BỘ Y TẾ
CỤC CÔNG NGHỆ THÔNG TIN

Số: 103 /CNTT-CSHT
V/v khuyến nghị một số biện pháp kỹ thuật để ngăn chặn thư điện tử giả mạo

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

Hà Nội, ngày 11 tháng 04 năm 2014

Kính gửi: - Văn phòng Bộ
- Các đơn vị trực thuộc Bộ Y tế
- Sở Y tế các tỉnh, thành phố trực thuộc Trung ương

Ngày 07 tháng 04 năm 2014, Cục Công nghệ thông tin nhận được công văn số 49/VNCERT-KTHT của trung tâm Ứng cứu khẩn cấp máy tính Việt nam (VNCERT) ngày 06 tháng 03 năm 2014 về việc khuyến nghị một số biện pháp kỹ thuật để ngăn chặn thư điện tử giả mạo. Để ngăn chặn các thư điện tử giả mạo của các đơn vị trong ngành Y tế, Cục Công nghệ thông tin đề nghị các đơn vị áp dụng các hướng dẫn theo công văn của VNCERT, Cụ thể:

1) Nghiên cứu tài liệu hướng dẫn phát hiện thư điện tử giả mạo kèm theo Công văn số 172/VNCERT-KTHT ngày 01/07/2013 của trung tâm VNCERT. Tài liệu trên có thể tải từ địa chỉ http://www.vncert.gov.vn.

2) Các đơn vị chỉ đạo cán bộ quản trị hệ thống thư điện tử nghiên cứu các khuyến nghị trong tài liệu hướng dẫn kèm theo công văn này để áp dụng các biện pháp kỹ thuật lọc và ngăn chặn thư điện tử giả mạo, phù hợp với điều kiện thực tế tại cơ quan, đơn vị.

3) Để công tác bảo vệ an toàn hệ thống thư điện tử được thực sự hiệu quả, và sát với tình hình thực thế, đề nghị các đơn vị trong ngành Y tế thông báo ngay cho Cục Công nghệ thông tin theo hướng dẫn tại công văn số 172/VNCERT-KHTT khi phát hiện thư rác, thư giả mạo để Cục làm đầu mối thông báo cho VNCERT.

Nếu có vấn đề nảy sinh trong quá trình thực hiện đề nghị các đơn vị liên hệ trực tiếp với Cục Công nghệ thông tin để nhận đươc hỗ trợ kỹ thuật./.

Xin trân trọng cảm ơn!

Nơi nhận:
- Như trên;
- TT. Lê Quang Cường (để b/c);
- Lưu: VT, CSHT

PHÓ CỤC TRƯỞNG PHỤ TRÁCH

CỤC CÔNG NGHỆ THÔNG TIN

Nguyễn Hoàng Phương

MỘT SỐ BIỆN PHÁP KỸ THUẬT ĐỂ NGĂN CHẶN THƯ ĐIỆN TỬ GIẢ MẠO CHO QUẢN TRỊ HỆ THỐNG

(Kèm theo công văn số 49/VNCERT-KTHT ngày 6/3/2014)

Qua công tác giám sát, Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) đã phát hiện gần đây trong các hệ thống thư điện tử của các cơ quan nhà nước xuất hiện nhiều thư điện tử giả mạo (có thể mạo danh người gửi là nhân viên, lãnh đạo hay những người nổi tiếng...) sử dụng nhiều kỹ thuật có chủ đích để qua mặt các bộ lọc thư rác nhằm phát tán thông tin sai lệch, phần mềm độc hại. Trung tâm VNCERT khuyến nghị các cơ quan, tổ chức áp dụng một số biện pháp kỹ thuật dưới đây để hạn chế tình trạng thư giả mạo tại máy chủ thư điện tử của cơ quan, tổ chức:

1. Sử dụng các công cụ phòng chống thư rác, thư giả mạo

Các công cụ phòng chống thư rác, thư giả mạo là thiết bị hoặc phần mềm có chức năng phát hiện, lọc và ngăn chặn các thư giả mạo được gửi đến hoặc gửi đi từ máy chủ thư điện tử. Đây là các công cụ không thể thiếu đối với các hệ thống thư điện tử trong công tác phòng chống thư rác và thư giả mạo. Công cụ này cho phép "xóa" hoặc "đánh dấu là thư rác" các thư điện tử dựa trên các bộ luật (rule) do quản trị hệ thống thiết lập. Trên thị trường hiện nay có một số sản phẩm phòng chống thư rác, thư giả mạo phổ biến như:

- Thiết bị phòng chống thư rác, thư giả mạo chuyên dụng: Bkav Antispam GW; Proventia Network Mail Security System; Mail Secure – PineApp; McAfee Email Gateway; Vade-Retro Email Security; Cisco Email Security Appliance v.v...
- Thiết bị tường lửa tích hợp có chức năng phòng chống thư rác của các hãng: Tường lửa Checkoint UTM, Fortinet, Cisco, Astaro v.v...
- Phần mềm phòng chống thư rác, thư giả mạo: Spam Assasin (phần mềm nguồn mở); Symantec Mail Security; GFI Mail Essentials; Lotus Protector for Mail Security v.v...

2. Thiết lập cấu hình cho công cụ phòng chống thư rác, thư giả mạo

Để hạn chế, ngăn chặn việc máy chủ thư điện tử nhận phải thư giả mạo, cần đặt cấu hình cho các công cụ phòng chống thư rác, thư giả mạo đáp ứng các yêu cầu sau đây:

- Đánh dấu thư rác đối với các thư điện tử gửi đến từ các địa chỉ IP nằm trong danh sách địa chỉ IP đen (Black List) do các tổ chức chống thư rác quốc tế có uy tín cung cấp (sbl.spamhaus.org, dnsbl.njabl.org, cbl.abuseat.org, bl.spamcop.net, dnsbl.sorbs.net v.v...).
- Đánh dấu thư rác với các thư điện tử có các bản ghi sau không hợp lệ: bản ghi MX; bản ghi PTR; bản ghi SPF; bản ghi DomainKeys Identified Mail (DKIM).

- Đánh dấu thư rác với các thư điện tử có chứa các dấu hiệu đặc trưng thu được khi phân tích thư giả mạo, thư rác đã nhận được (ví dụ: tên hòm thư, địa chỉ máy chủ thư, đoạn ký tự đặc biệt v.v...). Tuy nhiên biện pháp này dễ dẫn đến khả năng chặn nhầm. Do đó khi lựa chọn biện pháp này thì cần xác định thật rõ các dấu hiệu đặc trưng, duy nhất có thể phân biệt thư giả mạo và thư khác.

Chú ý: Khi áp dụng các chính sách lọc chặn thư điện tử giả mạo như trên, hệ thống thư điện tử có thể gặp phải một số trường hợp không mong muốn khi thư điện tử bình thường nhưng bị nhận dạng nhầm dẫn đến bị xóa hoặc gửi vào hòm thư rác, thường nguyên nhân do hai lý do chính sau: Máy chủ gửi thư điện tử không cấu hình đúng bản ghi MX, PTR hoặc SPF; Nội dung thư điện tử có dấu hiệu trùng lặp với dấu hiệu nhận diện thư rác đã được thiết lập. Có thể thực hiện xóa thư nếu tìm được các dấu hiệu chắc chắn cho phép phân biệt thư giả mạo và thư hợp lệ. Để hạn chế việc xóa hoặc đánh dấu nhầm thư điện tử hợp lệ, quản trị hệ thống cần thường xuyên theo dõi và kiểm tra tình hình để có biện pháp khắc phục, đồng thời đặt cấu hình hệ thống thư điện tử chuyển hướng thư rác cần xóa sang một hòm thư đặc biệt để phân tích trước khi xoá hoàn toàn.

3. Một số biện pháp quan trọng khác

3.1. Cấu hình đầy đủ và chính xác các bản ghi (DNS) phân giải tên miền và địa chỉ IP của máy chủ thư điện tử.

Việc cấu hình đầy đủ các bản ghi DNS dưới đây không giúp máy chủ thư điện tử của cơ quan, tổ chức lọc được thư giả mạo gửi đến nhưng giúp cho các máy chủ thư điện tử khác có thể lọc được các thư điện tử giả mạo địa chỉ của chính cơ quan, tổ chức của ta. Khi cấu hình tên miền (DNS) cần chú ý các bản ghi sau đây:

+ Bản ghi PTR: Đặt đúng giá trị tên miền của máy chủ thư điện tử. Việc này giúp phân giải địa chỉ IP ra tên miền được chính xác. Đồng thời hỗ trợ việc kiểm tra phân biệt thư hợp lệ và thư giả mạo được chính xác.

+ Bản ghi SPF: Đặt danh sách các địa chỉ IP được phép gửi thư theo tên miền của cơ quan, tổ chức. Người quản trị cần khai báo chính xác địa chỉ IP của máy chủ gửi thư điện tử để các hệ thống khác có thể loại trừ các địa chỉ IP gửi thư giả mạo địa chỉ của cơ quan. Cán bộ quản trị chú ý sử dụng tính năng "hard fail" ("-all") để loại bỏ tất cả các máy chủ khác gửi thư dưới tên miền của cơ quan.

+ Bản ghi DKIM: Đặt khoá công khai của máy chủ thư điện tử do chức năng DKIM của máy chủ thư điện tử tạo ra. Chức năng này thường chỉ có ở các phiên bản mới phát hành của hệ thống thư điện tử, chức năng này cho phép kiểm tra chính xác nguồn gốc máy chủ gửi thư dựa trên việc ứng dụng giải thuật mã hóa công khai (mã hóa bất đối xứng).

3.2. Thường xuyên theo dõi, kiểm tra tên miền và địa chỉ IP của máy chủ thư điện tử trên danh sách đen (Blacklist) các tổ chức chống thư rác để đảm bảo tên miền và địa chỉ IP không bị đưa vào danh sách địa chỉ đen. Một số tổ chức cung cấp chức năng

kiểm tra danh sách đen như: mxtoolsbox.com (http://mxtoolbox.com/blacklists.aspx), spamhaus (http://www.spamhaus.org/lookup/),DNSBL (http://www.dnsbl.info/). Nếu phát hiện địa chỉ IP hoặc tên miền của máy chủ thư điện tử bị lọt vào danh sách đen thì người quản trị cần liên hệ với các tổ chức chống thư rác để tìm hiểu nguyên nhân, xử lý và tìm cách đưa tên miền hoặc địa chỉ IP của cơ quan, tổ chức ra khỏi danh sách này.

3.3. Đào tạo kỹ năng và nâng cao nhận thức cho người dùng khi sử dụng thư điện tử, đặc biệt các vấn đề sau:

+ Đặt và quản lý an toàn mật khẩu thư điện tử,
+ Chỉ sử dụng các phương thức an toàn để truy cập hòm thư điện tử,
+ Phát hiện và báo cáo khi xuất hiện thư rác, thư giả mạo.

3.4. Cấp phát chữ ký số đến từng người sử dụng và sử dụng chữ ký số để ký thư điện tử trước khi gửi và kiểm tra thư điện tử khi nhận được. Đây là một trong các biện pháp an toàn nhất để phát hiện và phòng chống thư giả mạo.