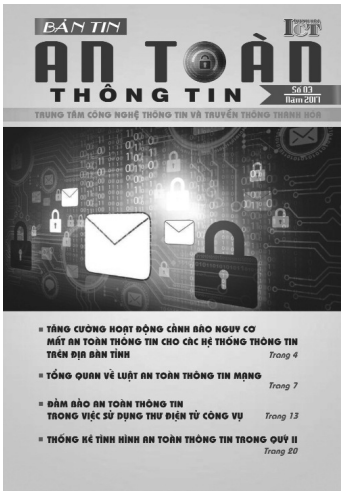
BẢN TIN
AN TOÀN THÔNG TIN
TRUNG TÂM CÔNG NGHỆ THÔNG TIN & TRUYỀN THÔNG THANH HÓA

Số 03
tháng 7/2017



CHỊU TRÁCH NHIỆM XUẤT BẢN
ThS. Lê Xuân Lâm
Giám đốc Trung tâm CNTT&TT
Thanh Hóa

BIÊN SOẠN
Cao Việt Cường; Trần Ngọc Hưng;
Trịnh Ngọc Quỳnh; Chúc Anh Hòa

THIẾT KẾ
Chung Nguyễn

TRUNG TÂM CÔNG NGHỆ THÔNG TIN
& TRUYỀN THÔNG THANH HÓA
Địa chỉ: 73 Hàng Than, TP Thanh Hóa
Điện thoại: 02373.718.298
Fax: 02373.718.299
Website: ict.thanhhoa.gov.vn
Giấy phép xuất bản số: 10/GP-XBBT
Sở TTTT Thanh Hóa cấp ngày 23/1/2017

In 500 cuốn, khổ 19x27cm
Tại Công ty TNHH In&TBGD Thanh Huệ
In xong và nộp lưu chiểu tháng 7/2017

Đ/c Phan Tâm, Thứ trưởng Bộ Thông tin và Truyền thông thăm quan hệ thống giám sát an toàn thông tin tại Trung tâm An ninh mạng và An toàn dữ liệu của tỉnh.

Tăng cường hoạt động cảnh báo nguy cơ mất an toàn thông tin cho các hệ thống thông tin trên địa bàn tỉnh

ThS. LÊ XUÂN LÂM
Giám đốc Trung tâm CNTT&TT Thanh Hóa

Ngày nay, với sự phát triển như vũ bão của khoa học công nghệ - đặc biệt là công nghệ thông tin, cùng với sự phổ dụng của mạng Internet, vấn đề bảo đảm an toàn, an ninh thông tin trên môi trường mạng cũng ngày càng trở nên cấp thiết. Tình hình an toàn thông tin mạng diễn biến phức tạp, xuất hiện nhiều nguy cơ đe dọa nghiêm trọng đến việc ứng dụng công nghệ thông tin để phát triển kinh tế - xã hội và đảm bảo quốc phòng, an ninh.

Tình hình mất an toàn thông tin mạng trong thời gian qua tiếp tục có những diễn biến phức tạp. Các cuộc tấn công mạng ở trong và ngoài nước đang gia tăng cả về quy mô, cường độ và mức độ tinh vi thì công tác bảo đảm an toàn, an ninh thông tin mạng của chúng ta lại đang bộc lộ một số bất cập về hạ tầng, nhân lực và nhận thức an toàn, an ninh thông tin. Đặc biệt

là trong các hệ thống thông tin, cổng/trang thông tin điện tử của các cơ quan nhà nước còn tồn tại nhiều điểm yếu và nguy cơ về mất an toàn thông tin, cùng với đó là nhận thức của một bộ phận không nhỏ cán bộ công chức, viên chức về an toàn thông tin còn chưa cao. Do đó, để phòng ngừa, giảm thiểu rủi ro về mất an toàn thông tin, đòi hỏi các cấp, các ngành cần có quan tâm đúng mực đến công tác cảnh báo sớm, xử lý ứng cứu sự cố đảm bảo an toàn thông tin cho các hệ thống thông tin. Trong đó hoạt động giám sát an toàn thông tin có một vai trò quan trọng, góp phần nâng cao năng lực đảm bảo an toàn thông tin, kịp thời phát hiện các cuộc tấn công mạng, phản ứng và đưa ra những cảnh báo kịp thời để qua đó có biện pháp khắc phục, ứng phó với những cuộc tấn công tiềm tàng và gây ra những hậu quả khó lường.

Nhận thức rõ vấn đề này, từ nhiều năm qua, Sở Thông tin và Truyền thông đã tham mưu cho UBND tỉnh triển khai nhiều giải pháp để đối phó với các nguy cơ gây mất an toàn, an ninh thông tin nói chung và công tác cảnh báo nói riêng. Với chức năng, nhiệm vụ được Chủ tịch UBND tỉnh, Giám đốc Sở Thông tin và Truyền thông giao trong vai trò là đầu mối tiếp nhận và xử lý ứng cứu sự cố máy tính nói chung và an toàn thông tin nói riêng; Trung tâm CNTT&TT (Trung tâm) luôn đề cao và triển khai tốt công tác phối hợp điều phối và cảnh báo sớm sự cố mất an toàn thông tin tới các cơ quan, tổ chức trên địa bàn tỉnh. Cụ thể như sau:

- Ngay từ đầu năm 2017, Trung tâm đã tham mưu cho Giám đốc Sở ban hành các văn bản nhằm tăng cường hoạt động hỗ trợ ứng cứu sự cố máy tính, đảm bảo an toàn thông tin cũng như xây dựng kế hoạch triển khai hoạt động phối hợp kiểm tra, rà soát, đánh giá đảm bảo an toàn thông tin cho các hệ thống thông tin và hỗ trợ ứng cứu sự cố trực tiếp tại các đơn vị như Công văn số 137/STTTT-CNTT, ngày 10/02/2017; Kế hoạch số 10/KH-TTCNTT&TT, ngày 16/01/2017 của Giám đốc Trung tâm... Qua công tác rà soát, đánh giá các điểm yếu, lỗ hổng có nguy cơ gây mất an toàn thông tin tại các hệ thống thông tin của các cơ quan, đơn vị trên địa bàn tỉnh. Trung tâm chủ động thực hiện các biện pháp và phương án khác nhau để qua đó triển khai công tác cảnh báo sớm tới các đơn vị để hạn chế tối đa các rủi ro do mất an toàn thông tin trên địa bàn tỉnh.

- Trung tâm đã kiện toàn về mặt tổ chức và ban hành quyết định về thành lập Tổ ứng cứu xử lý sự cố của Trung tâm với 08 thành viên là các cán bộ được đào tạo chuyên sâu về lĩnh vực an toàn thông tin trực tiếp thực hiện việc triển khai nhiệm vụ giám sát, cảnh báo và ứng cứu sự cố an toàn thông tin mạng cho các cơ quan, đơn vị trên địa bàn tỉnh. Việc thành lập Tổ ứng cứu sự cố máy tính là cần thiết nhằm nâng cao hiệu quả công tác an toàn thông tin mạng, nâng cao năng lực, đảm bảo chủ động sẵn sàng ứng phó, xử lý sự cố, giảm thiểu nguy cơ gây mất an toàn thông tin mạng trong cơ quan nhà nước trên địa bàn tỉnh, đúng theo tinh thần Thông tư số 27/2011/TT-BTTTT, ngày 03/10/2011 của Bộ Thông tin và Truyền thông quy định về điều phối các hoạt động ứng cứu sự cố mạng Internet Việt Nam.

- Tại Trung tâm An ninh mạng và An toàn dữ liệu của tỉnh do Trung tâm quản lý và vận hành, đã triển khai nhiều giải pháp kỹ thuật, xây dựng các hệ thống phần mềm để chủ động trong việc giám sát và cảnh báo các dấu hiệu, nguy cơ gây mất an toàn thông tin trên các hệ thống thông tin trên địa bàn tỉnh cũng như với các ứng dụng dùng chung trên địa bàn như phần mềm Quản lý văn bản và hồ sơ công việc; các phần mềm chuyên ngành, các trang/cổng thông tin điện tử của các cơ quan, đơn vị... Đồng thời phân công cán bộ trực 24/24 trong ngày để sẵn sàng ứng cứu các sự cố máy tính, an toàn thông tin và an ninh mạng.

- Tại Trung tâm An ninh mạng và An toàn dữ liệu của tỉnh do Trung tâm quản lý và vận hành, đã triển khai nhiều giải pháp kỹ thuật, các phương án khắc phục và quy trình xử lý sự cố. Bên cạnh đó bổ sung các trang thiết bị, phần mềm an ninh một cách đồng bộ về giải pháp để chủ động trong việc giám sát và cảnh báo các dấu hiệu, nguy cơ gây mất an toàn thông tin trên các hệ thống thông tin trên địa bàn tỉnh cũng như với các ứng dụng dùng chung trên địa bàn như phần mềm Quản lý văn bản và hồ sơ công việc; các phần mềm chuyên ngành, các

trang/cổng thông tin điện tử của các cơ quan, đơn vị... Đồng thời phân công cán bộ trực 24/24 trong ngày để sẵn sàng ứng cứu các sự cố máy tính, an toàn thông tin và an ninh mạng.

- Phối hợp và thiết lập kênh thông tin liên lạc thường xuyên với các đầu mối của Cục An toàn thông tin, Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) và các đơn vị liên quan để tiếp nhận cảnh bảo, điều phối và xử lý sự cố an toàn thông tin kịp thời trên địa bàn tỉnh. Đồng thời kết nối thường xuyên, liên tục với các đầu mối ứng cứu sự cố của các cơ quan, đơn vị trên địa bàn tỉnh. Để qua đó hình thành mạng lưới đảm bảo sự phối hợp ngăn chặn, xử lý kịp thời và khắc phục nhanh chóng các sự cố mất an toàn thông tin.

Lãnh đạo Trung tâm trực tiếp chỉ đạo Tổ Ứng cứu sự cố trong việc hỗ trợ, xử lý sự cố mã độc WannaCry cho các cơ quan, đơn vị trên địa bàn tỉnh.

Với những hoạt động trên, bình quân hàng năm Trung tâm thực hiện ứng cứu khoảng 600 lượt sự cố, ban hành 20 lượt văn bản cảnh báo sớm các sự cố gây mất an toàn thông tin. Trong năm 2016, đã thực hiện ứng cứu gần 400 lượt sự cố liên quan đến phần mềm ứng dụng, các trang thông tin điện tử và sự cố thông tin khác; thực hiện hỗ trợ ứng cứu sự cố máy tính, đảm bảo an toàn thông tin trực tiếp cho gần 20 đơn vị; cảnh báo và phối hợp xử lý kịp thời trang Website của một số cơ quan nhà nước; ghi nhận và hỗ trợ xử lý sự cố cho gần 10 đơn vị trên địa bàn tỉnh đã bị lây nhiễm mã độc trong hệ thống thông tin của đơn vị. Đặc biệt, trong những ngày trước, trong và sau các sự kiện lớn như Đại hội tỉnh Đảng bộ lần thứ XVIII, Đại hội Đảng toàn quốc lần thứ XII; dịp tết Nguyên đán; Bầu cử Đại biểu Quốc hội khóa XIV và bầu cử Đại biểu Hội đồng nhân dân các cấp, nhiệm kỳ 2016-2021, Trung tâm đã tăng cường cán bộ trực, theo dõi giám sát hệ thống để kịp thời phát hiện các dấu hiệu mất an toàn thông tin mạng nhằm giảm thiểu, không xảy ra các vụ phá hoại, sự cố gây lỗi, sai lệch thông tin phục vụ quản lý, điều hành của các cơ quan trên địa bàn. Qua đó, bước đầu đã có những chuyển biến tích cực trong việc giảm thiểu các rủi ro, nguy cơ gây mất an toàn thông tin tại các cơ quan, đơn vị trên địa bàn tỉnh. Tuy nhiên, với tình hình diễn biến phức tạp về mất an toàn thông tin hiện nay để hoạt động giám sát và cảnh báo nguy cơ gây mất an toàn thông tin được triển khai hiệu quả hơn nữa trong thời gian tới. Trung tâm đề xuất một số giải pháp như sau:

Một là, tiếp tục đẩy mạnh công tác quản lý nhà nước về an toàn thông tin trên địa bàn tỉnh. Tăng cường tuyên truyền, phổ biến, quán triệt các chủ trương, đường lối của Đảng, các chính sách, quy định của Chính phủ và của tỉnh trong hoạt động ứng dụng và phát triển CNTT. Đặc biệt là việc triển khai Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan quản lý nhà nước tỉnh Thanh Hóa theo quyết định số 1293/2017/QĐ-UBND ngày 25/4/2017 của UBND tỉnh Thanh Hóa. Để qua đó tạo được sự chuyển biến sâu sắc trong nhận thức của các cơ quan, đơn vị về tầm quan trọng của công

tác bảo đảm an toàn, an ninh mạng.

Hai là, sớm triển khai các nội dung trong Quyết định 05/2017/QĐ-TTg của Thủ tướng Chính phủ quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia như kiện toàn và bổ sung chức năng nhiệm vụ cho Ban chỉ đạo ứng dụng công nghệ thông tin của tỉnh đảm nhiệm chức năng Ban chỉ đạo ứng cứu khẩn cấp sự cố an toàn thông tin mạng trên địa bàn tỉnh; Kiện toàn tổ chức hoặc thành lập Đội ứng cứu sự cố;... Để qua đó xây dựng một hệ thống phương án ứng cứu khẩn cấp đồng bộ và toàn diện để có thể phối hợp ngăn chặn và phòng ngừa các nguy cơ tấn công mạng có thể xảy ra bất cứ lúc nào.

Ba là, cần quan tâm đầu tư trang thiết bị, giải pháp đồng bộ phục vụ công tác giám sát và cảnh báo sự cố mất an toàn thông tin trên địa bàn tỉnh. Đặc biệt, cần đầu tư hệ thống giám sát an toàn thông tin cho phép thu thập, chuẩn hóa, lưu trữ và phân tích tương quan toàn bộ thông tin về các sự kiện an toàn phát sinh trong hệ thống thông tin của các cơ quan, đơn vị trên địa bàn tỉnh. Thông qua hệ thống giám sát sẽ phát hiện kịp thời các tấn công mạng, xác định được các điểm yếu, lỗ hổng bảo mật của các thiết bị, ứng dụng và dịch vụ trong hệ thống. Đồng thời là giải pháp hữu hiệu hỗ trợ cho các chuyên gia phân tích, xử lý các sự kiện, cảnh báo tấn công đang xảy ra đối với hệ thống, thông qua những phân tích và xử lý để kịp thời đưa ra biện pháp ứng phó, giảm thiểu các tấn công vào hệ thống.

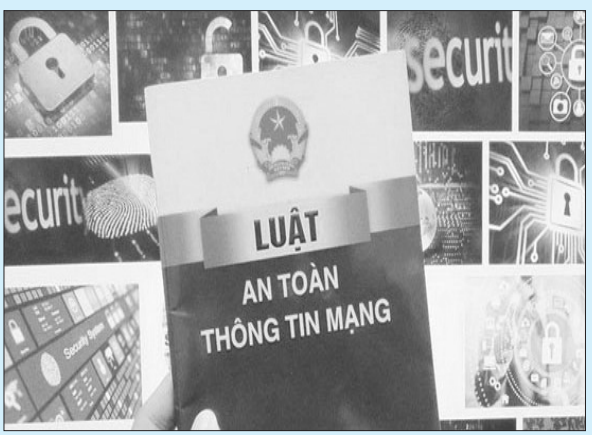
Bốn là, cần xây dựng đội ngũ cán bộ chuyên trách công nghệ thông tin phụ trách về công tác đảm bảo về an toàn, an ninh thông tin đủ trình độ chuyên môn và kỹ thuật, nghiệp vụ; đặc biệt là nâng cao đạo đức công vụ trong việc quản lý thông tin nội bộ, bí mật nhà nước... Khi có sự cố hoặc nguy cơ gây mất an toàn thông tin, thủ trưởng đơn vị có trách nhiệm chỉ đạo kịp thời, áp dụng mọi biện pháp để khắc phục và hạn chế thấp nhất mức thiệt hại có thể xảy ra trong đơn vị mình, góp phần giữ vững ổn định chính trị, phát triển kinh tế - xã hội của tỉnh trong thời gian tới./.

Tổng quan về Luật an toàn thông tin mạng

NGUYỄN THỊ THU HÀ
Phòng Quản lý CNTT, Sở TT&TT

Ngày 19/11/2015, trong phiên họp toàn thể tại hội trường của kỳ họp thứ 10 Quốc hội khóa XIII, đại biểu Quốc hội đã biểu quyết thông qua Luật An toàn thông tin mạng với 424/425 đại biểu có mặt tán thành. Luật An toàn thông tin mạng sẽ chính thức có hiệu lực thi hành kể từ ngày 1/7/2016.

Mục tiêu chính của Luật An toàn thông tin mạng được ban hành sẽ hướng đến giải quyết các yêu cầu về An toàn thông tin mạng quốc gia, qua đó góp phần hoàn thiện cơ sở pháp lý về An toàn thông tin mạng theo hướng áp dụng các quy định pháp luật đồng bộ, khả thi trong thực tiễn thi hành và phát huy các nguồn lực của đất nước để bảo đảm An toàn thông tin mạng, phát triển lĩnh vực An toàn thông tin mạng đáp ứng yêu cầu phát triển KT-XH và bảo đảm quốc phòng, an ninh, góp phần nâng cao chất lượng cuộc sống của nhân dân; bảo vệ quyền và lợi ích hợp pháp của tổ chức, cá nhân tham gia hoạt động ATTTM; đẩy mạnh công tác giám sát, phòng, chống nguy cơ mất ATTTM, đảm bảo hiệu quả công tác thực thi quản lý nhà nước trong lĩnh vực ATTTM; mở rộng hợp tác quốc tế



về ATTTM trên cơ sở tôn trọng độc lập, chủ quyền, bình đẳng, cùng có lợi, phù hợp với luật pháp Việt Nam và điều ước quốc tế mà Việt Nam tham gia ký kết.

1. Về nội dung chính của Luật An toàn thông tin mạng:

Luật An toàn thông tin mạng gồm 8 Chương, 54 Điều, quy định về hoạt động an toàn thông tin mạng (ATTTM), quyền và trách nhiệm của cơ quan, tổ chức, cá nhân trong việc bảo đảm ATTTM; mật mã dân sự; tiêu chuẩn; quy chuẩn kỹ thuật về ATTTM; kinh doanh trong lĩnh vực ATTTM; phát triển nguồn nhân lực ATTTM; quản lý nhà nước về ATTTM.

Chương I. Những quy định chung: Quy định phạm vi điều chỉnh; đối tượng áp dụng; giải thích từ ngữ; nguyên tắc bảo đảm an toàn thông tin mạng; chính sách của Nhà nước về an toàn thông tin mạng; hợp tác quốc tế về an toàn thông tin mạng; các hành vi bị nghiêm cấm; xử lý vi phạm pháp luật về an toàn thông tin mạng

Chương II. Bảo đảm an toàn thông tin mạng, bao gồm 04 mục:

+ Mục 1. Bảo vệ thông tin mạng: quy định về phân loại thông tin; quản lý gửi thông tin; phòng ngừa, phát hiện, ngăn chặn và xử lý phần mềm độc hại; bảo đảm an toàn tài nguyên viễn thông; ứng cứu sự cố an toàn thông tin mạng; ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia; trách nhiệm của cơ quan, tổ chức, cá nhân trong bảo đảm an toàn thông tin mạng.

+ Mục 2. Bảo vệ thông tin cá nhân: quy định về nguyên tắc bảo vệ thông tin cá nhân trên mạng; thu thập và sử dụng thông tin cá nhân; cập nhật, sửa đổi và hủy bỏ thông tin cá nhân; bảo đảm an toàn thông tin cá nhân trên mạng; trách nhiệm của cơ quan quản lý nhà nước trong bảo vệ thông tin cá nhân trên mạng.

Thứ trưởng Bộ TT&TT Nguyễn Thành Hưng phát biểu khai mạc Hội nghị.

+ Mục 3. Bảo vệ hệ thống thông tin: quy định về phân loại cấp độ an toàn hệ thống thông tin; nhiệm vụ bảo vệ hệ thống thông tin; biện pháp bảo vệ hệ thống thông tin; giám sát an toàn hệ thống thông tin; trách nhiệm của chủ quản hệ thống thông tin; hệ thống thông tin quan trọng quốc gia; trách nhiệm bảo đảm an toàn thông tin mạng cho hệ thống thông tin quan trọng quốc gia.

+ Mục 4. Ngăn chặn xung đột thông tin mạng: quy định về trách nhiệm của tổ chức, cá nhân trong việc ngăn chặn xung đột thông tin trên mạng; ngăn chặn hoạt động sử dụng mạng để khủng bố.

Chương III. Mật mã dân sự: Quy định về sản phẩm, dịch vụ mật mã dân sự; kinh doanh sản phẩm, dịch vụ mật mã dân sự; trình tự, thủ tục đề nghị cấp Giấy phép kinh doanh sản phẩm, dịch vụ mật mã dân sự; sửa đổi, bổ sung, cấp, gia hạn, tạm đình chỉnh và thu hồi Giấy phép kinh doanh sản phẩm, dịch vụ mật mã dân sự; xuất khẩu, nhập khẩu sản phẩm mật mã dân sự; trách nhiệm của doanh nghiệp kinh doanh sản phẩm, dịch vụ mật mã dân sự và trách nhiệm của tổ chức, cá nhân sử dụng sản phẩm, dịch vụ mật mã dân sự.

Chương IV. Tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng: Quy định về tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng; quản lý tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng; đánh giá hợp chuẩn, hợp quy về an toàn thông tin mạng.

Chương V. Kinh doanh trong lĩnh vực an toàn thông tin mạng, bao gồm 02 mục:

+ Mục 1. Quy định về cấp Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng gồm: kinh doanh

trong lĩnh vực an toàn thông tin mạng; sản phẩm dịch vụ trong lĩnh vực an toàn thông tin mạng; điều kiện cấp Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng; hồ sơ đề nghị cấp Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng; thẩm định hồ sơ và Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng; sửa đổi, bổ sung, gia hạn, tạm đình chỉ, thu hồi và cấp lại Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng; trách nhiệm của doanh nghiệp kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng.

+ Mục 2. Quy định về quản lý nhập khẩu sản phẩm an toàn thông tin mạng gồm: nguyên tắc quản lý nhập khẩu sản phẩm an toàn thông tin mạng; sản phẩm nhập khẩu theo giấy phép trong lĩnh vực an toàn thông tin mạng.

Chương VI. Phát triển nguồn nhân lực an toàn thông tin mạng: Quy định về đào tạo, bồi dưỡng nghiệp vụ về an toàn thông tin mạng; văn bằng, chứng chỉ đào tạo về an toàn thông tin mạng.

Chương VII. Quản lý nhà nước về an toàn thông tin mạng: Quy định về nội dung quản lý nhà nước về an toàn thông tin mạng; trách nhiệm quản lý Nhà nước về an toàn thông tin mạng. Trong đó, quy định rõ trách nhiệm của Bộ Thông tin và Truyền thông, Bộ Quốc phòng, Ban Cơ yếu Chính phủ, Bộ Công an và các Bộ, cơ quan ngang Bộ, UBND tỉnh, thành phố trực thuộc Trung ương trong phạm vi nhiệm vụ, quyền hạn của mình thực hiện quản lý nhà nước về an toàn thông tin mạng.

Chương VIII. Điều khoản thi hành: Quy định về thời điểm có hiệu lực của Luật an toàn thông tin mạng kể từ ngày 01/7/2016, Chính phủ, cơ quan nhà nước có thẩm quyền quy định chi tiết các điều, khoản được giao trong Luật.

2. Triển khai Luật An toàn thông tin mạng

Ngày 13/4/2016, tại Hà Nội, Bộ Thông tin và Truyền thông (Bộ TT&TT) đã tổ chức Hội nghị phổ biến Luật An toàn thông tin mạng (ATTTM) nhằm quán triệt tinh thần, nội dung của bộ Luật này tới các cơ quan, tổ chức hoạt động trong lĩnh vực an toàn thông tin.

Phát biểu khai mạc Hội nghị, Thứ trưởng Bộ TT&TT Nguyễn Thành Hưng nhấn mạnh: "Luật ATTTM là bước khởi đầu để hoàn thiện khung pháp luật về an toàn thông tin một cách đồng bộ, khả thi; Phát huy tối đa các nguồn lực để bảo đảm an toàn thông tin mạng; Bảo vệ quyền và lợi ích hợp pháp của tổ chức, cá nhân; Đáp ứng yêu cầu phát triển kinh tế xã hội, quốc phòng, an ninh".

Thứ trưởng cũng cho biết, để triển khai hiệu quả các quy định của Luật ATTTM, Bộ TT&TT theo thẩm quyền sẽ chủ trì xây dựng các văn bản dưới luật và hướng dẫn triển khai. Song song với đó là trách nhiệm phổ biến các quy định của Luật tới các cơ quan, tổ chức, cá nhân, là đối tượng thực thi và áp dụng luật trên toàn quốc, sao cho phải hiểu đúng và áp dụng đúng văn bản quy phạm.

Danh sách các văn bản dưới Luật An toàn thông tin mạng, bao gồm:

+ Nghị định 58/2016/NĐ-CP ngày 01/7/2016 quy định chi tiết về kinh doanh sản phẩm, dịch vụ mật mã dân sự và xuất khẩu, nhập khẩu sản phẩm mật mã dân sự.

+ Nghị định 142/2016/NĐ-CP ngày 14/10/2016 quy định về ngăn chặn xung đột thông tin trên mạng.

+ Nghị định 101/2016/NĐ-CP ngày 01/7/2016 quy định chi tiết trách nhiệm thực hiện và các biện pháp ngăn chặn hoạt động sử dụng không gian mạng để khủng bố.

+ Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

+ Nghị định số 108/2016/NĐ-CP ngày 01/7/2016 của Chính phủ quy định chi tiết điều kiện kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng.

+ Quyết định số 05/2017/NĐ-CP ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia.

+ Thông tư số 03/2017/TT-BTTTT ngày 24/04/2017 quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ.

+ Quyết định số 632/QĐ-TTg ngày 10/05/2017 Ban hành Danh mục lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng và hệ thống thông tin quan trọng quốc gia./.

Hướng dẫn sử dụng và khai thác phần mềm hỗ trợ ứng cứu sự cố TRÊN MÔI TRƯỜNG MẠNG

HOÀNG ANH TUẤN
Trung tâm CNTT&TT Thanh Hóa

Phần mềm hỗ trợ ứng cứu sự cố được xây dựng để triển khai nhiệm vụ hỗ trợ, tổng hợp các sự cố về máy tính, mạng, hệ thống công nghệ thông tin nói chung cũng như các sự cố về an toàn thông tin nói riêng tại các đơn vị, cơ quan trên địa bàn tỉnh Thanh Hóa.

Phần mềm được triển khai trực tuyến trên môi trường mạng Internet, cung cấp tài khoản truy cập vào phần mềm cho các đầu mối là cán bộ được giao phụ trách công nghệ thông tin tại các cơ quan, đơn vị để qua đó thiết lập kênh tiếp nhận các yêu cầu cần hỗ trợ xử lý các sự cố tới Tổ ứng cứu sự cố của Trung tâm CNTT&TT.

Thông qua phần mềm này, các cán bộ được giao phụ trách công nghệ thông tin có thể nhanh chóng gửi các thông tin đề nghị xử lý sự cố một cách nhanh chóng và thuận lợi. Đặc biệt, đối với các sự cố có tính chất phức tạp cần phải bổ sung liên tục các thông tin liên quan đến sự cố như các tệp hình ảnh, nhật ký, mẫu mã độc...Thông qua phần mềm này các cán bộ cũng có thể tham khảo các sự cố diễn ra tại đơn vị khác cũng như phương án, kết quả xử lý sự cố để qua đó điều chỉnh, triển khai các biện pháp để hạn chế các rủi ro có thể diễn ra tại hệ thống thông tin của đơn vị mình.

Các chức năng chính của phần mềm bao gồm:

- Chức năng tổng hợp các văn bản liên quan đến cảnh báo về an toàn thông tin từ Trung ương đến địa phương.

- Chức năng Phiếu yêu cầu xử lý sự cố: Bao gồm các tính năng liên quan đến việc gửi, tiếp nhận, xử lý và phản hồi kết quả xử lý sự cố. Bên cạnh đó còn hỗ trợ việc tìm kiếm, thống kê các sự cố trong phạm vi toàn tỉnh.

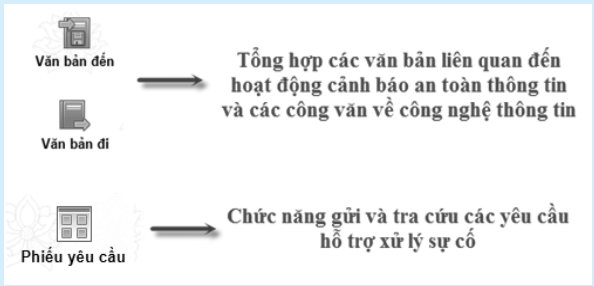
Thông tin truy cập phần mềm

Phần mềm được truy cập thông qua địa chỉ trên mạng Internet tại địa chỉ:

http://ungcuusuco.thanhhoaict.gov.vn

Giao diện phần mềm sau khi đăng nhập:

Các chức năng chính như sau:

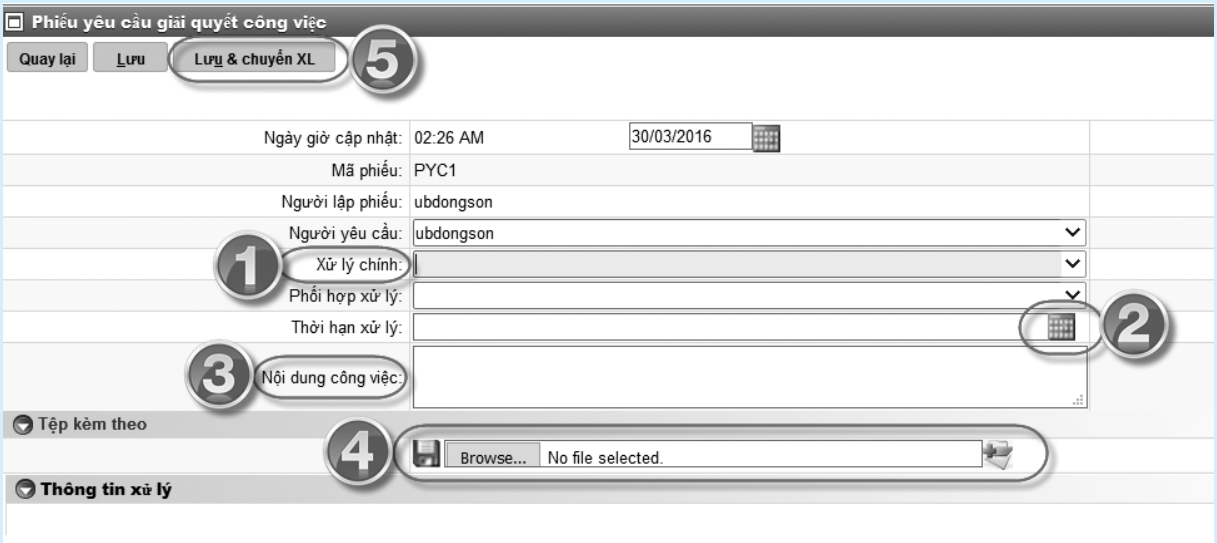


a) Chức năng tổng hợp các văn bản liên quan đến cảnh báo về an toàn thông tin từ Trung ương đến địa phương. Truy cập vào mục "Văn bản đến" hoặc "Văn bản đi" để tìm kiếm văn bản theo các tiêu chí khác nhau

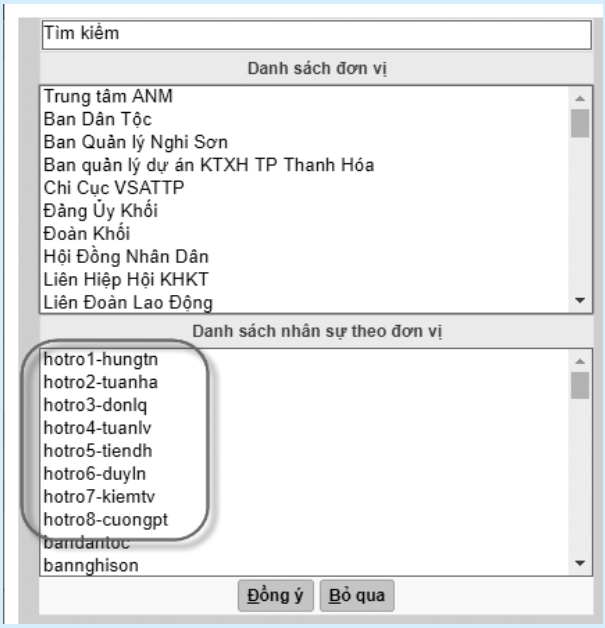
b) Chức năng Phiếu yêu cầu xử lý sự cố: Bao gồm các tính năng liên quan đến việc gửi, tiếp nhận, xử lý và phản hồi kết quả xử lý sự cố. Bên cạnh đó còn hỗ trợ việc tìm kiếm, thống kê các sự cố trong phạm vi toàn tỉnh.

Tạo mới phiếu yêu cầu:

- Sau khi lựa chọn chức năng "Nhập mới PYC"; điền đầy đủ các thông tin như hình dưới đây:



(1) Xử lý chính: Lựa chọn trong danh sách hiển thị, bao gồm các thành viên trong tổ ứng cứu sự cố có tên trong danh sách hiển thị:



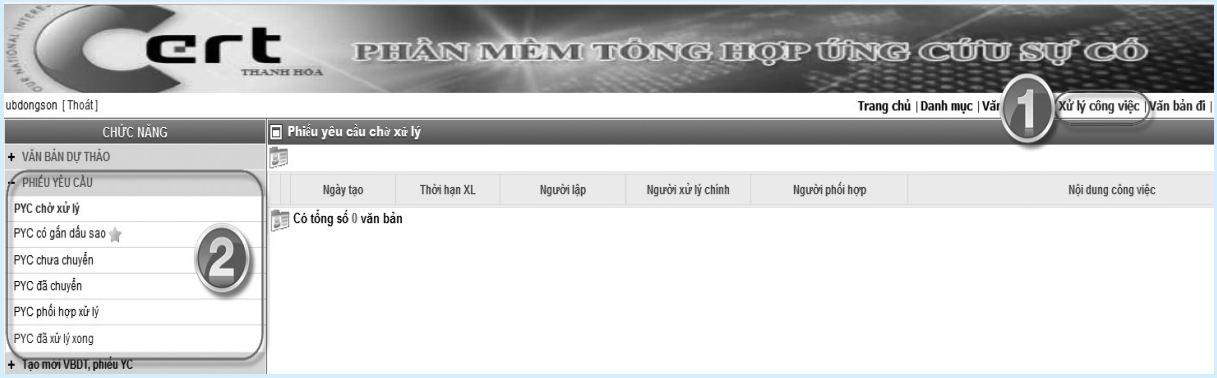
(2). Thời gian xử lý: Lựa chọn thời gian yêu cầu cần xử lý xong

(3). Nội dung công việc: Miêu tả sơ lược về sự cố cần hỗ trợ

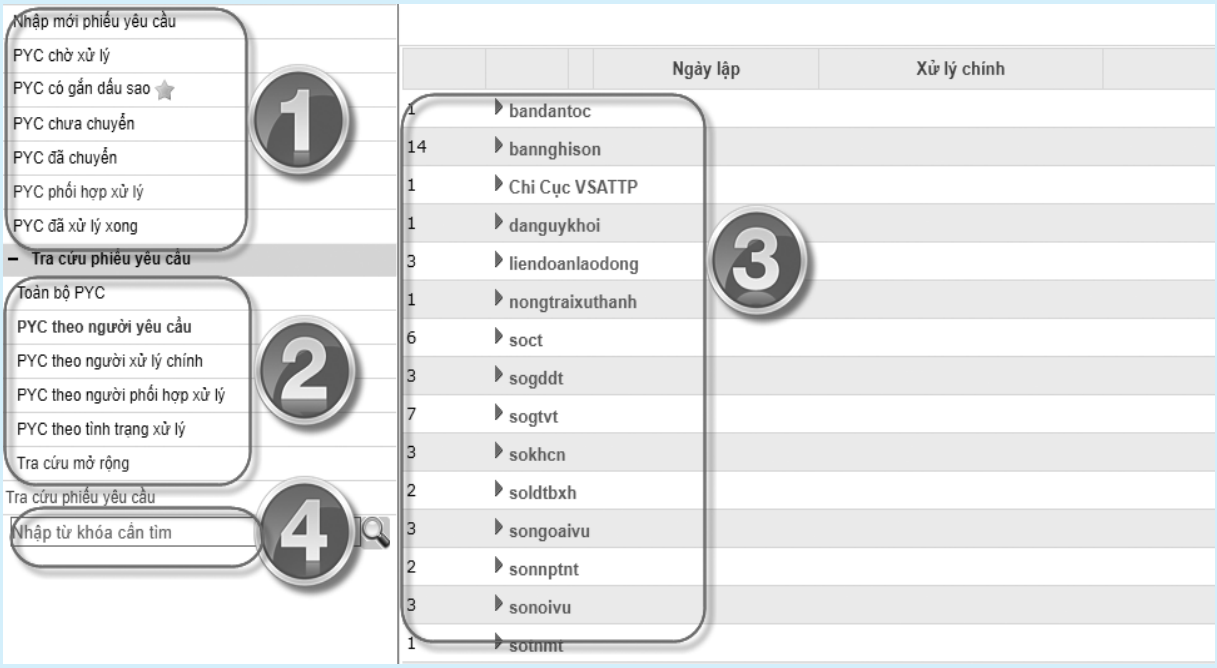
(4). Tệp kèm theo: Gắn kèm các file ảnh, file văn bản, file nhật ký... liên quan đến sự cố cần miêu tả chi tiết

(5). Lưu & chuyển xử lý: Chuyển xử lý nội dung cần hỗ trợ đến cho cán bộ hỗ trợ ứng cứu.

- Kiểm tra phiếu yêu cầu: Sau khi Phiếu yêu cầu đã được chuyển xử lý. Để kiểm tra xem thông tin phiếu yêu cầu đã được xử lý chưa. Những phiếu yêu cầu đã chuyển xử lý hoặc chưa chuyển xử lý. Ta thực hiện theo hướng dẫn dưới đây:



- Tra cứu phiếu yêu cầu: Để tra cứu các phiếu yêu cầu đã được chuyển xử lý trước đây, cũng như các phiếu yêu cầu của đơn vị khác. Ta thực hiện theo hướng dẫn dưới đây:



Bước 1: Truy cập vào modul Phiếu Yêu Cầu từ giao diện sau khi đăng nhập.

Bước 2:

(1): Danh mục các chức năng liên quan đến "Phiếu Yêu cầu" của cá nhân. Thông qua các chức năng này để kiểm tra các thông tin đến các yêu cầu đã được chuyển xử lý, kết quả xử lý và tình trạng xử lý...

(2): Danh mục các chức năng liên quan đến "Phiếu Yêu cầu" của các cá nhân và đơn vị khác. Tại đây ta có thể xem các sự cố đang được hỗ trợ hoặc đã được hỗ trợ trên phạm vi địa bàn tỉnh.

(3): Kết quả hiển thị tương ứng với các chức năng lựa chọn

(4): Tra cứu các yêu cầu theo các tiêu chí khác nhau.

ĐẢM BẢO AN TOÀN THÔNG TIN TRONG VIỆC SỬ DỤNG THƯ ĐIỆN TỬ CÔNG VỤ

CHÚC ANH HÒA
Phó Trưởng phòng Đào tạo dịch vụ
Trung tâm CNTT&TT Thanh Hóa

Trong thời gian gần đây, thư điện tử đã trở thành một công cụ hữu hiệu trong việc trao đổi thông tin góp phần quan trọng trong việc nâng cao hiệu quả công việc, giảm thời gian và chi phí thực hiện trong quá trình giải quyết công việc. Tuy nhiên, bên cạnh đó xuất hiện nhiều nguy cơ gây mất an toàn thông tin trong việc sử dụng thư điện tử, ngoài việc trực tiếp ảnh hưởng tới tài khoản của người sử dụng còn gián tiếp ảnh hưởng tới hệ thống thông tin. Do đó, gây ảnh hưởng xấu tới việc sử dụng thư điện tử trong hoạt động quản lý và trao đổi thông tin. Sau đây, là các hướng dẫn cơ bản trong việc đảm bảo an toàn thông tin khi sử dụng thư điện tử trên môi trường mạng:

i | Nguy cơ và hiểm họa

- Nguy cơ bị đọc trộm nội dung thư điện tử
- Lộ lọt thông tin bí mật, nhạy cảm.
- Bị chiếm quyền tài khoản thư điện tử

- Thư rác (Spam mail)
- Phát tán thư giả mạo, có nội dung lừa đảo hoặc quảng cáo không phù hợp

- Phát tán, lây lan mã độc, phần mềm quảng cáo trái phép,...
- Tấn công hệ thống thông tin của đơn vị
- Bị lợi dụng để phục vụ cho mục đích xấu

? Biện pháp đề phòng

Nguyên tắc chung sử dụng thư điện tử an toàn

- Hạn chế tối đa việc truy cập hòm thư điện tử bằng các máy tính không đảm bảo an toàn hoặc mạng máy tính không an toàn (máy tính đặt nơi công cộng).

- Hạn chế tối đa việc sử dụng máy tính cá nhân truy cập hòm thư điện tử công vụ thông qua các mạng Internet không an toàn như: truy cập mạng Internet thông qua các điểm truy cập không dây tại quán ăn, giải khát, sân bay, nhà chờ hoặc nơi không rõ nguồn gốc v.v..

- Không sử dụng hòm thư điện tử công vụ do cơ quan cấp cho mục đích cá nhân như: đăng ký các dịch vụ thương mại, dịch vụ trao đổi chia sẻ thông tin cá nhân.

- Không đặt chế độ chuyển thư tự động từ hòm thư điện tử công vụ được cấp tới hòm thư khác không phải do các cơ quan nhà nước cấp (yahoo, gmail...).

- Hạn chế sử dụng các ứng dụng duyệt thư điện tử có sẵn trên các thiết bị di động như Smart phone hoặc máy tính bảng để truy cập vào các hòm thư điện tử công vụ được cấp.

- Chú ý cảnh giác với những thư điện tử có nội dung, nguồn gốc khả nghi.

- Đánh dấu Spam ngay khi nhận được các thư rác.

- Khi nhận được thư điện tử gửi kèm tệp tin mà không phát hiện ra nghi ngờ thì thực hiện các bước sau: 1) Tải tệp tin về ổ cứng (tuyệt đối không mở hoặc kích hoạt tệp tin ngay); 2) Dùng phần mềm diệt mã độc quét kiểm tra tệp tin vừa tải về (nếu cần có thể liên lạc lại với người gửi thư để xác nhận tệp tin đã nhận được). Chỉ mở tệp tin nếu không phát hiện ra mã độc; 3) Nếu phát hiện ra mã độc, gửi thư điện tử đó dưới dạng file đính kèm về địa chỉ ungcuusuco@thanhhoa.gov.vn để xử lý.

- Không gửi, nhận tệp tin không có nguồn gốc rõ ràng qua hệ thống thư điện tử và hạn chế việc dùng tệp tin nén có mã hóa.

- Khuyến khích sử dụng chữ ký số để ký xác nhận trên thư điện tử gửi đi và kiểm tra nguồn gốc thư điện tử khi tiếp nhận bằng chữ ký số nếu thư đó đã được ký bằng chữ ký số của người gửi.

- Xóa thư khi không còn cần thiết để tránh bị mất mát thông tin nếu tài khoản bị lộ.

- Sử dụng và quản lý mật khẩu theo hướng dẫn sử dụng mật khẩu an toàn.

Sử dụng thư điện tử trong môi trường mạng kém an toàn

Nếu trong trường hợp cần thiết phải truy cập hộp thư điện tử qua máy tính cá nhân tại các địa điểm công cộng hoặc môi trường mạng không tin tưởng, không có khả năng kiểm soát an toàn thì sẽ có các nguy cơ: bị nghe lén, bị giả mạo thư điện tử hoặc chuyển hướng đến các trang web có thông tin không lành mạnh hoặc bị lấy các thông tin khi đăng nhập. Để đảm bảo an toàn thông tin cần tuân theo các nguyên tắc sau để đảm bảo an toàn:

- Truy cập hệ thống thư điện tử thông mạng riêng ảo (VPN) để đảm bảo an toàn.

- Sử dụng giao thức HTTPS khi truy cập vào các dịch vụ trên mạng yêu cầu xác thực.

- Hoặc thông qua máy tính cá nhân ở cơ quan hoặc ở nhà. Sau đó từ máy tính này truy cập đến thư điện tử để sử dụng email.

Sử dụng thư điện tử trên máy tính dùng chung

Sử dụng thư điện tử tại máy tính dùng chung vì có thể mắc phải các nguy cơ tương tự như việc sử dụng thư điện tử tại môi trường mạng kém an toàn. Ngoài ra có nguy cơ bị tự động lưu trữ mật khẩu và dữ liệu, hoặc cài cắm các phần mềm độc hại trong máy tính ghi lại thao tác bàn phím, chụp ảnh màn hình hay đánh cắp dữ liệu... Trong trường hợp bắt buộc phải sử dụng, cần lưu ý một số nguyên tắc sau:

- Trước khi sử dụng nên tiến hành kiểm tra máy tính bằng phần mềm diệt Virus bản quyền do cơ quan cài đặt.

- Sử dụng bàn phím ảo để tránh việc bị key-logger đánh cắp mật khẩu. Tuy nhiên việc này bị vô hiệu nếu máy tính đó cũng bị cài phần mềm chụp ảnh màn hình. Việc kết hợp sử dụng bàn phím vật lý và bàn phím ảo, mã hoá đường truyền sẽ hạn chế việc bị đánh cắp mật khẩu trong môi trường không an toàn.

- Tuyệt đối không lưu trữ mật khẩu trên trình duyệt.

KỸ NĂNG NHẬN BIẾT, PHÒNG CHỐNG THƯ RÁC, THƯ GIẢ MẠO

TRỊNH NGỌC QUỲNH
Phó Trưởng phòng Tổng hợp Hành chính
Trung tâm CNTT&TT Thanh Hóa

Một trong những mục tiêu ưa thích hiện nay của tội phạm mạng là lừa đảo người dùng thông qua việc gửi thư điện tử giả mạo, thư rác đến cho người dùng. Để phòng tránh được những hình thức tấn công này, người sử dụng cần có những cách thức để nhận thức cơ bản về các nguy cơ của thư điện tử và biện pháp để phòng tránh.

Thư điện tử rác (Spam mail)

- Thư rác (spam) là thư điện tử, tin nhắn được gửi đến người nhận mà người nhận đó không mong muốn hoặc không có trách nhiệm phải tiếp nhận.

- Thư rác không chỉ làm ảnh hưởng tới công việc hàng ngày. Với các phương thức gửi thư rác ngày càng đa dạng và tinh vi để vượt qua các bộ lọc thư rác thông dụng, gây ra nhiều nguy cơ và rủi ro về an toàn thông tin cho người dùng.

- Các hệ thống thông tin có chứa các máy tính bị tin tặc khống chế để phát tán hệ thống thư rác có thể gây quá tải, làm ảnh hưởng tới hoạt động mạng.

Tấn công thư điện tử có chủ đích (tấn công bằng email giả mạo)

- Tấn công email có chủ đích là tấn công bằng email giả mạo như thể được gửi từ một người quen biết. Email này có chứa một mã độc đính kèm làm hệ thống bị lây nhiễm mã độc hay phần mềm gián điệp.

- Một ví dụ điển hình là email nhằm vào một cá nhân hay một tổ chức cụ thể. Email được đính kèm một mã độc và được gửi từ một kẻ mạo danh là một đồng nghiệp hoặc một đơn vị bên ngoài.

- Các tấn công kiểu này đã được ghi nhận với hành vi đánh cắp mật khẩu hoặc lây nhiễm mã độc cho mục đích khác.

Các kỹ năng nhận biết, phòng chống thư giả mạo của tin tặc

1. Kiểm tra Email header

Thông thường khi soạn và gửi thư điện tử, người gửi thư chỉ biên soạn nội dung, tiêu đề thư (title), địa chỉ nơi nhận, lựa chọn các tập tin đính kèm, các thông tin còn lại khác sẽ do máy chủ gửi thư tự động cập nhật như: địa chỉ hòm thư nhận phản hồi khi thư bị trả lại (Return-Path); địa chỉ hòm thư tiếp nhận thư trả lại (Reply-To) và địa chỉ hòm thư người gửi (from).

Để đánh lừa người nhận tin, bước đầu tin tặc sẽ tìm cách tự biên soạn thư điện tử với các thông tin giả mạo về: địa chỉ hòm thư nhận phản hồi khi thư bị trả lại (ReturnPath); địa chỉ hòm thư tiếp nhận thư trả lời (Reply-To) và địa chỉ hòm thư người gửi (from). Sau đó tin tặc sẽ tìm một máy chủ thư điện tử hoặc tự cài đặt một phần mềm gửi thư (MTA) không yêu cầu xác thực hòm thư người gửi để phát tán thư điện tử giả mạo tới người cần lừa đảo.

Email header là nội dung được gửi kèm theo những email nhằm cung cấp các thông tin đầy đủ cho một email. Những thông tin này thông thường sẽ không được hiển thị cho người dùng, mà cần mở trong giao diện của Mail Client

```
Received: by 10.200.40.101 with SMTP id 34csp716207qtr;
        Thu, 28 Jul 2016 04:20:20 -0700 (PDT)
X-Received: by 10.36.26.194 with SMTP id 185mr110996407iti.28.1469704820777;
        Thu, 28 Jul 2016 04:20:20 -0700 (PDT)
Return-Path: <ww.@view.ocn.ne.jp>
Received: from mbkd0106.ocn.ad.jp (mbkd0106.ocn.ad.jp. [153.149.230.7])
        by mx.google.com with ESMTP id x28si32081079ita.90.2016.07.28.04.20.12;
        Thu, 28 Jul 2016 04:20:20 -0700 (PDT)
Received-SPF: pass (google.com: domain of ww.@view.ocn.ne.jp designates 153.149.230.7 as permitted sender) client-ip=153.149.230.7;
Authentication-Results: mx.google.com;
       spf=pass (google.com: domain of ww.@view.ocn.ne.jp designates 153.149.230.7 as permitted sender) smtp.mailfrom=ww.@view.ocn.ne.jp
Received: from mf-smf-ucb012.ocn.ad.jp (mf-smf-ucb012.ocn.ad.jp [153.149.228.230])
        by mbkd0106.ocn.ad.jp (Postfix) with ESMTP id BFC0BD8093E;
        Thu, 28 Jul 2016 20:20:11 +0900 (JST)
Received: from ntt.pod01.mv-mta-ucb030 (mv-mta-ucb030.ocn.ad.jp [153.149.230.164])
        by mf-smf-ucb012.ocn.ad.jp (Switch-3.3.4/Switch-3.3.4) with ESMTP id u65BJwh8034273;
        Thu, 28 Jul 2016 20:20:07 +0900
Received: from vcwebmail.ocn.ad.jp ([153.149.227.167])
        by ntt.pod01.mv-mta-ucb030 with
        id QBL61t0093dLKTM01BL6uU; Thu, 28 Jul 2016 11:20:07 +0000
Received: from mzcstore311.ocn.ad.jp (mz-fcb311p.ocn.ad.jp [180.37.198.99])
        by vcwebmail.ocn.ad.jp (Postfix) with ESMTP;
        Thu, 28 Jul 2016 20:20:06 +0900 (JST)
Date: Thu, 28 Jul 2016 20:20:06 +0900 (JST)
From: Vivian Douglas <ww.@view.ocn.ne.jp>
Reply-To: "courier485@yeah.net" <courier485@yeah.net>
```

Ví dụ về Email Header

Khi đọc các nội dung trong Email header, chúng ta cần chú ý đọc ngược từ dưới lên trên để xác định các thời điểm theo thứ tự từ cũ đến mới, trong đó chú ý một số thông tin như sau:

Received: Thông tin máy chủ SMTP đã tiếp nhận email này từ người gửi, đây là thông tin quan trọng hiển thị máy chủ đã tiếp nhận email và gửi đi. Nên cân nhắc những máy chủ SMTP phổ biến như Google, Hotmail hoặc Yahoo...Dựa theo các lần Received người dùng cũng hoàn toàn có thể biết đường đi của Email và các IP máy chủ đã chuyển tiếp Email. Nếu đường đi này quá lòng vòng và đi qua nhiều máy chủ nghi ngờ thì đó rất có thể là Email giả mạo.

From: Địa chỉ Email của người gửi. Tuy nhiên, trường hợp này hoàn toàn có thể giả mạo và không nên tin cậy các địa chỉ Email được khai báo trong trường này.

To: Địa chỉ Email của người nhận

Reply-To: Địa chỉ Email của người sẽ nhận Email trả lời, nếu trường giá trị này không trùng với trường giá trị From mà trong thư không trực tiếp nhắc đến việc chuyển tiếp nội dung thì khả năng lớn đây là thư giả mạo.

Return-Path: Địa chỉ hòm thư nhận phản hồi khi thư bị trả lại

X-Mailer: Thông tin ứng dụng được sử dụng để gửi Email. Khi kiểm tra thông tin này chúng ta có thể thu được tên ứng dụng và phiên bản của ứng dụng đó

Dựa vào những lần Received được liệt kê, chúng ta hoàn toàn có thể xác định được IP của người gửi đi thư giả mạo hoặc thư rác

Ví dụ với đoạn Email Header trong một thư rác:

```
Received: from c1-smtp-out43.am-mdn.com (c1-smtp-out43.am-mdn.com. [185.31.139.44])
        by mx.google.com with ESMTPS id g89si33546691fi.3.2016.08.03.05.52.17
        for <xxxxx@gmail.com>
        (version=TLS1 cipher=ECDHE-RSA-AES128-SHA bits=128/128);
        Wed, 03 Aug 2016 05:52:17 -0700 (PDT)
Received: from smtp-front1.authmailer.com (smtp-front1.authmailer.com [185.31.136.72])
         by smtp-cluster1.am-mdn.com (Postfix) with ESMTPS id AD93618008E90
         for <xxxxx@gmail.com>; Wed,  3 Aug 2016 09:38:28 +0000 (UTC)
Received: from localhost.localdomain (unknown [125.253.124.A])
         (Authenticated sender: u4715331)
         by smtp-front1.authmailer.com (Postfix) with ESMTPSA id A534926007B
         for <xxxxx@gmail.com>; Wed,  3 Aug 2016 12:38:26 +0300 (EEST)
```

Thì các mốc thời gian được hiểu như sau:

```
[1] Received: from localhost.localdomain (unknown [125.253.124.A])
        (Authenticated sender: u4715331)
        by smtp-front1.authmailer.com (Postfix) with ESMTPSA id A534926007B
        for <xxxxx@gmail.com>; Wed,  3 Aug 2016 12:38:26 +0300 (EEST)
[2]   Received:   from   smtp-front1.authmailer.com   (smtp-front1.authmailer.com
[185.31.136.72])
        by smtp-cluster1.am-mdn.com (Postfix) with ESMTPS id AD93618008E90
        for <xxxxx@gmail.com>; Wed,  3 Aug 2016 09:38:28 +0000 (UTC)
[3] Received: from c1-smtp-out43.am-mdn.com (c1-smtp-out43.am-mdn.com. [185.31.139.44])
by mx.google.com with ESMTPS id g89si3354669lfi.3.2016.08.03.05.52.17
        for <xxxxx@gmail.com>
        (version=TLS1 cipher=ECDHE-RSA-AES128-SHA bits=128/128);
        Wed, 03 Aug 2016 05:52:17 -0700 (PDT)
```

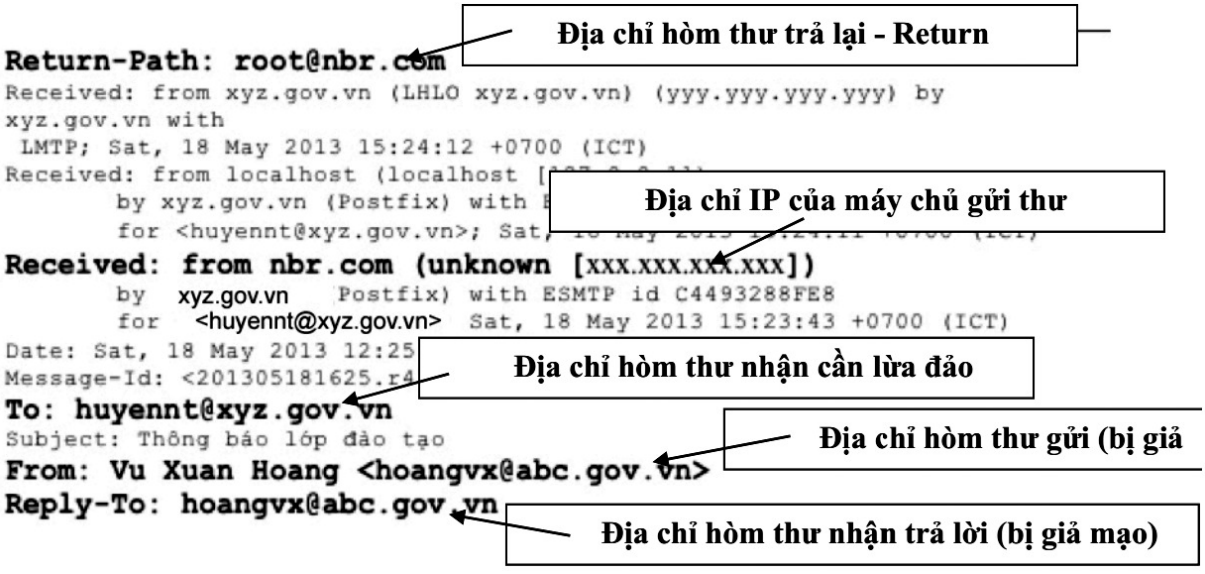
Như vậy ban đầu Email được gửi từ địa chỉ 125.253.124.A thông qua dịch vụ Authmailer SMTP, sau đó được máy chủ 185.31.136.72 của dịch vụ Authmailer và cuối cùng là gửi đến máy chủ của Gmail tại địa chỉ 185.31.139.44

2. Phát hiện thư giả mạo:

Qua phân tích các thư điện tử giả mạo đã gửi đến các cơ quan nhà nước trong thời gian vừa qua, có hai dấu hiệu chính để có thể phát hiện ra các thư giả mạo theo phương thức này là:

Một là: Khi mở xem nguồn gốc chi tiết của thư điện tử, địa chỉ hòm thư "Return-Path" không trùng với địa chỉ hòm thư người gửi đến (From). Hầu hết các thư điện tử được gửi từ các hệ thống thư điện tử của cơ quan nhà nước (có đuôi .gov.vn) đều có hai địa chỉ này trùng nhau.

Hai là: Địa chỉ IP của máy chủ gửi thư không trùng với địa chỉ IP của hệ thống thư điện tử thật nơi bị giả mạo là gửi thư điện tử. Hiện nay, các địa chỉ IP giả mạo này thường có nguồn gốc từ nước ngoài trong khi địa chi IP các hệ thống cơ quan nhà nước thường có địa chỉ IP trong nước.



3. Kiểm tra kỹ các file tải về

Khi nhận được những Email giả mạo, một số người dùng thường chủ quan và tải trực tiếp các file đính kèm về và khởi chạy. Điều này tạo cơ hội cho các hình thức tấn công lây lan và cài đặt các phần mềm độc hại. Để phòng tránh được điều này, người dùng có thể thực hiện theo cách thức như sau:

- Đối với các file văn bản, có thể sử dụng các dịch vụ Documents trực tuyến để xem và chỉnh sửa

trực tiếp trên Website

Sử dụng công cụ Google Doc của Google để tải lên và mở các file đính kèm là văn bản

- Chỉ mở file đính kèm từ những địa chỉ quen thuộc, với những địa chỉ lạ hoặc nghi ngờ là giả mạo, cần tải về và kiểm tra lại trên các trang kiểm tra phần mềm độc hại trực tuyến

Để giúp các cơ quan, đơn vị trong việc khắc phục và xử lý sự cố, ngay khi phát hiện sự cố liên quan đến hệ thống thư điện tử cần nhanh chóng thông tin về ***Tổ Ứng cứu sự cố mạng máy tính*** của Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa theo địa chỉ dưới đây, để được hỗ trợ, xử lý kịp thời, hạn chế tối đa các nguy cơ mất an toàn thông tin mạng.

Thông tin liên hệ: Điện thoại: (0237) 3718699; Fax (0237) 3718299

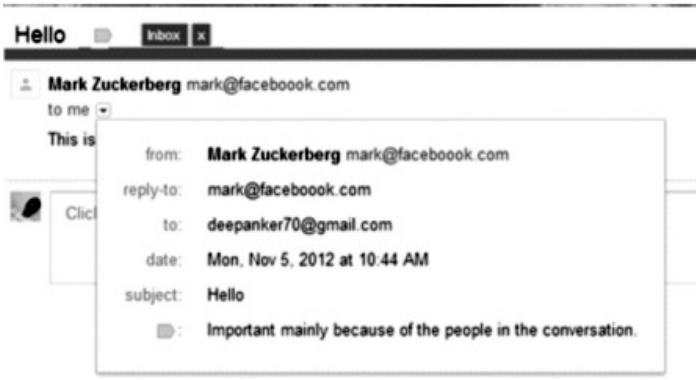
Email: ungcuusuco@thanhhoa.gov.vn

HƯỚNG DẪN PHÒNG TRÁNH THƯ GIẢ MẠO

Ghi nhớ số 1: "Không nên tin tưởng tên hiển thị trong Email"

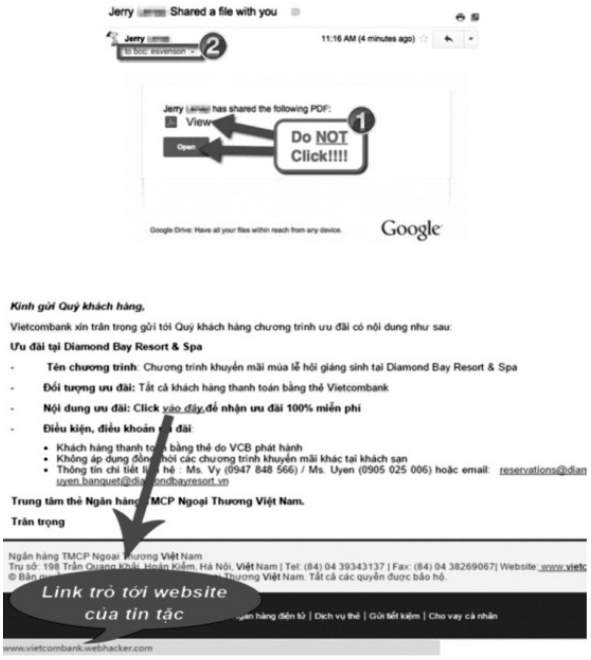
Một chiến thuật lừa đảo yêu thích của các tin tặc là giả mạo tên hiển thị của một email để đánh lừa người nhận được

Các tên hiển thị hay được giả mạo như tên của các Công ty, tổ chức, hãng lớn; Người quen của bạn; Người nổi tiếng...



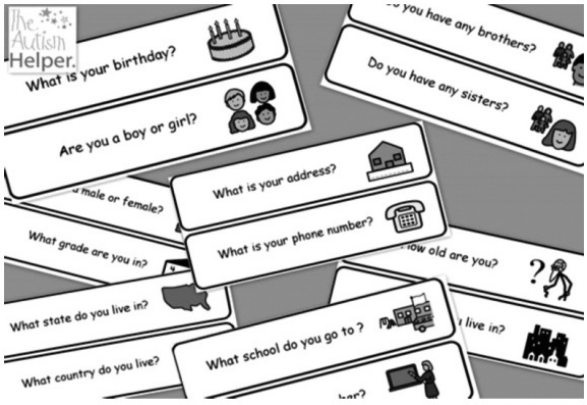
Ghi nhớ số 2: "Cân nhắc kỹ lưỡng khi bấm vào liên kết (link) trong email"

Cẩn trọng khi bấm vào bất cứ liên kết (link) được gửi trong nội dung email. Liên kết (link) đó có thể dẫn bạn tới một website lừa đảo giả mạo, quảng cáo hay một website độc hại mà tin tặc dựng lên để tấn công.



Ghi nhớ số 3: "Bỏ qua các email yêu cầu cung cấp thông tin cá nhân của bạn"

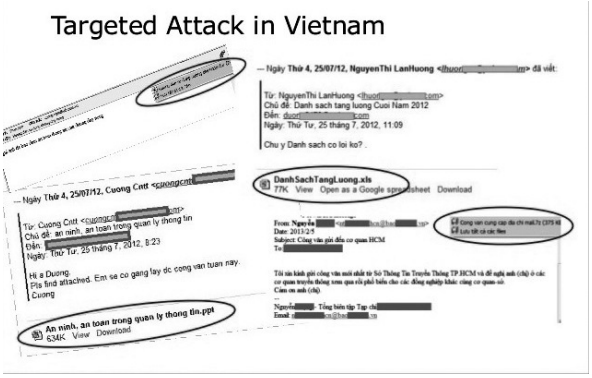
Một tổ chức, công ty, ngân hàng,... sẽ không bao giờ yêu cầu người sử dụng cung cấp thông tin cá nhân. Do vậy bạn hoàn toàn có thể bỏ qua chúng khi nhận được các email với nội dung đó.



Và thậm chí hạn chế tối đa, cân nhắc cẩn thận khi cung cấp thông tin cá nhân cho bất kỳ tổ chức nào.

Ghi nhớ số 4: "Cẩn trọng với các email có tiêu đề Hấp dẫn - Nhạy cảm- Khẩn cấp"

Đánh vào tâm lý của người dùng, các tin tặc thường xuyên sử dụng các tiêu đề có tính Hấp dẫn - Nhạy cảm - Khẩn cấp trong email để lừa người dùng. Chúng ta bị tiêu đề đó làm chủ quan, mất cảnh giác, hay thậm chí là hoảng hốt và cảm thấy cần phải xử lý gấp. Ví dụ như: "Cập nhật bảng lương công ty Quý 2/2016";"Cảnh báo: Tài khoản của bạn bị đình chỉ:...

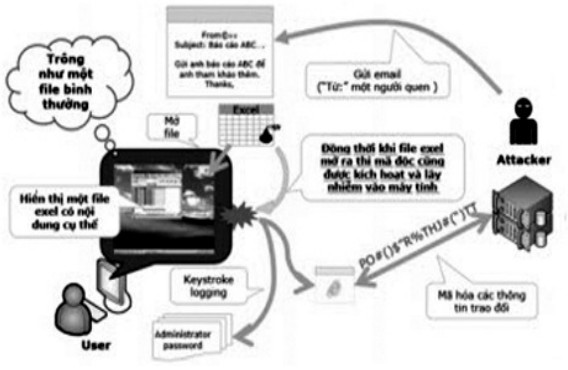


Ghi nhớ số 5: "Cẩn thận, cân nhắc khi tải về các File đính kèm trong email"

Tấn công bằng việc sử dụng cài mã độc, virus trong các file đính kèm trong email là phương thức tấn công phổ biến và nguy hiểm nhất hiện nay.

Không nên tải và mở chạy file ngay khi nhận được các email có file đính kèm.

Chú ý tới định dạng file và tạo thói quen quét virus với các file đính kèm trước khi mở chúng.



Ghi nhớ số 6: "Nhận diện các email spam - email quảng cáo"

Bạn cần cảnh giác khi nhận các email spam, email quảng cáo từ Internet. Trong các email này thường đi kèm với nhiều rủi ro mất an toàn thông tin mà chúng ta không mong muốn như lừa đảo, mã độc, gây ảnh hưởng tới công việc khi nhận quá nhiều...

Ghi nhớ số 7: "Cẩn trọng với các tin nhắn rác"

Cũng tương tự như email spam thì các tin nhắn rác (sms spam) cũng gây cho người dùng rất nhiều phiền toái. Bên cạnh đó ngày nay các tin nhắn rác thường xuyên được sử dụng như một phương thức để lừa đảo người dùng như:

Bạn trúng thưởng một xe SH...

Nhắn tin, gọi tới 1800XXXX, 1900XXXX, 1900XXXXXX, 6XXX, 7XXX, 8XXX, 9XXX,...

Truy cập vào đường link, trang web

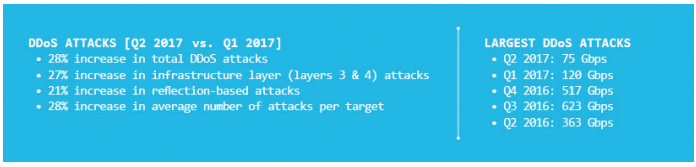
(Nguồn Cục An toàn thông tin - Bộ Thông tin và Truyền thông)

THỐNG KÊ TÌNH HÌNH AN TOÀN THÔNG TIN
TỔ ỨNG CỨU SỰ CỐ

I. Tình hình An toàn thông tin Quý II năm 2017 trong nước và quốc tế

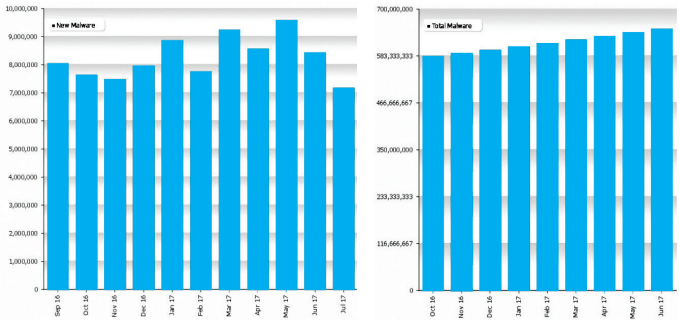
1. Tình hình tấn công DDoS và Ứng dụng Web

Theo báo cáo của Akamai - Q2 2017 State of the Internet/Security Report, các cuộc tấn công DDoS và tấn công ứng dụng web trong Quý II đã gia tăng đáng kể.



Số lượng các cuộc tấn công DDoS trong Quý II tăng 28% so với Quý I.

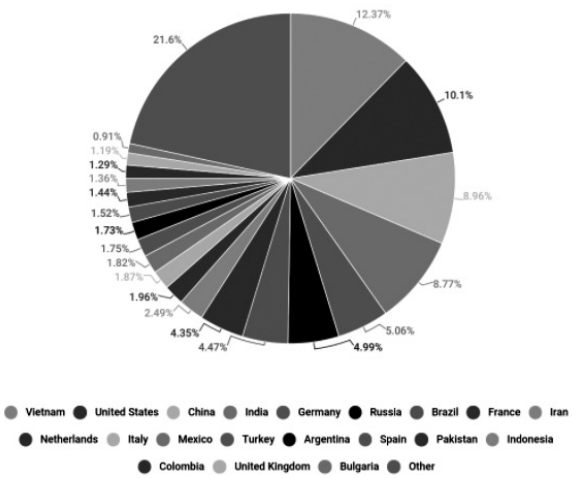
2. Tình hình mẫu mã độc xuất hiện mới trong từng tháng và tổng số mã độc



Nguồn: shadowserver

3. Tình hình Spam trong Quý II

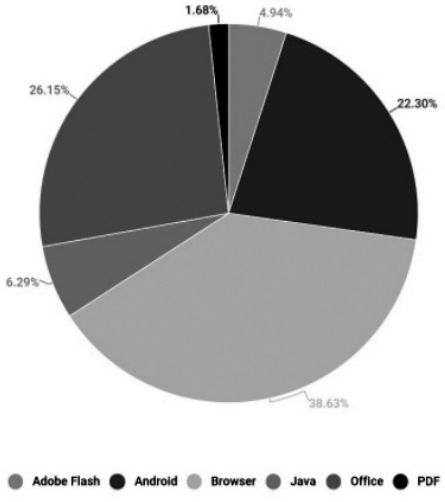
Báo cáo của Kaspersky Lab về tình hình thư rác và lừa đảo trực tuyến trong quý II cho biết, số lượng thư rác trung bình trên thế giới đã tăng lên 56,97%. Việt Nam trở thành quốc gia có nguồn phát tán thư rác đứng đầu (12,37%), vượt qua Hoa Kỳ (10,1%) và Trung Quốc (8,96%).



Nguồn: Kaspersky Lab

4. Tình hình khai thác lỗ hổng ứng dụng trong Quý II

Báo cáo của Kaspersky Lab về thống kê tỉ lệ khai thác lỗ hổng ứng dụng trong quý II cho biết bên cạnh việc khai thác lỗ hổng chủ yếu qua trình duyệt Web (chiếm 38,63%) thì trong quý II với việc khai thác các lỗ hổng liên quan đến ứng dụng Office của Microsoft chiếm vị trí thứ 2 (với 26,15%), trong đó lỗ hổng 0-day có mã là CVE-2017-0199 chiếm 71% cuộc tấn công của tin tặc, bên cạnh đó là vào các lỗ hổng như CVE-2017-0261 và CVE-2017-2062



Thống kê tỉ lệ mã khai thác sử dụng để lây nhiễm mã độc trên các ứng dụng *(Nguồn Kaspersky)*

4. Lỗ hổng trên Microsoft Word ảnh hưởng hầu hết các máy tính chạy Windows

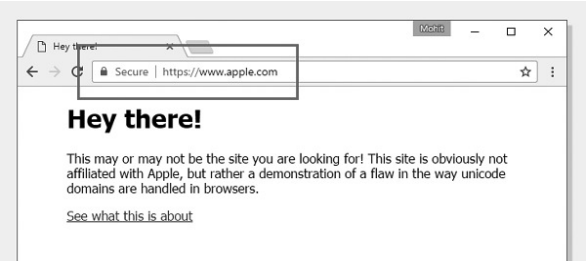
Một lỗ hổng nghiêm trọng trên Microsoft Word bị phát hiện có khả năng gây ảnh hưởng tới toàn bộ phiên bản Windows, bao gồm cả Windows 10. Theo các chuyên gia, lỗ hổng có tính chất nghiêm trọng bởi cho phép hacker vượt qua các cơ chế an ninh của Microsoft.

Cuộc tấn công nhằm vào Microsoft Office khởi đầu bằng việc gửi một email đính kèm tệp tin Word độc hại chứa OLE2link. Khi người dùng mở file, mã khai thác sẽ được thực thi và kết nối tới máy chủ từ xa do hacker kiểm soát. Tại đây mã khai thác tải về một file ứng dụng HTML (HTA) độc hại giả mạo file tài liệu RTF (Rich Text Format) của Microsoft. File HTA sau đó tự động thực thi trên máy nạn nhân, tải thêm các mã độc khác về để chiếm quyền kiểm soát máy tính nạn nhân, đồng thời đóng tập tin Word lại.

Hãng Microsoft đã biết đến lỗ hổng sau khi được các chuyên gia thông báo về các cuộc tấn công khai thác lỗ hổng chưa được vá từ tháng 1/2017. Đã được MITRE Corporation đặt mã tên quốc tế: CVE - 2017-0199.

5. Tấn công lừa đảo gần như không thể bị phát hiện trên Chrome, Firefox và Opera

Một chuyên gia phát hiện cách thức tấn công phishing Punycode "gần như không thể phát hiện" với cả những người sử dụng cẩn thận nhất trên Internet. Theo đó, hacker khai thác một lỗ hổng đã biết trên các trình duyệt web để hiển thị tên miền giả mạo các nhà cung cấp dịch vụ hợp pháp như Apple, Google hay Amazon. Từ đó, hacker có thể ăn cắp thông tin đăng nhập, thông tin tài chính và các thông tin nhạy cảm khác của người dùng.



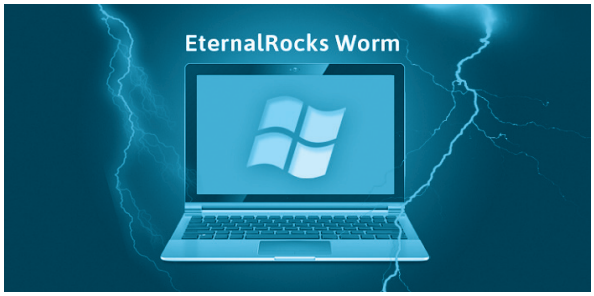
6. 1.900 máy tính tại Việt Nam nhiễm mã độc tống tiền WannaCry

Mã độc tống tiền WannaCry đã tạo ra một "cơn địa chấn" trên thế giới trong tháng 5 vừa qua. Thông qua việc khai thác lỗ hổng Eternal-Blue trên Windows, WannaCry có khả năng lây nhiễm với tốc độ lây lan rất nhanh. Tại Việt Nam,

hệ thống của Bkav ghi nhận 1.900 máy tính nhiễm WannaCry và có tới 52% máy tính tồn tại lỗ hổng EternalBlue có nguy cơ bị tấn công. Ngay sau đó, công cụ kiểm tra WannaCry cũng đã được hãng cung cấp miễn phí tới người dùng.

7. Mã độc EnternalRocks đặt các hệ thống trước nguy cơ tấn công APT

Mã độc EnternalRocks được cho là nguy hiểm hơn cả WannaCry bởi có khả năng lây rộng hơn WannaCry nhờ sử dụng tới 7 công cụ tấn công bị rò rỉ của NSA. Thay vì thả mã độc tống tiền, EnternalRocks giành quyền kiểm soát trái phép trên máy tính bị nhiễm để thực hiện tấn công có chủ đích APT trong tương lai.



8. Lỗ hổng nghiêm trọng ẩn nấp trong chip Intel suốt 7 năm

Lỗ hổng nằm trong tính năng quản lý từ xa trên máy tính sử dụng bộ vi xử lý Intel, cho phép hacker kiểm soát máy tính từ xa. Lỗ hổng ảnh hưởng tới tất cả hệ thống Intel gồm PC, laptops, máy chủ bật tính năng AMT (Active Management Technology - Tính năng quản lý năng động). Intel xếp lỗ hổng này ở mức đặc biệt nghiêm trọng và phát hành các bản firmware mới trong đó có hướng dẫn khắc phục dành cho các tổ chức không thể cài đặt bản cập nhật ngay lập tức.

9. Mã độc mã hóa dữ liệu Petya nguy hiểm hơn cả WannaCry

Mã độc tống tiền mã hóa dữ liệu Petya xuất hiện và làm tê liệt hàng loạt ngân hàng, sân bay, máy ATM và một số doanh nghiệp lớn tại châu Âu. Kết quả phân tích mã độc cho thấy, Petya nguy hiểm hơn nhưng số lượng máy tính bị lây nhiễm sẽ ít hơn rất nhiều so với WannaCry do không có module tự động quét các máy trên Internet để phát tán.

10. Hơn 800 ứng dụng trên Google Play chứa mã độc quảng cáo Xavier

Giữa tháng 6, một loại mã độc quảng cáo, Xavier, lây nhiễm hơn 800 ứng dụng Android, âm thầm thu thập dữ liệu nhạy cảm của người dùng. Khu vực có số lượng người dùng nhiễm mã độc cao nhất là các nước Đông Nam Á trong đó có Việt Nam.

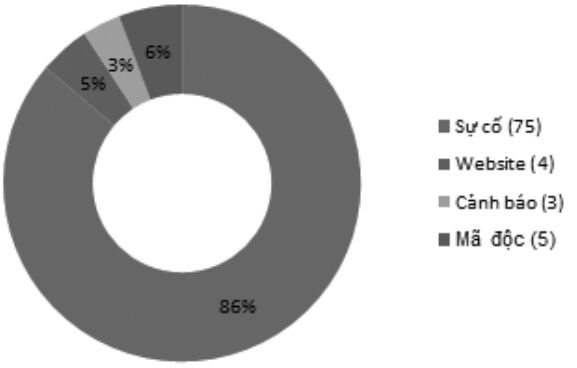
Để tránh lây nhiễm mã độc Xavier, người dùng cần cẩn trọng khi tải các ứng dụng, nên cài phần mềm diệt virus thường trực cho thiết bị của mình, thường xuyên cập nhật bản mới cho thiết bị và cho phần mềm bảo vệ đó.

II. Tình hình An toàn thông tin trên địa bàn tỉnh trong quý II/2017

1. Thống kê các website trên địa bàn tỉnh bị tấn công

Ngày	Domain
03/4/2017	duongsatthanhhoa.vn
25/4/2017	syt.thanhhoa.gov.vn/null.html
25/4/2017	ytethanhhoa.gov.vn/null.html
18/5/2017	nhakhach25b.thanhhoa.gov.vn/sh.html
29/6/2017	dongphucthanhhoa.com/by.htm
29/6/2017	daxanhthanhhoa.com/by.htm
17/5/2017	giongcaytrongthanhhoa.vn/TFS.html
10/4/2017	tmdl.edu.vn
13/4/2017	danguykhoithanhhoa.org.vn/images/tech.txt
18/4/2017	dongson.gov.vn/NewsImages/1937CNteam.txt
24/4/2017	ftcthanhhoa.com.vn/by.htm

2. Tổng hợp tình hình ứng cứu sự cố trên địa bàn tỉnh



TIN HOẠT ĐỘNG

Khai mạc lớp tập huấn "Kiểm tra, đánh giá an toàn thông tin và bảo mật cho các hệ thống thông tin"

Sáng ngày 03/6/2017, Trung tâm CNTT&TT Thanh Hóa đã phối hợp với Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) - Chi nhánh miền trung về việc tổ chức lớp đào tạo "Kiểm tra, đánh giá an toàn thông tin và bảo mật cho các hệ thống thông tin" cho đối tượng là các cán bộ trực tiếp vận hành Trung tâm An ninh mạng và An toàn dữ liệu của tỉnh và các học viên của Trung tâm CNTT&TT Sơn La, Quảng Trị.

Tham dự khai mạc lớp tập huấn có đ/c Lê Xuân Lâm - Giám đốc Trung tâm CNTT&TT Thanh Hóa; đại diện lãnh đạo Trung tâm CNTT&TT Quảng Trị và Sơn La và Trung tâm VNCERT.

Phát biểu tại buổi khai mạc lớp đào tạo, đồng chí Giám đốc Trung tâm CNTT&TT Thanh Hóa nhấn mạnh: Trước tình hình diễn biến phức tạp về mất an toàn thông tin hiện nay, để hoạt động đảm bảo an toàn thông tin được triển khai hiệu quả hơn nữa, đặc biệt trong kỷ nguyên cách mạng công nghiệp lần thứ 4, nguy cơ chiến tranh mạng ngày càng hiện hữu; Trung tâm CNTT&TT tổ chức lớp đào tạo với mục đích giúp cho các cán bộ trực tiếp làm về công tác an toàn thông tin nâng cao kỹ năng, phương pháp trong việc kiểm tra, rà soát và đánh giá các nguy cơ mất an toàn thông tin cho các hệ thống thông tin nói chung và bảo đảm bảo mật cho các ứng dụng trên nền Web nói riêng. Để qua đó chủ động, sẵn sàng đối phó, ngăn chặn và giảm thiểu các nguy cơ đe dọa gây mất an toàn thông tin.

Lớp học được tổ chức từ ngày 03 đến 06/6/2017 với sự hướng dẫn trực tiếp của cán bộ Trung tâm VNCERT. Kết thúc khóa học, các học viên thực hiện bài kiểm tra và được cấp giấy chứng nhận hoàn thành khóa học do VNCERT cấp./.

NGÔ PHƯƠNG

Khai trương Trang thông tin điện tử Tạp chí Văn nghệ Xứ Thanh

Sáng 14/6/2017, Ban biên tập tạp chí Văn nghệ Xứ Thanh phối hợp với Trung tâm CNTT&TT tổ chức lễ ra mắt và đi vào hoạt động chính thức Trang thông tin điện tử. Tới dự lễ ra mắt có đại diện Ban Tuyên giáo Tỉnh ủy, Sở Thông tin và Truyền thông, Hội Nhà báo Thanh Hóa; lãnh đạo và phóng viên các cơ quan báo chí: báo Thanh Hóa, báo Văn hóa-Đời sống, Đài PT-TH Thanh Hóa; phóng viên thường trú báo Nhân dân, Phân xã TTXVN, Thường vụ Hội VHNT Thanh Hóa...

Tạp chí Xứ Thanh là diễn đàn Văn học nghệ thuật trực thuộc Hội Văn học nghệ thuật Thanh Hóa, được phép xuất bản chính thức từ tháng 01/1994, 23 năm qua, được sự quan tâm của lãnh đạo tỉnh và các cơ quan liên quan, tạp chí đã làm tốt chức năng nhiệm vụ của mình.

Việc xây dựng trang TTĐT tổng hợp Tạp chí Văn nghệ xứ Thanh là yêu cầu cấp thiết trong thời đại công nghệ số, đồng thời cũng là việc thực hiện "Đề án quy hoạch và phát triển báo chí trên địa bàn tỉnh Thanh Hóa giai đoạn 2012-2020" mà UBND tỉnh Thanh Hóa đã phê duyệt, giúp cho việc Tuyên truyền, phổ biến quan điểm, đường lối của Đảng về phát triển văn học, nghệ thuật, giới thiệu các sáng tác văn học, nghệ thuật phục vụ các nhiệm vụ chính trị, kinh tế, xã hội của địa phương. Từ những ngày đầu tiên hình thành đề án, Trung tâm CNTT&TT đã tích cực tư vấn, hỗ trợ Tạp chí trong việc xây dựng đề án, thiết kế trang thông tin điện tử, báo cáo Sở TT&TT, Cục phát thanh truyền hình và thông tin điện tử (Bộ TT&TT) trong việc cấp phép thiết lập trang thông tin điện tử chạy chính thức trên môi trường mạng tại địa chỉ tapchixuthanh.vn. Trang thông tin điện tử của Tạp chí Văn nghệ xứ Thanh ra đời là một thuận lợi to lớn trong việc đáp ứng nhu cầu phổ cập CNTT trên mạng internet, giúp cho việc tuyên truyền, phổ biến quan điểm, đường lối của Đảng về phát triển văn học, nghệ thuật, giới thiệu các sáng tác văn học, nghệ thuật phục vụ các nhiệm vụ chính trị, kinh tế, xã hội của địa phương. Thông tin về các hoạt động văn học, nghệ thuật của địa phương; đăng tải các bài nghiên cứu, lý luận, phê bình nhằm định hướng sáng tạo và thị hiếu thẩm mỹ. Bồi dưỡng lực lượng sáng tác văn học, nghệ thuật, góp phần xây dựng nền văn hóa Việt Nam tiên tiến, đậm đà bản sắc dân tộc và mang đậm

sắc thái địa phương./.

LÊ NGỌC DUY

Trung tâm CNTT&TT Thanh Hóa làm việc với Ban Thi đua Khen thưởng Trung ương về Giải pháp phần mềm trực tuyến hỗ trợ công tác quản lý nhà nước về Thi đua Khen thưởng

Sáng ngày 10 tháng 5 năm 2017, Đoàn công tác của Trung tâm đã có buổi làm việc với Ban Thi đua Khen thưởng Trung ương để giới thiệu Giải pháp phần mềm trực tuyến hỗ trợ công tác quản lý nhà nước về thi đua khen thưởng đang được triển khai áp dụng tại Thanh Hóa.

Tham dự buổi làm việc có đồng chí Trần Thị Hà - Thứ trưởng Bộ Nội vụ, Trưởng Ban Thi đua khen thưởng Trung ương; đ/c Nguyễn Quốc Tuấn - Phó Giám đốc Sở Nội vụ, Trưởng Ban thi đua khen thưởng tỉnh Thanh Hóa; đ/c Lê Xuân Lâm - Giám đốc Trung tâm CNTT&TT Thanh Hóa.

Sau khi nghe Trung tâm CNTT&TT Thanh Hóa giới thiệu giải pháp phần mềm trực tuyến, đ/c Trần Thị Hà đánh giá cao sản phẩm phần mềm, tính hiệu quả và quá trình nghiên cứu công phu, nghiêm túc của tập thể cán bộ Trung tâm. Biểu dương và ghi nhận Ban Thi đua Khen thưởng Thanh Hóa là một trong những đơn vị dẫn đầu cả nước trong việc đẩy mạnh ứng dụng Công nghệ thông tin trong công tác quản lý nhà nước về Thi đua khen thưởng (TĐ-KT), đóng góp vào sự phát triển chung của ngành Thi đua Khen thưởng toàn quốc.

Qua đây đ/c cũng yêu cầu Trung tâm CNTT - Ban TĐKT TW hỗ trợ Trung tâm CNTT&TT Thanh Hóa đồng bộ và kết nối đến hệ thống "Quản lý Hồ sơ Thi đua Khen thưởng điện tử" hiện tại đã được áp dụng tại Ban TĐKT TW và đề nghị Trung tâm CNTT&TT tiếp tục hoàn thiện giải pháp và tư vấn cho Ban TĐKT tỉnh Thanh Hóa ban hành Quy chế sử dụng giải pháp, quy chế quản lý, cập nhật và xây dựng cơ sở dữ liệu, nhanh chóng đưa vào áp dụng triển khai toàn tỉnh từ ngày 01/7/2017 và sớm có phương án triển khai nhân rộng sản phẩm phần mềm này cho các đơn vị khác trên toàn quốc./.

CAO VIỆT CƯỜNG

Trung tâm CNTT&TT Thanh Hóa tổ chức thi cấp Chứng chỉ ứng dụng Công nghệ thông tin đợt 2 năm 2017

Theo Quyết định số 46/QĐ-SGDĐT và 47/QĐ-SGDĐT của Sở GD-ĐT tỉnh Thanh Hóa, Trung tâm CNTT&TT Thanh Hóa là đơn vị đầu tiên và cũng là duy nhất của tỉnh được cấp phép việc tổ chức bồi dưỡng, ôn thi, tổ chức thi và cấp chứng chỉ Công nghệ thông tin; Chứng chỉ được quy định tại Thông tư 03/2014/TT-2014 của Bộ Thông tin và Truyền thông.

Sáng ngày 21 tháng 5 năm 2017, Trung tâm CNTT&TT Thanh Hóa tổ chức kỳ thi sát hạch cấp Chứng chỉ công nghệ thông tin chuẩn cơ bản, đợt 2 năm 2017; Hội đồng thi được Sở GD-ĐT thành lập gồm 14 người, bao gồm đầy đủ các Ban theo quy định về việc tổ chức thi và cấp chứng chỉ ứng dụng công nghệ thông tin tại Thông tư liên tịch số 17/2016/TTLT-BGDĐT-BTTT ngày 21 tháng 6 năm 2016 giữa Bộ GD-ĐT và Bộ Thông tin và Truyền thông.

Kỳ thi Đợt 2 năm 2017, có 34 thí sinh đăng ký dự thi và chỉ có 24/34 thí sinh đã vượt qua 2 phần thi của mình là phần thi trắc nghiệm lý thuyết trực tuyến trên phần mềm và phần thi thực hành kỹ năng trên máy tính; toàn bộ hồ sơ về kỳ thi đã được gửi Sở GD-ĐT tỉnh để tiến hành cấp chứng chỉ, phôi chứng chỉ được Bộ GD-ĐT cấp theo số lượng thí sinh thi đậu, được Sở GD-ĐT Thanh Hóa phê duyệt.

Theo kế hoạch, Trung tâm liên tục thu hồ sơ đăng ký bồi dưỡng, ôn thi và được tổ chức thi 01 lần vào hằng tháng trong năm.

Mọi thông tin về đăng ký bồi dưỡng, ôn thi và đăng ký thi xin liên hệ về: **Phòng Đào tạo và Dịch vụ - Trung tâm CNTT&TT Thanh Hóa, số 73 Hàng Than, phường Lam Sơn, thành phố Thanh Hóa - ĐT: 02373.718.698 hoặc thông qua website: http://ict.thanhhoa.gov.vn**

NGUYỄN TÌNH

Chi bộ Trung tâm CNTT đại hội điểm

Thực hiện Kế hoạch số 178-KH/ĐU ngày 06/6/2017 của Đảng bộ Sở Thông tin và Truyền thông về tổ chức Đại hội chi bộ trực thuộc nhiệm kỳ 2017 - 2020. Trong các ngày 26 và 27/7/2017 Chi bộ Trung tâm CNTT đã tổ chức Đại hội lần thứ III, nhiệm kỳ 2017 - 2020.

Đây là 02 chi bộ được Đảng bộ Sở Thông tin và Truyền thông chỉ đạo tổ chức Đại hội điểm nhằm rút kinh nghiệm tổ chức Đại hội cho các chi bộ khác. Dự và chỉ đạo Đại hội có đồng chí Trần Hồng Trang - Ủy viên Ban Thường vụ, Ủy ban kiểm tra Đảng ủy khối các cơ quan tỉnh; các đồng chí trong Đảng ủy Sở, Bí thư các chi bộ trực thuộc Đảng bộ Sở và các đảng viên của các chi bộ.

Căn cứ Điều lệ Đảng lệ Đảng Cộng sản Việt Nam, các quy định trong việc tổ chức Đại hội Chi bộ, sự chỉ đạo chặt chẽ, trực tiếp của Đảng ủy Sở trong việc xây dựng các văn kiện và các bước tiến hành Đại hội, Đại hội điểm ở 02 Chi bộ đã diễn ra

theo đúng Kế hoạch và thành công tốt đẹp.

Báo cáo chính trị của Chi bộ Trung tâm CNTT khóa II trình tại Đại hội Chi bộ lần thứ III, nhiệm kỳ 2017-2020 chỉ rõ: Trong nhiệm kỳ 2015 - 2017, chi bộ đã bám sát sự lãnh đạo, chỉ đạo của BCH Đảng ủy, Ban Giám đốc để lãnh đạo cán bộ đảng viên, CBCCVC, NLĐ, triển khai hoàn thành tốt chức năng, nhiệm vụ được giao và các chương trình, kế hoạch công tác trọng tâm của Sở, Chi bộ Trung tâm CNTT đạt 100% khối lượng công việc được giao đều hoàn thành đảm bảo chất lượng và tiến độ thời gian. Công tác xây dựng Đảng luôn được chú trọng, đổi mới nội dung phương thức sinh hoạt phù hợp với tình hình thực tế, nêu cao tinh thần phê bình và tự phê bình theo tinh thần Nghị quyết Trung ương 4 (khóa XI) và thực hiện Nghị quyết Trung ương 4 (khóa XII) gắn với thực hiện "Học tập và làm theo tư tưởng, đạo đức, phong cách Hồ Chí Minh". Công tác giáo dục chính trị tư tưởng cho cán bộ đảng viên luôn được chi bộ quan tâm chú trọng.

Phát biểu chỉ đạo tại đại hội Chi bộ Trung tâm CNTT, đồng chí Trần Hồng Trang - Ủy viên Ban Thường vụ, Ủy ban kiểm tra Đảng ủy khối các cơ quan tỉnh đã biểu dương những kết quả mà Chi bộ Trung tâm CNTT đạt được trong nhiệm kỳ qua, đánh giá cao công tác tổ chức Đại hội của Chi bộ Trung tâm CNTT. Đồng chí yêu cầu trong nhiệm kỳ tới, các đồng chí đảng viên trong chi bộ tiếp tục gương mẫu đi đầu, nêu cao trách nhiệm trong mọi lĩnh vực; đoàn kết, đổi mới, tập trung thực hiện kế hoạch công tác hàng năm; nâng cao năng lực lãnh đạo và sức chiến đấu của tổ chức Đảng, chú trọng tự phê bình và phê bình; tuyên truyền, vận động đảng viên trong chi bộ chấp hành tốt chủ trương, chính sách của Đảng, pháp luật của Nhà nước, xây dựng chi bộ trong sạch vững mạnh. Đồng chí cũng nhấn mạnh: từ thành công của đại hội điểm, Đảng ủy Sở sẽ tổ chức họp rút kinh nghiệm, tiếp tục chỉ đạo, đôn đốc các chi bộ còn lại chuẩn bị tốt công tác tổ chức Đại hội đảm bảo theo kế hoạch đề ra.

VĂN BẢN MỚI

Ngày 16 tháng 3 năm 2017, Thủ tướng Chính phủ ban hành Quyết định số 05/2017/QĐ-TTg quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia.

Quyết định này quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia. Hệ thống thông tin do Bộ Quốc phòng, Bộ Công an quản lý không thuộc phạm vi điều chỉnh của Quyết định này.

Theo quyết định này, sự cố an toàn thông tin mạng nghiêm trọng là sự cố đáp ứng đồng thời các tiêu chí. Thứ nhất, hệ thống thông tin bị sự cố là hệ thống thông tin cấp độ 4, cấp độ 5 hoặc thuộc Danh mục hệ thống thông tin quan trọng quốc gia và bị một trong các sự cố sau: Hệ thống bị gián đoạn dịch vụ; Dữ liệu tuyệt mật hoặc bí mật nhà nước có khả năng bị tiết lộ; Dữ liệu quan trọng của hệ thống không bảo đảm tính toàn vẹn và không có khả năng khôi phục được; Hệ thống bị mất quyền điều khiển; Sự cố có khả năng xảy ra trên diện rộng hoặc gây ra các ảnh hưởng dây chuyền, làm tổn hại cho các hệ thống thông tin cấp độ 4 hoặc cấp độ 5 khác. Thứ hai, chủ quản hệ thống thông tin không đủ khả năng tự kiểm sát, xử lý được sự cố.

Quyết định cũng quy định cụ thể hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia. Trong đó, phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia là phương án ứng cứu cho sự cố an toàn thông tin mạng nghiêm trọng đáp ứng các tiêu chí nêu trên và hệ thống thông tin bị sự cố là hệ thống thông tin cấp độ 5 hoặc thuộc Danh mục Hệ thống thông tin quan trọng quốc gia.

Quyết định quy định cụ thể phân cấp tổ chức thực hiện ứng cứu sự cố bảo đảm an toàn thông tin mạng quốc gia. Cụ thể, Ban Chỉ đạo an toàn thông tin quốc gia đảm nhiệm chức năng Ban Chỉ đạo quốc gia về ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng (Ban Chỉ đạo quốc gia).

Ngày 25 tháng 4 năm 2017, UBND tỉnh Thanh Hóa ban hành Quyết định số 1293/2017/QĐ-UBND về Ban hành Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan quản lý nhà nước tỉnh Thanh Hóa.

Đối tượng áp dụng của Quy chế là các sở, ban, ngành cấp tỉnh, các đơn vị sự nghiệp công lập trực thuộc UBND tỉnh; UBND các huyện, thị xã, thành phố, UBND các xã, phường, thị trấn; các cán bộ, công chức, viên chức, người lao động và các tổ chức, cá nhân có liên quan tham gia vận hành, khai thác các hệ thống thông tin tại các cơ quan quản lý nhà nước; các doanh nghiệp cung cấp dịch vụ viễn thông, CNTT, Internet, các doanh nghiệp, tổ chức, cá nhân có tham gia vào các hoạt động ứng dụng CNTT của các cơ quan quản lý nhà nước. Quy chế cũng khuyến khích các cơ quan, đơn vị khác có hoạt động ứng dụng và phát triển CNTT trên địa bàn tỉnh áp dụng.

Quy chế quy định các nội dung về bảo vệ thông tin cá nhân, bảo vệ hệ thống thông tin, giám sát an toàn hệ thống thông tin và ngăn chặn xung đột thông tin trên mạng nhằm tuân thủ các quy định của Luật An toàn thông tin mạng và các văn bản pháp luật có liên quan để giúp các cơ quan quản lý nhà nước giảm thiểu tối đa các nguy cơ gây mất an toàn thông tin mạng trong hoạt động ứng dụng CNTT.

Một số quy định mới của Luật An toàn thông tin mạng và các văn bản pháp luật có liên quan được UBND tỉnh Thanh Hóa cập nhật, bổ sung quy định cụ thể tại quy chế này.

CAO VIỆT CƯỜNG

Hội thảo "Cách mạng Công nghiệp 4.0 và triển khai chính quyền điện tử trên địa bàn tỉnh Thanh Hóa"

Ngày 28-7, Tại TP Thanh Hóa, Sở Thông tin và Truyền thông phối hợp với Hội Tin học Thanh Hóa và Công ty dịch vụ Mobifone Khu vực VI tổ chức hội thảo "Cách mạng Công nghiệp 4.0 và triển khai chính quyền điện tử trên địa bàn tỉnh Thanh Hóa".

Hội thảo nhằm nâng cao nhận thức, hiểu đúng và đầy đủ để tiếp cận cuộc cách mạng công nghiệp lần thứ 4, đồng thời nêu các giải pháp để tổ chức thực hiện các đề án, kế hoạch của tỉnh trong triển khai xây dựng chính quyền điện tử, các dịch vụ thành phố thông minh trên các lĩnh vực, góp phần thúc đẩy phát triển kinh tế, xã hội, quốc phòng, an ninh của tỉnh Thanh Hóa.

Cuộc cách mạng công nghiệp lần thứ 4 được mở đầu bằng những đột phá khoa học vào thế giới vĩ mô, hình thành những công nghệ mới như công nghệ nano, in 3D, công nghệ sinh học phân tử, di truyền, trí tuệ nhân tạo (AI), Internet kết nối vạn vật (Internet of Things - IoT)... đã và đang làm biến đổi toàn bộ hệ thống sản xuất, quản lý, quản trị của mỗi quốc gia. Trong thời gian không xa, cuộc cách mạng này sẽ có tác động mạnh mẽ tới đời sống sản xuất của con người, kết nối IoT trở nên phổ biến, nhiều hoạt động sẽ được thực hiện bằng trí tuệ nhân tạo.

Toàn cảnh hội thảo.

Thực hiện chủ trương của Nhà nước về việc tăng cường năng lực tiếp cận cuộc cách mạng công nghiệp 4.0, trong thời gian qua Trung ương, Chính phủ và tỉnh Thanh Hóa đã ban hành nhiều chủ trương để đẩy mạnh ứng dụng CNTT xây dựng chính quyền điện tử, phát triển các dịch vụ thành phố thông minh, từng bước tiếp cận với các công nghệ mới trong cuộc cách mạng công nghiệp lần thứ 4.

Đối với tỉnh Thanh Hóa, những năm qua, việc ứng dụng CNTT đã có tác động tích cực đến quá trình thực hiện cải cách hành chính nhằm bảo đảm việc công khai, minh bạch, dân chủ, công bằng trong việc tiếp cận thông tin, từng bước cung cấp các dịch vụ hành chính công qua môi trường mạng, góp phần hạn chế các tiêu cực, tăng tính chính xác, kịp thời, tiện ích và hiệu quả trong giao dịch giữa chính quyền với tổ chức và công dân. Việc tổ chức hội thảo "Cách mạng Công nghiệp 4.0 và triển khai chính quyền điện tử trên địa bàn tỉnh Thanh Hóa" là điều kiện quan trọng để tổ chức thực hiện các đề án, kế hoạch của tỉnh trong triển khai xây dựng chính quyền điện tử, các dịch vụ thành phố thông minh trên các lĩnh vực, góp phần thực hiện thắng lợi Nghị quyết số 36-NQ/TW ngày 01-7-2014 của Bộ Chính trị (khóa XI) về đẩy mạnh ứng dụng, phát triển công nghệ thông tin, đáp ứng yêu cầu phát triển bền vững và hội nhập quốc tế; Nghị quyết số 36a/NQ-CP ngày 14-10-2015 của Chính phủ về Chính phủ điện tử, phấn đấu đến năm 2030 trở thành tỉnh công nghiệp theo hướng hiện đại.

Theo thanhhoa.gov.vn