Tối ưu hóa hệ điều hành về các mặt sau:
  + Chính sách mật khẩu: sử dụng cơ chế mật khẩu phức tạp (trên 7 ký tự và bao gồm: ký tự hoa, ký tự thường, ký tự đặc biệt và chữ số) nhằm chống lại các kiểu tấn công brute force.
  + Tinh chỉnh các thông số mạng: tối ưu hóa một số thông tin trong tập tin /etc/sysctl.conf.
  + Cho phép hoặc không cho phép các dịch vụ truy cập đến hệ thống thông qua hai tập tin /etc/hosts. allow và /etc/host.deny.
  + Gỡ bỏ các dịch vụ không cần thiết: việc gỡ bỏ các gói, dịch vụ không cần thiết sẽ hạn chế khả năng tiếp cận của kẻ tấn công và cải thiện hiệu năng của hệ thống.
  + Điều khiển truy cập: chỉ định các truy cập được phép đến hệ thống thông qua tập tin /etc/security/access.conf, /etc/security/time.conf,

/etc/security/limits.conf, giới hạn tài khoản được phép sử dụng quyền *sudo* thông qua tập tin /etc/pam.d/su.

+ Sử dụng kết nối SSH thay cho các kênh kết nối không an toàn như Telnet, FTP, v.v...
+ Quản lý hệ thống ghi nhật ký (log) một cách tập trung và nhất quán nhằm phục vụ cho mục đích điều tra khi có sự cố xảy ra.

3.3.2. Hệ thống máy chủ Windows

Máy chủ Windows được sử dụng khá phổ biến, việc bảo vệ cho máy chủ Windows là thực sự cần thiết. Để đảm bảo cho hệ thống cần thực hiện một số biện pháp sau:

- Đối với các dịch vụ và cổng:
  + Các dịch vụ đang chạy thiết lập với tài khoản có quyền tối thiểu.
  + Vô hiệu hóa các dịch vụ DHCP, DNS, FTP, WINS, SMTP, NNTP, Telnet và các dịch vụ không cần thiết khác nếu không có nhu cầu sử dụng.
  + Nếu là ứng dụng web thì chỉ mở cổng 80 (và cổng 443 nếu có SSL).
- Đối với các giao thức:
  + Vô hiệu hóa WebDAV nếu không sử dụng bởi ứng dụng nào hoặc nếu nó được yêu cầu thì nó phải được bảo mật.
  + Vô hiệu hóa NetBIOS và SMB (đóng các cổng 137, 138, 139, và 445).
- Tài khoản và nhóm người dùng:
  + Gỡ bỏ các tài khoản chưa sử dụng khỏi máy chủ.
  + Vô hiệu hóa tài khoản Windows Guest .
  + Đổi tên tài khoản Administrator và thiết lập một mật khẩu mạnh.
  + Vô hiệu hóa tài khoản IUSR_MACHINE nếu nó không được sử dụng bởi ứng dụng khác.
  + Nếu một ứng dụng khác yêu cầu truy cập anonymous, thì thiết lập tài khoản anonymous có quyền tối thiểu.
  + Chính sách về tài khoản và mật khẩu phải đảm bảo an toàn, sử dụng cơ chế mật khẩu phức tạp (trên 7 ký tự và bao gồm: ký tự hoa, ký tự thường, ký tự đặc biệt và chữ số).
  + Phải giới hạn Remote logons. (Chức năng này phải được gỡ bỏ khỏi nhóm Everyone).
  + Tắt chức năng Null sessions (anonymous logons).
- Tập tin và thư mục:

+ Tập tin và thư mục phải nằm trên phân vùng định dạng NTFS.
+ Tập tin nhật ký (log) không nằm trên phân vùng NTFS hệ thống.
+ Các nhóm Everyone bị giới hạn (không có quyền truy cập vào \Windows\system32).
+ Mọi tài khoản anonymous bị cấm quyền ghi (write) vào thư mục gốc.

- Tài nguyên chia sẻ:
  + Gỡ bỏ tất cả các chia sẻ không sử dụng (bao gồm cả chia sẻ mặc định).
  + Các chia sẻ khác (nếu có) cần được giới hạn (nhóm Everyone không được phép truy cập).
- Các phiên bản vá lỗi:
  + Cập nhật các phiên bản mới nhất.
  + Theo dõi thông tin cập nhật từ nhiều nguồn khác nhau.
  + Nên triển khai cập nhật trên hệ thống thử nghiệm trước khi cập nhật vào hệ thống thật.

3.3.3. Máy chủ web

3.3.3.1. Máy chủ IIS:

Máy chủ IIS được sử dụng khá phổ biến hiện nay trên các máy chủ Windows. Để bảo vệ cho máy chủ IIS cần thực hiện một số biện pháp sau:

- Nên sử dụng các giao thức mã hóa như SSL hoặc TLS nhằm mã hóa các kết nối an toàn.

- Cần thiết lập các thuộc tính trong Audit Policy trên máy chủ IIS trong môi trường làm việc đảm bảo toàn bộ thông tin của người dùng khi đăng nhập vào hệ thống sẽ đều được ghi lại. Tất cả những dữ liệu khi truy cập đều được ghi lại nhật ký.

- Cần thiết lập "*Deny access to this computer from the network*", với thiết lập này sẽ quyết định những tài khoản nào bị cấm truy cập tới máy chủ IIS từ mạng và các tài khoản người dùng sẽ bị hạn chế và đảm bảo tính bảo mật cao hơn. Sau đây là những tài khoản người dùng cần phải thiết lập chế độ cấm nêu trên: ANONYMOUS LOGON, Built-in Administrator và Guest.

- Nên tắt tất cả chi tiết thông báo lỗi mà có khả năng đưa ra quá nhiều thông tin. Việc đưa ra quá chi tiết các thông báo lỗi sẽ dẫn đến việc các tin tặc có thể lợi dụng để tìm hiểu thông tin về hệ thống.

- Nên cài đặt thư mục gốc của ứng dụng web trên phân vùng đĩa có định dạng NTFS, bởi vì khả năng kiểm soát quyền truy cập trên hệ thống tập tin với phân vùng định dạng NTFS mạnh hơn so với các định dạng FAT, FAT32. Khi

đã cài đặt thư mục gốc trên phân vùng NTFS thì cũng phải thiết lập quyền truy cập thấp nhất cho thư mục gốc này, tránh trường hợp thư mục gốc của ứng dụng web được mặc định là Everyone: Full Control.

- Trong IIS có rất nhiều thành phần (module) bổ trợ. Nên gỡ bỏ những thành phần không cần thiết ra khỏi IIS được cài đặt, vì những thành phần này khi bị lỗi có khả năng dẫn đến IIS bị tấn công và chiếm quyền kiểm soát một cách gián tiếp.

- Nên cài đặt URLScan để bổ sung thêm nhiều tính năng bảo mật cho IIS.

3.3.3.2. Apache HTTP:

Một số biện pháp cần thực hiện nhằm bảo vệ máy chủ Apache HTTP một cách an toàn:

- Tối ưu hóa việc sử dụng các thành phần (module) bằng việc gỡ bỏ những thành phần không cần thiết. Một số thành phần khuyến cáo nên gỡ bỏ ra khỏi Apache là: mod_userid, mod_info, mod_status, mod_include.

- Giới hạn các quyền truy cập: Tạo các tài khoản, nhóm người dùng riêng (khác root) để thực thi apache. Không cho phép sử dụng các tài khoản này để đăng nhập bằng cách chỉnh sửa nội dung trong tập tin passwd.

- Điều khiển truy cập: Sử dụng các chỉ mục (Directory) để điều khiển quá trình truy cập đến các thư mục hệ thống cần hạn chế quyền thâm nhập (ví dụ như các thư mục: root, admin, administrator). Không cho phép duyệt qua thư mục gốc (root). Cấu hình được thiết lập trong tập tin cấu hình httpd.conf:

```
<Directory/>
      order deny,allow
      deny from all
</Directory>
<Directory /www/htdocs>
      order allow,deny
      allow from all
</Directory>
```

- Hạn chế tối đa việc sử dụng các lựa chọn (option) sau: MultiViews, ExecCGI, FollowSymLinks, SymLinksIfOwnerMatch. Gỡ bỏ tất cả các trang html mặc định, hướng dẫn sử dụng, thông tin liên quan về web server, điều khiển Server Status, Server Information. Tắt chức năng HTTP TRACE. Bảo vệ các tập tin cấu hình .htaccess.

- Tổ chức quá trình ghi nhật ký: Cấu hình Error Log, Cấu hình Access Log theo một số gợi ý sau:

```
#
# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
```

```
#
LogLevel notice
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\""_
combined
CustomLog log/access_log combined
```

- Đối với một số trang thông tin cần mã hóa truy cập có thể sử dụng qua SSL/TLS nhờ module mod_ssl.

- Hạn chế các thông tin về Web Server:

```
ServerTokens Prod
ServerSignature Off
```

- Điều chỉnh các thông số tối ưu: một số thiết lập tham khảo:

+ Thông số timeout:

```
Timeout 10
```

+ Thông số KeepAlive:

```
KeepAlive On
```

+ Thông số MaxKeepAliveRequests:

```
MaxKeepAliveRequests 100
```

+ Thông số KeepAliveTimeout:

```
KeepAliveTimeout 15
```

+ Thêm các thông số sau:

```
LimitRequestline 512
LimitRequestFields 100
LimitRequestFieldsize 1024
LimitRequestBody 102400
```

3.3.3.3. Apache Tomcat:

Một số biện pháp cần thực hiện nhằm bảo vệ máy chủ Apache Tomcat một cách an toàn:

- Gỡ bỏ các tài nguyên không liên quan: Trong quá trình cài đặt có thể xuất hiện các ứng dụng mẫu, tài liệu hướng dẫn và một số các thư mục không cần thiết khác. Vì vậy cần gỡ bỏ các tập tin, thư mục này nhằm hạn chế thấp nhất nguy cơ bị khai thác thông tin liên quan đến ứng dụng đang sử dụng:

```
$ rm -rf $CATALINA_HOME/webapps/js-examples \
$CATALINA_HOME/webapps/servlet-example \
$CATALINA_HOME/webapps/webdav \
$CATALINA_HOME/webapps/tomcat-docs \
$CATALINA_HOME/webapps/balancer \
$CATALINA_HOME/webapps/ROOT/admin \
$CATALINA_HOME/webapps/examples
```

- Giới hạn các thông tin về hệ thống:

+ Thay đổi thông tin server.info.

+ Tiến hành đóng gói lại tập tin CATALINA_HOME/server/lib/catalina.jar sau khi đã sửa đổi nội dung file ServerInfo.properties. Ví dụ:

```
cd CATALINA_HOME/server/lib
jar xf catalina.jar org/apache/catalina/util/ServerInfo.properties
```

+ Trong tập tin ServerInfo.properties thay đổi giá trị server.info thành giá trị server.info=Apache Tomcat, sau đó đóng gói lại catalina.jar:

```
jar uf catalina.jar org/apache/catalina/util/ServerInfo.properties
```

+ Thay đổi thông tin trong server.number. Thuộc tính thay đổi cũng tương tự như thông số server.info. Ví dụ:

```
cd CATALINA_HOME/server/lib
jar xf catalina.jar org/apache/catalina/util/ServerInfo.properties
```

+ Trong tập tin ServerInfo.properties thêm thuộc tính server.number=<Version>, sau đó đóng gói lại catalina.jar:

```
jar uf catalina.jar org/apache/catalina/util/ServerInfo.properties
```

+ Thay đổi thông tin trong server.built. Thuộc tính này cung cấp thông tin về thời gian mà Tomcat được biên dịch và đóng gói. Ví dụ:

```
cd CATALINA_HOME/server/lib
jar xf catalina.jar org/apache/catalina/util/ServerInfo.properties
```

+ Trong tập tin ServerInfo.properties thêm thuộc tính server.built=< BuildDate>, sau đó đóng gói lại catalina.jar:

```
jar uf catalina.jar org/apache/catalina/util/ServerInfo.properties
```

- Bảo vệ cổng shutdown:

+ Apache Tomcat sử dụng cổng 8005 để tiếp nhận các yêu cầu shutdown. Cập nhật thuộc tính shutdown trong tập tin server.xml ở $CATALINA_HOME/conf/server.xml:

```
<Server port="8005" shutdown="NOSHUTDOWN">
```

+ Hoặc bỏ chức năng shutdown trên cổng này:

```
<Server port="-1" shutdown="SHUTDOWN">
```

- Bảo vệ cấu hình Apache Tomcat:

+ Giới hạn truy cập đến $CATALINA_HOME: Gán quyền sở hữu cho tài khoản tomcat_admin:tomcat; gỡ bỏ các quyền đọc, ghi, thực thi; gỡ bỏ quyền ghi đối với nhóm:

```
chown tomcat_admin.tomcat $CATALINA_HOME
# chmod g-w,o-rwx $CATALINA_HOME
```

+ Giới hạn truy cập đến $CATALINA_BASE: Gán quyền sở hữu cho tài khoản tomcat_admin:tomcat; gỡ bỏ các quyền đọc, ghi, thực thi; gỡ bỏ quyền ghi đối với nhóm:

```
# chown tomcat_admin.tomcat $CATALINA_BASE
# chmod g-w,o-rwx $CATALINA_BASE
```

+ Giới hạn truy cập đến thư mục cấu hình Tomcat: Gán quyền sở hữu cho tài khoản tomcat_admin.tomcat; gỡ bỏ các quyền đọc, ghi, thực thi; gỡ bỏ quyền ghi đối với nhóm:

```
# chown tomcat_admin:tomcat $CATALINA_HOME/conf
# chmod g-w,o-rwx $CATALINA_HOME/conf
```

+ Giới hạn truy cập đến thư mục chứa các tập tin nhật ký (log): Gán quyền sở hữu cho tài khoản tomcat_admin:tomcat; gỡ bỏ các quyền đọc, ghi, thực thi:

```
# chown tomcat_admin:tomcat $CATALINA_HOME/logs
# chmod o-rwx $CATALINA_HOME/logs
```

+ Giới hạn truy cập đến thư mục chứa các tập tin thực thi: Gán quyền sở hữu cho tài khoản tomcat_admin:tomcat; gỡ bỏ các quyền đọc, ghi, thực thi:

```
# chown tomcat_admin:tomcat $CATALINA_HOME/bin
# chmod g-w,o-rwx $CATALINA_HOME/bin
```

+ Giới hạn truy cập đến thư mục chứa ứng dụng web: Gán quyền sở hữu cho tài khoản tomcat_admin:tomcat; gỡ bỏ các quyền đọc, ghi, thực thi:

```
# chown tomcat_admin:tomcat $CATALINA_HOME/webapps
# chmod g-w,o-rwx $CATALINA_HOME/webapps
```

+ Giới hạn truy cập đến tập tin context.xml: Gán quyền sở hữu cho tài khoản tomcat_admin:tomcat; gỡ bỏ các quyền đọc, ghi, thực thi; gỡ bỏ quyền ghi đối với nhóm:

```
# chown tomcat_admin:tomcat $CATALINA_HOME/conf/context.xml
# chmod g-w,o-rwx $CATALINA_HOME/conf/context.xml
```

+ Giới hạn truy cập đến tập tin logging.properties: Gán quyền sở hữu cho tài khoản tomcat_admin:tomcat; gỡ bỏ các quyền đọc, ghi, thực thi; gỡ bỏ quyền ghi đối với nhóm:

```
# chown tomcat_admin:tomcat $CATALINA_HOME/conf/logging.properties
# chmod g-w,o-rwx $CATALINA_HOME/conf/logging.properties
```

+ Giới hạn truy cập đến tập tin server.xml: Gán quyền sở hữu cho tài khoản tomcat_admin:tomcat; gỡ bỏ các quyền đọc, ghi, thực thi; gỡ bỏ quyền ghi đối với nhóm:

```
# chown tomcat_admin:tomcat $CATALINA_HOME/conf/server.xml
# chmod g-w,o-rwx $CATALINA_HOME/conf/server.xml
```

+ Giới hạn truy cập đến tập tin tomcat-users.xml: Gán quyền sở hữu cho tài khoản tomcat_admin:tomcat; gỡ bỏ các quyền đọc, ghi, thực thi; gỡ bỏ quyền ghi đối với nhóm:

```
# chown tomcat_admin:tomcat $CATALINA_HOME/conf/tomcat-users.xml
# chmod g-w,o-rwx $CATALINA_HOME/conf/tomcat-users.xml
```

+ Giới hạn truy cập đến tập tin web.xml: Gán quyền sở hữu cho tài khoản tomcat_admin:tomcat; gỡ bỏ các quyền đọc, ghi, thực thi; gỡ bỏ quyền ghi đối với nhóm:

```
# chown tomcat_admin:tomcat $CATALINA_HOME/conf/web.xml
# chmod g-w,o-rwx $CATALINA_HOME/conf/web.xml
```

3.4. Vận hành ứng dụng web an toàn

3.4.1. Kiểm tra hoạt động web an toàn

Để đảm bảo cho ứng dụng web vận hành an toàn, tránh được các nguy cơ tấn công từ bên ngoài hệ thống có thể tiến hành các bước cơ bản sau:

- Kiểm tra việc lộ thông tin nhạy cảm qua các công cụ tìm kiếm, bước này nhằm đảm bảo ứng dụng web sẽ không hiển thị các thông tin riêng như phiên bản, cấu trúc thư mục, v.v... lên kết quả của các công cụ tìm kiếm.

- Kiểm tra chức năng đăng xuất, đăng nhập có hoàn thành đúng nhiệm vụ hay không.

- Thiết đặt các quyền truy cập thích hợp vào các tập tin và thư mục nhạy cảm. Xóa các tập tin sao lưu dự phòng ra khỏi hệ thống.

- Sử dụng CAPTCHA và chế độ mật khẩu mạnh nhằm tránh trường hợp vượt qua CAPTCHA hay đoán được mật khẩu ngắn (không cho phép người dùng đặt mật khẩu yếu).

- Kiểm tra quá trình quản lý tài khoản và phiên của ứng dụng, việc truyền gửi những thông tin quan trọng như tên đăng nhập và mật khẩu cần được mã hóa nhằm tránh tình trạng nghe lén dữ liệu trên đường truyền. Bên cạnh đó việc cấp phát và mã hóa phiên đăng nhập cho người dùng cũng cần đảm bảo an toàn nhằm tránh tình trạng tin tặc đoán hay giả mạo phiên.

- Xác định loại mã nguồn hỗ trợ web (JSP, ASP, PHP,...) và kiểu framework phát triển web (mã nguồn mở, tự phát triển,...) để có biện pháp bảo vệ hợp lý cũng như cập nhật khắc phục các lỗ hổng được phát hiện.

- Xây dựng hoặc triển khai một hệ thống máy chủ Proxy dùng để chắc rằng các kết nối từ bên ngoài vào và từ bên trong ra sẽ được giám sát để tránh các mối đe dọa cũng như điều tra nguyên nhân khi hệ thống bị tấn công.

- Nếu có nhiều website được đặt chung trên máy chủ web, cần có biện pháp cách ly các website này ra, nhằm đảm bảo nếu có một website bị tấn công và chiếm quyền kiểm soát thì các website còn lại sẽ ít bị ảnh hưởng.

- Thiết kế trang báo lỗi chung để trả về cho tất cả các lỗi mà hệ thống có thể gặp phải. Biện pháp này nhằm giảm nguy cơ bị tấn công dựa theo thông báo lỗi của ứng dụng.

3.4.2. Khắc phục các lỗi phổ biến trên web

Trong trang web thường có các điểm cho người dùng nhập dữ liệu vào như mục "đăng nhập", mục "tìm kiếm", mục ID bài viết trên URL, v.v... Ngoài việc giúp cho người dùng dễ dàng tương tác với ứng dụng web, các mục này nếu không được quản lý chặt chẽ sẽ trở thành một nguy cơ lớn để thực hiện các cuộc tấn công vào ứng dụng web. Các dữ liệu bất hợp pháp nên được lọc trước để bỏ qua không đưa vào truy vấn trong cơ sở dữ liệu như các siêu ký tự, các biểu thức chính quy, các ký tự được mã hóa,... nhằm tránh cho ứng dụng trước những nguy cơ tấn công.

Có thể sử dụng biểu thức chính quy (áp dụng cho tất cả các ngôn ngữ lập trình) để thực hiện các công việc này. Ví dụ, sử dụng biểu thức chính quy để lọc các siêu ký tự:

```
w*((\|)|(\%7c)|(\<)|(\%3c)|(\%3e)|>|(`)|(\%60)|(&&)|(\%26\%26))
```

Hoặc để quy định giá trị mật khẩu nhập vào, ví dụ: cho phép mật khẩu từ 4 đến 8 ký tự gồm chữ thường và chữ hoa:

```
^(?=.*\d)(?=.*[a-z])(?=.*[A-Z]).{4,8}$
```

Cũng có thể sử dụng biểu thức chính quy để lọc tấn công Path Traversal:

```
\w*((\%5c)|(\/)|(\%2f)|(\\\))((\.\.)|(\%2e\%2e))
```

Hoặc lọc tấn công chia nhỏ hồi đáp HTTP (HTTP Response Splitting):

```
(((\%0d)+)((\%0a)+))+\w*(\:)
```

Trong số mười lỗi ATTT phổ biến trên cổng/trang TTĐT, mỗi lỗi sẽ có những biện pháp riêng để khắc phục như sau:

- *Tấn công Injection (bao gồm các kiểu tấn công như SQL* Injection, *OS Injection, LDAP Injection):*

  + Giới hạn quyền truy cập CSDL và phân quyền giữa các tài khoản người dùng, điều này giúp giảm khả năng khai thác CSDL của tin tặc ngay cả khi đã thực hiện thành công lệnh Injection.
  + Sử dụng thủ tục lưu trữ để đảm bảo các câu lệnh SQL từ ứng dụng được lưu trữ và triển khai ở máy chủ CSDL, điều này giúp cho dữ liệu do người dùng nhập vào không thể được tùy chỉnh dưới dạng một câu lệnh SQL. Để làm được điều này, ứng dụng phải được định dạng để sử dụng những thủ tục lưu trữ với giao diện an toàn như câu lệnh Callable của JDBC hay lệnh Object của ADO.
  + Sử dụng biểu thức chính quy để phát hiện tấn công SQL Injection:

Đối với các siêu ký tự:

```
(((\%3D)|(=))|((\%3C)|(\<))|((\%3D)|(\>)))[^\\n]*((\%27)|(\')|(\-\-)|(\%3B)|(;))
```

Với tấn công sử dụng từ khóa UNION:

```
((\%27)|(\'))(\W)*union
```

Với tấn công vào máy chủ MS SQL:

```
exec(\s|\+)+(s|x)p\w+
```

+ Sử dụng biểu thức chính quy để lọc tấn công LDAP Injection:

```
.(\)|\(|\||&)
```

- *Cross Site Scripting (XSS):*
  + Lọc tất cả các dữ liệu chưa tin tưởng một cách phù hợp dựa trên nội dung HTML.
  + Tạo một "danh sách trắng" để kiểm tra dữ liệu đầu vào một cách phù hợp.
  + Sử dụng biểu thức chính quy trong việc kiểm tra dữ liệu đầu vào để phát hiện tấn công XSS:

```
((\%3c)|<)[^\n]+((\%3e)|>)
```

- *Insecure Direct Object References (Tham chiếu trực tiếp đối tượng không an toàn):* Kiểm tra quá trình tham chiếu trực tiếp đến các tài nguyên hạn chế trên hệ thống để đảm bảo rằng người dùng bình thường không thể truy cập được các nguồn tài nguyên mà họ không có quyền truy cập. Nên sử dụng một cơ chế truy cập gián tiếp thay vì trực tiếp.

- *Cross Site Request Forgery (CSRF):* Việc ngăn chặn CSRF yêu cầu phải gộp những token không có khả năng đoán trước trong mỗi phiên giao dịch. Những token không những là duy nhất cho mỗi phiên người sử dụng mà còn duy nhất cho mỗi yêu cầu gửi đến ứng dụng.

- *Failure to Restrict URL Access (Thất bại trong việc hạn chế truy cập các URL quản trị):* Việc truy cập vào các URL có chức năng quản trị cần phải được kiểm tra thông qua quá trình xác thực và kiểm tra quyền của người dùng trước khi cho phép họ truy cập.

- *Bẻ gãy sự chứng thực và quản lý phiên:* Thiết đặt một phương pháp chứng thực và điều khiển phiên người sử dụng đủ mạnh để tránh khỏi bị những lỗi XSS mà có thể bị đánh cắp phiên sử dụng hoặc có thể giải mã phiên một cách dễ dàng.

- *Cấu hình bảo mật không an toàn:* Bảo mật một hệ thống nói chung phụ thuộc vào việc cấu hình bảo mật cho các thành phần riêng lẻ trong hệ thống như ứng dụng web, máy chủ web, hệ điều hành máy chủ, các thiết bị vật lý,... Tất cả các thiết đặt bảo mật này cần được xác định, thực hiện, bảo trì và tuyệt đối không nên sử dụng các cấu hình bảo mật mặc định có sẵn.

- *Chuyển hướng và chuyển tiếp không được kiểm tra:* Hạn chế sử dụng chuyển tiếp và chuyển hướng, nếu sử dụng thì phải có cơ chế chứng thực.

- *Lưu trữ mã hóa không an toàn:* Nhận biết nguy cơ và lên phương án bảo vệ đối với dữ liệu từ những tấn công bên trong hay bên ngoài, dữ liệu nhạy cảm phải luôn luôn mã hóa.

- *Thiếu sự bảo vệ lớp vận chuyển:* Cung cấp một cơ chế bảo vệ cho lớp vận chuyển bằng việc cấu hình SSL/TLS phù hợp.

3.5. Thiết đặt và cấu hình cơ sở dữ liệu an toàn

Việc thiết đặt và cấu hình cơ sở dự liệu an toàn là một quá trình phức tạp, đòi hỏi người quản trị phải hiểu rõ về cơ sở dữ liệu đang sử dụng. Để bảo vệ cho cơ sở dữ liệu an toàn cần thực hiện một số biện pháp sau:

- Luôn cập nhật phiên bản vá lỗi cho cơ sở dữ liệu mới nhất nhằm tránh các lỗi đã được công bố và khai thác.
- Gỡ bỏ các cơ sở dữ liệu không sử dụng.
- Gỡ bỏ hoặc vô hiệu hóa các thủ tục lưu trữ hoặc những hàm nhạy cảm có tương tác với hệ thống nhằm tránh việc tương tác đến hệ thống từ cơ sở dữ liệu.
- Tách biệt các cơ sở dữ liệu sử dụng cho mục các đích khác nhau.
- Khóa tất cả các kết nối từ hệ thống hoặc từ ứng dụng khác ngoài ứng dụng web và máy chủ web, không cho phép bất kỳ kết nối trực tiếp nào từ Internet đến database.
- Cấu hình ghi nhật ký và theo dõi nhật ký làm việc của cơ sở dữ liệu một cách hợp lý.
- Giới hạn truy cập đối với các tài khoản sử dụng (không có quyền xóa hoặc thay đổi cấu trúc cơ sở dữ liệu).
- Phân quyền cho các tài khoản và các tập tin hệ thống.
- Gỡ bỏ hoặc thay đổi các tài khoản mặc định và thiết lập mật khẩu mạnh cho các tài khoản đang sử dụng.
- Có cơ chế sao lưu dữ liệu và mã hóa các dữ liệu sao lưu.
- Sử dụng các công cụ để tìm kiếm lỗ hổng trên máy chủ SQL như MBSA (MS SQL).

3.6. Cài đặt các ứng dụng bảo vệ

3.6.1. Chống virus (Anti-Virus) và bảo vệ an toàn máy tính cá nhân

Việc cài đặt các ứng dụng bảo vệ như Anti-Virus có tác dụng rất lớn trong việc bảo vệ hệ thống. Chúng có thể hạn chế được việc bị cài thêm mã độc trong trường hợp kẻ tấn công đã xâm nhập được vào hệ thống, hoặc hạn chế việc

upload các mã độc khi ứng dụng web bị lỗi. Các chương trình Anti-Virus phải thỏa mãn yêu cầu sau:

- Luôn ở trạng thái đang hoạt động nhằm đảm bảo hệ thống luôn được bảo vệ.
- Đảm bảo tính toàn vẹn của tập tin và tài nguyên.
- Quét các mã độc đính kèm trong e-mail.
- Cập nhật dấu hiện nhận diện virus mới nhất.

Đối với máy tính cá nhân có thể xem xét cài đặt phần mềm bảo vệ an toàn máy tính tích hợp thường bao gồm cả chức năng chống virus, lọc tường lửa cá nhân. Xem Phụ lục 3 thông tin tham khảo về các phần mềm chống virus và bảo vệ an toàn máy tính cá nhân.

3.6.2. Hệ thống phát hiện xâm nhập máy tính (Host Based IDS)

Host Based IDS là hệ thống phát hiện xâm nhập máy tính (thường hay áp dụng đối với các máy chủ), đồng thời đưa ra cảnh báo về các hành động bất thường đối với tài nguyên trên hệ thống. Sử dụng Host Based IDS nhằm:

- Cảnh báo khi có sự thay đổi đối với mã nguồn ứng dụng.
- Cảnh báo khi có sự thay đổi đối với các tập tin hệ thống.
- Cảnh báo khi có sự thay đổi đối với các tập tin hệ thống.

3.7. Thiết lập cơ chế sao lưu và phục hồi

3.7.1. Cơ chế sao lưu

Sao lưu dữ liệu là điều kiện không thể thiếu khi triển khai các giải pháp kỹ thuật nhằm đảm bảo tính sẵn sàng của dữ liệu. Vì vậy khi thực hiện sao lưu cần xác định một số yêu cầu sau:

- *Phạm vi sao lưu:*

+ Sao lưu toàn bộ dữ liệu của hệ thống. Cơ chế này đảm bảo được tính toàn vẹn của dữ liệu và có thể phục hồi toàn bộ dữ liệu một cách nhanh chóng khi hệ thống bị sự cố. Tuy nhiên, đòi hỏi phải xây dựng một hệ thống sao lưu quy mô lớn.

+ Sao lưu từng phần riêng trong hệ thống. Cơ chế này nhằm phục hồi những phần gặp sự cố và không cần một hệ thống sao lưu quy mô lớn.

- *Thời gian sao lưu:*

Cần thiết lập một cơ chế sao lưu theo định kỳ (ngày, tuần, tháng,...) một cách tự động, nhằm đảm bảo việc sao lưu đầy đủ các dữ liệu theo yêu cầu.

- *Nội dung sao lưu:*

+ Sao lưu hệ điều hành máy chủ.

+ Sao lưu máy chủ web, Cơ sở dữ liệu, v.v...

+ Sao lưu thư mục và tập tin.

3.7.2. Cơ chế phục hồi

Tùy thuộc vào tình trạng hiện tại của hệ thống và cơ chế sao lưu đã được thiết lập mà lựa chọn cơ chế phục hồi dữ liệu cho hệ thống một cách thích hợp:

– Khôi phục nguyên trạng hệ thống.

– Khôi phục từng phần riêng biệt (hệ điều hành, cơ sở dữ liệu, các ứng dụng khác).

– Thường xuyên kiểm tra bản sao lưu để đảm bảo khả năng phục hồi thành công khi cần thiết.

4. ĐỐI PHÓ VỚI TẤN CÔNG TỪ CHỐI DỊCH VỤ

4.1 Tấn công từ chối dịch vụ:

- Tấn công từ chối dịch vụ (DoS) là kiểu tấn công vào hệ thống mạng bằng cách làm tăng đột biến lưu lượng băng thông, số lượng yêu cầu kết nối sử dụng dịch vụ vượt quá khả năng mà hệ thống có thể đáp ứng xử lý, dẫn đến dịch vụ của hệ thống hoạt động bị chậm, mất khả năng đáp ứng hoặc mất kiểm soát.

- Tấn công từ chối dịch vụ phân tán (DDoS) là dạng tấn công DoS nguy hiểm nhất khi nguồn tấn công nhiều và phân bố trên diện rộng trên mạng Internet toàn cầu, rất khó ngăn chặn triệt để. Thông thường các cuộc tấn công DDoS được gây ra bởi một số lượng khá lớn các máy tính trên mạng Internet bị điều khiển bởi tin tặc do nhiễm mã độc thường gọi là mạng botnet.

- Nguyên tắc chống tấn công DoS là cần phải lọc và gạt bỏ được các luồng tin tấn công, và tốt hơn nữa là ngăn chặn được các nguồn tấn công. Để chống DDoS phải vô hiệu hóa được hoạt động của các mạng botnet. Để làm được điều này một cách hiệu quả thường đòi hỏi các biện pháp điều phối ứng cứu sự cố ở quy mô quốc gia hay thậm chí phối hợp nhiều nước. Do đó khi phát hiện có các cuộc tấn công DoS hay DDoS, các đơn vị quản lý cổng/trang TTĐT cần báo cho Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) càng sớm càng tốt. Mặt khác, việc áp dụng các biện pháp và công cụ kỹ thuật tại chỗ để nâng cao năng lực bảo vệ các cổng/trang TTĐT cũng có hiệu quả rõ rệt.

4.2. Một số biện pháp kỹ thuật phòng chống tấn công từ chối dịch vụ:

- Tăng cường khả năng xử lý của hệ thống:
  + Tối ưu hóa các thuật toán xử lý, mã nguồn của máy chủ web,
  + Nâng cấp hệ thống máy chủ,

+ Nâng cấp đường truyền và các thiết bị liên quan,
+ Cài đặt đầy đủ các bản vá cho hệ điều hành và các phần mềm khác để phòng ngừa khả năng bị lỗi tràn bộ đệm, cướp quyền điều khiển, v.v...

- Hạn chế số lượng kết nối tại thiết bị tường lửa tới mức an toàn hệ thống cho phép.
- Sử dụng các tường lửa cho phép lọc nội dung thông tin (tầng ứng dụng) để ngăn chặn các kết nối nhằm tấn công hệ thống.
- Phân tích luồng tin (traffic) để phát hiện các dấu hiệu tấn công và cài đặt các tường lửa cho phép lọc nội dung thông tin (tầng ứng dụng) ngăn chặn theo các dấu hiệu đã phát hiện.

4.3. Một số công cụ kỹ thuật phòng chống tấn công từ chối dịch vụ:

Tùy khả năng đầu tư, các cổng/trang TTĐT có thể trang bị giải pháp hoặc sử dụng dịch vụ chống DoS/DDoS với các công cụ kỹ thuật sau:

- Sử dụng hệ thống thiết bị, phần mềm hoặc dịch vụ giám sát an toàn mạng (đặc biệt về lưu lượng) để phát hiện sớm các tấn công từ chối dịch vụ.
- Sử dụng thiết bị bảo vệ mạng có dịch vụ chống tấn công DDoS chuyên nghiệp kèm theo, ví dụ như: Arbor, Checkpoint, Imperva, Perimeter,...

PHỤ LỤC I. MƯỜI LỖI ATTT PHỔ BIẾN TRÊN CỔNG/TRANG TTĐT

1. ***Tấn công Injection***: bao gồm các lỗi cho phép thực hiện thành công các kiểu tấn công như SQL Injection, OS Injection, LDAP Injection. Kiểu tấn công này xảy ra khi người dùng gửi các dữ liệu không tin cậy đến ứng dụng web, những dữ liệu này có tác dụng như các câu lệnh với hệ điều hành hoặc các câu truy vấn với cơ sở dữ liệu nhằm phục vụ cho mục đích xấu.

2. ***Cross Site Scripting (XSS)***: Lỗi XSS xảy ra khi ứng dụng web nhận các dữ liệu độc hại và chuyển nó đến trình duyệt cho người dùng mà không xác nhận lại dữ liệu đó có hợp lệ hay không. Kiểu tấn công này cho phép kẻ tấn công thực thi các đoạn mã độc trong trình duyệt của nạn nhân và có thể cướp phiên người dùng hoặc chuyển hướng người dùng đến các trang độc hại khác.

3. ***Insecure Direct Object References (Tham chiếu trực tiếp đối tượng không an toàn)***: Việc tham chiếu xảy ra khi nhà phát triển ứng dụng web đưa ra tham chiếu đến một đối tượng bên trong ứng dụng như là một tập tin, một thư mục hay một khóa cơ sở dữ liệu. Nếu việc kiểm tra quá trình tham chiếu này không an toàn, kẻ tấn công có thể dựa theo để tham chiếu đến các dữ liệu mà họ không có quyền truy cập.

4. ***Cross Site Request Forgery (CSRF)***: là kiểu tấn công mà người dùng bị lợi dụng để thực thi những hành động không mong muốn ngay trên phiên đăng nhập của họ. Thông qua việc gửi người dùng một liên kết qua email hay chat, tin tặc có thể hướng người dùng thực thi một số hành động ngay trên trình duyệt của người dùng (như gửi bài viết, xóa bài viết, v.v...).

5. ***Failure to Restrict URL Access (Thất bại trong việc hạn chế truy cập các URL quản trị)***: Thông thường để vào được các đường dẫn quản trị thì ứng dụng phải kiểm tra người dùng có đủ quyền để truy cập vào đó hay không rồi mới hiển thị URL và các giao diện quản trị tương ứng khác. Để tránh tình trạng người dùng bình thường cũng truy cập vào các URL quản trị, mỗi lần truy cập vào các URL này cần được kiểm tra quyền kỹ càng, nếu không tin tặc có thể truy cập vào các URL này nhằm thực hiện các hành vi độc hại.

6. ***Bẻ gãy sự chứng thực và quản lý phiên***: Những chức năng của ứng dụng liên quan đến sự chứng thực và sự quản lý phiên làm việc thường không khởi tạo đúng, cho phép tin tặc tấn công mật khẩu, khóa và token của phiên làm việc hoặc khai thác lỗ hổng từ những sự khởi tạo này để gán định danh một người sử dụng khác.

7. ***Cấu hình bảo mật không an toàn***: là lỗi liên quan đến việc đặt cấu hình cho ứng dụng, framework, máy chủ web, ứng dụng máy chủ và platform sử dụng những giá trị thiết đặt mặc định hoặc khởi tạo và duy trì những giả trị không an toàn.

8. ***Chuyển hướng và chuyển tiếp không được kiểm tra***: Nhiều ứng dụng thường xuyên chuyển tiếp hoặc chuyển hướng người sử dụng đến những trang hoặc những website và sử dụng những dữ liệu chưa tin tưởng để xác định những trang đích. Không có sự kiểm tra phù hợp, tin tặc có thể chuyển hướng nạn nhân đến các trang giả mạo hoặc các trang có chứa mã độc, hoặc chuyển tiếp đến các trang web đòi làm thủ tục xác thực nhằm đánh cắp thông tin cá nhân.

9. ***Lưu trữ mã hóa không an toàn***: Ứng dụng web không có cơ chế bảo vệ hoặc tuy có cơ chế mã hóa và hashing (băm) dữ liệu để lưu trữ nhưng sử dụng không đúng cách đối với những dữ liệu quan trọng, như là thông tin thẻ tín dụng, thông tin cá nhân và những thông tin chứng thực. Do đó tin tặc có thể lợi dụng những kẽ hở này để đánh cắp những dữ liệu cần được bảo vệ.

10. ***Thiếu sự bảo vệ lớp vận chuyển***: Các ứng dụng không mã hóa dữ liệu khi truyền những thông tin quan trọng, hoặc nếu có mã hóa thì lại chỉ có thể sử dụng các chứng thực hết hạn hoặc không hợp lệ.

PHỤ LỤC 2. THÔNG TIN THAM KHẢO VỀ CÁC TƯỜNG LỬA

1. ***Firewall cứng***

+ Checkpoint (*http://www.checkpoint.com*)
+ Juniper (*http://www.juniper.net*)
+ Cisco (*http://www.cisco.com*)
+ Endian (*http://www.endian.com*)
+ Astaro (*http://www.astaro.com*)

2. ***Firewall mềm***

- Bản thương mại:
  + Microsoft Internet Security and Acceleration (ISA) Server (*http://www.microsoft.com*)
- Bản miễn phí (mã nguồn mở):
  + netfilter/iptables (*http://www.netfilter.org*)
  + pfSense (*http://www.pfsense.org*)
  + IPCop (*http://www.ipcop.org*)
  + Shorewall (*http://shorewall.net*)
  + SmoothWall (*http://www.smoothwall.org*)
  + Vyatta (*http://www.vyatta.org*)

3. ***Web Application Firewall (WAF)***

- Các phiên bản mã nguồn mở WAF phổ biến:
  + WebKnight (*http://www.aqtronix.com/?PageID=99*)
  + ModSecurity (*http://www.modsecurity.org*)
  + URLScan (*http://www.iis.net/download/urlscan*)
- Ngoài ra còn các bản WAF thương mại nổi tiếng sau:
  + Hyperguard (*http://www.artofdefence.com/en/products/hyperguard.html*)
  + WebDefend (*http://www.breach.com/products/webdefend.html*)
  + DotDefender (*http://www.applicure.com/*)
  + NetScaler application firewalls (*http://www.citrix.com*)
  + Eeye's SecureIIS (*http://www.eeye.com/Products/SecureIIS-Web-Server-Security.aspx*)
  + Appwall (*http://www.radware.com*)

ModSecurity: là phần mềm nguồn mở có thể hoạt động như một module trong máy chủ Apache hoặc là một thành phần độc lập. ModSecurity sử dụng biểu thức chính quy trong việc bảo vệ máy chủ web từ các cuộc tấn công được xác định trước dựa theo các dấu hiệu hoặc các cuộc tấn công bất thường khác. Bên cạnh đó, ModSecurity cũng có khả năng lọc các siêu ký tự do người dùng chèn vào ứng dụng web. Toàn bộ quá trình cài đặt và cấu hình có thể tham khảo thêm tại: *http://www.modsecurity.org/documentation*

URLScan: là một sản phẩm của Microsoft dành riêng cho các máy chủ web IIS. URL scan không chỉ bảo vệ máy chủ IIS 6 khỏi các điểm yếu từ các phiên bản cũ hơn mà còn cung cấp thêm các biện pháp bảo vệ khác như lọc dữ liệu mã hóa trên URL hoặc lọc các siêu ký tự do người dùng chèn vào để chống lại các loại tấn công như XSS, SQL Injection, v.v... Tham khảo cách cài đặt và sử dụng URLScan tại: *http://www.iis.net/download/urlscan*

PHỤ LỤC 3. THÔNG TIN THAM KHẢO VỀ CÁC PHẦN MỀM CHỐNG VIRUS VÀ BẢO VỆ AN TOÀN MÁY TÍNH CÁ NHÂN

1. ***Bản sản xuất trong nước:***

+ BKAV (*http://www.bkav.com.vn*)
+ CMC AntiVirus (*http://www3.cmcinfosec.com*)

2. ***Bản thương mại nước ngoài:***

+ AirScanner (*www.airscanner.com*)
+ BitDefender (*www.bitdefender.com*)
+ Computer Associates (*www.ca.com*)
+ F-Secure (*www.f-secure.com*)
+ Kaspersky (*www.kaspersky.com*)
+ McAfee (*www.mcafee.com*)
+ Symantec (*www.symantec.com*)
+ Trend Micro (*trendmicro.com*)
+ Avast (*www.avast.com*)
+ Avira (*www.avira.com*)

3. ***Bản miễn phí:***

+ Avast Free AntiVirus (*http://www.avast.com*)
+ Avira AntiVir Personal Free (*http://www.avira.com*)
+ Microsoft Security Essentials (*http://www.microsoft.com*)
+ Panda Cloud AntiVirus (*http://www.pandasecurity.com*)
+ Comodo Internet Security (*http://comodo.com*)
+ AVG AntiVirus (*http://www.free.avg.com*)

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: **29**/CATTT-TTTV
V/v cảnh báo chiến dịch tấn công lừa đảo thông qua các chương trình khuyến mại, giảm giá, tặng quà tri ân cho khách hàng

Hà Nội, ngày 24 tháng 01 năm 2018

Kính gửi:

- Đơn vị chuyên trách về CNTT các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn, Tổng công ty nhà nước; Các Ngân hàng TMCP; Các tổ chức tài chính.

Qua công tác giám sát và theo dõi tình hình, Cục An toàn thông tin đã phát hiện đang có nhiều chiến dịch tấn công lừa đảo nhắm vào người sử dụng Internet Việt Nam, đặc biệt là những người dùng mạng xã hội Facebook. Những chiến dịch lừa đảo này tạo ra hàng loạt trang web giả mạo các mạng xã hội, các ngân hàng, các cơ sở dịch vụ lớn, các chương trình trúng thưởng để thu thập thông tin cá nhân người sử dụng, các tài khoản mạng xã hội, các tài khoản ngân hàng, thẻ tín dụng .v.v…

Các đối tượng tấn công lợi dụng thời điểm cuối năm, cận tết Âm Lịch có nhiều chương trình khuyến mại, giảm giá, tặng quà tri ân cho khách hàng đồng thời tâm lý và thói quen mua sắm vội vàng cuối năm làm cho nhiều người dùng mất cảnh giác.

Cục An toàn thông tin đã phát hiện có ít nhất 700 tên miền được sử dụng để phục vụ cho các chiến dịch tấn công lừa đảo nói trên *(thông tin chi tiết về chiến dịch tấn công và một số tên miền phishing xin tham khảo tại Phụ lục kèm theo).*

Nhằm bảo đảm an toàn thông tin và phòng tránh nguy cơ bị tấn công lừa đảo, Cục An toàn thông tin khuyến nghị:

- Người dùng cần cảnh giác với những tin nhắn với các thông tin khuyến mãi, trúng thưởng, nhận thưởng. Không click vào bất cứ liên kết lạ nào được nhận từ tin nhắn trên facebook, kể cả từ các tài khoản bạn bè và người thân và các kênh tương tự như Zalo, Viber;

- Cảnh giác với những địa chỉ web lạ, gợi mở về việc nhận thưởng, trao giải. Trong trường hợp cần thiết, xin vui lòng liên hệ với chủ quản của nhãn hiệu đó để xác minh;

- Cập nhật mật khẩu tài khoản facebook, sử dụng các mật khẩu mạnh, chưa từng được sử dụng trước đó, bật tính năng xác thực 2 bước do facebook cung cấp;

- Không cung cấp tài khoản mạng xã hội, tài khoản ngân hàng, thông tin cá nhân hay các thông tin riêng khác trên bất kỳ trang web không chính thống nào;

- Trong trường hợp cần thiết, xin vui lòng liên hệ Cục An toàn thông tin, số điện thoại: 024.3943.6684, thư điện tử ais@mic.gov.vn hoặc fanpage Trung tâm xử lý tấn công mạng Internet Việt Nam theo đường dẫn https://www.facebook.com/govSOC/ để được hỗ trợ kịp thời.

Trân trọng./.

Nơi nhận:
- Như trên;
- Lãnh đạo Bộ (để b/c);
- Cục trưởng (để b/c);
- Lưu: VT, TTTV.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

Nguyễn Huy Dũng

Phụ lục

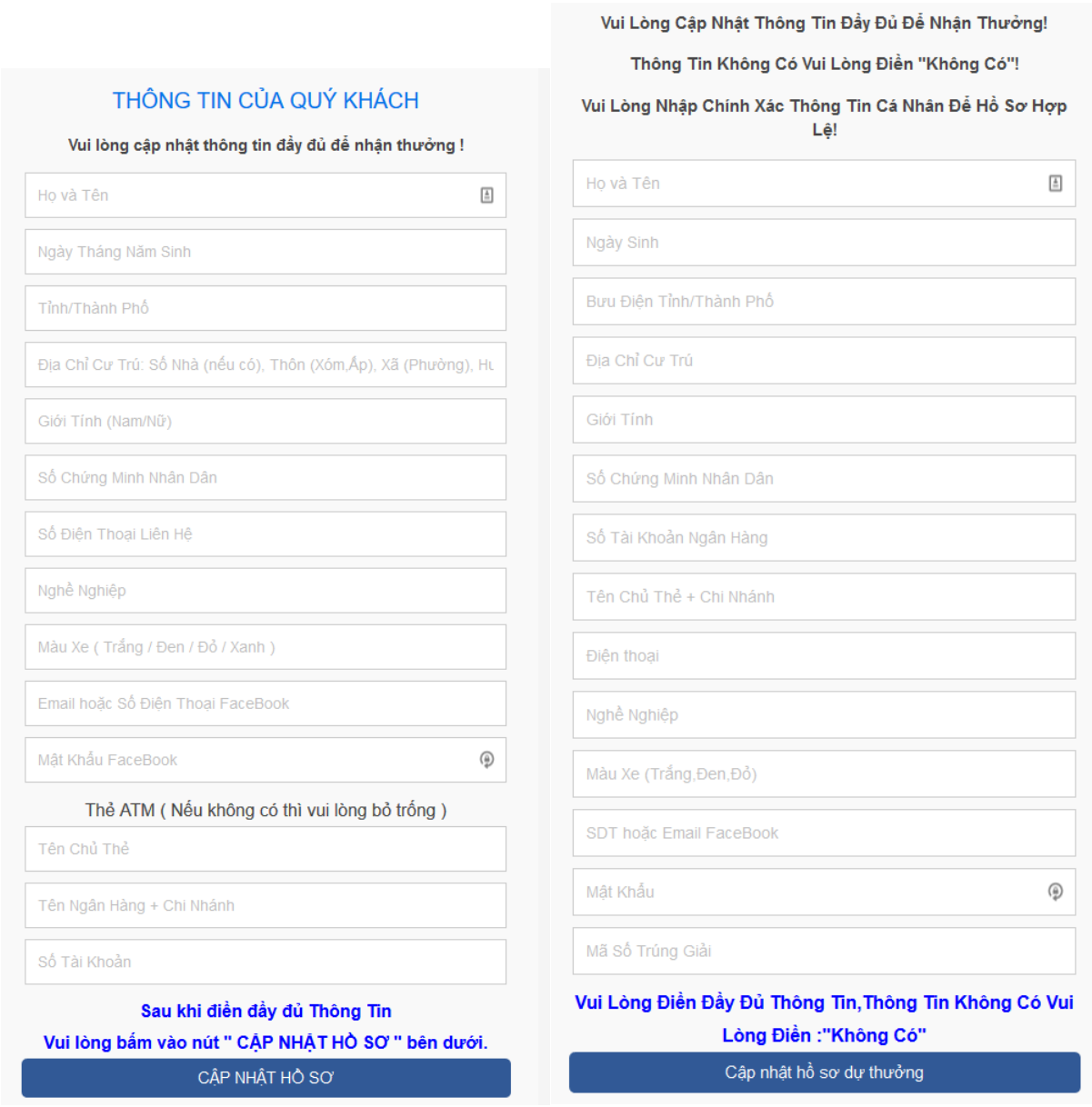
Chiến dịch tấn công lừa đảo thông qua các chương trình khuyến mại, giảm giá, tặng quà tri ân cho khách hàng

(Kèm theo Công văn số 29/CATTT-TTTV ngày 24/01/2018)

Qua công tác giám sát và theo dõi tình hình, Cục An toàn thông phát hiện đang có nhiều chiến dịch tấn công lừa đảo nhắm vào người sử dụng mạng Internet tại Việt Nam, đặc biệt là những người dùng mạng xã hội Facebook. Các chiến dịch lừa đảo này tạo ra hàng loạt trang web giả mạo các mạng xã hội, ngân hàng, nhà cung cấp dịch vụ lớn, các chương trình trúng thưởng để thu thập thông tin cá nhân, tài khoản mạng xã hội, tài khoản ngân hàng, thẻ tín dụng .v.v… của người sử dụng.

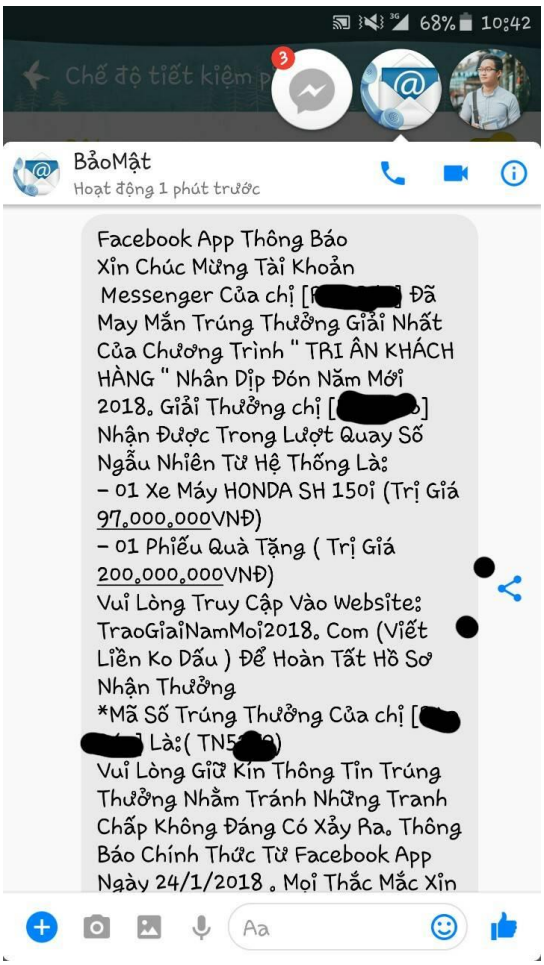
Một số hình ảnh sử dụng trong chiến dịch tấn công phishing

Các đối tượng tấn công lợi dụng thời điểm cuối năm, thời gian cận tết Âm lịch có nhiều chương trình khuyến mại, giảm giá, tặng quà tri ân cho khách hàng; đồng thời tâm lý và thói quen mua sắm vội vàng cuối năm làm cho nhiều người dùng mất cảnh giác.



Các trang web lừa đảo yêu cầu người dùng nhập thông tin cá nhân, thẻ ATM và mật khẩu Facebook

Các trang web lừa đảo được đối tượng tấn công lan truyền và quảng bá đến người dùng thông qua nhiều kênh khác nhau, trong đó kênh được sử dụng nhiều nhất hiện tại là Facebook Messenger. Để gia tăng sự tin tưởng của người dùng, các thông tin lừa đảo khi lan truyền còn được kèm theo các đoạn mã được quảng cáo là mã trúng thưởng.



Tấn công phishing lan truyền qua Facebook Messenger.

Cục An toàn thông tin đã phát hiện có ít nhất 700 tên miền được sử dụng để phục vụ cho các chiến dịch tấn công lừa đảo nói trên. Hầu hết các trang web đều sử dụng tên miền được đăng ký gợi mở đến chương trình trúng thưởng, trao giải như:

- hosofacebook.com
- hosofb68669.com
- hopqua2018.com
- nhanquatet2018.com
- nhanthuong2018.com
- traogiainammoi2018.com
- quacuoinam2018.com
- mochathuongtet2018.com

(Số lượng các trang web lừa đảo rất lớn sẽ được Cục ATTT cập nhật thường xuyên tại https://khonggianmang.vn/warn/phishing.txt)