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

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