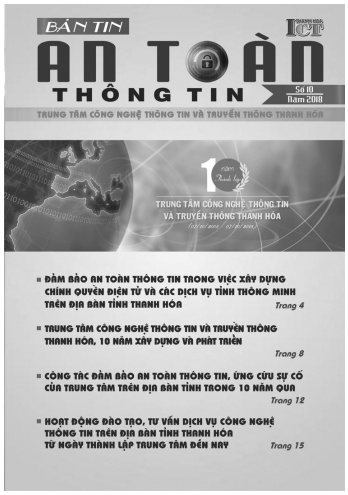
BẢN TIN
AN TOÀN THÔNG TIN
TRUNG TÂM CÔNG NGHỆ THÔNG TIN & TRUYỀN THÔNG THANH HÓA

Số 10
tháng 9/2018



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; Trần Lê Phúc

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 12/02/2018

In 500 cuốn, khổ 19x27cm
Tại Công ty TNHH In & TBGD Thanh Huệ
In xong và nộp lưu chiểu tháng 9/2018

Chủ tịch UBND tỉnh Nguyễn Đình Xứng phát biểu tại hội thảo khoa học "Triển khai mô hình xây dựng Thanh Hóa thành tỉnh thông minh giai đoạn 2017 - 2020".

Đảm bảo an toàn thông tin trong việc xây dựng chính quyền điện tử và các dịch vụ tỉnh thông minh trên địa bàn tỉnh Thanh Hóa

ThS. ĐỖ HỮU QUYẾT
Giám đốc Sở Thông tin và Truyền thông

Trong những năm qua, việc đẩy mạnh ứng dụng công nghệ thông tin (CNTT) trong hoạt động của cơ quan hành chính nhà nước, phát triển chính quyền điện tử, nhằm nâng cao hiệu lực, hiệu quả hoạt động của cơ quan nhà nước, phục vụ người dân và doanh nghiệp được Tỉnh ủy, HĐND, UBND tỉnh Thanh Hóa quan tâm lãnh đạo, chỉ đạo đã đạt được những kết quả khả quan. Theo đó, một trong số những nhiệm vụ quan trọng được tỉnh quan tâm là công tác đảm bảo an toàn, an ninh thông tin trong việc triển khai đề án xây dựng chính quyền điện tử và các dịch vụ tỉnh thông minh trên địa bàn tỉnh Thanh Hóa.

Theo báo cáo số liệu về phát triển Chính quyền điện tử tỉnh Thanh Hóa quý III/2018, hầu hết các ứng dụng CNTT phục vụ công tác quản lý, chuyên môn, nghiệp vụ được triển khai ở các sở, ban, ngành, UBND cấp huyện trên địa bàn tỉnh. Hệ thống phần mềm dùng chung đã triển khai như phần mềm quản lý văn bản và điều hành, hệ thống thư điện tử công vụ, hệ thống chữ ký số chuyên dùng, hệ thống hội nghị trực tuyến, hệ thống cổng thông tin điện tử, hệ thống một cửa điện tử tích hợp cổng dịch vụ công

trực tuyến. Các phần mềm được ứng dụng phục vụ công tác chuyên môn nghiệp vụ như: Phần mềm kế toán, kê khai thuế, bảo hiểm, phần mềm hộ tịch ở 100% các xã, phường, thị trấn trên địa bàn tỉnh...

Để đảm bảo các hệ thống ứng dụng CNTT hoạt động tốt trên mạng Internet, đa số các cơ quan quản lý nhà nước đã bước đầu quan tâm thực hiện theo các quy định của pháp luật nhằm đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng CNTT trên địa bàn tỉnh.

Hệ thống phần mềm dùng chung, phần mềm chuyên ngành, phần mềm ứng dụng nội bộ cơ bản được đảm bảo an toàn, an ninh thông tin đều được sự hỗ trợ tích cực của Sở Thông tin và Truyền thông là cơ quan quản lý nhà nước chuyên ngành về lĩnh vực Công nghệ thông tin trên địa bàn tỉnh. Hằng năm, Sở đã tổ chức các lớp đào tạo, tập huấn về CNTT và cho đội ngũ chuyên trách CNTT các sở, ban, ngành, UBND các huyện thành thị về tuyên truyền, nâng cao nhận thức giúp cho cán bộ, công chức, người dân và doanh nghiệp hiểu rõ tầm quan trọng, từ đó chủ động thực hiện các biện pháp bảo đảm an toàn, an ninh thông tin; nâng cao kiến thức về chuyên môn và kỹ năng sử dụng CNTT, đảm bảo an toàn thông tin mạng cho đội ngũ cán bộ chuyên trách CNTT trong các cơ quan Nhà nước. Đồng thời yêu cầu các cơ quan, đơn vị, doanh nghiệp tổ chức kiểm tra, rà soát và đánh giá tổng thể về công tác đảm bảo an toàn thông tin cho các hệ thống thông tin thuộc phạm vi quản lý, tổ chức thực hiện các biện pháp kỹ thuật cơ bản đảm bảo an toàn thông tin cho trang thông tin điện tử. Nhờ đó, hệ thống thông tin quan trọng của tỉnh và của các cơ quan cấp tỉnh, UBND các huyện, thành, thị đã được đầu tư, trang bị các giải pháp đảm bảo an toàn.

Tuy nhiên, công tác đảm bảo an toàn thông tin mạng ở các cơ quan, đơn vị vẫn chưa được quan tâm đúng mức. Nhiều đơn vị hệ thống mạng kết nối ngang hàng, thiếu các trang thiết bị đảm bảo an toàn thông tin mạng, các hệ thống thông tin còn tồn tại lỗ hổng bảo mật, tiềm ẩn nguy cơ gây mất dữ liệu, lây nhiễm các phần mềm độc hại ảnh hưởng đến ứng dụng và phát triển CNTT.

Mặt khác, kinh phí tổng thể đầu tư cho xây dựng hạ tầng kỹ thuật CNTT và công tác đảm bảo an toàn và an ninh thông tin còn hạn chế; việc đảm bảo an toàn, an ninh thông tin đối với các hệ thống thông tin nói chung và các hệ thống thư điện tử, quản lý văn bản và điều hành, trang thông tin điện tử nói riêng tại các cơ quan chưa được quan tâm đầu tư tương xứng; việc đảm bảo an toàn, an ninh thông tin nội bộ tại một số đơn vị vẫn chưa được đồng bộ. Đa số mới chỉ dừng lại ở mức trang bị các phần mềm diệt virus có bản quyền cho các máy tính, chưa có biện pháp đảm bảo an toàn an ninh thông tin được cài đặt đồng bộ trên toàn cơ quan do vậy khả năng phòng chống virus, bảo mật không cao. Các phần mềm diệt virus thường được sử dụng là phần mềm của các hãng BKAV, Kaspersky,...

Đội ngũ cán bộ chuyên viên phụ trách an toàn, an ninh thông tin tại các cơ quan, đơn vị còn thiếu, cần được đào tạo, tập huấn chuyên sâu về an toàn, an ninh thông tin. Từ thực tế việc chưa quan tâm đúng mức trong bảo đảm an toàn, an ninh thông tin mạng của các sở, ban, ngành, UBND các huyện, thành, thị đã dẫn đến tình trạng một số trang thông tin điện tử trên địa bàn tỉnh bị hacker tấn công dưới nhiều hình thức như: Tấn công vào cơ sở dữ liệu, chiếm quyền điều khiển, thay đổi giao diện với nội dung, hình ảnh sai lệch trên trang thông tin điện tử.

Do đó, để bảo đảm tuyệt đối an toàn cho hạ tầng và ứng dụng CNTT trong việc triển khai thành công xây dựng Chính quyền điện tử trên địa bàn tỉnh và công tác đảm bảo an toàn, an ninh thông tin trong hoạt động các cơ quan nhà nước trên địa bàn tỉnh hiệu quả hơn nữa, các Sở, ban, ngành và UBND các cấp cần coi đây là nhiệm vụ quan trọng, cấp bách, thường xuyên và lâu dài, thể hiện trách nhiệm người đứng đầu trong công tác bảo đảm an toàn thông tin mạng nhằm góp phần tạo sự chuyển biến chung trong cả tỉnh. Đồng thời, cần phải triển khai đồng bộ các giải pháp cơ bản về an toàn thông tin như sau:

1. Về môi trường pháp lý:

Rà soát, chỉnh sửa bổ sung, ban hành đầy đủ các quy chế, quy định về an toàn an ninh

thông tin; Xây dựng các tiêu chuẩn, quy chuẩn kỹ thuật, xác định chiến lược, quy hoạch chính sách ATTT của tỉnh; Tại các cơ quan, đơn vị ban hành đầy đủ các quy định nội bộ về công tác đảm bảo an toàn an ninh thông tin trong hoạt động ứng dụng CNTT phù hợp với tình hình an toàn thông tin mạng trong tình hình mới;...

Tiếp tục triển khai thực hiện tốt các nội dung đảm bảo an toàn an ninh thông tin theo yêu cầu, cụ thể như: Luật an toàn thông tin mạng; Chỉ thị số 28-CT/TW ngày 16/9/2013 của Ban Bí thư Trung ương Đảng (Khóa XI) về tăng cường công tác bảo đảm an toàn thông tin; Chỉ thị số 15/CT-TTg ngày 17/6/2014 của Thủ tướng Chính phủ về tăng cường công tác bảo đảm an ninh và an toàn thông tin mạng trong tình hình mới; Chỉ thị số 22/CT-UBND ngày 19/10/2015 của UBND tỉnh Thanh Hóa về việc tăng cường đảm bảo an ninh và an toàn thông tin mạng trong các cơ quan nhà nước trên địa bàn tỉnh Thanh Hóa; Quy chế đảm bảo An toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin (CNTT) của các cơ quan quản lý nhà nước tỉnh tại Quyết định số 1293/2017/QĐ-UBND...

2. Về triển khai các giải pháp kỹ thuật đảm bảo an toàn, an ninh thông tin:

Đầu tư nâng cấp Trung tâm An ninh mạng và An toàn dữ liệu của tỉnh để trở thành Trung tâm điều hành an ninh mạng đảm bảo an toàn, an ninh mạng cho hệ thống cơ sở dữ liệu lớn tập trung (Big Data) của tỉnh đảm bảo các quy chuẩn, tiêu chuẩn của Kiến trúc Chính quyền điện tử tỉnh Thanh Hóa để quản lý, lưu trữ các hệ thống phần mềm, CSDL của sở, ban, ngành; UBND cấp huyện, cấp xã và lưu trữ các hệ thống thông tin, dịch vụ thành phố thông minh của một số lĩnh vực tỉnh đang triển khai. Đồng thời triển khai hệ thống giám sát thông tin điện tử đảm bảo lưu trữ, kết nối các dịch vụ thành phố thông minh của tỉnh, kết nối tương tác với các Trung tâm an toàn, an ninh thông tin của Bộ Thông tin và Truyền thông và các Bộ, ngành liên quan để thực hiện nhiệm vụ giám sát, cảnh báo, ứng cứu sự cố mạng, máy tính; xử lý xung đột thông tin, an toàn thông tin mạng cho tất cả các sở, ngành, UBND cấp huyện, cấp xã.

Triển khai xác định, đánh giá hệ thống thông tin và cấp độ an toàn hệ thống thông tin tại các cơ quan trên địa bàn tỉnh theo Nghị định 85/2016/NĐ-CP về bảo đảm an toàn hệ thống thông tin theo cấp độ. Đồng thời áp dụng biện pháp quản lý và kỹ thuật nhằm bảo vệ hệ thống thông tin phù hợp theo cấp độ.

Quan tâm đầu tư trang bị thiết bị về an toàn thông tin; xem đầu tư hạng mục an toàn, an ninh thông tin là khoản đầu tư thiết yếu; có kế hoạch mua sắm, trang bị phần mềm diệt virus có bản quyền; các thiết bị chuyên dụng cho an toàn và bảo mật thông tin; thực hiện bảo trì bảo dưỡng định kỳ các thiết bị an toàn, bảo mật thông tin.

Tăng cường ký số các loại văn bản điện tử theo quy định nhằm đảm bảo an toàn trong việc trao đổi văn bản điện tử qua môi trường mạng; hệ thống xác thực tài khoản và mã hóa dữ liệu...

Tăng cường sử dụng thư điện tử công vụ để gửi các văn bản, trao đổi công việc trong các cơ quan nhà nước, tuyệt đối không sử dụng các hộp thư điện tử miễn phí (gmail, yahoo...) nhằm bảo đảm bảo mật, an toàn thông tin trên môi trường mạng.

Thường xuyên cập nhật các bản vá cập nhật phần mềm từ các nhà cung cấp sản phẩm, dịch vụ. Ngoài ra, với các tài khoản ứng dụng dùng chung cần thay đổi mật khẩu theo định kỳ, hạn chế việc sử dụng email miễn phí, trong trường hợp có đính kèm các tài liệu quan trọng gửi qua email phải đặt mật khẩu để đảm bảo an toàn...

Triển khai giải pháp lưu nhật ký đối với các hệ thống thông tin quan trọng; Đầu tư, trang bị các hệ thống giám sát mạng và cảnh báo sớm các dấu hiệu tấn công mạng. Thiết lập hệ thống sao lưu dự phòng, đảm bảo tránh rủi ro mất dữ liệu khi có sự cố xảy ra.

3. Về tăng cường công tác thông tin tuyên truyền, phổ biến:

Tổ chức thông tin tuyên truyền để cán bộ, đảng viên và nhân dân nhận thức đầy đủ vị trí, vai trò và tầm quan trọng của công tác đảm bảo an toàn thông tin mạng. Tiếp tục tăng

Các đại biểu dự hội nghị quốc tế về đô thị thông minh và Chính phủ điện tử năm 2018 tổ chức tại Thanh Hóa chụp ảnh lưu niệm.

cường triển khai các hình thức tuyên truyền, phổ biến chuyên đề về an toàn, an ninh thông tin số trước tình hình an ninh và an toàn thông tin mạng có nhiều diễn biến phức tạp như hiện nay. Qua đó nâng cao hơn nữa nhận thức, trách nhiệm của cán bộ, công chức, viên chức trên địa bàn tỉnh về các nguy cơ mất ATTT trong việc sử dụng máy tính, hệ thống mạng và khai thác thông tin trên môi trường mạng; đồng thời trang bị một số kỹ năng cơ bản sử dụng thiết bị và dịch vụ CNTT an toàn.

4. Về xây dựng, kiện toàn chức năng nhiệm vụ và nguồn nhân lực thực hiện công tác an toàn, an ninh thông tin:

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 theo Quyết định số 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

Thành lập Đội ứng cứu sự cố và tổ chức hoạt động ứng cứu sự cố trong lĩnh vực, địa bàn, phạm vi mình quản lý như: Tổ chức nghiên cứu, xây dựng các kịch bản tấn công, các nguy cơ, tình huống sự cố có khả năng xảy ra; xây dựng các phương án ứng cứu, đối phó, ngăn chặn theo kịch bản, tình huống dự kiến; Triển khai các giải pháp giám sát, phát hiện, cảnh báo sớm, kiểm tra, rà quét, đánh giá an toàn thông tin; phòng ngừa, dự phòng rủi ro; Triển khai hoạt động thường trực, điều phối, dự phòng ứng cứu, xử lý sự cố; Tổ chức đào tạo, huấn luyện, diễn tập và hoạt động của Đội ứng cứu sự cố;

Triển khai các hoạt động nghiệp vụ đặc thù bảo đảm an toàn thông tin mạng cho các hệ thống thông tin thuộc phạm vi quản lý; Tiếp tục đào tạo, tập huấn bồi dưỡng kiến thức chuyên sâu về an toàn, bảo mật thông tin cho cán bộ chuyên trách CNTT.

5. Về đẩy mạnh phối hợp trong công tác đảm bảo an toàn, an ninh thông tin:

Đẩy mạnh phối hợp với các cơ quan chức năng về an toàn thông tin mạng như: Cục An toàn thông tin mạng, Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) và các tổ chức an ninh mạng khác để thực hiện các giải pháp đảm bảo an toàn an ninh thông tin cũng như xử lý, khắc phục sự cố về an toàn thông tin mạng./.

Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa
10 NĂM XÂY DỰNG VÀ PHÁT TRIỂN

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

Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa (Trung tâm) là đơn vị sự nghiệp trực thuộc Sở Thông tin và Truyền thông tỉnh Thanh Hóa được thành lập ngày 07/10/2008 theo Quyết định số 3133/QĐ-UBND của Ủy ban nhân dân tỉnh Thanh Hóa. Trải qua 10 năm xây dựng và phát triển, vượt qua nhiều khó khăn, thách thức, Trung tâm đang ngày một vững mạnh và khẳng định được vị trí, vai trò của mình.

Với chức năng, nhiệm vụ được giao, Trung tâm đã triển khai đảm bảo an toàn thông tin, an ninh mạng máy tính và xử lý ứng cứu các sự cố liên quan đến dữ liệu, chương trình phần mềm, máy tính, mạng thông tin của các cơ quan, đơn vị, cá nhân và doanh nghiệp trên địa bàn tỉnh; Phối hợp với Trung tâm ứng cứu khẩn cấp máy tính quốc gia (VNCERT), điều phối các hoạt động ứng cứu sự cố máy tính trong tỉnh; cảnh báo kịp thời các vấn đề về an toàn, an ninh mạng máy tính; phối hợp triển khai các tiêu chuẩn kỹ thuật về an toàn, an ninh mạng máy tính; tuyên truyền phổ biến kiến thức về an toàn dữ liệu, an ninh thông tin trên địa bàn tỉnh; Phối hợp với Trung tâm chứng thực chữ ký số Quốc gia, cung cấp các dịch vụ về chứng thực chữ ký số và triển khai các biện pháp bảo đảm an toàn trong các hoạt động giao dịch điện tử, thương mại điện tử của các tổ chức, cá nhân trên địa bàn tỉnh; Tổ chức khảo sát, điều tra, thống kê, tổng hợp, phân tích số liệu về công nghệ thông tin để phục vụ cho các hoạt động quản lý nhà nước về công nghệ thông tin trên địa bàn tỉnh; Phối hợp với các cơ sở giáo dục trong và ngoài tỉnh để thực hiện việc đào tạo, bồi dưỡng, nâng cao trình độ về công nghệ thông tin cho các cơ quan, đơn vị, cá nhân và doanh nghiệp trên cơ sở kế hoạch đào tạo, bồi dưỡng đã được UBND tỉnh phê duyệt; Nghiên cứu, ứng dụng, sản xuất và chuyển giao công nghệ thông tin và truyền thông; tư vấn, dịch vụ về công nghệ thông tin và truyền thông cho các tổ chức, cá nhân và doanh nghiệp.

Về tổ chức bộ máy của Trung tâm

Những ngày đầu mới thành lập, Trung tâm gặp không ít khó khăn về cơ sở vật chất cũng như con người, với chỉ tiêu chế là 10 người. Đến nay, Trung tâm có tổng số 25 cán bộ, công chức, viên chức và người lao động và 03 phòng chuyên môn: phòng Tổng hợp Hành chính, phòng Đào tạo - Dịch vụ và phòng Quản trị hệ thống. Trên 90% cán bộ, viên chức có trình độ đại học và trên đại học (03 thạc sỹ). Đội ngũ cán bộ, công chức, viên chức được đào tạo cơ bản, nhiệt tình trong công việc, tích cực nghiên cứu và triển khai các ứng dụng CNTT cho các cơ quan, đơn vị trên địa bàn tỉnh.

Về hoạt động bảo đảm an toàn thông tin

Để Trung tâm thực hiện tốt chức năng nhiệm vụ được giao về đảm bảo an toàn thông tin mạng trên địa bàn tỉnh, ngày 15/5/2009 Chủ tịch UBND tỉnh đã có Quyết định số 1437/QĐ-UBND về việc Đầu tư trang thiết bị và công nghệ nâng cao năng lực hoạt động của Trung tâm CNTT&TT, qua đó đã đầu tư trang thiết bị và công nghệ cơ bản để hình thành Trung tâm An ninh mạng và An toàn dữ liệu của tỉnh thực hiện các nhiệm vụ lưu trữ phần mềm, trang thông tin điện tử và CSDL chuyên nghành cho các sở, ban, ngành và UBND cấp huyện. Kết nối dự phòng với Trung tâm tích hợp dữ liệu tỉnh đặt tại Văn phòng UBND tỉnh. Ngày 16/4/2015, Chủ tịch UBND tỉnh phê duyệt chủ trương đầu tư dự án "Tăng cường an ninh mạng và an toàn thông tin trên địa bàn tỉnh Thanh Hóa" tại Quyết định số 1381/QĐ-UBND, qua đó bổ sung thêm các trang thiết bị và phần mềm phục vụ cho công tác đảm bảo an toàn thông tin tại Trung tâm. Hiện nay, tại Trung tâm

An ninh mạng và An toàn dữ liệu ngoài việc lưu trữ và cung cấp các ứng dụng CNTT cho các cơ quan, đơn vị trên địa bàn tỉnh như phần mềm Quản lý văn bản và Hồ sơ công việc; trang thông tin điện tử; CSDL phần mềm chuyên ngành... Trung tâm đã triển khai các giải pháp theo dõi, giám sát tình hình hoạt động của hệ thống mạng; các dịch vụ, trang/cổng thông tin điện tử đang cung cấp tại Trung tâm đảm bảo hệ thống hoạt động ổn định 24/24. Tăng cường kiểm tra bảo mật, cập nhật các bộ lọc cho hệ thống tường lửa; hệ thống phát hiện xâm nhập; hệ thống phòng chống mã độc; hệ điều hành máy chủ và ứng dụng, dịch vụ đang hoạt động tại Trung tâm. Đồng thời, theo dõi và ghi nhận kịp thời các thông tin đăng tải trên mạng có nội dung gây kích động và có thông tin sai lệch nhằm chống phá Đảng và đi ngược lại với chính sách của Nhà nước. Đặc biệt là những thông tin có xuất phát từ các trang Web có máy chủ đặt trên địa bàn tỉnh để kịp thời báo cáo các cấp có thẩm quyền và có biện pháp xử lý nhanh và kịp thời để gỡ bỏ ngay các nội dung.

Bên cạnh đó, để chủ động bảo đảm an toàn thông tin cho hoạt động ứng dụng CNTT của các cơ quan, đơn vị trên địa bàn tỉnh. Trung tâm đã chủ động thành lập và kiện toàn nhân sự của Tổ ứng cứu sự cố mạng, máy tính của Trung tâm với 09 thành viên nhằm nâng cao hiệu quả công tác đảm bảo an toàn thông tin mạng, 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. Hàng năm, Trung tâm đã hỗ trợ ứng cứu hàng trăm lượt sự cố liên quan đến các phần mềm dùng chung, hệ thống thông tin của các cơ quan, đơn vị trên địa bàn tỉnh. Đồng thời thông qua hệ thống giám sát tại Trung tâm, đã kịp thời ban hành các công văn cảnh báo lỗ hổng an toàn thông tin và website bị tin tặc tấn công trên địa bàn tỉnh. Theo đó, trong 10 năm qua, một số hệ thống thông tin quan trọng của tỉnh mặc dù có hiện tượng bị rà quét, tấn công, nhưng đều được ngăn chặn kịp thời nên không có thiệt hại lớn. Các hệ thống thông tin trọng yếu thường xuyên được cập nhật các bản vá, rà quét các lỗ hổng. Mặt khác, để nâng cao nhận thức về an toàn thông tin cho cán bộ, công chức, viên chức và người lao động trên địa bàn tinh. Từ năm 2017 đến nay, Trung tâm đã xây dựng các Bản tin An toàn thông tin định kỳ 02 tháng/01 số, với nội dung tập trung vào việc hướng dẫn các kỹ năng cơ bản và nâng cao trong việc đảm bảo an toàn thông tin trong hoạt động ứng dụng CNTT tại các cơ quan, đơn vị.

Năm 2018, Trung tâm được giao quản lý, vận hành kỹ thuật hệ thống thiết bị phục vụ Hội nghị truyền hình trực tuyến, gồm 31 điểm cầu bao gồm: điểm cầu Văn phòng UBND tỉnh, điểm cầu Văn phòng Tỉnh ủy, điểm cầu Ban quản lý khu kinh tế Nghi Sơn và các Khu công nghiệp, điểm cầu Sở TT&TT và 27 điểm cầu tại Văn phòng UBND của 27 huyện, thị xã, thành phố. Trung tâm thường xuyên làm tốt công tác vận hành hệ thống, trong năm 2018 Trung tâm CNTT&TT Thanh Hóa đã phục vụ được hơn 30 cuộc Hội nghị trực tuyến của UBND tỉnh, các Ban của Tỉnh

ủy, các sở, ngành cấp tỉnh với địa phương. Hầu hết các cuộc Hội nghị trực tuyến triển khai được nhanh, số lượng cán bộ, bộ phận dự họp được nhiều hơn, chất lượng hình ảnh, âm thanh, ánh sáng đảm bảo tiêu chuẩn kỹ thuật.

Về hoạt động nghiên cứu, sản xuất phần mềm và chuyển giao các ứng dụng Công nghệ thông tin

Ban Giám đốc Trung tâm xác định xây dựng phát triển và chuyển giao phần mềm là hoạt động trọng tâm xuyên suốt, bằng sự nổ lực của các cán bộ làm công tác nghiên cứu, phát triển phần mềm, sự hợp tác của các chuyên gia, sau 10 năm hoạt động Trung tâm đã xây dựng các phần mềm phục vụ quản lý hành chính Nhà nước cho các sở, ban, ngành như: phần mềm trực tuyến phục vụ công tác chỉ đạo, điều hành, quản lý của tỉnh về đất đai; phần mềm Viễn thông công ích; Phần mềm Font chữ Thái cổ; xây dựng các giải pháp Cổng thông tin điện tử Đoàn Đại biểu Quốc hội và HĐND tỉnh; Trang thông tin điện tử các đơn vị: Đảng ủy khối các cơ quan tỉnh, Sở Tài nguyên & Môi trường, Sở Thông tin & Truyền thông, Sở Tư pháp, Liên đoàn lao động tỉnh, Liên hiệp các hội KHKT tỉnh, Trang thông tin điện tử Thành nhà Hồ, đã giúp quảng bá hình ảnh Khu di tích Thành nhà Hồ đến các du khách trong và ngoài nước, góp phần đưa Thành nhà Hồ thành di sản Văn hóa Thế giới, được UNESCO công nhận vào tháng 8 năm 2011, Trang thông tin điện tử cho Huyện ủy Quan Sơn, Sở Tư pháp, Sở Giao thông vận tải; Ban dân tộc, Đài khí tượng thủy văn Thanh Hóa, Công ty TNHH MTV Xổ số kiến thiết Thanh Hoá, Chi cục An toàn vệ sinh thực phẩm... Đặc biệt, sản phẩm Phần mềm trực tuyến quản lý thông tin hồ sơ về Người có công của trung tâm đạt giải thưởng "Sáng tạo trẻ" toàn quốc lần thứ VIII năm 2015 do Trung ương Đoàn TNSC Hồ Chí Minh tổ chức, giải Nhất hội thi Sáng tạo Khoa học kỹ thuật Thanh Hóa năm 2015...

Về hoạt động đào tạo, dịch vụ của Trung tâm

Với vai trò là đơn vị trực thuộc Sở Thông tin và Truyền thông, ngay từ những ngày đầu thành lập, Trung tâm đã tham gia đào tạo, hướng dẫn cán bộ, công chức, viên chức sử dụng các phần mềm CNTT phục vụ các hoạt động quản lý nhà nước. Trung tâm đã tiến hành tập huấn sử dụng và thường xuyên hỗ trợ phần mềm Quản lý văn bản và Hồ sơ công việc (TDOffice) cho cán bộ của 48 đơn vị thuộc sở, ban, ngành, huyện, thị xã, thành phố trên địa bàn tỉnh. Tập huấn triển khai sử dụng phần mềm Mã nguồn mở; Phối hợp đào tạo cho gần 1.400 cán bộ, giáo viên ngành Giáo dục & Đào tạo theo chuẩn của Dự án Hỗ trợ đổi mới quản lý Giáo dục (SREM); Đã đào tạo tin học ứng dụng thuộc Dự án Ứng dụng CNTT trong các cơ quan Đảng cho huyện, thị ủy và các đơn vị trực thuộc của các huyện, thị ủy; Xây dựng tài liệu và tham gia giảng dạy lớp đào tạo đảm bảo an toàn thông tin và tiêu chuẩn ISO 27001:2005 cho cán bộ quản trị mạng của các đơn vị trên địa bàn tỉnh; Phối hợp triển khai đào tạo, hướng dẫn sử dụng phần mềm thi đua khen thưởng tỉnh Thanh Hóa cho cán bộ thi đua khen thưởng và cán bộ làm công tác thi đua khen thưởng các đơn vị trên địa bàn tỉnh và phối hợp với Sở khoa học và công nghệ tổ chức lớp đào tạo hệ thống thông tin Khoa học và công nghệ cho cán bộ hoạt động khoa học công nghệ; Triển khai tổ chức đào tạo kỹ năng duy trì bền vững Dự án cho cán bộ thư viện huyện, xã và điểm Bưu điện văn hóa xã cho 06 tỉnh (Sơn La, Điện Biên, Lai Châu, Lào Cai, Phú Thọ, Yên Bái) của gói thầu D12.05 thuộc dự án Nâng cao khả năng sử dụng máy tính và truy nhập internet công cộng tại Việt Nam; Tổ chức lớp đào tạo "Kiểm tra, đánh giá an toàn thông tin và bảo mật cho các hệ thống thông tin"; Xây dựng giáo trình, tài liệu, ngân hàng câu hỏi, hồ sơ đăng ký cấp phép đào tạo, bồi dưỡng, tổ chức thi sát hạch và cấp chứng chỉ theo Thông tư 03/2014/TT-BTTTT ngày 11/3/2014 của Bộ Thông tin và Truyền thông quy định Chuẩn kỹ năng sử dụng CNTT cơ bản; Để hoàn thiện tiêu chí số 8 về thông tin truyền thông theo chuẩn nông thôn mới, đã triển khai đào tạo, tập huấn phần mềm Quản lý văn bản và Hồ sơ công việc cho các đơn vị cấp xã trên địa bàn tỉnh.

Song song với các chương trình đào tạo, các dự án CNTT cũng được triển khai trên diện rộng như: Tư vấn lập dự án, Tư vấn giám sát, triển khai các dự án, dịch vụ (phần mềm quản lý văn bản, lắp đặt mạng LAN cho các sở, ban ngành, huyện, thị xã, thành phố...). Với những kinh nghiệm dần được tích lũy cả về chất và lượng, năng lực của

Trung tâm đã đáp ứng đủ các điều kiện tham gia các dự án với tư cách nhà thầu liên danh và nhà thầu độc lập. Trong thời gian qua Trung tâm đã và đang triển khai có hiệu quả các nhiệm vụ, hoạt động về tư vấn, xây dựng hồ sơ thiết kế kỹ thuật, giám sát thi công, nghiên cứu phát triển phần mềm. Bên cạnh đó, Trung tâm cũng tham gia tích cực triển khai hỗ trợ kỹ thuật, lắp đặt mạng máy tính, trực kỹ thuật phục vụ các sự kiện chính trị lớn của Tỉnh như: Đại hội Đảng, bầu cử HĐND tỉnh, các sự kiện quốc gia tổ chức tại Thanh Hóa; các hội nghị, hội thảo, hội chợ,... do các cơ quan, đơn vị tổ chức. Triển khai các dịch vụ CNTT: Hosting, thiết kế website cho một số cơ quan, đơn vị trên địa bàn tỉnh.

Về hoạt động Khoa học công nghệ

Với mong muốn thúc đẩy công tác nghiên cứu khoa học, nâng cao hiệu quả công tác, Trung tâm khuyến khích phát huy tinh thần làm chủ, tự chịu trách nhiệm, phát huy sáng kiến của tập thể cán bộ, viên chức, người lao động trong việc nghiên cứu đúc kết các sáng kiến kinh nghiệm thiết thực phục vụ các nhu cầu cụ thể như: Đề tài khoa học: "Xây dựng phần mềm trực tuyến, hỗ trợ chỉ đạo điều hành quản lý đất đai của tỉnh" đã được hoàn thiện và đã được Hội đồng khoa học cấp tỉnh xếp loại xuất sắc. Kết quả của đề tài đang được ứng dụng thành công tại Sở Tài nguyên & Môi trường, UBND huyện Vĩnh Lộc. Ngoài ra, Trung tâm đã phối hợp thực hiện các đề tài, dự án cho đến nay các đề tài đã đưa vào áp dụng trong thực tiễn như: "Nghiên cứu, sưu tầm, biên soạn tài liệu, xây dựng Font chữ và số hoá chữ Thái cổ Thanh Hoá"; Dự án "Xây dựng phần mềm trực tuyến quản lý các trạm thu, phát sóng thông tin di động (BTS) phục vụ sự chỉ đạo, điều hành của tỉnh"; Đề tài "Nghiên cứu giải pháp đồng bộ nâng cao tính bảo mật và an toàn thông tin của Báo Thanh Hóa"; "Nghiên cứuxây dựng cơ sở dữ liệu đồng bộphục vụ công tác thi đua khen thưởng tỉnh Thanh Hoá".

Về công tác tổ chức đoàn thể

Cùng với việc tổ chức bộ máy các phòng chuyên môn, các tổ chức đoàn thể quần chúng cũng từng bước được thành lập, bước đầu cũng có nhiều thuận lợi vì được sinh hoạt ghép với các tổ chức của Sở như: Chi bộ Đảng đang sinh hoạt ghép cùng với Phòng QL CNTT, tổ Công đoàn đang sinh hoạt chung với Công đoàn Sở, đoàn Thanh niên đang sinh hoạt chung với Chi đoàn Thanh niên của Sở..., các tổ chức đoàn thể quần chúng dần dần đi vào hoạt động ổn định với nhiều chương trình hoạt động sôi nổi, bổ ích và thiết thực. Cho đến thời điểm hiện tại Trung tâm đã có Chi bộ Trung tâm CNTT (có 07 đảng viên); Công đoàn Bộ phận Trung tâm CNTT&TT (có 25 đoàn viên).

Công tác phát triển Đảng được quan tâm, 10 năm qua đã giới thiệu kết nạp được 07 quần chúng ưu tú đứng vào hàng ngũ của Đảng; 01 quần chúng ưu tú đang được xem xét kết nạp vào hàng ngũ của Đảng; 100% cán bộ mới tiếp nhận về Trung tâm công tác được gia nhập tổ chức công đoàn và đoàn thanh niên. Các đoàn viên Công đoàn, Đoàn Thanh niên luôn tích cực tham gia các hoạt động văn hóa văn nghệ, thể dục thể thao do Công đoàn, Đoàn TN Sở, Công đoàn Viên chức và Đoàn Cơ quan cấp tỉnh tổ chức. Trung tâm cũng đã tích cực tham gia các hoạt động từ thiện, hoạt động xã hội do các tổ chức trong tỉnh phát động.

Với những kết quả, thành tích đạt được trong 10 năm qua, CB,VC, người lao động Trung tâm đã được các cấp ghi nhận khen thưởng. Về tập thể, từ năm 2010- 2017, Trung tâm có 6 năm đạt danh hiệu"Tập thể lao động xuất sắc" và 4 năm được tặng Bằng khen của Bộ Thông tin và Truyền thông, Chủ tịch UBND tỉnh, Liên hiệp Hội Khoa học Việt Nam, Hội Tin học Việt Nam. Về cá nhân, trong 10 năm qua, nhiều cá nhân được Bộ trưởng Bộ TT &TT, Chủ tịch UBND tỉnh, Liên hiệp Hội Khoa học Việt Nam, Hội Tin học Việt Nam tặng Bằng khen và Giám đốc Sở tặng Giấy khen.

Cùng với kết quả thành tích đạt được của Trung tâm trong chặng đường 10 năm đã đi qua, chặng đường tiếp theo đang mở ra nhiều cơ hội và thách thức đối với đội ngũ CBCCVC, người lao động của Trung tâm đòi hỏi cần phát huy hơn nữa trí tuệ, khả năng, đoàn kết chung sức, chung lòng, xây dựng Trung tâm CNTT&TT ngày càng phát triển, phấn đấu hoàn thành nhiệm vụ được giao, góp phần xây dựng sự nghiệp thông tin và truyền thông của tỉnh ngày càng phát triển./.

Công tác đảm bảo an toàn thông tin, ứng cứu sự cố của Trung tâm trên địa bàn tỉnh trong 10 năm qua

TRẦN NGỌC HƯNG
Phó Trưởng phòng Quản trị hệ thống
Trung tâm CNTT&TT Thanh Hóa

Trong những năm qua trên địa bàn tỉnh, hạ tầng, ứng dụng công nghệ thông tin (CNTT) được tích cực triển khai đầu tư mạnh mẽ. Hệ thống mạng tại các cơ quan nhà nước được xây dựng phát triển mở rộng, kết nối thông suốt từ cấp tỉnh đến cấp huyện, thị xã, thành phố và mạng Internet phát triển đến cấp xã phường, thị trấn. Trong đó, có nhiều phần mềm ứng dụng dùng chung quy mô lớn, triển khai từ cấp tỉnh đến cấp xã, phường, thị trấn như: Phần mềm quản lý văn bản và Hồ sơ công việc; Thư điện tử công vụ; Phần mềm một cửa điện tử liên thông; hệ thống hội nghị truyền hình trực tuyến...tuy nhiên bên cạnh đó cũng tiềm ẩn nhiều nguy cơ mất an toàn thông tin (ATTT) bởi các cuộc tấn công mạng ngày càng gia tăng. Trên địa bàn tỉnh cũng đã xảy ra một số cuộc tấn công mạng nguy hiểm, với thủ đoạn tinh vi, phức tạp nhằm vào hệ thống mạng CNTT của các cơ quan nhà nước. Điều này đang đặt ra vấn đề cấp bách, đòi hỏi cần tăng cường công tác đảm bảo bảo mật và ATTT trên địa bàn tỉnh Thanh Hóa.

Với vai trò là đơn vị có chức năng đảm bảo an toàn thông tin, an ninh mạng máy tính và xử lý ứng cứu sự cố liên quan đến dữ liệu, chương trình phần mềm, máy tính, mạng thông tin của các cơ quan, đơn vị, cá nhân và doanh nghiệp trên địa bàn tỉnh và các nhiệm vụ khác theo Quyết định 3133/QĐ-UBND ngày 07/10/2008 của Chủ tịch UBND tỉnh Thanh Hóa. Ngay từ ngày đầu thành lập Trung tâm, Ban Giám đốc và lãnh đạo phòng Quản trị hệ thống đã xác định đây là nhiệm vụ hàng đầu của Trung tâm trong việc đảm bảo an toàn thông tin cho các cơ quan, đơn vị trên địa bàn tỉnh. Qua đó đề ra các biện pháp, cách thức triển khai phù hợp với thực trạng ứng dụng CNTT trên địa bàn tỉnh và lộ trình cho những năm tiếp theo, cụ thể như sau:

Về tổ chức hoạt động, quy trình, nhân lực:

- Với số lượng 07 cán bộ ban đầu được giao về phòng Quản trị hệ thống, lãnh đạo phòng đã sắp xếp, phân công tổ chức thành các nhóm làm việc khác nhau. Trong đó, tập trung các cán bộ có trình độ về kỹ thuật hệ thống để bước đầu hình thành nên nhóm hệ thống phụ trách công tác về an toàn thông tin và ứng cứu xử lý sự cố. Đến nay Trung tâm đã kiện toàn về mặt tổ chức và ban hành quyết định về thành lập Tổ ứng cứu xử lý sự cố mạng, máy tính của Trung tâm với 09 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 ứng cứu sự cố 24/7 cho các cơ quan, đơn vị trên địa bàn tỉnh. Việc thành lập Tổ ứng cứu sự cố 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. Đồng thời, Trung tâm cũng đã ban hành Quy định về việc ứng cứu sự cố, xử lý sự cố mạng, máy tính. Đây là các quy định bao quát đầy đủ các nội dung trong việc xử lý và khắc phục khi có sự cố xảy ra là cơ sở để hoạt động ứng cứu sự cố được triển khai khoa học và đảm bảo sự cố được xử lý nhanh chóng và kịp thời.

- 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

Phần mềm tổng hợp ứng cứu sự cố trực tuyến.

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 với các đầu mối liên hệ tại các cơ quan, đơn vị quản lý nhà nước để hình thành mạng lưới và được kết nối thường xuyên, liên tục trên địa bàn toàn tỉnh. Đồng thời, đảm bảo sự phối hợp ngăn chặn, xử lý kịp thời và khắc phục nhanh chóng các sự cố mạng ở các cơ quan, đơn vị trên địa bàn tỉnh.

- Trung tâm cũng đã triển khai phần mềm tổng hợp xử lý ứng cứu sự cố trực tuyến trên môi trường mạng và cung cấp các tài khoản truy cập cho các đầu mối tại các cơ quan, đơn vị để triển khai nhanh chóng các thông tin sự cố và hướng dẫn khắc phục sự cố một cách nhanh chóng và hiệu quả.

- Hàng năm, Trung tâm tiến hành rà soát bổ sung trang thiết bị chuyên dụng phục vụ công tác ứng cứu sự cố như các phần mềm dò quét lỗ hổng, thiết bị sao lưu dữ liệu phục vụ điều tra số... Đồng thời cử các thành viên trong Tổ ứng cứu sự cố tham gia các lớp đào tạo về an toàn thông tin, diễn tập an ninh mạng nhằm tăng cường năng lực, kỹ năng trong hoạt động đảm bảo an toàn thông tin mạng.

Về hoạt động triển khai công tác ứng cứu sự cố và đảm bảo an toàn thông tin mạng

- Với vai trò là cơ quan tham mưu cho Sở Thông tin và Truyền thông và UBND tỉnh trong việc quản lý nhà nước về an toàn thông tin trên địa bàn tỉnh. Trong những năm qua 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 cho các cơ quan và các tổ chức, doanh nghiệp trên địa bàn tỉnh. Đồng thời theo chức năng, nhiệm vụ được giao, Trung tâm chủ động triển khai các kế hoạch 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 xử lý sự cố tại các cơ quan, đơn vị trên địa bàn tỉnh. Qua đó giúp các đơn vị giảm thiểu các rủi ro, nguy cơ mất an toàn thông tin trong việc ứng dụng CNTT tại đơn vị mình.

- Hằng năm, bình quân Trung tâm thực hiện ứng cứu khoảng 600 lượt sự cố liên quan đến phần mềm ứng dụng, các trang thông tin điện tử và sự cố thông tin khác, ban hành hàng chục các văn bản cảnh báo sớm các sự cố gây mất an toàn thông tin như mã độc hại, tấn công trang thông tin điện tử... Đặc biệt, trong những ngày trước, trong và sau các sự kiện lớn của đất nước và tỉnh, 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.

Trải qua 10 năm xây dựng và phát triển, vượt qua nhiều khó khăn và thách thức về nhân lực, trang thiết bị... Đặc biệt là tình hình an toàn thông tin mạng ngày càng diễn biến phức tạp. Tập thể Trung tâm đã chủ động triển khai những giải pháp đồng bộ, kịp thời, nên vấn đề về an toàn thông tin mạng và ứng cứu xử lý sự cố cho các cơ quan, đơn vị của tỉnh Thanh Hóa trong những năm gần đây luôn được đảm bảo. Điều này giúp cho các hệ thống CNTT của tỉnh luôn hoạt động thống nhất, ổn định, hiệu quả, đáp ứng sự chỉ đạo điều hành của các cấp ủy Đảng, Chính quyền, cũng như phục vụ tốt người dân và doanh nghiệp./.

Trung tâm An ninh mạng và An toàn dữ liệu của tỉnh.

Hoạt động đào tạo, tư vấn dịch vụ công nghệ thông tin trên địa bàn tỉnh Thanh Hóa từ ngày thành lập Trung tâm đến nay

TRỊNH NGỌC QUỲNH
Phó Trưởng phòng Đào tạo dịch vụ
Trung tâm CNTT&TT Thanh Hóa

Chính thức được thành lập từ ngày 07/10/2008, sau 10 năm phát triển, Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa (Trung tâm) đã đạt được nhiều bước phát triển ấn tượng, nhất là trong lĩnh vực đào tạo, tập huấn công nghệ thông tin. Trong hành trình 10 năm qua, Trung tâm đã luôn là đơn vị tiên phong trong việc trang bị kiến thức tin học căn bản như cách sử dụng máy tính và internet an toàn cho cán bộ, công chức, nhân dân, góp phần phổ cập sâu rộng và đưa công nghệ trở thành một phần cuộc sống của người dân Thanh Hóa như hiện nay.

Với vai trò, chức năng Đào tạo, liên kết đào tạo, bồi dưỡng chuyên môn nghiệp vụ về công nghệ thông tin và truyền thông để góp phần phát triển nguồn nhân lực về công nghệ thông tin và truyền thông phục vụ nhu cầu phát triển kinh tế xã hội của tỉnh; ngay từ những ngày đầu thành lập, phòng Đào tạo và Dịch vụ của Trung tâm đã tham gia đào tạo, hướng dẫn cán bộ, công chức, viên chức sử dụng các phần mềm công nghệ thông tin phục vụ các hoạt động quản lý nhà nước, hướng dẫn cho cán bộ cấp xã, phường các kiến thức cơ bản về máy tính, phần cứng, phần mềm, internet.

Bắt đầu từ năm 2009, chương trình đào tạo mã nguồn mở với hệ điều hành Ubuntu, phần mềm soạn thảo Open Office... được phổ cập đến cán bộ và người dân một cách bài bản và thực tế. Trong quá trình đi triển khai đào tạo ứng dụng CNTT tại các đơn vị trên địa bàn tỉnh, cán bộ phòng Đào tạo và Dịch vụ cũng giới thiệu và khuyến khích người dùng cài đặt và sử dụng các phần mềm tiện ích miễn phí để tránh vi phạm bản quyền. Những ngày đầu làm công tác đào tạo, cán bộ phòng Đào tạo và Dịch vụ gặp rất nhiều khó khăn như: trang thiết bị thiếu, cơ sở vật chất yếu, người dân hoàn toàn không biết, chưa thấy, chưa được sờ vào chiếc máy tính. Lớp đông, máy ít, có khi 4-5 người học chung một máy, trình độ học viên không đều. Các lớp phổ cập tin học đến tận vùng sâu, vùng xa nên cả cán bộ đào tạo lẫn học viên đều đi lại rất vất vả. Các xã miền núi điều kiện kinh tế khó khăn, nhiều xã thậm chí chưa có điện, chưa kết nối internet nên học xong học viên không có điều kiện thực hành thường xuyên, dẫn đến học trước quên sau...Đội ngũ cán bộ đào tạo của Trung tâm khi đó còn rất trẻ, kinh nghiệm thực tiễn chưa nhiều, nhưng bù lại có được nhiệt huyết tuổi trẻ, trình độ chuyên môn, niềm tin, dám nghĩ dám làm, dám đương đầu với thử thách. Thêm vào đó, sự nhiệt tình, háo hức, ham học hỏi của các học viên đã tiếp thêm sức mạnh cho lý tưởng, mục tiêu của cán bộ triển khai, cố gắng hết sức mình hoàn thành mục tiêu đã đề ra.

Năm 2009, UBND tỉnh phê duyệt dự án "Hoàn thiện một số hệ thống thông tin số, phục vụ sự chỉ đạo, điều hành và quản lý của tỉnh", quyết định đưa phần mềm Quản lý văn bản và Hồ sơ công việc (TDOffice) vào sử dụng trong các cơ quan hành chính nhà nước tại tỉnh Thanh Hóa nhằm đẩy mạnh ứng dụng công nghệ thông tin gắn với cải cách thủ tục hành chính; thay thế phương thức gửi nhận văn bản truyền thống giữa các cơ quan hành chính nhà nước bằng phương pháp gửi nhận điện tử thông qua văn bản điện tử. Trung tâm CNTT&TT Thanh Hóa được giao nhiệm vụ cài đặt, tập huấn, hướng dẫn sử dụng phần mềm TDOffice cho 48 đơn vị (27 huyện thị và 21 sở, ban, ngành) thụ hưởng dự án trên địa bàn tỉnh. Cán bộ phòng Đào tạo và Dịch vụ với chuyên môn vững vàng và tinh thần nhiệt huyết cao đã hoàn thành xuất sắc công tác đào tạo, hướng dẫn sử dụng phần mềm TDOffice cho

cán bộ, công chức của 48 đơn vị, góp phần lớn vào thành công của dự án. Kể từ đó, hình ảnh Trung tâm CNTT&TT Thanh Hóa đã được tất cả các đơn vị trong tỉnh biết đến, đưa vị thế của Trung tâm lên một tầm cao mới. Xứng đáng là đơn vị đi đầu trong lĩnh vực đào tạo và dịch vụ về CNTT trên địa bàn tỉnh.

Qua thời gian, công tác đào tạo của Trung tâm CNTT&TT Thanh Hóa ngày càng phát triển. Đội ngũ cán bộ, nhân viên ngày càng lớn mạnh về số lượng và chất lượng. Điều đó được thể hiện qua việc Trung tâm luôn là đơn vị được UBND tỉnh và Sở TT&TT Thanh Hóa tin tưởng giao nhiệm vụ đào tạo, tập huấn các dự án về CNTT trên địa bàn tỉnh. Không chỉ dừng lại ở phạm vi trong tỉnh, Trung tâm còn triển khai tổ chức đào tạo kỹ năng duy trì bền vững Dự án cho cán bộ thư viện huyện, xã và điểm Bưu điện văn hóa xã cho 06 tỉnh (Sơn La, Điện Biên, Lai Châu, Lào Cai, Phú Thọ, Yên Bái) của gói thầu D12.05 thuộc dự án Nâng cao khả năng sử dụng máy tính và truy nhập internet công cộng tại Việt Nam. Trung tâm CNTT&TT Thanh Hóa đã trở thành địa chỉ tin cậy của các cá nhân và tổ chức mỗi khi cần tư vấn, hỗ trợ về lĩnh vực CNTT.

Bên cạnh đó, Trung tâm CNTT&TT Thanh Hóa cũng được các đơn vị trong tỉnh lựa chọn để phối hợp thực hiện công tác đào tạo, tập huấn cho các dự án, tiêu biểu trong đó là các đơn vị như: Sở NN&PTNT, Sở Giáo dục và Đào tạo, Đảng ủy khối cơ quan tỉnh...

Năm 2016, sau khi nghiên cứu Thông tư số 03/2014/TT-BTTTT của Bộ TT&TT quy định chuẩn kỹ năng sử dụng CNTT và Thông tư liên tịch số 17/2016/TTLT-BGDĐT-BTTTT ngày 21/6/2016 của Liên Bộ Giáo dục và Đào tạo và Bộ Thông tin và Truyền thông quy định tổ chức thi và cấp chứng chỉ ứng dụng Công nghệ thông tin cơ bản. Trung tâm đã chuẩn bị đầy đủ các điều kiện về nhân lực, cơ sở vật chất cũng như nội dung đào tạo để xin cấp phép tổ chức thi và cấp chứng chỉ ứng dụng công nghệ thông tincông nghệ thông tin. Ngày 20/01/2017 Trung tâm đã được Sở Giáo dục và Đào tạo Thanh Hóa ký quyết định về việc cho phép Trung tâm Công nghệ thông tin và Truyền thông tổ chức thi và cấp chứng chỉ ứng dụng công nghệ thông tin. Trung tâm trở thành đơn vị đầu tiên trong tỉnh được cấp phép tổ chức thi và cấp chứng chỉ ứng dụng công nghệ thông tin.

Sau khi được cấp phép, trong hai năm 2017 - 2018 Trung tâm đã tiến hành tuyển sinh, đào tạo, tổ chức thi và cấp chứng chỉ ứng dụng công nghệ thông tin được 13 đợt thi cho hàng ngàn lượt học viên đạt yêu cầu. Nhìn lại chặng đường 10 năm hoạt động của Trung tâm CNTT&TT, thấy được công tác đào tạo đã có những thành công rực rỡ, góp phần lớn vào sự lớn mạnh và phát triển chung của Trung tâm).

Nhìn lại chặng đường 10 năm hoạt động của Trung tâm CNTT&TT, thấy được công tác đào tạo đã có những thành công rực rỡ, góp phần lớn vào sự lớn mạnh và phát triển chung của Trung tâm./.

Hoạt động xây dựng, chuyển giao phần mềm
TẠI TRUNG TÂM CNTT&TT THANH HÓA

TRẦN LÊ PHÚC
Phó Trưởng phòng Quản trị hệ thống
Trung tâm CNTT&TT Thanh Hóa

Được xác định là một trong những lĩnh vực chính trong hoạt động của trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa (Trung tâm), ngay từ những ngày đầu thành lập, Ban Giám đốc Trung tâm đã xác định xây dựng, phát triển và chuyển giao phần mềm là hoạt động trọng tâm, lâu dài và xuyên suốt, là động lực để thúc đẩy các hoạt động chuyên môn khác của trung tâm. Trong 10 năm qua (giai đoạn 2008-2018), Phòng Quản trị hệ thống với chức năng nhiệm vụ được giao đã tổ chức các cán bộ trong phòng có năng lực, kỹ năng về phần mềm để hình thành nên nhóm Phần mềm, từng bước thực hiện các nhiệm vụ về nghiên cứu, sản xuất, gia công, chuyển giao phần mềm.

Bằng sự nỗ lực của Ban Giám đốc, bộ phận phần mềm, các cán bộ làm công tác nghiên cứu, phát triển, sự hợp tác của các chuyên gia, hoạt động xây dựng, chuyển giao phần mềm tại Trung tâm đã khắc phục những khó khăn về nhân sự, cơ sở vật chất, các yếu tố đặc thù trong tư vấn, ứng dụng công nghệ thông tin của khối cơ quan nhà nước, từng bước đưa các sản phẩm phần mềm phát triển theo chiều sâu, tăng hàm lượng chất xám, dần hình thành những sản phẩm phù hợp yêu cầu của các doanh nghiệp trong và ngoài tỉnh, nâng cao giá trị gia tăng trong nguồn thu của Trung tâm.

Một trong những sản phẩm nổi bật được Trung tâm xây dựng và phát triển phải kể đến nhóm phần mềm phục vụ quản lý hành chính Nhà nước cho các sở, ban, ngành như: phần mềm trực tuyến phục vụ công tác chỉ đạo, điều hành, quản lý của tỉnh về đất đai; phần mềm Viễn thông công ích; phần mềm phục vụ công tác Thi đua khen thưởng; Phần mềm thống kê công tác Dân tộc, phần mềm quản lý ngân hàng dữ liệu tổng hợp khí tượng thủy văn; xây dựng hệ thống Cổng/trang thông tin điện tử cho nhiều cơ quan tiêu biểu như: Đoàn Đại biểu Quốc hội và Hội đồng nhân dân tỉnh, Đảng ủy khối các cơ quan tỉnh, Sở Tài nguyên và Môi trường, Sở Thông tin và Truyền thông, Sở Tư pháp, Sở Giao thông vận tải, Liên đoàn lao động tỉnh, Liên hiệp các hội Khoa học kỹ thuật tỉnh; Một số trang thông tin điện tử đặc thù, quảng bá hoạt động du lịch Thanh Hóa như: Trang thông tin điện tử Thành nhà Hồ quảng bá hình ảnh Khu di tích Thành nhà Hồ, di sản được UNESCO công nhận vào tháng 8/2011 cũng như đất và người Xứ Thanh đến các du khách trong và ngoài nước; trang thông tin điện tử quảng bá hoạt động du lịch cộng đồng của Bản Ngàm, Huyện Quan Sơn...

Ngoài ra, Trong những năm qua Trung tâm đã tích cực đấu mối, mở rộng mối quan hệ với các cơ quan, gắn kết với nhiều doanh nghiệp có thế mạnh trên các lĩnh vực công nghệ thông tin đặc thù, từ đó xây dựng mối quan hệ hợp tác, phát huy sở trường, thế mạnh của nhau cùng phát triển. Trung tâm còn làm tốt hoạt động chuyển giao công nghệ, phần mềm, thực hiện liên kết chặt chẽ với một số đơn vị hoạt động trong lĩnh vực công nghệ thông tin như Viện Công nghệ phần mềm và Nội dung số, các đơn vị khác thuộc Bộ Thông tin và Truyền thông, Bộ Khoa học và Công nghệ, Bộ Tài nguyên và Môi trường để xây dựng những sản phẩm mang tính chiến lược, đề xuất ứng dụng trên phạm vi toàn quốc. Những sản phẩm chủ lực chuyển giao tại Trung tâm với quy mô lớn, triển khai trên địa bàn toàn tỉnh, đáp ứng được nhu cầu sử dụng của

nhiều ngành, nhiều đơn vị được đánh giá điển hình trong việc ứng dụng công nghệ thông tin như phần mềm quản lý Văn bản và Hồ sơ công việc (TDoffice); phần mềm giúp giải quyết các vấn đề bức bách, cấp thiết của xã hội như Phần mềm trực tuyến phục vụ công tác chỉ đạo, điều hành, quản lý của tỉnh về đất đai; Phần mềm quản lý người có công...

Đồng thời, Trung tâm còn làm tốt công tác tham mưu, phối hợp với các phòng chuyên môn thuộc Sở Thông tin và Truyền thông, thiết lập, xây dựng mối quan hệ cộng tác chặt chẽ trong quá trình thực hiện các nhiệm vụ do Giám đốc Sở giao. Xây dựng được mối quan hệ tốt với đội ngũ cán bộ làm công nghệ thông tin của các Sở, ban, ngành và UBND các huyện, thị, xã, thành phố. Thông qua đó đã tạo nên sự gắn kết, hợp tác giúp đỡ, trao đổi hỗ trợ kỹ thuật trong quá trình triển khai, vận hành các dự án, phần mềm công nghệ thông tin tại các đơn vị.

Để có được kết quả đáng khích lệ trên, Ban Giám đốc Trung tâm đã quan tâm đến việc đào tạo, bồi dưỡng, nâng cao kiến thức chuyên môn, kiến thức quản lý và ngoại ngữ cho đội ngũ cán bộ. Trung tâm đã cử các cán bộ làm phần mềm tham gia các hội thảo khoa học, các khóa đào tạo dài hạn, ngắn hạn khác nhau nhằm nâng cao kỹ năng chuyên môn cho đội ngũ phần mềm. Tập trung chỉ đạo, ưu tiên xây dựng chất lượng đội ngũ lập trình viên có thể đáp ứng các yêu cầu kỹ

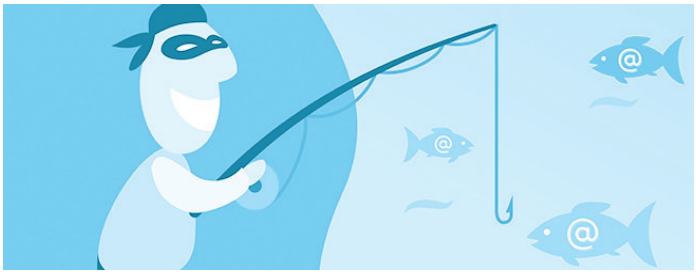
thuật từ đơn giản đến phức tạp, sẵn sàng xây dựng các phần mềm ứng dụng ở mức độ trung bình, cũng như có thể đáp ứng các điều kiện cần thiết để tham gia xây dựng các phần mềm có quy mô và mức độ phức tạp lớn hơn. Tích cực đẩy mạnh hợp tác trong việc phát triển, chuyển giao các sản phẩm phần mềm, ứng dụng công nghệ thông tin trên địa bàn cả nước, khẳng định vị thế, xây dựng lòng tin trong quan hệ với khách hàng, đối tác, ngày một nâng cao vị thế của Trung tâm trong lĩnh vực công nghệ thông tin và truyền thông.

Theo Đề án Tái cơ cấu và phát triển ngành dịch vụ tỉnh Thanh Hóa đến năm 2020 và định hướng đến năm 2025 đã khẳng định vai trò động lực của Công nghệ thông tin (CNTT) trong quá trình tái cơ cấu. "Phát triển dịch vụ thông tin và truyền thông theo hướng tập trung, phát triển nhanh dịch vụ viễn thông và CNTT với công nghệ hiện đại, chất lượng cao. Ưu tiên phát triển sản phẩm dịch vụ phần mềm CNTT và nội dung số...". Đây là cơ hội để Trung tâm nói chung, nhóm Phần mềm nói riêng khẳng định vai trò của mình trong việc tham mưu, chủ trì xây dựng, chuyển giao các sản phẩm CNTT phục vụ xây dựng chính quyền điện tử, các dịch vụ hướng tới thành phố thông minh, góp phần hiện thực hóa đưa CNTT trở thành ngành kinh tế mũi nhọn của tỉnh, xây dựng mô hình tăng trưởng kinh tế xã hội của tỉnh theo chiều sâu đáp ứng yêu cầu phát triển bền vững, để Trung tâm ngày một vững bước, đương đầu với những thử thách, đón lấy cơ hội của cuộc cách mạng công nghiệp 4.0 đem lại, góp phần xây dựng Trung tâm CNTT&TT Thanh Hóa trở thành một đơn vị mạnh hoạt động trong lĩnh vực công nghệ thông tin và truyền thông của tỉnh, đồng thời xây dựng tỉnh Thanh Hóa phải trở thành tỉnh kiểu mẫu, như sinh thời Bác Hồ hằng mong ước./.

KỸ NĂNG NHẬN BIẾT VÀ PHÒNG CHỐNG lừa đảo trực tuyến

HOÀNG ANH TUẤN
Trung tâm CNTT&TT Thanh Hóa

Các cuộctấn công Phishinglà một trong những thách thức an ninh mạng phổ biến nhất mà cả cá nhân và các tổ chức, doanh nghiệp phải đối mặt trong việc đảm bảo an toàn thông tin của họ khi tham gia trên không gian mạng. Bạn đã bao giờ nhận ra lý do tại sao mỗi ngày bạn nhận được càng nhiều thư rác hoặc email giả? Những email này đang giả dạng là hợp pháp khi chúng được làm cho giống như là đang được gửi đến từ các tổ chức có uy tín của chính phủ, các công ty doanh nghiệp, và các tổ chức nổi tiếng, trong khi thực tế thì không phải như vậy.



Vậy Phising là gì? **Phương thức Phishing** được biết đến vào năm 1987. Nguồn gốc của từ *Phishing* là sự kết hợp của hai từ Fishing (câu cá) và Phreaking (trò đùa phạm pháp liên quan đến hệ thống điện thoại). Câu cá ở trong trường hợp nay tức là "câu" thông tin của người dùng. Thêm nữa tính chất của nó cũng gần giống như kiểu tấn công Phreaking, vì thế chữ F được thay thế bằng Ph do cách phát âm gần giống nhau. Từ đó cái tên ***Phishing*** được ra đời.

Cụ thể hơn nữa thì **Phishing** là việc xây dựng những hệ thống lừa đảo nhằm đánh cắp các thông tin nhạy cảm, như tên đăng nhập, mật khẩu hay thông tin về các loại thẻ tín dụng của người dùng. Phishing xuất hiện như một thực thể đáng tin cậy, một trang thông tin điện tử, eBay, Paypal, gmail, hay các ngân hàng trực tuyến là những mục tiêu hướng đến của hình thức tấn công này. Phishing thường được thực hiện qua email, những tin nhắn nhanh và thường tập trung vào hướng lừa người dùng nhập các thông tin vào một form hay click vào một đường dẫn của website lừa đảo.

Các hình thức lừa đảo trực tuyến bao gồm:

1. Lừa đảo qua thư điện tử: Giả mạo hay gian lận qua emaillà công cụ được sử dụng phổ biến nhất để thực hiện tấn công Phishing. Trong hầu hết các trường hợp tin tặc có thể lấy một email giả mạo mà có đia chỉ từ một từ một website tin cậy như *abc@thanhhoa.gov.vn* chẳng hạn. Khi đó, các tin tặc có thể yêu cầu nạn nhân xác nhận tên đăng nhập và mật khẩu bằng cách gửi lại đến một địa chỉ email nhất định.

Nhận biết thư lừa đảo:

Các nội dung thư điện tử lừa đảo được tin tặc sử dụng rất phong phú. Dưới đây là một số dấu hiệu nhận biết chung:

- Yêu cầu người dùng cung cấp thông tin cá nhân, thông tin tài khoản truy cập.

- Đưa thông tin về các giải thưởng, sự kiện cho người dùng.

- Các tin liên quan đến các vấn đề nóng trong xã hội tại thời điểm hiện tại.

- Gửi các tập tin đính kèm liên quan đến công việc, tuyển dụng hay các thông tin về lĩnh vực mà người dùng quan tâm.

- Thư chỉ bao gồm các hình ảnh. Khi bấm vào bất kỳ vùng nào trong ảnh hoặc thư điện tử đó đều có thể dẫn đến trang web giả mạo dụ người dùng đăng nhập thông tin cá nhân hoặc lây nhiễm mã độc.

- Thư chứa nhiều thông tin bôi đậm bất thường nhằm thu hút sự chú ý của người dùng.

- Thư với những lời chào hỏi, làm quen chung mà không cụ thể tới đối tượng. Thường bắt đầu theo kiểu "chào bạn", "chào anh/chị", "Dear Friend"....

- Gửi một tập tin HTML với dạng trang đăng nhập thanh toán, ngân hàng, trang web nổi tiếng.

Cách phòng tránh

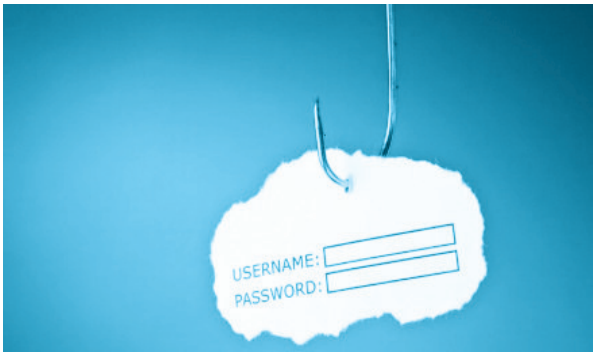
- Với mỗi thư điện tử nhận được, người dùng cần kiểm tra kỹ địa chỉ người gửi. Thông thường, các địa chỉ thư lừa đảo sẽ được giả mạo gần giống với một địa chỉ thư điện tử mà người sử dụng tin tưởng.

- Tuyệt đối không trả lời các thư điện tử được gửi từ nước ngoài có nội dung nhờ giúp đỡ chuyển tiền, hứa hẹn về việc sẽ trích một khoản thù lao, nhưng cũng yêu cầu người dùng phải gửi thông tin tài khoản ngân hàng để chi trả các khoản phụ phí khác.

- Không nhấn vào bất kỳ liên kết hay mở bất kỳ tệp tin đính kèm nào nếu không biết chính xác người gửi hoặc chưa kiểm tra qua các công cụ phòng chống mã độc hại.

- Thông báo tới nhà cung cấp dịch vụ và xóa khỏi trong hòm thư các thư điện tử lừa đảo; phổ biến cho đồng nghiệp, bạn bè, người thân, mọi người biết về thư này và các hình thức lừa đảo tương tự để phòng tránh.

2. Lừa đảo qua trang website giả mạo: Giả mạo Website là một kỹ thuật lừa đảo khác có thể hoạt động bằng cách tạo một trang web độc hại giả mạo một trang đích xác thực để khiến người dùng truy cập cung cấp thông tin nhạy cảm của



họ như chi tiết tài khoản, mật khẩu, số thẻ tín dụng v.v... Khi người dùng truy cập trang web lừa đảo và đăng nhập, toàn bộ thông tin sẽ được chuyển về cho tin tặc.

Nhận biết web lừa đảo:

Thông thường, lừa đảo để chiếm đoạt tài khoản ngân hàng sẽ được thực hiện thông qua các thư điện tử, diễn đàn hoặc mạng xã hội. Tin tặc sẽ gửi các thư lừa đảo giả mạo là ngân hàng để thông báo tới người dùng về việc cập nhật thông tin cá nhân hoặc thông báo có giao dịch bất thường. Các thư điện tử này sẽ có đường liên kết tới trang web giả mạo của ngân hàng đó. Khi người dùng truy cập trang web lừa đảo và đăng nhập, toàn bộ thông tin sẽ được chuyển về cho tin tặc.

Các nội dung thư điện tử lừa đảo được tin tặc sử dụng rất phong phú. Dưới đây là một số dấu hiệu nhận biết chung:

- Yêu cầu người dùng cung cấp thông tin cá nhân, thông tin tài khoản truy cập.

- Đưa thông tin về các giải thưởng, sự kiện cho người dùng.

- Các tin liên quan đến các vấn đề nóng trong xã hội tại thời điểm hiện tại.

- Gửi các tập tin đính kèm liên quan đến công việc, tuyển dụng hay các thông tin về lĩnh vực mà người dùng quan tâm.

- Thư chỉ bao gồm các hình ảnh. Khi bấm vào bất kỳ vùng nào trong ảnh hoặc thư điện tử đó đều có thể dẫn đến trang web giả mạo dụ người dùng đăng nhập thông tin cá nhân hoặc lây nhiễm mã độc.

- Thư chứa nhiều thông tin bôi đậm bất thường nhằm thu hút sự chú ý của người dùng.

- Thư với những lời chào hỏi, làm quen chung

mà không cụ thể tới đối tượng. Thường bắt đầu theo kiểu "chào bạn", "chào anh/chị", "Dear Friend"....

- Gửi một tập tin HTML với dạng trang đăng nhập thanh toán, ngân hàng, trang web nổi tiếng.

Cách phòng tránh

Cách phòng tránh duy nhất là không bao giờ nhấp vào liên kết ngân hàng được gửi trong thư điện tử, các diễn đàn hay mạng xã hội. Hãy nhập địa chỉ trang web của ngân hàng ngay trên chính thanh địa chỉ trình duyệt.

Thực hiện các biện pháp kỹ thuật khác theo bài viết "Nhận biết và phòng tránh tấn công Phishing qua Website giả mạo" tại bản tin số 09.

3. Lừa đảo trên mạng xã hội: Trong khi mạng xã hội được xem là phương tiện giao tiếp tốt với mọi người thì nó cũng trở thành mục tiêu cho tội phạm mạng. Việc sử dụng mạng xã hội để đánh cắp thông tin cũng như lừa đảo nhằm mục đích kiếm tiền xảy ra ngày càng phổ biến, phức tạp và khó phát hiện hơn.

Cách nhận biết lừa đảo qua mạng xã hội

- Khi truy cập vào địa chỉ lừa đảo, thường sẽ yêu cầu thực hiện thêm một số bước, chẳng hạn như cho phép thực hiện thêm một số chức năng hay chia sẻ lại thông điệp.

- Nội dung gây sốc hoặc gây tò mò.

- Hứa hẹn những điều mà các trang mạng xã hội không có tính năng đó hoặc không bao giờ làm (xem ai ghé thăm nhiều nhất, ai là bạn bè thân thiết nhất...).

Cách phòng chống

- Tìm hiểu về ứng dụng hoặc bài viết trước khi truy cập và cài đặt thông qua cụm từ "tên-ứng-dụng/nội-dung-quảng-cáo-lừa đảo". Ví dụ: "ai xem tường của bạn nhiều nhất - lừa đảo".

- Tìm hiểu về các tính năng của trang mạng xã hội để biết những chức năng mà nhà cung cấp có và những chức năng đáng ngờ mà tin tặc có thể lợi dụng.

- Kiểm tra quyền truy cập của các ứng dụng trên mạng xã hội, đặc biệt lưu ý các quyền truy cập tới thông tin cá nhân, cho phép viết lên trang của bạn bè, gửi tin nhắn tới bạn bè....

Dưới đây là tổng hợp một số hình thức lừa đảo trực tuyến và cách phòng tránh:

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 hình thức tấn công lừa đảo trực tuyến cần nhanh chóng thông tin về Tổ Ứng cứu sự cố 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.

HƯỚNG DẪN NHẬN BIẾT VÀ GỠ BỎ
MÃ ĐỘC GÂY KHỞI ĐỘNG LẠI MÁY TÍNH
TẠI CÁC CƠ QUAN TRÊN ĐỊA BÀN TỈNH

NGUYỄN THỊ LIÊN
Trung tâm CNTT&TT Thanh Hóa

Trong thời gian qua, Tổ Ứng cứu sự cố của Trung tâm đã xử lý các sự cố liên quan đến mã độc hại đang lây nhiễm thông qua hệ thống mạng nội bộ của các cơ quan, đơn vị trên địa bàn tỉnh. Trong số đó xuất hiện loại mã độc có tốc độ lây nhiễm nhanh sử dụng phương thức lây nhiễm trong mạng nội bộ dựa trên các lỗ hổng đang tồn tại trên hệ điều hành Windows. Thông qua việc lây nhiễm này, tin tặc có thể khai thác và đánh cắp thông tin cũng như có khả năng ảnh hưởng rộng tới các hệ thống thông tin của các cơ quan, đơn vị. Bài viết này giúp các cán bộ phụ trách CNTT nhận biết và xử lý sự cố liên quan đến mã độc này.

Dấu hiệu nhận biết:

- Các máy trạm chạy hệ điều hành Windows (phần lớn là Windows 7) có hiện tượng khi kết nối mạng Internet sẽ tự động quá trình khởi động lại sau một vài phút là lặp lại liên tục.
- Một số máy khi khởi động lại bị lỗi màn hình xanh
- Một số máy không bị lỗi khởi động thì không kết nối được máy in chia sẽ qua mạng nội bộ
- Nếu ngắt kết nối mạng Internet sẽ không xuất hiện hiện tượng khởi động lại máy như trên.
- Danh sách các hệ điều hành của máy trạm bị ảnh hưởng: Windows Vista, Windows 7, Windows 8
- Danh sách các hệ điều hành của máy chủ bị ảnh hưởng: Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012

Nguyên nhân:

Các máy tính trên bị lây nhiễm loại mã độc mới (Microsoft phát hiện vào ngày 2/6/2017 đặt tên là Win32/Aybo.B và xếp ở mức lây nhiễm "rất cao". Do một máy trong hệ thống mạng bị nhiễm mã độc thông qua các nguồn lây nhiễm khác nhau. Bản chất mã độc ban đầu là dạng sâu (Worm) nên có thể nhân bản và lây lan qua môi trường mạng. Bằng việc khai thác lỗ hổng liên quan đến dịch vụ SMB trên hệ điều hành Windows, mã độc tự động lây lan qua các cổng TCP (139, 445) cùng các cổng UDP (137,138) trên hệ thống mạng ngang hàng. Sau khi lây nhiễm, mã độc mở cổng hậu kết nối ra máy chủ bên ngoài Internet và tải về các mã độc khác.

Phương thức lây nhiễm:

Thông qua một máy bị lây nhiễm (qua nhiều môi trường khác nhau như mở file có chứa mã độc qua email; sử dụng phần mềm không rõ nguồn gốc, qua USB...). Máy chứa mã độc sẽ khai thác lỗ hổng SMB chưa được khắc phục trên các máy chạy Windows trong hệ thống mạng của đơn vị. Tiến hành lây lan mã độc đến các máy này. Sau khi lây nhiễm mã độc, file thực thi sẽ tiến hành thực hiện các thao tác sau:

- Tiến hành quét và kết nối toàn bộ các thư mục chia sẽ trong mạng nội bộ
- Tạo các chương trình phục vụ quá trình lây nhiễm
- Tạo các file kịch bản và các tiến trình tự động khởi động cùng Windows
- Tạo luật trên firewall chặn theo chiều từ ngoài vào máy tính theo cổng 445 để ngăn chặn các mã độc khác khai thác theo cổng này.
- Xóa/ khóa các tài khoản quản trị trên máy tính (Administrator/ System/ IISUSER_ACCOUNTXX): nhằm mục đích chiếm quyền quản trị đối với những máy sử dụng tài khoản này để đăng

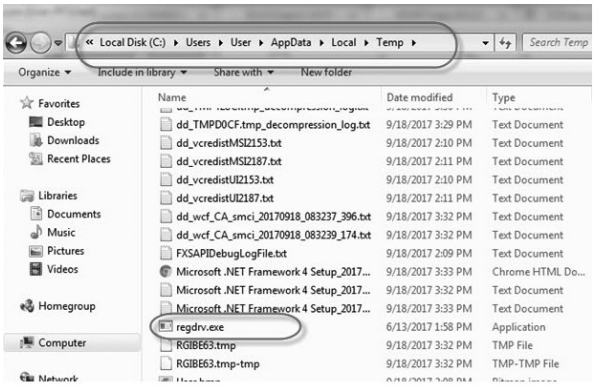
nhập.

- Thiết lập hành vi cho phép download và thực thi các chương trình của hacker vượt qua cơ chế kiểm soát của Windows.

- Mở các cổng hậu và kết nối ra máy chủ bên ngoài để tải các mã độc khác vào máy bị lây nhiễm.

Cách thức phát hiện:

- Kiểm tra trên phân vùng cài đặt hệ điều hành (thường là ổ C) có tồn tại file thực thi mã độc: ll.exe



- Kiểm tra trên các đường dẫn có các file do mã độc tạo ra hay không:

C:\WINDOWS\Registration\R000000000007.clb

C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\regdrv.exe

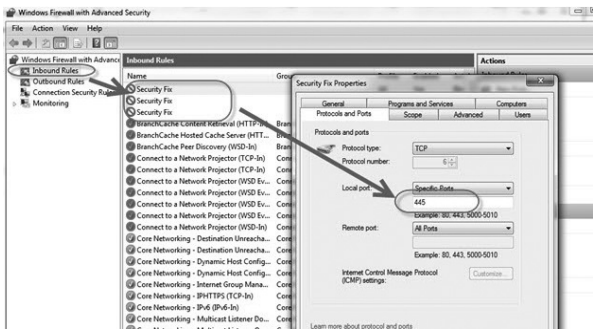
C:\USERS\<USER>\APPDATA\LOCAL\TEMP\REGDRV.EXE

C:\WINDOWS\registration\regdrv.exe

C:\WINDOWS\WindowsShell.Manifest

C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\regdrv.exe:Zone.Identifier

- Kiểm tra trên firewall của Windows có luật sau được thêm vào: *Security Fix*



- Kiểm tra các tài khoản người dùng trên Windows đã bị khóa hoặc xóa chưa: Administrator/ System/ IISUSER_ACCOUNTXX

- Kiểm tra tác vụ lập lịch chạy tự động trên Windows, bằng cách trên RUN gõ msconfig và Kiểm tra trong tab Startup có dịch vụ chứa đường dẫn:

C:\WINDOWS\registration\regdrv.exe" /f /RU "SYSTEM"

- Kiểm tra các chương trình chạy tự động do mã độc tự thêm vào trong *Windows Task Scheduler*

Biện pháp khắc phục:

Bước 1. Ngắt kết nối mạng trên máy bị lây nhiễm

Bước 2. Tắt chức năng System Restore trên Windows

- Click Start.
- Right-click My Computer then click Properties.
- Click the System Protection tab.
- In the list under Available Drives, choose a drive
- Click Configure....

- Choose "Turn off System Restore".
- Click Apply then Yes, and then OK.
- Click OK to exit the window.

Bước 3. Sử dụng các công cụ phát hiện và diệt mã độc sau để quét trên các máy bị lây nhiễm

(download các công cụ này trên máy tính chưa bị lây nhiễm vào USB)

- Malwarebytes bản Free tại địa chỉ sau: https://www.malwarebytes.com/

- BKAV bản Home tại địa chỉ sau: bkav.com.vn

Bước 4. Sau khi tiến hành quét xong, tiến hành bóc gỡ các nội dung mã độc đã cài cắm trên máy

- Khởi động lại máy và vào chế độ Safemode

- Tiến hành xóa các giá trị trong registry.

In KEY_CURRENT_USER\ Software\ Microsoft\ Windows\CurrentVersion\Run

Registry Driver = %Windows%\registration\ regdrv.exe

- Tìm kiếm và xóa các file do mã độc tạo ra như ở trên

Bật chức năng hiển thị các file ẩn trong windows, trước khi thực hiện bước này

- Quét lại máy tính một lần nữa

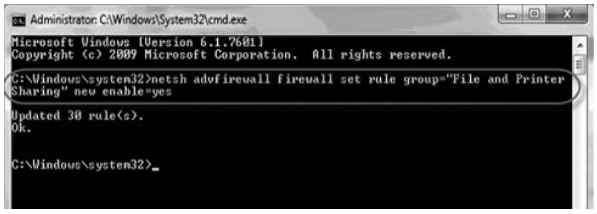
Bước 5.

- Xóa các luật trên Firewall do mã độc thiết lập

- Bật các luật liên quan đến dịch vụ in ấn qua mạng (do mã độc thiết lập chặn)

Chạy cmd bằng quyền quản trị, chạy câu lệnh sau:

netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=yes



Bước 6. Khi mã độc lây nhiễm trên máy sẽ tự động disable dịch vụ SMB, dẫn đến các máy bị nhiễm không thể kết nối đến các máy in được chia sẽ trên môi trường mạng.

Cần tiến hành enable lại các dịch vụ SMB trên các máy trạm

- Chạy cmd bằng quyền quản trị

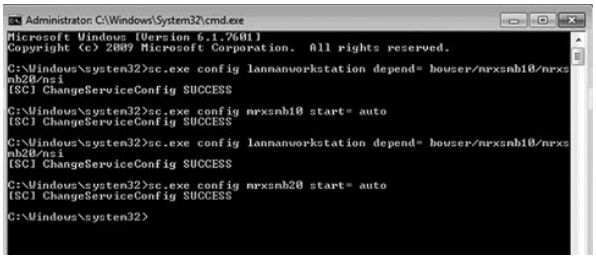
- Chạy câu lệnh sau:

sc.exe config lanmanworkstation depend= bowser/mrxsmb10/mrxsmb20/nsi

sc.exe config mrxsmb10 start= auto

sc.exe config lanmanworkstation depend= bowser/mrxsmb10/mrxsmb20/nsi

sc.exe config mrxsmb20 start= auto

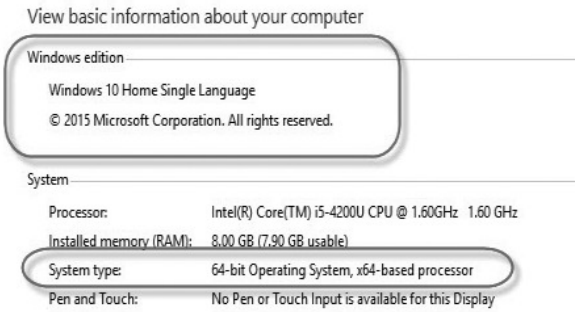


Bước 7. Sau khi quét và loại bỏ các mã độc trên, tiến hành cập nhật lại bản vá bảo mật cho hệ điều hành theo hướng dẫn sau:

7.1. Kiểm tra phiên bản Windows đang sử dụng

Cách 1: Vào Run, gõ câu lệnh "winver" để xem phiên bản Windows và Service Park đi kèm.

Cách 2: Click chuột phải vào My Computer, chọn Properties



Lưu ý với phiên bản Windows, xem phiên bản đang chạy là 32bit hay 64bit để xác định bản vá tương ứng

7.2. Kiểm tra đã cập nhật bản vá tương ứng với ký hiệu của Microsoft chưa?

Trước khi tiến hành cần kiểm tra dịch vụ Windows Update trong Control Panel đã được bật chưa.

7.3. Danh sách các bản cập nhật

Trong quá trình thực hiện, nếu gặp khó khăn, vướng mắc về kỹ thuật liên quan đến các nội dung, công việc trên đề nghị liên hệ về Tổ Ứng cứu sự cố 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.

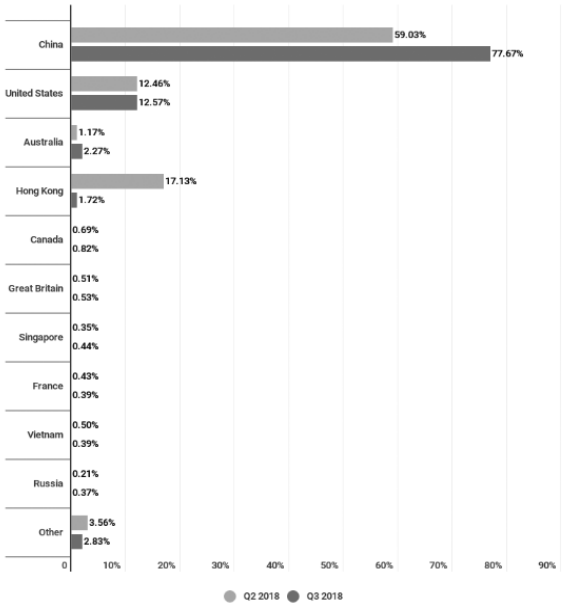
Thông tin liên hệ: Điện thoại: (0237)3718699; Fax (0237) 3718299.

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

I - Tình hình An toàn thông tin Quý III năm 2018 trong nước và quốc tế

1. Tình hình tấn công DDoS

Theo báo cáo DDoS Intelligence mới nhất của Kaspersky Lab, trong quý III năm 2018, Trung Quốc là quốc gia đứng đầu danh sách hứng chịu các vụ tấn công DDoS, đứng thứ hai là Mỹ, thứ ba là Úc... Trong số 10 quốc gia bị tấn công nhiều nhất, Việt Nam đứng thứ 9.



Danh sách 10 quốc gia bị tấn công DDoS trong quý III/2018 (nguồn securelist.com)

2. Tình hình website bị tấn công

Theo báo cáo an ninh website của CyStack trong 03 quý năm 2018 đã có 129.722 website trên thế giới bị tin tặc tấn công và chiếm quyền điều khiển. Như vậy, cứ mỗi phút trôi qua lại có 1 website bị tin tặc kiểm soát. Con số này ở tháng 7 là 43.110, sau đó giảm còn 41.405 ở tháng 8 và tăng mạnh lên 45.207 vào tháng 9.

Số lượng Website được phục hồi tính đến cuối tháng 9/2018 thì có đến 21,48% website bị tấn công ở tháng 7 vẫn chưa được khôi phục nguyên trạng; số liệu ở tháng 8 và tháng 9 lần lượt là 33,87% và 44,08%.

Trong tổng số các website bị tin tặc tấn công thì có hơn 60 ngàn website có tên miền .com. Đây cũng là loại tên miền được sử dụng nhiều nhất trên thế giới. Ngoài ra, một số tên miền quốc gia cũng là mục tiêu tấn công hàng đầu của tin tặc như: .in (Ấn Độ), .ru (Nga), .hk (Hồng Kông), .id (Indonesia)...

Theo thống kê, Việt Nam đứng thứ 19 (chiếm 0.9%) trong số các quốc gia có website bị tin tặc tấn công. Cụ thể trong quý 3 năm 2018 đã có 1.183 website của Việt Nam bị tin tặc tấn công và kiểm soát. Các website giới thiệu sản phẩm và dịch vụ của Doanh nghiệp là đối tượng bị tin tặc tấn công nhiều nhất, chiếm tới 71,51%. Vị trí thứ hai là các website Thương mại điện tử chiếm 13,86%. Các website có tên miền .gov.vn của chính phủ chỉ chiếm 1.9% trong danh sách này với tổng số 23 website bị tấn công.

3. Tình hình Spam và tấn công Phishing

Báo cáo tổng kết của Kaspersky Lab về tình hình thư rác và lừa đảo trực tuyến trong quý III/2018 cho biết, Việt Nam tiếp tục nằm trong nhóm các quốc gia có nguồn phát tán thư rác đứng đầu với vị trí thứ 5 (4,41%), đứng thứ 1 là Trung Quốc (13,47%) và thứ 2 là Mỹ (10,89%).

Báo cáo của Kaspersky Lab về tình hình tấn công Phishing trên phạm vi toàn cầu trong quý III/2018. Dẫn đầu là Gutermala với 18.97%, thứ 2 là Brazil với 18.62%...

Country	%*
Guatemala	18,97
Brazil	18,62
Spain	17,51
Venezuela	16,75
Portugal	16,01
China	15,99
Australia	15,65
Panama	15,33
Georgia	15,10
Ecuador	15,03

Thống kê tình hình tấn công Phishing trên phạm vi toàn cầu (Nguồn: Kaspersky)

Trong số các quốc gia bị tấn công bởi mã độc trong thư rác, Việt Nam ở vị trí thứ 4 đứng sau các quốc gia như Đức, Nga và Mỹ.

4. Bùng phát virus gây khởi động lại máy tính đột ngột

Ngày 23/8/2018 Công ty An ninh mạng BKAV vừa phát đi cảnh báo loại virus mới nguy hiểm

W32.CrashSMB, virus này gây ra hiện tượng máy tính đang sử dụng bị lỗi khởi động lại đột ngột. Hàng loạt hệ thống mạng với số lượng máy tính lớn đã bị đình trệ bởi sự cố virus. Theo thống kê của Bkav, hiện đã có 329.000 máy tính tại Việt Nam được ghi nhận nhiễm loại mã độc này.

Virus W32.CrashSMB phát tán bằng kỹ thuật tấn công, khai thác các máy tính tồn tại lỗ hổng SMB. Đây là hình thức tấn công tương tự như của virus "nổi tiếng" WannaCry đã sử dụng. Sau khi lây nhiễm, virus sẽ chiếm quyền điều khiển máy tính, biến máy của nạn nhân thành một máy tính ma (zombie), từ đó tiếp tục tấn công sang các máy khác trong cùng mạng. Dấu hiệu dễ thấy khi một máy tính bị virus W32.CrashSMB tấn công là thỉnh thoảng hệ điều hành hiện thông báo lỗi, sau đó máy tính bị khởi động lại đột ngột hoặc bị lỗi màn hình xanh (Blue Screen).

Do W32.CrashSMB chiếm quyền điều khiển máy tính nên người dùng sẽ phải đối mặt với các nguy cơ bị theo dõi, bị lấy cắp dữ liệu, thông tin cá nhân, lấy cắp tài khoản ngân hàng, tài khoản Gmail, Facebook... Đồng thời, máy tính sẽ bị chạy rất chậm vì virus sử dụng tài nguyên hệ thống để thực hiện hành vi đào tiền ảo.

Chuyên gia Bkav khuyến cáo, người sử dụng nên thường xuyên cập nhật bản vá mới nhất của hệ điều hành, đồng thời cài đặt phần mềm diệt virus thường trực để được bảo vệ một cách tự động.

5. Hơn nửa triệu máy tính tại VN bị theo dõi bởi phần mềm gián điệp BrowserSpy

Hệ thống giám sát virus của Bkav vừa phát hiện một loại mã độc gián điệp nằm vùng nguy hiểm BrowserSpy. Loại mã độc này có khả năng theo dõi người dùng, lấy cắp thông tin cá nhân, tài khoản ngân hàng, mật khẩu Gmail, Facebook... Tại Việt Nam, đã có hơn 560.000 máy tính bị theo dõi bởi BrowserSpy, số lượng này đang tiếp tục tăng nhanh. Bkav khuyến cáo người dùng cần xử lý ngay virus và đổi mật khẩu cho các tài khoản Gmail, Facebook... đặc biệt là tài khoản ngân hàng.

BrowserSpy ẩn mình trong các phần mềm giả mạo được hacker đưa lên Internet để lừa người dùng tải về. Khi được kích hoạt, BrowserSpy sẽ cài một plug-in (extention) độc hại vào trình duyệt để theo dõi, giám sát người dùng. Theo đó, BrowserSpy có thể âm thầm đánh cắp thông tin cá nhân, thu thập nội dung tìm kiếm, đọc trộm email, lịch sử truy cập web... Nghiêm trọng hơn, BrowserSpy có khả năng cập nhật và tải thêm các mã độc khác nhằm kiểm soát máy tính, thực hiện tấn công có chủ đích APT

Bkav cũng khuyến cáo người dùng không tùy tiện tải các phần mềm từ nguồn không đảm bảo, tốt nhất nên cài thường trực phần mềm diệt virus trên máy tính để được bảo vệ toàn diện.

6. Bản cập nhật an ninh tháng 8 của Microsoft vá 60 lỗ hổng - hai lỗi đã bị khai thác trong thực tế

Ngày 14/8, Microsoft phát hành bản cập nhật an ninh khắc phục 60 lỗ hổng ảnh hưởng đến Windows, Microsoft Edge, Internet Explorer, Office, ChakraCore, .NET Framework, Exchange Server, Microsoft SQL Server và Visual Studio.

Hai trong số các lỗ hổng này đã bị khai thác trong thực tế. Tất cả 19 lỗ hổng được đánh giá nghiêm trọng trong bản cập nhật này đều dẫn đến thực thi mã từ xa (RCE), một số trong đó có thể cho phép kẻ tấn công kiểm soát hệ thống bị ảnh hưởng nếu khai thác thành công. Người dùng được khuyến cáo cài đặt các bản vá an ninh sớm nhất có thể.

7. Cảnh báo mã độc tấn công có chủ đích vào ngân hàng và hạ tầng quốc gia

Trung tâm ứng cứu khẩn cấp máy tính quốc gia (VNCERT) vừa phát cảnh báo khẩn về việc theo dõi, ngăn chặn kết nối và xoá các tập tin mã độc tấn công có chủ đích vào ngân hàng và các tổ chức hạ tầng quan trọng quốc gia.

Theo VNCERT, từ đầu tháng 7/2018 đến nay, Trung tâm VNCERT đã ghi nhận các hình thức tấn công có chủ đích của tin tặc nhắm vào hệ thống thông tin của một số ngân hàng và hạ tầng quan trọng quốc gia tại Việt Nam.

Với hình thức tấn công có chủ đích này, tin tặc đã tìm hiểu kỹ về đối tượng tấn công và thực hiện các thủ thuật lừa đảo, kết hợp với các biện pháp kỹ thuật cao để qua mặt các hệ thống bảo vệ ATTT của các ngân hàng và các tổ chức hạ tầng quan trọng nhằm chiếm quyền điều khiển máy tính của người dùng và thông qua đó tấn công các hệ thống máy tính nội bộ chứa thông tin

quan trọng khác.

Mục đích chính của tin tặc là đánh cắp các thông tin quan trọng của ngân hàng và các tổ chức hạ tầng quan trọng quốc gia. Với việc sử dụng các kỹ thuật cao để tấn công thì các hệ thống bảo vệ ATTT của ngân hàng hoặc các tổ chức hạ tầng quan trọng sẽ khó phát hiện kịp thời và đồng thời giúp tin tặc duy trì quyền kiểm soát hệ thống thông tin.

8. Cảnh báo chiến dịch tấn công APT và các quốc gia Đông Nam Á trong đó có Việt Nam

Đầu tháng 8 năm 2018 Cục An toàn thông tin nhận được một báo cáo về tấn công APT vào các quốc gia Đông Nam Á, trong đó có nhiều mẫu mã độc sử dụng các tài liệu bằng Tiếng Việt để cài đặt mã độc vào máy tính người dùng.

Những mã độc này có tên ENFAL và ENDCMS (Hussarini, Sarhust), mã khai thác được đính kèm vào tập tin tài liệu tiếng Anh và Tiếng Việt để khai thác lỗ hổng CVE-2017-11882 và CVE-2012-0158, sau đó sẽ tiếp tục tải về máy tính các mã độc khác. Tập tin bằng Tiếng Anh gồm những nội dung liên quan đến chính trị và ngoại giao của Việt Nam, Philippines và Myanmar; những tập tin bằng Tiếng Việt lợi dụng nội dung rất phổ biến; quen thuộc và đa dạng (như góp ý dự thảo văn bản từ Văn phòng Chính phủ, phiếu đăng ký, báo cáo thu chi Đảng phí, đặc biệt có cả văn bản sử dụng thông tin về cảnh báo mã độc GrandCrab của Trung tâm VNCERT).

Qua kiểm tra sơ bộ của Cục An toàn thông tin, những mẫu mã độc này hầu hết đã được đưa lên các kho lưu trữ và phân tích mã độc (như Virus-total) và nhiều giải pháp anti-virus đã nhận dạng và lại khai thác những lỗ hổng cũ, đã có bản vá do vậy người dùng, các cơ quan tổ chức nếu đã cập nhật bản vá thường xuyên cho hệ điều hành, ứng dụng Microsoft Office và có sử dụng giải pháp phòng chống mã độc được cập nhật thường xuyên thì có thể không đáng lo ngại. Đối với những trường hợp chưa thực hiện kịp thời việc cập nhật bản vá cho lỗ hổng bảo mật và giải pháp phòng chống mã độc cần kiểm tra, rà soát dựa trên những thông tin kỹ thuật bên dưới để tránh nguy cơ mất an toàn thông tin, và thiệt hại có thể xảy ra đối với cơ quan, tổ chức và không gian mạng Việt Nam.

9. Trình dọn dẹp máy tính CCleaner không thể tắt tính năng thu thập thông tin

Trước đây, CCleaner từng được coi là một phần mềm đáng tin cậy, hoàn toàn miễn phí mà không hề có quảng cáo. Tuy nhiên, trong thời gian gần đây, phần mềm này liên tục gặp các nguy cơ về an toàn thông tin đối với người dùng cuối. Cách đây không lâu, hacker đã có thể thay đổi mã nguồn của phần mềm này, chèn mã độc và phân phối tới người dùng dưới dạng bản cập nhật.

Với phiên bản mới nhất, Ccleaner không thể tắt tính năng thu thập thông tin mặc dù có tùy chọn để tắt chức năng này nhưng nó sẽ được kích hoạt lại một cách tự động mà không hề thông báo cho người dùng. Về phần mình, CCleaner nói rằng, tất cả thông tin thu thập được hoàn toàn là những thông tin ẩn danh, và chỉ được dùng để giúp cải thiện chương trình. Công ty cũng cho biết, sắp tới sẽ có những thay đổi nhằm cung cấp cho người dùng nhiều lựa chọn hơn.

CCleaner có thể từng là công cụ hữu ích, nhưng giờ đã là 2018, các hệ điều hành đã làm rất tốt trong việc tối ưu và quản lý rác hệ thống. Nếu bạn vẫn còn đang dùng CCleaner, hãy đừng do dự mà gỡ cài đặt nó đi.

10. Hacker có thể lấy cắp dữ liệu doanh nghiệp thông qua số fax

Máy fax hiện vẫn được các doanh nghiệp sử dụng rộng rãi và một lỗ hổng trong giao thức kết nối của thiết bị này có thể tạo điều kiện cho các cuộc tấn công mạng.

Máy fax có vẻ đã cổ tuy nhiên vẫn là thiết bị phổ biến đối với người dùng doanh nghiệp như ngân hàng, công ty bất động sản, tổ chức chăm sóc sức khỏe... Theo một nghiên cứu năm 2015, có khoảng 46,3 triệu máy fax đang được sử dụng trên thế giới, trong đó Mỹ chiếm khoảng 17 triệu máy.

Trong khi nhiều công ty công nghệ, chuyên gia bảo mật mạng trên toàn thế giới hướng tới khắc phục các lỗ hổng an ninh trên công nghệ hiện đại như thiết bị di động, hệ điều hành, trình duyệt... thì các công nghệ cũ có thể đã vô tình bị bỏ qua. Chính vì vậy, các nhà nghiên cứu lật lại vấn đề và công bố phát hiện về lỗ hổng trong

giao thức kết nối của máy fax, cho phép hacker xâm nhập cả mạng doanh nghiệp và người dùng. Tại Hội nghị Def Con 26 (ngày 12/8) ở Las Vegas, nhóm nghiên cứu về mã độc của Check Point đã trình bày những phát hiện của mình về an ninh trên thiết bị fax. Các chuyên gia đã chứng minh sự tồn tại của lỗ hổng an ninh trên dòng máy in hỗ trợ fax HP Officejet Pro All-in-One, cụ thể là HP Officejet Pro 6830 và OfficeJet Pro 8720.

Trên thực tế, hoàn toàn dễ dàng để có số fax một doanh nghiệp thông qua trang web của doanh nghiệp đó hoặc trực tiếp hỏi thông tin. Và đó là tất cả những gì cần thiết để khai thác những lỗ hổng vừa được công bố. Khi có được số fax của mục tiêu nhắm tới, kẻ tấn công có thể dùng fax gửi một tập tin hình ảnh độc hại tới thiết bị nạn nhân.

Các vấn đề được phát hiện bao gồm lỗ hổng tràn bộ đệm dựa trên stack và Devil's Ivy (CVE 2017-976), cho phép thực thi mã từ xa thông qua các lỗi xử lý cơ sở dữ liệu. Theo các nhà nghiên cứu, một tập tin hình ảnh có thể được chèn thêm mã độc tống tiền, mã độc đào tiền ảo, công cụ giám sát... Hacker sẽ khai thác lỗ hổng trong giao thức kết nối của máy fax và tải các payload độc hại vào bộ nhớ máy fax. Khi thiết bị này kết nối vào mạng, mã độc sẽ phát tán và xâm nhập hệ thống, từ đó theo dõi, làm gián đoạn dịch vụ hoặc lấy cắp thông tin. Check Point đã thông báo cho HP về lỗ hổng và nhà sản xuất sau đó đã đưa ra các bản vá lỗi.

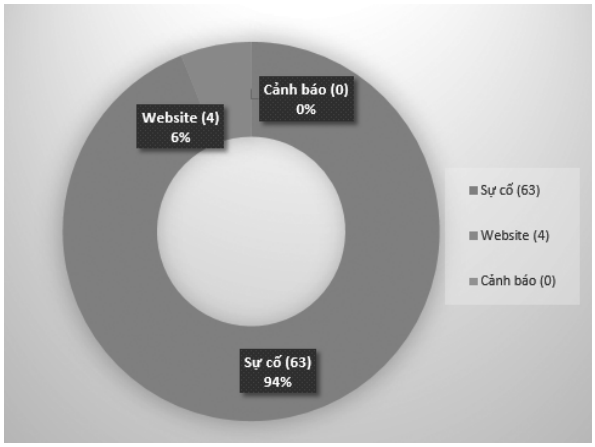
"Các giao thức tương tự cũng được sử dụng cho nhiều máy fax, máy in đa chức năng và dịch vụ fax online của các nhà cung cấp khác, do đó cũng sẽ bị ảnh hưởng bởi phương thức tấn công nói trên".

Điều này đặt ra vấn đề an ninh nghiêm trọng khi các doanh nghiệp có thể không nhận thức được việc toàn bộ mạng của mình có thể bị truy cập, cũng như thông tin nhạy cảm có thể bị lộ chỉ do thiết bị đã "cũ kỹ" đó.

II - Tình hình An toàn thông tin trên địa bàn tỉnh trong quý III/2018

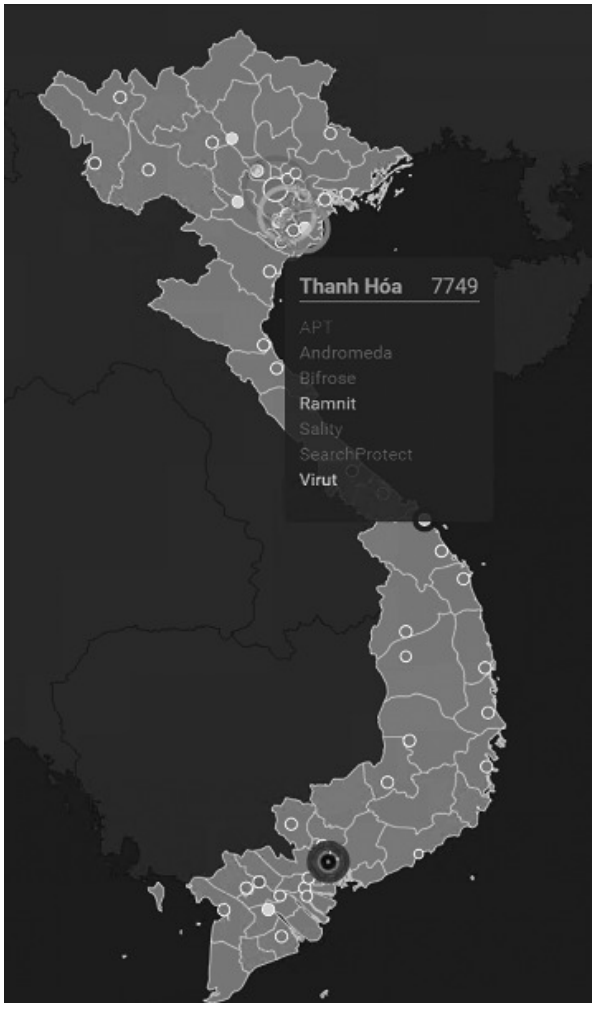
1. Tổng hợp tình hình ứng cứu sự cố trên địa bàn tỉnh

Trong tháng 7 và 8 năm 2018, Tổ Ứng cứu sự cố của Trung tâm hỗ trợ ứng cứu sự cố cho các cơ



quan nhà nước trên địa bàn tỉnh với 63 lượt hỗ trợ. 04 website bị tin tặc tấn công thay đổi giao diện.

Theo số liệu giám sát an toàn thông tin của nhà mạng Viettel, trên địa bàn tỉnh ghi nhận hàng chục nghìn các lượt kết nối và tham gia vào mạng máy tính ma Botnet như Andromeda, APT, Kazy, Ramnit, Sality...



Theo ghi nhận của Trung tâm An ninh mạng và An toàn dữ liệu, trong thời gian từ 01/07-30/9 ghi nhận có 88 cuộc tấn công khai thác chiếm quyền quản trị; 118 cuộc tấn công bằng mã độc; 181 cuộc tấn công vào ứng dụng Website

2. Công văn an toàn thông tin

- Ngày 26/7/2018 Sở Thông tin và Truyền thông ban hành công văn số 936/STTT-CNTT về việc theo dõi, ngăn chặn kết nối và xóa các tập tin mã độc tấn công có chủ đích vào ngân hàng và các tổ chức hạ tầng quan trọng.

- Ngày 17/7/2018 Bộ Thông tin và Truyền thông ban hành công văn số 2290/BTTT-CATTT về việc hướng dẫn kết nối chia sẻ thông tin mã độc giữa các hệ thống kỹ thuật.

- Ngày 24/8/2018 Sở Thông tin và Truyền thông ban hành công văn số 1104/STTT-CNTT về việc hướng dẫn kết nối chia sẻ thông tin mã độc giữa các hệ thống kỹ thuật.

- Ngày 29/8/2018 Sở Thông tin và Truyền thông ban hành công văn số 1128/STTT-CNTT về việc Tăng cường đảm bảo an toàn thông tin mạng dịp nghỉ Lễ Quốc khánh 02/9/2018.

TIN HOẠT ĐỘNG

Trung tâm CNTT&TT Thanh Hóa tổ chức thi cấp Chứng chỉ ứng dụng Công nghệ thông tin cơ bản đợt10, 11 năm 2018

Theo Quyết định số 46/QĐ-SGDĐT và 47/QĐ-SGDĐT của Sở Giáo dục và Đào tạo tỉnh Thanh Hóa, Trung tâm Công nghệ thông tin và truyền thông 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 cơ bản; Chứng chỉ được quy định tại Thông tư 03/2014/TT-2014 của Bộ Thông tin và Truyền thông.

Trongtháng 7 năm 2018, Trung tâm Công nghệ thông tin và truyền thông Thanh Hóa tổ chức kỳ thi sát hạch cấp Chứng chỉ công nghệ thông tin cơ bản,đợt 10,11năm 2018; Hội đồng thi được Sở Giáo dục và đào tạo thành lập 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 Giáo dục và Đào tạo và Bộ Thông tin và Truyền thông.

Kỳ thi Đợt 10, 11 năm 2018, có 503 thí sinh đăng ký dự thi và tham dự 2 phần thicủa 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 Giáo dục và Đào tạo tỉnh để tiến hành cấp chứng chỉ, phôi chứng chỉ được Bộ Giáo dục và Đào tạo cấp theo số lượng thí sinh thi đậu, được Sở Sở Giáo dục và Đào tạo 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:

Trung tâm CNTT&TT Thanh Hóa, số 73 Hàng Than, phường Lam Sơn, thành phố Thanh Hóa - ĐT: 02373.718.698

Lê Văn Tuấn

Trung tâm CNTT&TT tham gia Hội nghị Thượng đỉnh về Thành phố thông minh ASOCIO 2018

Ngày 19/8, Trung tâm CNTT&TT tham gia đoàn công tác của Sở Thông tin và Truyền thông tham gia Hội nghị Thượng đỉnh về Thành phố thông minh ASOCIO 2018 - Hà Nội (ASOCIO Smart City Summit 2018 - Hanoi) với chủ đề 'Xây dựng thành phố thông minh hơn, an toàn hơn

bằng các giải pháp số' đã chính thức khai mạc tại Thủ đô Hà Nội. Sự kiện do UBND thành phố Hà Nội phối hợp cùng ASOCIO - liên minh quốc tế lớn nhất, uy tín nhất về công nghệ thông tin của khu vực châu Á - châu Đại Dương và WITSA - liên minh các hiệp hội CNTT lớn nhất thế giới tổ chức

Tham dự hội nghị có cùng hơn 600 đại biểu là lãnh đạo cấp cao các cơ quan Trung ương và thành phố Hà Nội; các tỉnh, thành phố có kế hoạch xây dựng Thành phố thông minh; các hội, hiệp hội, tổ chức, doanh nghiệp chuyên ngành CNTT; gần 70 đại biểu quốc tế từ 20 quốc gia và nền kinh tế trên thế giới...

Các bài trình bày tại Hội nghị đề cập đến các vấn đề: Đề án phát triển đô thị thông minh của Việt Nam; các chuẩn kết nối cho thành phố thông minh, bảo mật an toàn thông tin khi các thành phố trở nên kết nối hơn; phân tích dữ liệu và lập kế hoạch dựa trên các dữ liệu và đặc biệt là kinh nghiệm xây dựng thành phố thông minh của Thụy Điển; mô hình "xã hội 5.0" của Nhật Bản; các bài học kinh nghiệm trong xây dựng Thành phố thông minh của Malaysia và các xu hướng công nghệ mới cho Thành phố thông minh của Google. Trong khuôn khổ Hội nghị thượng đỉnh cũng diễn ra 6 hội thảo chuyên đề, bao gồm: Chính quyền số và chiến lược xây dựng thành phố thông minh; Thành phố thông minh hơn với ít giao dịch tiền mặt hơn; Hạ tầng, nền tảng - cơ sở quan trọng cho các thành phố thông minh; Dữ liệu định hướng: Thu thập, phân tích dữ liệu và lập kế hoạch cho các thành phố; Công nghiệp thông minh; Các ứng dụng và giải pháp cho thành phố thông minh.

Cao Việt Cường

Giao lưu hợp tác cùng phát triển các Trung tâm Công nghệ thông tin và truyền thông khu vực Bắc Trung Bộ lần thứ III

Trong 2 ngày 14 và 15/7/2018 tại Quảng Trị, Trung tâm Công nghệ thông tin và truyền thông Quảng Trị, Sở Thông tin và Truyền thông Quảng Trị đã đăng cai tổ chức Chương trình Giao lưu hợp tác cùng phát triển các Trung tâm Công nghệ thông tin và truyền thông khu vực Bắc Trung Bộ lần thứ III với chủ đề "Tăng cường năng lực bảo đảm an toàn thông tin phục vụ xây dựng chính quyền điện tử".

Tham dự có đại diện lãnh đạo Sở Thông tin và Truyền thông Quảng Bình, Sở Thông tin và Truyền thông Quảng Trị và hơn 80 thành viên của Trung tâm Công nghệ thông tin và truyền thông các tỉnh, thành phố: Thanh Hóa, Nghệ An, Quảng Bình, Quảng Trị và Thừa Thiên Huế, Đà Nẵng và Trung tâm Đào tạo CNTT&TT Hà Nội.

Đây là hoạt động giao lưu được tổ chức hàng năm nhằm tăng cường tình đoàn kết, trao đổi học tập kinh nghiệm công tác giữa các Trung tâm. Chương trình giao lưu năm nay được tổ chức với các nội dung: tọa đàm, học tập và trao đổi kinh nghiệm, nâng cao trình độ chuyên môn nghiệp vụ, giao lưu thể thao, văn nghệ giữa các đoàn tạo sân chơi lành mạnh, làm phong phú thêm đời sống tinh thần của cán bộ, công nhân viên chức. Qua đó tăng cường mối quan hệ đoàn kết, cùng chia sẻ kinh nghiệm công tác giữa các đơn vị.

Trong thời gian qua, Trung tâm CNTT&TT các tỉnh khu vực Bắc Trung Bộ đã có những chia sẻ kinh nghiệm giúp nhau vừa làm tốt nhiệm vụ chính trị được giao, vừa làm tốt các hoạt động dịch vụ. Các đoàn cũng đã chia sẻ kinh nghiệm trong việc tổ chức đào tạo; Hỗ trợ kỹ thuật, ứng cứu sự cố máy tính, bảo đảm an toàn an ninh thông tin; Tổ chức các sự kiện truyền thông; Chia sẻ kinh nghiệm và phối hợp trong việc tổ chức đào tạo, bồi dưỡng trong lĩnh vực thông tin và truyền thông...

Vấn đề bảo đảm an toàn thông tin trong thời gian qua đã được Đảng và Nhà nước ta quan tâm, chỉ đạo. Vì vậy qua diễn đàn, các đơn vị đã đề xuất đẩy mạnh liên kết, hợp tác để chia sẻ kinh nghiệm, hình thành mạng lưới để hỗ trợ và tư vấn giúp đỡ nhau trong lĩnh vực bảo đảm an toàn thông tin phục vụ xây dựng chính quyền điện tử tại mỗi địa phương...

Nhân dịp tháng 7 đầy ý nghĩa và hướng tới kỷ niệm 71 năm ngày Thương binh liệt sĩ (27/7/1947 - 27/7/2018), các đoàn đã đến viếng, dâng hương tại Nghĩa trang liệt sĩ Quốc gia Trường Sơn, Thành Cổ Quảng Trị và tham quan di tích lịch sử quốc gia Địa đạo Vịnh Mốc, Quảng Trị.

Lê Duy