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

Số 01
tháng 3/2017

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; Cầm Vương; Ngô Thị Phương

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 3/2017

Toàn cảnh Hội thảo khoa học "Xây dựng và phát triển khu công nghệ thông tin tập trung về phần mềm, nội dung số tỉnh Thanh Hóa giai đoạn 2016 - 2020, định hướng đến năm 2030".

Tăng cường đẩy mạnh phát triển ngành Thông tin và Truyền thông Thanh Hóa trong thời kỳ hội nhập - phát triển

Ths. TRẦN DUY BÌNH
Bí thư Đảng ủy, Giám đốc Sở TT&TT

Năm 2016 là năm diễn ra nhiều sự kiện chính trị quan trọng, Đại hội Đảng toàn quốc lần thứ XII nhiệm kỳ 2016 - 2021, Bầu cử Đại biểu Quốc hội và Hội đồng nhân dân các cấp, cũng là năm đầu tiên thực hiện Nghị quyết Đại hội Đảng toàn quốc lần thứ XII, Nghị quyết Đại hội Đảng bộ tỉnh lần thứ XVIII nhiệm kỳ 2015 - 2016 và Kế hoạch phát triển KT-XH 5 năm (2016 - 2020). Bên cạnh những thuận lợi là nền kinh tế vĩ mô của cả nước ổn định, lạm phát được kiểm soát, môi trường đầu tư kinh doanh tiếp tục được cải thiện, tháo gỡ khó khăn và hỗ trợ cho sản xuất kinh doanh, nhiều ngành, lĩnh vực tiếp tục đã phục hồi. Tuy nhiên, hoạt động sản xuất kinh doanh của các doanh nghiệp trên địa bàn tỉnh vẫn còn gặp nhiều khó khăn, trong đó có các doanh nghiệp hoạt động trong lĩnh vực thông tin và truyền thông (TT&TT). Song dưới sự lãnh đạo, chỉ đạo của Tỉnh ủy, HĐND và UBND tỉnh; sự chỉ đạo, hướng dẫn về chuyên môn, nghiệp vụ của Bộ Thông tin và Truyền thông; sự phối hợp chặt chẽ của các cấp, các ngành trong tỉnh cùng sự nỗ lực phấn đấu của toàn thể cán bộ công chức, viên chức trong ngành, các hoạt động trong lĩnh vực (TT&TT) trên địa bàn

tỉnh năm 2016 tiếp tục ổn định và có bước phát triển, công tác quản lý nhà nước được tăng cường, hoàn thành tốt nhiệm vụ được giao.

Để góp phần thực hiện thắng lợi 5 chương trình trọng tâm và 4 nhiệm vụ đột phá trong nhiệm kỳ của Ban chấp hành Đảng bộ tỉnh lần thứ XVIII. Sở TT&TT Thanh Hóa đã tập trung chỉ đạo xây dựng các kế hoạch trình Chủ tịch UBND tỉnh ban hành như: Kế hoạch số 01/KH-UBND về việc thực hiện Nghị quyết 36a/NQ-CP ngày 14/10/2015 của Chính phủ về Chính phủ điện tử; Kế hoạch ứng dụng CNTT trong hoạt động của các cơ quan nhà nước giai đoạn 2016 - 2020; Kế hoạch tuyên truyền nâng cao nhận thức của xã hội về phát triển du lịch và đẩy mạnh hoạt động quảng bá, xúc tiến du lịch tỉnh Thanh Hóa giai đoạn 2016 - 2020. Xây dựng kế hoạch triển khai các nhiệm vụ trọng tâm của ngành trong giai đoạn 2016 - 2020 để tổ chức triển khai thực hiện các nội dung của ngành theo các kế hoạch; Triển khai 5 chương trình trọng tâm, 4 khâu đột phá theo Nghị quyết Đại hội Đảng bộ tỉnh lần thứ XVIII; Tham mưu trình UBND tỉnh, Chủ tịch UBND tỉnh ban hành các quy chế, các quy định quản lý nhà nước trong lĩnh vực TT&TT, đồng thời triển khai hướng dẫn kịp thời các văn bản quy phạm pháp luật chuyên ngành TT&TT của Bộ Thông tin và Truyền thông, UBND tỉnh, Chủ tịch UBND tỉnh đến các tổ chức, cá nhân tham gia hoạt động trong lĩnh vực TT&TT. Tăng cường công tác thanh tra, kiểm tra, hướng dẫn việc chấp hành các quy định pháp luật của các tổ chức, cá nhân tham gia trong lĩnh vực TT&TT, nhằm tạo điều kiện thuận lợi cho các doanh nghiệp TT&TT trên địa bàn tỉnh, cạnh tranh lành mạnh, đẩy mạnh phát triển cơ sở hạ tầng TT&TT theo đúng quy hoạch, kế hoạch đã được phê duyệt. Các doanh nghiệp TT&TT trên địa bàn tỉnh chấp hành tốt các quy định của pháp luật, không ngừng đầu tư xây dựng mở rộng cơ sở hạ tầng TT&TT đến các vùng miền trên địa bàn tỉnh.

- Hệ thống mạng lưới bưu cục, điểm Bưu điện - Văn hóa xã được duy trì và củng cố, cung cấp các dịch vụ bưu chính, viễn thông đến với người dân; Phát hành báo chí, chuyển phát kịp thời phục vụ các tổ chức, công dân; Xây dựng các mô hình kinh doanh đa dịch vụ tại các điểm Bưu điện - Văn hóa xã đáp ứng nhu cầu trao đổi thông tin và giao lưu văn hóa của nhân dân, phục vụ xây dựng nông thôn mới. Bên cạnh các dịch vụ bưu chính, viễn thông truyền thống, các dịch vụ trả lương hưu, bảo hiểm; Tiếp nhận và trả kết quả dịch vụ hành chính công như: Nhận chuyển phát chứng minh nhân dân, giấy phép lái xe, thu tiền phạt và chuyển phát giấy tờ tạm giữ cho người vi phạm giao thông... đã góp phần không nhỏ vào công cuộc cải cách hành chính.

- Hạ tầng mạng lưới viễn thông tiếp tục được mở rộng, chất lượng dịch vụ ổn định, đáp ứng yêu cầu chỉ đạo, điều hành của cấp ủy, chính quyền địa phương và nhu cầu sử dụng thông tin liên lạc của nhân dân, đặc biệt các vùng miền núi, vùng sâu, vùng xa, biên giới, hải đảo của tỉnh. Năm 2016 các doanh nghiệp viễn thông đã đầu tư xây dựng mới 322 trạm BTS, nâng tổng số trạm BTS trên địa bàn tỉnh là 4.679 (2.751 trạm 2G, 1.928 trạm 3G) được lắp đặt tại 2580 vị trí trên địa bàn 635 xã, phường, thị trấn; đầu tư xây dựng mới 304 trạm truy cập Internet băng thông rộng hữu tuyến, nâng tổng số trạm truy cập Internet băng thông rộng hữu tuyến hiện có trên địa bàn là 1.725 trạm (616 trạm DSLAM, 1.109 trạm truy nhập quang), đáp ứng nhu cầu cung cấp các dịch vụ Internet băng thông rộng và dịch vụ truyền hình trả tiền qua mạng viễn thông. Mật độ thuê bao điện thoại cố định di động đạt 79,32 máy/100 dân, mật độ thuê bao Internet đạt 22,30 thuê bao/100 dân. Doanh thu toàn ngành năm 2016 ước đạt 3.390 tỷ đồng, bằng 110% kế hoạch được giao.

- Ứng dụng công nghệ thông tin (CNTT) trong hoạt động của các cơ nhà nước tiếp tục được quan tâm đầu tư, sử dụng có hiệu quả hạ tầng kỹ thuật, các hệ thống thông tin hiện có, triển khai kế hoạch thực hiện Nghị quyết 36a của chính phủ, nâng cấp liên thông, mở rộng các phần mềm ứng dụng đến cấp xã như: phần mềm quản lý văn bản và hồ sơ công việc, phần mềm theo dõi

thực hiện nhiệm vụ, thư điện tử công vụ, phần mềm một cửa điện tử và một số phần mềm ứng dụng khác, nhằm nâng cao chất lượng giải quyết công việc. Đến nay 100% các đơn vị có mạng LAN được kết nối Internet tốc độ cao; 95,99 % cán bộ công chức từ cấp tỉnh đến cấp huyện được trang bị máy tính nối mạng để làm việc; 98% cán bộ, công chức đã được cấp hộp thư điện tử công vụ có tên miền @thanhhoa.gov.vn, tỷ lệ cán bộ, công chức thường xuyên sử dụng hệ thống thư điện tử công vụ phục vụ công việc là 96%; 100% các sở, ban, ngành cấp tỉnh, UBND cấp huyện và 132 UBND cấp xã sử dụng có hiệu quả phần mềm quản lý văn bản, hồ sơ công việc (TDOffice) trong chỉ đạo điều hành; 100% các sở, ban, ngành và UBND cấp huyện có Trang/Cổng thông tin điện tử hoạt động ổn định và phát huy được hiệu quả; cung cấp các văn bản quy phạm pháp luật, các dịch vụ hành chính công. Đến hết năm 2016, có 7 đơn vị cấp tỉnh (bằng 36,84%), 20 đơn vị cấp huyện (bằng 74,07%), 132 đơn vị cấp xã (bằng 20,47%) có hệ thống một cửa điện tử liên thông hiện đại cung cấp các dịch vụ công tại bộ phận một cửa phục vụ người dân và doanh nghiệp góp phần đẩy mạnh cải cách hành chính cải thiện môi trường đầu tư kinh doanh.

- Công tác quản lý báo chí, xuất bản, phát thanh truyền hình và thông tin đối ngoại, thông tin cơ sở được tăng cường và đẩy mạnh, hoạt động có hiệu quả, 100% các huyện, các xã có hệ thống đài truyền thanh cơ sở. Năm 2016 đã rà soát, lập hồ sơ đề nghị cấp bổ sung, đổi thẻ Nhà báo giai đoạn 2016 - 2020 cho 166 phóng viên, biên tập viên, lãnh đạo các phòng nghiệp vụ của các cơ quan báo chí. Các cơ quan báo chí và hệ thống Đài Truyền thanh - Truyền hình cấp huyện, đài truyền thanh cơ sở đã thông tin, tuyên truyền, phản ánh đầy đủ, chính xác và kịp thời các sự kiện quan trọng của đất nước; công tác chỉ đạo, điều hành của chính quyền địa phương; tình hình phát triển KT-XH, QP-AN; công tác bảo vệ chủ quyền biên giới, biển, đảo. Đặc biệt, năm 2016 đã thực hiện tốt công tác tuyên truyền bầu cử Quốc hội và HĐND các cấp, tuyên truyền Nghị quyết Đại hội Đảng và các chương trình, kế hoạch hành động triển khai Nghị quyết Đại hội Đảng toàn quốc lần thứ XII, Nghị quyết Đại hội Đảng bộ tỉnh lần thứ XVIII và Đại hội Đảng bộ các cấp. Trong năm, bên cạnh công tác tuyên truyền, công tác cung cấp thông tin cho báo chí cũng luôn được kịp thời. Định kỳ hàng tháng Sở TT&TT phối hợp Ban Tuyên giáo Tỉnh ủy, Hội Nhà báo tổ chức họp giao ban báo chí để đánh giá công tác báo chí và định hướng công tác thông tin; trong năm phối hợp Văn phòng UBND tỉnh tham mưu cho UBND tỉnh tổ chức 14 kỳ giao ban báo chí cung cấp kịp thời các thông tin cho báo chí; Hoạt động thông tin đối ngoại được quan tâm, đã tham mưu cho tỉnh thành lập Ban chỉ đạo Thông tin đối ngoại, tổ chức tập huấn các lớp về Luật Báo chí, thông tin đối ngoại cho người phát ngôn của các sở, ban, ngành và UBND các huyện, thị xã, thành phố, phối hợp tổ chức triển lãm, trưng bày tư liệu về "Hoàng Sa, Trường Sa - những bằng chứng lịch sử" tại 7 đơn vị cấp huyện và 1 trường đại học. Tham mưu hoàn thành và đưa vào sử dụng cụm thông tin đối ngoại tại của khẩu Quốc tế Na Mèo, huyện Quan Sơn.

- Hoạt động thanh tra, kiểm tra theo đúng kế hoạch và hướng dẫn của Thanh tra Bộ, Thanh tra tỉnh. Trong năm 2016 đã tập trung thanh tra, kiểm tra những vấn đề được dư luận quan tâm như quản lý thuê bao di động trả trước; việc thiết lập và hoạt động của các trang thông tin điện tử tổng hợp... phối hợp với Công an tỉnh xử lý sai phạm trong việc đưa tin xuyên tạc, bịa đặt, hạ uy tín các đồng chí lãnh đạo Đảng, Nhà nước và lãnh đạo địa phương trên mạng Internet.

- Công tác quản lý nhà nước về TT&TT trên địa bàn các huyện, thị xã, thành phố tiếp tục được tăng cường, đạt nhiều kết quả, góp phần tích cực vào sự phát triển chung của ngành, cụ thể: Tham mưu cho UBND huyện, thị xã, thành phố ban hành nhiều văn bản chỉ đạo trong hoạt động và công tác quản lý nhà nước về TT&TT trên địa bàn; Tham mưu cho UBND huyện, thị xã, thành phố đẩy mạnh ứng dụng CNTT trong

hoạt động của các cơ quan nhà nước, ứng dụng CNTT phục vụ cải cách hành chính phục vụ doanh nghiệp và người dân; cập nhật kịp thời các thông tin chỉ đạo, điều hành, các thủ tục hành chính cấp huyện, xã lên Trang thông tin điện tử của huyện, thị xã, thành phố. Phối hợp tổ chức quản lý các hoạt động đầu tư, phát triển hạ tầng viễn thông - Internet, các lớp tập huấn phổ biến pháp luật về TT&TT, công tác thanh tra, kiểm tra, kịp thời phát hiện, xử lý đối với các tổ chức, cá nhân vi phạm các quy định trong hoạt động cung cấp các dịch vụ TT&TT; thẩm định kết quả thực hiện tiêu chí số 8 (bưu điện) đề nghị xét, công nhận đạt chuẩn xây dựng NTM năm 2016.

Nhiệm vụ và giải pháp hoạt động ngành thông tin và truyền thông năm 2017:

Năm 2017 là năm thứ hai thực hiện Nghị quyết Đại hội Đảng toàn quốc lần thứ XII, Nghị quyết Đại hội Đảng bộ tỉnh lần thứ XVIII nhiệm kỳ 2015 - 2020 cũng là năm có ý nghĩa rất quan trọng trong việc thực hiện kế hoạch phát triển KT-XH giai đoạn 2016 - 2020 của tỉnh. Để góp phần thực hiện thắng lợi 5 chương trình trọng tâm và 4 nhiệm vụ đột phá trong nhiệm kỳ của Ban chấp hành Đảng bộ tỉnh lần thứ XVIII, Kế hoạch phát triển KT-XH tỉnh Thanh Hóa năm 2017. Định hướng hoạt động ngành TT&TT năm 2017 tập trung vào những nhiệm vụ trọng tâm và các giải pháp sau:

Một là: Tiếp tục làm tốt công tác tham mưu cho Tỉnh ủy, HĐND, UBND thực hiện công tác quản lý nhà nước trong lĩnh vực TT&TT. Trong đó cần tập trung rà soát, bổ sung ban hành các chủ trương, chính sách, các văn bản quy phạm pháp luật nhằm thúc đẩy ngành TT&TT trong thời kỳ hội nhập và phát triển bền vững.

Hai là: Tăng cường chỉ đạo, quản lý nhà nước đối với hoạt động báo chí, phát thanh truyền hình, thông tin điện tử, thông tin đối ngoại, phát hành xuất bản phẩm; Phát huy vai trò của các cơ quan báo chí trong công tác chính trị tư tưởng, định hướng dư luận xã hội nhằm thông tin tuyên truyền, phổ biến quán triệt các quan điểm, chủ trương của Đảng, chính sách, pháp luật của Nhà nước và sự chỉ đạo, điều hành của Trung ương, của tỉnh theo đúng tôn chỉ, mục đích và các quy định của pháp luật; Tập trung thông tin, tuyên truyền Nghị quyết Đại hội Đảng các cấp, 5 chương trình trọng tâm và 4 nhiệm vụ đột phá trong nhiệm kỳ của Ban chấp hành Đảng bộ tỉnh Thanh Hóa lần thứ XVIII, các sự kiện chính trị, KT-XH nổi bật, các ngày lễ của đất nước và của tỉnh, các mô hình, các điển hình tiên tiến, các phong trào thi đua của tỉnh tạo sự đồng thuận trong nhân dân để vượt qua mọi khó khăn, thách thức, góp phần thực hiện thắng lợi các chỉ tiêu nhiệm vụ phát triển KT-XH của tỉnh năm 2017.

Ba là: Tiếp tục phối hợp chặt chẽ với các ngành, các cấp để tham mưu tháo gỡ khó khăn vướng mắc, hỗ trợ, tạo điều kiện thuận lợi để các doanh nghiệp trong toàn ngành TT&TT đẩy mạnh phát triển hạ tầng, cung cấp các dịch vụ có chất lượng cao, đặc biệt là các xã vùng sâu, vùng xa, vùng biên giới, hải đảo, đáp ứng yêu cầu lãnh đạo, chỉ đạo điều hành của cấp ủy đảng, chính quyền và nhu cầu sử dụng dịch vụ của người dân.

Bốn là: Triển khai thực hiện tốt các nội dung của Kế hoạch thực hiện Nghị quyết 36a/NQ-CP ngày 14/10/2015 của Chính phủ về Chính phủ điện tử; Kế hoạch ứng dụng CNTT trong hoạt động của các cơ quan nhà nước tỉnh Thanh Hóa giai đoạn 2016 - 2020; Xây dựng hệ thống phòng họp trực tuyến tại các huyện, thị xã, thành phố trên địa bàn tỉnh Thanh Hóa; Triển khai mô hình xây dựng Thanh Hóa thành "tỉnh thông minh" nhằm từng bước hoàn thiện cơ sở hạ tầng công nghệ thông tin, xây dựng chính quyền điện tử, tăng cường các hoạt động đảm bảo an ninh, an toàn thông tin mạng trên địa bàn tỉnh, góp phần đẩy mạnh cải cách thủ tục hành chính, cải thiện môi trường đầu tư kinh doanh trên địa bàn tỉnh.

Năm là: Xây dựng kế hoạch và triển khai thực hiện có hiệu quả các nhiệm vụ của ngành trong Đề án tái cơ cấu và phát triển ngành dịch vụ đến năm 2020 - định hướng đến năm 2030; các nhiệm vụ "Tăng cường cơ sở vật chất cho hệ thống thông tin và truyền

thông cơ sở" trong chương trình mục tiêu quốc gia xây dựng NTM giai đoạn 2016 - 2020; "Truyền thông và giảm nghèo thông tin" trong chương trình mục tiêu quốc gia giảm nghèo bền vững giai đoạn 2016 - 2020, góp phần thực hiện thắng lợi phong trào thi đua ngành TT&TT chung sức xây dựng nông thôn mới; Chương trình giảm nghèo nhanh bền vững tỉnh Thanh Hóa giai đoạn 2016 - 2020 theo Quyết định số 289-QĐ/TU ngày 27/5/2016 của BCH Đảng bộ tỉnh khóa XVIII.

Sáu là: Chú trọng xây dựng đội ngũ cán bộ, công chức, viên chức và người lao động ngành TT&TT có phẩm chất đạo đức, có tinh thần trách nhiệm, có chuyên môn nghiệp vụ sâu. Tổ chức triển khai thực hiện tốt Nghị quyết Trung ương 4, khóa XII về xây dựng, chỉnh đốn Đảng; ngăn chặn, đẩy lùi sự suy thoái về tư tưởng chính trị, đạo đức, lối sống, những biểu hiện "tự diễn biến", "tự chuyển hóa" trong nội bộ gắn với việc "Đẩy mạnh học tập và làm theo tư tưởng, đạo đức, phong cách Hồ Chí Minh" ở tất cả các cơ quan, đơn vị, doanh nghiệp trong ngành TT&TT.

Để Sở TT&TT hoàn thành tốt các nhiệm vụ chính trị năm 2017, Sở tiếp tục mong muốn nhận được sự quan tâm chỉ đạo của Tỉnh ủy, HĐND, UBND tỉnh và Bộ TT&TT; sự phối hợp của các cấp, các ngành, các doanh nghiệp TT&TT trên địa bàn tỉnh./.

Đồng chí Lê Xuân Lâm - GĐ Trung tâm phát biểu tại hội nghị Tổng kết Công tác điều phối, ứng cứu sự cố và đảm bảo an toàn thông tin mạng trên địa bàn tỉnh năm 2016.

Công tác điều phối, ứng cứu sự cố và đảm bảo an toàn thông tin mạng trên địa bàn tỉnh

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

Ngày nay, cùng với sự phát triển như vũ bão của công nghệ thông tin, đặc biệt là mạng Internet, tình hình mất an toàn thông tin mạng diễn biến ngày càng phức tạp, xuất hiện nhiều nguy cơ đe dọa nghiêm trọng đến việc ứng dụng công nghệ thông tin nhằm phát triển KT-XH và đảm bảo quốc phòng, an ninh. Tuy nhiên, trong khi 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

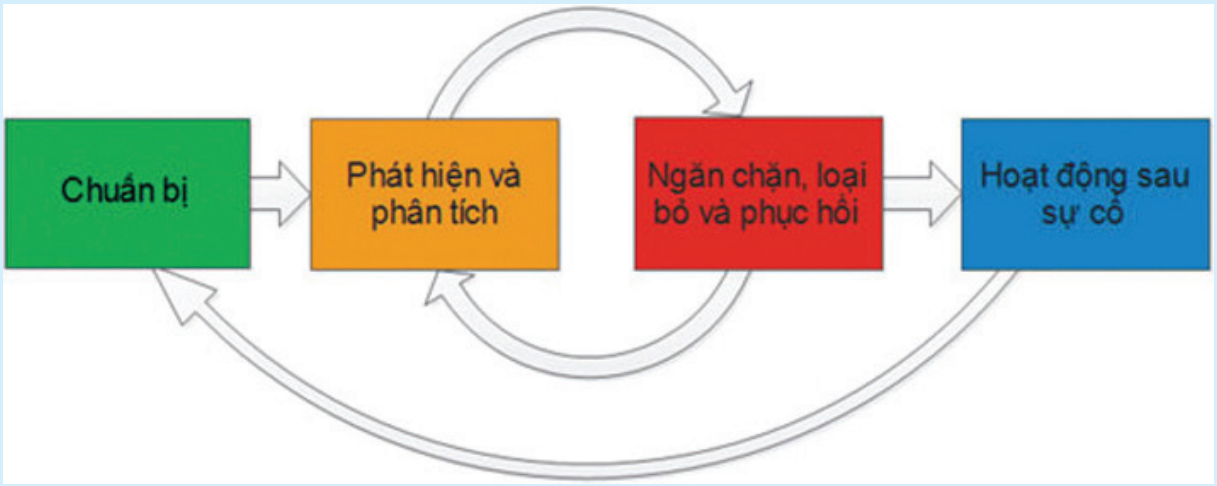
thông tin còn chưa cao. Do đó, để phòng ngừa, giảm thiểu rủi ro về mất an toàn thông tin, đòi hỏi các cấp, các ngành cần có quan tâm đúng mực đến công tác cảnh báo sớm, xử lý ứng cứu sự cố đảm bảo an toàn thông tin cho các hệ thống thông tin.

Tại Việt Nam, trong những năm qua, tình hình an toàn thông tin trong nước có nhiều diễn biến rất phức tạp, các loại sự cố xảy ra với mạng máy tính trong nước đã tăng gấp nhiều lần so với cùng kỳ các năm trước đây. Các hình thức tấn công mạng đối với doanh nghiệp, người dùng cũng như các cơ quan và tổ chức trên toàn quốc như lừa đảo chiếm đoạt tài khoản trên mạng xã hội, thông tin cá nhân, mã hóa dữ liệu người dùng... ngày càng gia tăng. Đặc biệt, trong khoảng thời gian cuối tháng 7 đầu tháng 8 năm 2016, một loạt các hệ thống thông tin quan trọng bị tin tặc tấn công như việc tấn công thay đổi giao diện website và các hệ thống thông tin thuộc sự quản lý của Tổng công ty Hàng không Việt Nam (Vietnam Airlines) và một số đơn vị liên quan khác bị tấn công, gây ra các thiệt hại trực tiếp về kinh tế cho các đơn vị, tăng nguy cơ làm lọt, lộ các bí mật của các cơ quan đơn vị.

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 ứng cứu xử lý sự cố máy tính 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 tới các cơ quan, tổ chức trên địa bàn tỉnh. Bên cạnh các hình thức hỗ trợ gián tiếp qua số điện thoại đường dây nóng, qua phần mềm hỗ trợ công tác ứng cứu từ xa. Trung tâm đã chủ động xây dựng kế hoạch từ đầu năm để triển khai trực tiếp hỗ trợ tại các các cơ quan, tổ chức, doanh nghiệp thực hiện các hoạt động phòng ngừa, ngăn chặn, ứng cứu, khôi phục nhằm đối phó với các loại tấn công phá hoại trên môi trường mạng cho các hệ thống thông tin của tỉnh, cụ thể như sau:

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

- 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 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 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



Sơ đồ quy trình ứng cứu sự cố.

Thông tin và Truyền thông quy định về điều phối các hoạt động ứng cứu sự cố mạng Internet Việt Nam. 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 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.

Phần mềm tổng hợp ứng cứu sự cố trực tuyến.

- 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.

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

- 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, Công văn số 935/STTTT-CNTT, ngày 01/8/2016, về tăng cường kiểm tra rà soát hệ thống đảm bảo hệ thống an toàn thông tin; công văn số 955/STTTT-CNTT, ngày 04/8/2016 về theo dõi, ngăn chặn kết nối và xóa các tệp tin chứa mã độc...

- Hằng năm, bình quân 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 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

Hoạt động giám sát an toàn thông tin cho các đơn vị thông qua hệ thống phần mềm giám sát từ xa.

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 ứng cứu xử lý sự cố được triển khai hiệu quả hơn nữa, đề nghị các cơ quan, đơn vị cần thực hiện tốt một số nội dung sau:

Một là, để công tác phối hợp trong các hoạt động ứng cứu khẩn cấp an toàn mạng thì điều quan trọng là ngay tại các cơ quan, đơn vị cần chủ động xây dựng quy trình ứng cứu sự cố riêng kết hợp phù hợp với đặc điểm, tình hình của hệ thống thông tin đang hoạt động. Qua đó, khi phát hiện có sự cố hoặc được cảnh báo sự cố, đơn vị sẽ chủ động trong việc khắc phục để giảm thiểu hậu quả do sự cố gây ra đến mức thấp nhất.

Hai là, các cơ quan, đơn vị cần phối hợp liên kết chặt chẽ với các đơn vị khác để hình thành một mạng lưới ứng cứu khẩn cấp trên địa bàn tỉnh có sự gắn kết chặt chẽ theo tinh thần quyết định số 31/QĐ-STTTT, ngày 08/4/2016 của Giám đốc Sở Thông tin và Truyền thông. Đồng thời phải phối hợp, trao đổi thông tin giữa các đơn vị một cách thường xuyên, chủ động để cập nhập các thông tin cảnh báo, kỹ thuật, công nghệ mới để qua đó có được các phương án chiến lược phòng chống, ngăn chặn sự cố một cách nhanh chóng và hiệu quả hơn.

Ba là, cần quan tâm đầu tư trang thiết bị phục vụ công tác ứng cứu sự cố; 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 KT-XH của tỉnh trong thời gian tới./.

Tổng kết tình hình, sự kiện an toàn thông tin tiêu biểu TRONG NĂM 2016

BAN BIÊN TẬP

Năm 2016 đã đi qua với nhiều sự kiện về an toàn thông tin nổi bật cũng như bùng nổ các sự cố mất an toàn thông tin nghiêm trọng... Dưới đây, Bản tin An toàn thông tin điểm lại 10 tình hình, sự kiện an toàn thông tin tiêu biểu trong năm 2016 do Ban biên tập lựa chọn, tổng hợp và đánh giá.

1. Luật An toàn thông tin mạng chính thức có hiệu lực

Luật An toàn thông tin mạng là bộ luật quan trọng để triển khai các hoạt động an toàn thông tin tại Việt Nam. Với kết cấu 8 chương 54 điều, Luật An toàn thông tin mạng đề cập đến rất nhiều vấn đề mới, "nóng bỏng" trong lĩnh vực An toàn thông tin hiện nay, cụ thể hóa nhiều vấn đề đang gây bức xúc dư luận xã hội như thư rác; thu thập, phát tán thông tin cá nhân trái phép...

Ngay sau khi Luật An toàn thông tin mạng (ATTTM) được thông qua trong năm 2016, Chính phủ đã ban hành bốn Nghị định hướng dẫn thi hành luật, đã kịp thời cụ thể hóa các nội dung cơ bản trong Luật ATTTM, tạo điều kiện để các cơ quan quản lý nhà nước thực thi công tác quản lý và các tổ chức thấy rõ trách nhiệm trong công tác đảm bảo an toàn các hệ thống thông tin của mình. Bên cạnh đó, các tổ chức, cá nhân hoạt động trong lĩnh vực ATTT đã có hành lang pháp lý cụ thể cho các hoạt động sản xuất, kinh doanh.

2. Phương hướng bảo đảm an toàn thông tin mạng giai đoạn 2016 - 2020

Ngày 27/5/2016, Phó Thủ tướng Chính phủ Vũ Đức Đam đã ký Quyết định số 898/QĐ-TTg phê duyệt phương hướng, mục tiêu, nhiệm vụ bảo đảm ATTT mạng giai đoạn 2016 - 2020. Ba nhiệm vụ trọng tâm trong giai đoạn tới là: Bảo đảm ATTT mạng quy mô quốc gia; Bảo đảm ATTT mạng trong hoạt động của cơ quan, tổ chức; Phát triển thị trường sản phẩm và dịch vụ ATTT mạng.

3. Ngày An toàn thông tin Việt Nam 2016

Ngày ATTT là sự kiện thường niên được tổ chức hàng năm và là một trong những hoạt động CNTT quan trọng trong năm được đông đảo cộng đồng ứng dụng và phát triển CNTT, ATTT, giới truyền thông và xã hội quan tâm. Năm 2016 là năm thứ 9 diễn ra sự kiện này.

Ngày ATTT Việt Nam năm 2016 gồm chuỗi các sự kiện về ATTT với trọng tâm là Hội thảo quốc tế được tổ chức tại Hà Nội ngày 2/12/2016, với chủ đề "Kỷ nguyên mới của an ninh mạng". Tại Hội thảo, các báo cáo điều tra, đánh giá thực trạng ATTT tại Việt Nam năm 2016 của VNISA đã đưa ra Chỉ số ATTT Việt Nam (Vietnam Information Security Index) năm 2016 là 59,9%; tăng đáng kể so

với mức 47,4% của năm 2015.

4. Tấn công mạng vào Vietnam Airlines

Sự kiện xảy ra chiều ngày 29/7/2016 là cuộc tấn công mạng có chủ đích (APT), xâm nhập cả theo chiều sâu và chiều rộng. Việc phát động tấn công đã được thực hiện đồng loạt. Website của Vietnam Airlines bị chiếm quyền kiểm soát và bị tấn công thay đổi giao diện, đồng thời dữ liệu của hơn 400 nghìn khách hàng Bông Sen Vàng của Vietnam Airlines bị rò rỉ lên mạng. Cùng chiều ngày 29/7, hệ thống âm thanh và thông báo tại cảng hàng không Tân Sơn Nhất và Nội Bài bị can thiệp, sửa đổi hiển thị hình ảnh và âm thanh.

Dù được xác định đây chỉ là vụ tấn công vào phần hệ thống ngoại vi, chưa xâm nhập được vào các hệ thống trọng yếu bên trong cũng như không thể ảnh hưởng tới an toàn bay, nhưng vụ việc là hồi chuông báo động về thực trạng an toàn thông tin của các hệ thống trọng yếu như các cảng hàng không, cũng như mức độ sẵn sàng của các hệ thống trước nguy cơ bị tấn công mạng vẫn còn quá yếu kém.

5. An ninh ngành ngân hàng bị đe dọa nghiêm trọng

Trong tháng 5/2016, TPBank đã suýt bị hacker quốc tế lừa đảo, lấy 1,13 triệu USD. TPBank cho biết, tin tặc có thể đã dùng mã độc cài vào một ứng dụng phần mềm do bên thứ ba cung cấp để ngân hàng này kết nối với hệ thống thanh toán quốc tế SWIFT. Đến ngày 5/8/2016, một khách hàng của Vietcombank phát hiện tài khoản của mình tự động có giao dịch chuyển đi 500 triệu đồng.

Các vụ việc trên cho thấy giới tội phạm công nghệ cao đang hướng đến mục tiêu là các ngân hàng và người sử dụng tại Việt Nam chưa có nhiều kinh nghiệm trong việc bảo mật thông tin tài khoản ngân hàng.

6. Hàng loạt mạng xã hội lớn bị rò rỉ thông tin người dùng

Trước hết, phải kể đến vụ mất cắp dữ liệu lớn nhất xảy ra ở Mỹ, liên quan đến Yahoo. Hơn 1,5 tỷ người dùng bị đánh cắp tài khoản trong 2 vụ lộ lọt dữ liệu được công bố hồi tháng 9 và tháng 12/2016. Yahoo vẫn chưa thể xác định nguồn gốc vụ tấn công. Đến lượt mạng xã hội MySpace với hơn 427 triệu mật khẩu và 360 triệu địa chỉ email của khách hàng bị tin tặc thu thập và công bố trên Internet.

2016 là năm bộc lộ các vấn đề an ninh mạng của các mạng xã hội lớn. Hàng tỷ dữ liệu người dùng bị đánh cắp và rao bán trên Internet, gióng lên hồi chuông cảnh báo về sự cấp thiết của việc nâng cao đảm bảo an toàn dữ liệu cá nhân. Với lượng người dùng khổng lồ, mạng xã hội đang là tâm điểm của những cuộc tấn công lấy cắp dữ liệu.

7. Bùng nổ mã độc mã hóa dữ liệu Ransomware

Thống kê từ hệ thống giám sát virus của Bkav cho thấy, có tới 16% lượng email lưu chuyển trong năm 2016 là email phát tán ransomware, nhiều gấp 20 lần năm 2015. Như vậy cứ trung bình 10 email nhận được trong năm 2016 thì người sử dụng sẽ gặp 1,6 email chứa ransomware, một con số rất đáng báo động.

Hình thức phát tán chủ yếu của ransomware

trong năm 2016 là thông qua file đính kèm từ các email spam. Khi người dùng mở trực tiếp file đính kèm, mã độc sẽ chạy trực tiếp hoặc được file đính kèm tải về từ máy chủ C&C của hacker. Một số hình thức phát tán khác mà ransomware sử dụng là khai thác lỗ hổng, giả mạo trang web, giả mạo các chương trình thông dụng...

8. Tấn công DDoS sử dụng mã độc Mirai trên các thiết bị IoT

Năm 2016 chứng kiến sự bùng nổ của các cuộc tấn công theo hình thức từ chối dịch vụ (DoS/DdoS) cả về quy mô và sức mạnh. Theo ghi nhận của mạng lưới phân bố nội dung khổng lồ Akamai, số lượng các cuộc tấn công DoS/DDoS trong quý 3/2016 tăng 71% so với cùng kỳ năm

trước, tăng 8% so với quý 2/2016.

2016 cũng được xem là năm phát triển mạnh mẽ của nghành công nghiệp IoT. Tuy nhiên, vấn đề an ninh trong lĩnh vực này chưa theo kịp tốc độ phát triển và mở rộng của thiết bị. Các nhà sản suất sản phẩm IoT chưa quan tâm đúng mức tới vấn đề an ninh.

9. Mã độc lây lan qua thiết bị USB vẫn phát triển mạnh

Việc loại bỏ tính năng Auto Run trong các hệ điều hành của Microsoft không làm cho virus USB trở nên hết thời. Theo chương trình đánh giá an ninh mạng 2016 của Bkav, tỷ lệ USB bị nhiễm virus trong năm 2016 vẫn ở mức rất cao 83%.

Theo thống kê từ hệ thống giám sát virus của Bkav, có tới 16,7 triệu lượt máy tính được phát hiện là nhiễm virus lây qua USB trong năm 2016. Trong đó chỉ 11% là đến từ dòng virus lây trực tiếp bằng Auto Run, còn tới 89% là dòng W32.UsbFakeDrive.

10. Tấn công có chủ đích APT - quả bom hẹn giờ

Vụ việc Vietnam Airlines bị tấn công ngày 29/07/2016 là cảnh báo mạnh mẽ về nguy cơ các cuộc tấn công có chủ đích APT tại Việt Nam sẽ còn tiếp tục trong thời gian tới.

Kịch bản tấn công APT thường được hacker sử dụng là gửi email đính kèm file văn bản chứa mã độc. Với tâm lý cho rằng file văn bản thì an toàn, rất nhiều người sử dụng đã mắc lừa và mở file đính kèm, sau đó máy tính đã bị nhiễm mã độc. Theo thống kê năm 2016 của Bkav, có tới hơn 50% người dùng cho biết vẫn giữ thói quen mở ngay các file được đính kèm trong email, không giảm so với năm 2015./.

Cán bộ phòng Cơ yếu - CNTT Văn phòng Tỉnh ủy Thanh Hóa phục vụ Đại hội đại biểu Đảng bộ tỉnh lần thứ XVIII.

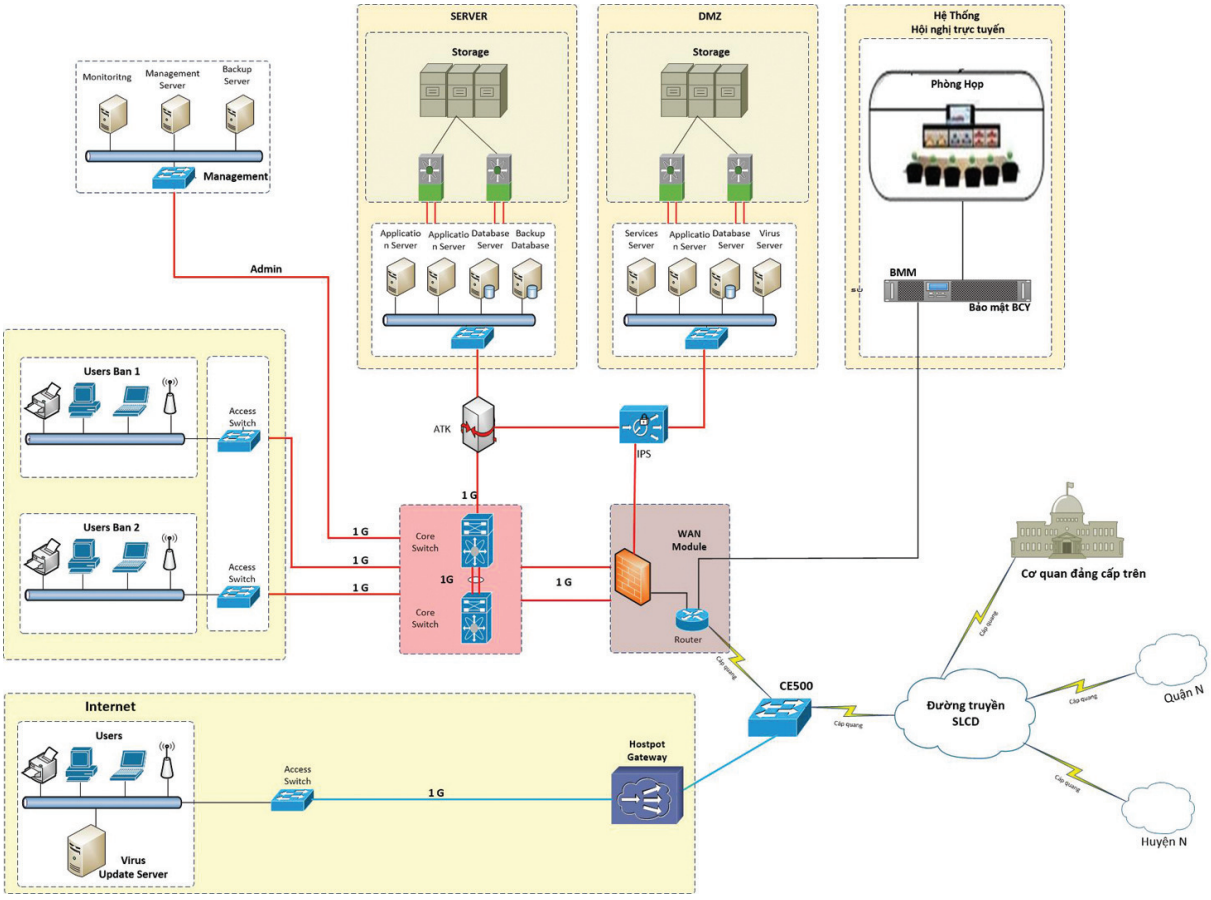
Công tác đảm bảo an toàn thông tin cho các hệ thống thông tin khối các cơ quan Đảng tỉnh Thanh Hóa

MAI VĂN TIỆP

Phòng Cơ yếu - CNTT Văn phòng Tỉnh ủy Thanh Hóa

Trong những năm vừa qua hạ tầng kỹ thuật mạng CNTT các cơ quan Đảng trong tỉnh được đầu tư đồng bộ từ tỉnh đến cơ sở, đáp ứng nhu cầu khai thác của cán bộ, công chức khối các cơ quan Đảng trong tỉnh, phục vụ công tác lãnh đạo, chỉ đạo của các cấp uỷ trong tỉnh. Đến nay trong toàn tỉnh tỉ lệ máy tính trên đầu cán bộ công chức ở cấp tỉnh 1,3 người/máy, cấp huyện 1,5 người/máy, quy mô mạng CNTT diện rộng các cơ quan đảng là 674 đầu mối trong tỉnh gồm các Ban xây dựng đảng, 33 huyện, thị, thành ủy, đảng ủy trực thuộc và 635 đảng ủy xã, phường, thị trấn với hơn trên 1.328 người dùng, thường xuyên kết nối khai thác. Các đầu mối được xây dựng trên nền tảng IP.DCS được phân cấp từ Trung ương đến địa phương thông qua đường truyền số liệu chuyên dùng do Cục Bưu điện Trung ương cung cấp.

Trong toàn tỉnh, các cấp ủy đảng thực hiện lãnh đạo, chỉ đạo qua các hệ thống thông tin đặc thù trong từng lĩnh vực



Mô hình mạng trong các cơ quan Đảng tỉnh Thanh Hoá.

công tác gồm: Công tác điều hành tác nghiệp, công tác xây dựng đảng, công tác kiểm tra - giám sát, công tác tuyên giáo, dân vận, nội chính,... Các hệ thống trên được tích hợp thành hệ thống thông tin (HTTT) tổng hợp phục vụ sự lãnh đạo, chỉ đạo của các cấp ủy. HTTT tổng hợp trong các cơ quan Đảng được xây dựng thống nhất từ trung ương đến địa phương với mục tiêu tự động hóa các quy trình lãnh đạo, chỉ đạo của cấp ủy các cấp, hệ thống này có khối lượng thông tin rất lớn được tập trung tại trung tâm tích hợp dữ liệu của Văn phòng Trung ương Đảng và các tỉnh, thành ủy.

Tại Thanh Hóa các cơ sở dữ liệu trên HTTT tổng hợp có khối lượng thông tin lớn, trong toàn tỉnh đã cập nhật vào các kho điện tử trên 204.324 tài liệu, văn kiện; cập nhật trên 208.000 hồ sơ đảng viên, phiếu 4 trang trên phần mềm "Quản lý đảng viên phiên bản 2.6; 350 bản tin trên phần mềm "Thông tin tuần"; 1.500 bản tin trên phần mềm "Bản tin ngày"; trên 7.600 bản ghi địa chỉ hồ sơ trên phần mềm "Quản lý Mục lục hồ sơ"; 3.060 bản tin tham khảo trên phần mềm "Thông tin phục vụ lãnh đạo" và 21.060 tin, bài đăng trên Website của Đảng bộ tỉnh. Các thông tin trên được lưu trữ tại trung tâm tích hợp dữ liệu đặt tại Tỉnh uỷ và một số cơ sở dữ liệu lưu trữ phân tán tại các huyện thị thành uỷ, trong đó có nhiều thông tin mật trở lên cần đảm bảo an toàn tránh lộ lọt, phát tán trên mạng Internet.

Từ mức độ quan trọng của thông tin trong HTTT tổng hợp nên công tác đảm bảo an toàn thông tin mạng, chống xâm nhập luôn được xem là nhiệm vụ trọng tâm. Trung tâm CNTT Tỉnh ủy đã xây dựng nhiều giải pháp kỹ thuật, phương án tổ chức đảm bảo hệ thống mạng CNTT an toàn, hoạt động thông suốt thông qua hệ thống Fire-wall mềm và Firewall cứng, các thiết bị chống

xâm nhập IPS. Cụ thể như sau:

Thứ nhất: Đảm bảo an toàn thông tin thông qua mô hình mạng đồng bộ. Việc xây dựng hạ tầng kỹ thuật mạng CNTT phù hợp với mô hình tổ chức của hệ thống các cơ quan Đảng, đảm bảo yêu cầu kỹ thuật tiêu chuẩn, công nghiệp, hiện đại đáp ứng yêu cầu triển khai thực hiện các ứng dụng. Khi xây dựng trung tâm dữ liệu phải luôn ưu tiên các phương án có thành phần thực hiện kiểm soát truy nhập, giám sát hoạt động và bảo đảm an toàn hệ thống cho trung tâm dữ liệu đảm bảo các chính sách về an ninh, an toàn hệ thống.

Hệ thống kết nối mạng của các cơ quan đảng tỉnh Thanh Hóa hiện nay được xây dựng đảm bảo an toàn an ninh mạng với các giải pháp cụ thể như:

- Tường lửa cứng (thiết bị CISCO ASA 5520): Kiểm soát truy cập vào/ra Trung tâm dữ liệu theo chính sách an ninh, bảo đảm an ninh cho các vùng trong hệ thống như DMZ, người dùng, quản trị, kiểm soát vòng ngoài cho vùng máy chủ. Chỉ sử dụng những cổng dịch vụ cần thiết để trao đổi thông tin với các cơ quan Trung ương và cho phép người dùng (tỉnh, thành, quận, huyện) truy cập, khai thác thông tin an toàn.

- Hệ thống giám sát chống truy nhập trái phép IPS/IDS (thiết bị Cisco IPS 4240): Giám sát việc truy cập các phân mạng trong trung tâm dữ liệu, gồm thiết bị và phần mềm kiểm soát, giám sát hoạt động truy cập hệ thống, báo cáo, thống kê khi cần thiết.

- Phần mềm tường lửa ATK (cài trên hệ điều hành Redhat 6.4): Theo dõi, kiểm soát truy cập vào vùng máy chủ (server) thông qua chính sách an ninh được thiết lập trên máy chủ tường lửa. Bảo vệ vùng quản trị và cấu hình để máy cán bộ quản trị mạng kiểm soát các vùng trong hệ thống mạng của tỉnh uỷ, thành uỷ.

- Bộ mã hóa và giải mã dữ liệu (BMM): Bằng thiết bị BMM của Ban cơ yếu Chính phủ đảm bảo an toàn thông tin cho các phiên họp trực tuyến giữa Tỉnh ủy với các điểm cầu của Trung ương cũng như các huyện, thị, thành ủy.

Thứ hai: Giải pháp ảo hoá kết hợp hệ thống sao lưu dữ liệu tự động. Phương pháp ảo hoá các server chạy các phần mềm ứng dụng kết hợp với hệ thống tự động sao lưu cũng là giải pháp đang áp dụng hiệu quả. Với giải pháp này cho phép chúng ta định kỳ sao lưu toàn bộ hệ thống máy chủ (bao gồm cả cấu hình phần mềm và các cơ sở dữ liệu), trường hợp có sự cố xảy ra chúng ta sẽ khôi phục toàn bộ server trong khoảng thời gian cho phép. Giải pháp này cho phép chúng ta thiết lập các firewall giả định, firewall này có khả năng chống xâm nhập tương đương với các thiết bị firewall cứng.

Thứ ba: Sử dụng phần mềm tự động giám sát, phát hiện, tiêu diệt hoặc cảnh báo các phần mềm virus, trojans, spyware,... Tại hệ thống mạng khối các cơ quan Đảng trong tỉnh đang sử dụng phần mềm phòng/chống virus Kaspersky và xây dựng mô hình cập nhật theo giải pháp của Kaspersky. Một máy chủ được đặt tại trung tâm có chức năng tự động cập nhật các bản mới từ website của Kaspersky, các máy trạm sẽ cập nhật thông qua máy chủ từ trung tâm. Như vậy máy trạm tuy không trực tiếp kết nối internet song vẫn có thể thường xuyên cập nhật các bản mới từ Kaspersky.

Thứ tư: Mã hoá các thông tin mật bằng thiết bị Chứng thư số và phần mềm kèm theo do Ban Cơ yếu Chính phủ phát triển và chuyển giao. Trong toàn hệ thống các cơ quan đảng từ Trung ương đến địa phương sử dụng thống nhất sản phẩm eToken của Ban cơ yếu Chính phủ để ký điện tử các văn bản điện tử, mã hóa các tài liệu mật, tối mật và truy nhập vào các hệ thống thông tin, phần mềm chuyên ngành của các ban xây dựng đảng.

Thứ năm: Giải pháp chính sách và phát triển con người. Các giải pháp phần cứng, phần mềm dù có hiệu quả đến mấy nếu con người vận hành và sử dụng hệ thống không đạt đến trình độ nhất định về ứng dụng CNTT thì cũng không thể phát huy hết tác dụng. Do đó để đảm bảo an toàn thông tin ngoài xây dựng hệ thống đồng bộ, hiện đại cần có hệ thống các văn bản quy định về quản lý, khai thác và vận hành mạng nội bộ của các cơ quan đơn vị. Các cơ quan Đảng trong tỉnh trong thời gian qua đã ban hành nhiều các văn bản chỉ đạo thực hiện chính sách đảm bản an toàn an ninh mạng diện rộng các cơ quan Đảng.

Hằng năm tổ chức tập huấn cho cán bộ quản trị mạng các đơn vị về nâng cao chất lượng chuyên môn, nâng cao khả năng đảm bảo an toàn thông tin mạng, duy trì ổn định mạng thông tin diện rộng các cơ quan Đảng./.

Công tác đảm bảo ATTT các hệ thống thông tin phục vụ sự chỉ đạo, điều hành của UBND tỉnh, Chủ tịch UBND tỉnh

PHẠM VĂN CƯỜNG
Phòng Quản lý Cổng thông tin điện tử và CNTT
Văn phòng UBND tỉnh Thanh Hóa

Trong những năm qua, thực hiện nhiệm vụ được giao, Văn phòng UBND tỉnh đã tích cực triển khai các ứng dụng và phát triển hạ tầng CNTT để phục vụ sự chỉ đạo, điều hành của UBND tỉnh, Chủ tịch UBND tỉnh; nhằm phục vụ doanh nghiệp và người dân được tốt hơn. Đồng thời, cung cấp phổ biến thông tin giúp doanh nghiệp, người dân tiếp cận các chủ trương chính sách và các dịch vụ công trực tuyến mức độ cao trên môi trường mạng, góp phần xây dựng nền hành chính của tỉnh đảm bảo minh bạch, hiệu quả, cải thiện môi trường đầu tư, kinh doanh, nâng cao chỉ số cạnh tranh phục vụ phát triển kinh tế - xã hội và đảm bảo quốc phòng - an ninh của tỉnh.

Hiện nay, Văn phòng UBND tỉnh đang quản lý Trung tâm tích hợp dữ liệu, Cổng thông tin điện tử, Hệ thống thư điện tử công vụ, Phần mềm theo dõi thực hiện nhiệm vụ giao cho các đơn vị của UBND tỉnh và một số phần mềm ứng dụng trong quản lý nội bộ của cơ quan. Do đó, công tác đảm bảo an ninh, an toàn thông tin mạng tại Văn phòng UBND tỉnh được quan tâm đầu tư các trang thiết bị chuyên dùng để nâng cao năng lực đảm bảo an ninh, an toàn thông tin cho các hệ thống. Tại Trung tâm tích hợp dữ liệu của tỉnh đã được đầu tư các thiết bị như tường lửa, thiết bị phát hiện, cảnh báo và phòng chống xâm nhập trái phép, thiết bị chống thư rác, spam và quét virus phục vụ việc triển khai các ứng dụng CNTT trong các cơ quan nhà nước trên địa bàn tỉnh. Việc bảo mật thông tin, văn bản trên môi trường mạng tại Văn phòng UBND tỉnh luôn được chú trọng, toàn bộ văn bản đi, đến (trừ các văn bản có độ mật trở lên) được ký số trước khi cập nhật lên phần mềm hoặc gửi thư điện tử. Đối với các văn bản có mức độ mật trở lên được soạn thảo, lưu trữ trên máy tính riêng (không có kết nối mạng, không kết nối thiết bị lưu trữ), đảm bảo theo đúng quy định về bảo vệ bí mật nhà nước. Công tác đào tạo, bồi dưỡng nguồn nhân lực luôn được lãnh đạo quan tâm, tạo điều kiện tham gia các khóa học về ATTT.

Trung tâm tích hợp dữ liệu của tỉnh.

Nhìn chung, công tác đảm bảo an toàn, an ninh thông tin cho các hệ thống thông tin do Văn phòng UBND tỉnh quản lý, vận hành được hoạt động an toàn, ổn định, gửi nhận thông suốt, chưa phát hiện sự cố hoặc các hoạt động xâm nhập trái phép gây mất an toàn thông tin. Qua đó đã góp phần tích cực trong việc chỉ đạo, điều hành của UBND tỉnh, Chủ tịch UBND tỉnh./.

VNPT CHỦ ĐỘNG NÂNG CAO NĂNG LỰC HỆ THỐNG, TĂNG CƯỜNG HỖ TRỢ ĐẢM BẢO AN TOÀN THÔNG TIN CHO KHÁCH HÀNG SỬ DỤNG DỊCH VỤ

NGUYỄN VĂN THÀNH
Trung tâm CNTT VNPT Thanh Hóa

Thời gian gần đây, trong bối cảnh công nghệ thông tin và viễn thông phát triển mạnh mẽ thì tình trạng mất an ninh, an toàn mạng trên toàn cầu nói chung, Việt Nam nói riêng đã và đang diễn ra rất phức tạp và nguy hiểm. Cùng với việc gia tăng sự tấn công, tội phạm mạng thâm nhập vào hệ thống mạng thông tin trọng yếu để thu thập, đánh cắp thông tin bí mật nhà nước và doanh nghiệp, các nhóm tội phạm cũng đang không ngừng câu kết với nhau, chia sẻ hạ tầng để triển khai các chiến dịch tấn công. Trình độ tấn công của các băng nhóm tội phạm mạng ngày càng cao, sự thiếu hụt về nhân lực quản trị CNTT cao cấp, sự phát triển tốc độ của điện toán đám mây, di động và IoT(Internet of Things - Internet kết nối vạn vật) cùng với sự chủ quan của doanh nghiệp, người dùng trước các cảnh báo bảo mật... chính là những lý do lớn dẫn đến những sự cố liên quan đến bảo mật thông tin của doanh nghiệp, cơ quan nhà nước.

Riêng ở Việt Nam, liên tiếp xảy ra các vụ tấn công mạng đối với Vietnam Airlines và nhiều ngân hàng thương mại trong nước. Đối tượng tội phạm trên mạng - Hacker- tập chung chủ yếu vào một số hình thức chủ yếu như sau:

Lập các website lừa đảo (Facebook; Gmail;...): Người dùng lầm tưởng các website này là những website thường truy cập (do có giao diện tương đồng) để người dùng nhập các thông tin cá nhân. Sau đó các đối tượng phạm tội sẽ thay đổi mật khẩu và chiếm đoạt thông tin người dùng.

Gửi thư có đính kèm phần mềm mã hóa dữ liệu: Lợi dụng sự mất cảnh giác của người dùng trong việc gửi nhận thư điện tử Email. Đối tượng phạm tội sẽ giả mạo để gửi email cho người dùng trong đó có kèm theo phần mềm mã hóa các file dữ liệu (word; excel...). Sau khi người dùng mở email thì phần mềm mã hóa dữ liệu sẽ tự động kích hoạt và mã hóa toàn bộ dữ liệu trên máy tính người dùng. Tiếp theo đối tượng sẽ gửi cho người dùng một thông báo tống tiền để giải mã các file dữ liệu này.

Tấn công từ chối dịch vụ phân tán DDoS (Distributed Denial of Service): Kẻ tấn công nhằm ngăn cản người dùng truy cập các thông tin hoặc dịch vụ trên mạng bằng cách lợi dụng và điều khiển nhiều hệ thống thiết bị của người dùng trên mạng tạo thành một Bot-net để thực hiện tấn công liên tục vào một hệ thống dịch vụ nào đó của nhà cung cấp làm nghẽn băng thông mạng. Tiêu biểu như hôm 21/10/2016 vừa qua, một vụ tấn công DDos cực lớn khiến một nửa nước Mỹ mất Internet (http://genk.vn/hieu-ky-hon-ve-vu-tan-cong-ddos-cuc-lon-khien-mot-nua-nuoc-my-mat-internet-vao-hom-qua-20161022165520 19.chn).

Việc ngăn chặn các hình thức tội phạm mạng nêu trên đã được các nhà mạng và các nhà cung cấp dịch vụ tập trung giải quyết và đối phó. Tuy nhiên, sự biến tướng và thay đổi cách thức tấn công của các đối tượng phạm tội ngày càng tinh vi và phức tạp do đó mới cũng chỉ hạn chế được một phần nào đó để giảm thiểu tối đa khả năng phá hoại và khắc phục sự cố một cách nhanh chóng nhất.

Trước tình hình phức tạp của tình trạng mất an toàn, an ninh mạng đến mức báo động như hiện nay, VNPT Thanh Hóa nói riêng và tập đoàn VNPT nói chung nhận thức được cấp độ nguy hiểm rất cao và tập trung trọng tâm vào các giải pháp ổn định hệ thống, hỗ trợ khách hàng sử dụng dịch vụ trước những nguy cơ tấn công mạng để đảm bảo hạ tầng cung cấp

Chuyên gia VNPT đang rà soát bản đồ mục tiêu bị Malware tấn công.

dịch vụ cho người dùng. VNPT Thanh Hóa đã chủ động triển khai các giải pháp cụ thể:

Một là, đầu tư xây dựng các hệ thống giám sát, cảnh báo tình trạng mạng lưới cung cấp dịch vụ có chất lượng để kiểm soát an ninh an toàn mạng như: Kiểm soát lưu lượng, băng thông bất thường; Kiểm soát hiệu suất sử dụng thiết bị truy nhập; Kiểm soát các hành vi xâm nhập bất thường...

Hai là, thường xuyên rà quét xử lý và khắc phục những lỗ hổng an ninh, an toàn của các hệ thống cung cấp dịch vụ cho khách hàng. Cập nhật các bản vá lỗi hệ thống, nâng cấp firmware có tính năng an toàn, an ninh cao cho các thiết bị cung cấp dịch vụ trên mạng.

Ba là, tích cực phối hợp với các tổ chức an ninh an toàn mạng trong nước, quốc tế để ngăn ngừa và nhanh chóng xử lý, triệt để các cuộc tấn công mạng, tội phạm mạng.

Bốn là, hỗ trợ khách hàng các biện pháp an ninh phù hợp ngăn chặn khả năng và nguy cơ xảy ra mất an toàn cao, đặc biệt đối với với các tổ chức, doanh nghiệp và khách hàng sử dụng các thiết bị IoT.

Hiện tại số lượng và các ứng dụng, dịch vụ hỗ trợ hữu ích trên mạng gia tăng nhanh chóng đáp ứng hầu hết các nhu cầu của người dùng. Tuy nhiên, việc tìm hiểu, lựa chọn dịch vụ và sử dụng các tiện ích như thế nào cho hiệu quả để tránh bị lợi dụng hoặc là nạn nhân của tội phạm mạng, người sử dụng cần phải trang bị cho mình một số kỹ năng cần thiết để đảm bảo an toàn khi tham gia vào thế giới mạng.

Đúc rút từ kinh nghiệm hỗ trợ và xử lý sự cố thực tế, VNPT Thanh Hóa khuyến nghị khách hàng sử dụng một số biện pháp phòng chống cụ thể:

Đối với dạng **website lừa đảo**, người dùng cần phải tìm hiểu kỹ những **đường link** (kết nối) xem có đúng của nhà cung cấp dịch vụ tạo ra hay không hay là giả mạo với giao diện tương tự. Người dùng tuyệt đối không cung cấp các thông tin nhạy cảm của cá nhân như (mật khẩu; mã số cá nhân; tài khoản...) một cách tùy tiện. Bởi vì, các nhà cung cấp dịch vụ hiện nay hỗ trợ người dùng cung cấp các thông tin nhạy cảm cần phải được xác thực bằng nhiều key khác nhau (VD: muốn đổi mật khẩu Gmail phải thông qua điện thoại đăng ký để nhận mã xác thực...).

Đối với dạng **thư có đính kèm phần mềm mã hóa dữ liệu**, người dùng cần phải cân nhắc và xem xét kỹ tiêu đề, đối tượng gửi thư đến cho mình, không tùy tiện mở thư và file đính kèm, nếu nghi ngờ thư giả mạo thì phải xóa bỏ triệt để ngay. Việc giải mã các tập tin đã bị mã hóa rất khó được thực hiện, khả năng thành công rất thấp. Người dùng tuyệt đối không được làm theo các hướng dẫn của tội phạm như: Gửi tiền cho tài khoản của tội phạm để nhận được key mở khóa vì điều đó xảy ra chưa chắc tội phạm đã đưa ngay key cho người dùng mà còn sẽ lợi dụng để đòi thêm tiền chuộc nữa. Để giảm thiểu khả năng bị mã hóa dữ liệu, người dùng phải lưu trữ dữ liệu khoa học, hợp lý và ở nhiều nơi.

Đối với dạng **tấn công từ chối dịch vụ phân tán - DDoS**,

để tránh bị các đối tượng phạm tội lợi dụng các thiết bị của mình (Camera, máy tính...) - IoT (internet of thing) để tạo thành một hệ thống tấn công trên mạng, khai thác thông tin cá nhân thì người ìi dùng cần lưu ý một số vấn đề sau:

- Sử dụng các thiết bị có nguồn gốc xuất xứ rõ ràng, các hãng có tên tuổi trên thị trường.

- Thay đổi các mật khẩu truy cập mặc định của nhà sản xuất thiết bị bằng những mật khẩu đảm bảo an toàn (mật khẩu nhiều ký tự, có chữ hoa, chữ thường, số và ký tự đặc biệt).

- Tìm hiểu kỹ tài liệu hướng dẫn kỹ thuật, nhờ những người am hiểu thiết bị, hoặc các nhân viên của các đơn vị cung cấp dịch vụ cài đặt và hạn chế các tính năng không cần thiết của thiết bị.

- Hợp tác chặt chẽ với các nhà cung cấp dịch vụ để khắc phục sự cố và ngăn chặn nguy cơ mất an ninh an toàn mạng.

Tình trạng mất an ninh, an toàn mạng đã và đang là nguy cơ tồn tại, hiện hữu trong mọi tổ chức, doanh nghiệp và người dùng ở những cấp độ khác nhau. Việc đảm bảo an ninh, an toàn mạng nói riêng và an toàn thông tin nói chung không chỉ là nhiệm vụ của riêng cá nhân, tổ chức nào, mà là sự tin tưởng, chia sẻ và phối hợp chặt chẽ của các cơ quan chức năng nhà nước, sự chung tay góp sức của các doanh nghiệp và cá nhân trong toàn xã hội, cả trong nước và quốc tế nhằm đảm bảo cho sự phát triển ổn định của đất nước./.

Hoạt động triển khai đảm bảo an toàn trước trong và sau tết Nguyên đán Đinh

Thực hiện Công văn số 83/BTTTT-CATTT ngày 11/01/2017 của Bộ Thông tin và Truyền thông, về việc đôn đốc thực hiện các biện pháp tăng cường đảm bảo an toàn thông tin trong dịp tết Nguyên đán Đinh Dậu 2017, Công văn số 04/VNCERT-ĐPƯC của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam về việc tăng cường kiểm tra công tác bảo đảm an toàn thông tin trong dịp nghỉ lễ tết Nguyên đán Đinh Dậu 2017 và Kế hoạch số 50/STTTT-CNTT ngày 16/01/2017 của Giám đốc Sở TT&TT về việc đảm bảo an toàn thông tin mạng trong các cơ quan nhà nước trong dịp trước, trong và sau tết Nguyên đán Đinh Dậu năm 2017. Trung tâm Công nghệ thông tin và Truyền thông (trung tâm) đã ban hành và triển khai thực hiện Công văn số 11/TTCNTT&TT-QTHT ngày 16/01/2017 của Giám đốc Trung tâm về việc tăng cường công tác đảm bảo an toàn thông tin trong dịp nghỉ lễ tết Nguyên đán Đinh Dậu 2017 đến các Sở Ban, ngành cấp tỉnh; UBND các huyện, thị xã, thành phố trên địa bàn tỉnh.

Nhận thức được trách nhiệm, vai trò và nhiệm vụ quan trọng trong việc tăng cường hướng dẫn, triển khai các giải pháp đảm bảo an toàn thông tin cho hệ thống thông tin của tỉnh; xây dựng, rà soát các phương án tấn công mạng, ứng cứu sự cố và hoạt động dự phòng trong các trường hợp hệ thống bị tấn công, cũng như sự chỉ đạo sát sao của Đảng ủy, Ban Giám đốc Sở Thông tin và Truyền thông, Ban Giám đốc Trung tâm CNTT&TT đã chỉ đạo các phòng chuyên môn nghiên cứu, triển khai đồng bộ một số giải pháp sau:

Quán triệt đến toàn thể đội ngũ cán bộ, viên chức, người lao động của Trung tâm nâng cao ý thức trách nhiệm, chủ động và cảnh giác đối với những nguy cơ mất an toàn thông tin trong việc quản lý, trao đổi, cung cấp và sử dụng thông tin trên môi trường mạng. Nâng cao ý thức trong việc quản lý và sử dụng các phần mềm Thư điện tử công vụ, phần mềm Quản lý văn bản đi đến và hồ sơ công việc... nhất là việc quản lý thông tin tài khoản cá nhân.

Tăng cường phân công cán bộ tham gia trực tại Trung tâm

thông tin trong thời gian Dậu 2017

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

An ninh mạng và An toàn dữ liệu để đảm bảo các hệ thống cơ sở dữ liệu và phần mềm dùng chung phục vụ công tác quản lý điều hành phần lớn của các cơ quan, đơn vị trên địa bàn tỉnh được thông suốt, ổn định. Trong mỗi ca trực lãnh đạo Trung tâm đã chỉ đạo tăng từ 1 lên 2 cán bộ để đảm bảo thực hiện xử lý các sự cố khi có yêu cầu.

Cán bộ trực vận hành Trung tâm ANM&ATDL.

Phân công cán bộ kỹ thuật ngoài việc thực hiện sao lưu cơ sở dữ liệu, mã nguồn website, phần mềm chuyên ngành theo quy định định kỳ của Trung tâm, còn thực hiện phương án sao lưu đột xuất, để có phương án khắc phục khi có sự cố xảy ra, đây cũng là cơ sở để rà soát phát hiện nguyên nhân gây ra sự cố.

Thực hiện rà soát các mã nguồn, tài khoản quản trị của các hệ thống thông tin, từ đó phòng tránh việc tin tặc có thể tạo thêm tài khoản để sử dụng cho lần đăng nhập chính thống sau, tiến hành thay đổi tất cả mật khẩu của phần mềm hệ thống đang hoạt động; đồng thời đối với các máy chủ, cán bộ kỹ thuật tiến hành cập nhật các bản vá bảo mật và quét mã độc trên toàn hệ thống.

Chủ động phân công đầu mối phối hợp với Trung tâm ứng cứu khẩn cấp máy tính Việt Nam, Cục An toàn thông tin và các cơ quan đơn vị trên địa bàn tỉnh để cảnh báo, ứng cứu sự cố kịp thời.

Ngoài ra, Trung tâm tiến hành ra soát, kiểm tra các trang thiết bị thiết yếu để đảm bảo hỗ trợ hệ thống hoạt động tốt nhất như hệ thống lưu điện, xăng dầu dự trữ, hệ thống giám sát camera cửa ra vào phòng máy chủ Trung tâm Dữ liệu và An ninh mạng, các trang thiết bị phòng chống cháy nổ được trang bị đủ, luôn trong trạng thái sẵn sàng.

Nhờ áp dụng triệt để biện pháp về tăng cường nhân lực kịp thời tiếp nhận, xử lý các sự cố, thực hiện nghiêm các quy trình rà soát, sao lưu mang tính kỹ thuật, trong thời gian trước, trong và sau tết Nguyên đán Đinh Dậu 2017 tại Trung tâm An ninh mạng và An toàn dữ liệu của tỉnh, các dịch vụ trang/cổng thông tin điện tử, phần mềm, cơ sở dữ liệu chuyên ngành đang cung cấp tại trung tâm hoạt động đảm bảo, ổn định 24/24, không xảy ra hiện tượng mất an toàn an ninh thông tin. Cán bộ thường xuyên theo dõi và ghi nhận kịp thời các thông tin đăng tải trên mạng internet, không phát hiện có nội dung kích động và thông tin sai lệch nhằm ảnh hưởng đến trật tự, an toàn thông tin trên địa bàn tỉnh. Qua đó phục vụ tốt công tác lãnh đạo, chỉ đạo, điều hành trước, trong và sau tết Nguyên đán, của các cấp, ngành, chính quyền và truy cập thông tin của nhân dân trong tỉnh./.

Tổ chức ôn tập, bồi dưỡng, tổ chức thi và cấp chứng chỉ ứng dụng CNTT theo chuẩn kỹ năng sử dụng công nghệ thông tin Thông tư số 03/2014/TT-BTTTT

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

Việc tồn tại quá nhiều chương trình đào tạo, giáo trình, chứng chỉ tin học với chất lượng ngoài tầm kiểm soát và thiếu tính ứng dụng thực tế ở các đơn vị đào tạo, các ngành nghề KT-XH đã khiến cho người sử dụng CNTT chưa đáp ứng được nhu cầu của các đơn vị tuyển dụng, sử dụng lao động. Nhiều cơ sở đào tạo chưa đảm bảo về cơ sở vật chất, trang thiết bị, nhân lực, trình độ vẫn tổ chức đào tạo và cấp chứng chỉ. Trước thực tế như vậy Bộ Thông tin và Truyền thông (Bộ TTTT) đã ban hành Thông tư 03/2014/TT-BTTTT quy định về chuẩn kỹ năng sử dụng CNTT, có hiệu lực thi hành từ ngày 28/4/2014. Đây được xem là căn cứ để các đơn vị sử dụng lao động tuyển dụng và sử dụng nhân lực về góc độ sử dụng CNTT. Đây là văn bản làm căn cứ thống nhất về yêu cầu năng lực về tin học trong tiêu chuẩn chức danh, nghề nghiệp của cán bộ, công chức, viên chức, đồng thời để áp dụng giảng dạy trong hệ thống giáo dục quốc dân, là căn cứ để xây dựng tiêu chí trong kiểm tra, thi và đánh giá ở từng cấp học, trình độ đào tạo.

Từ đó ngày 21/6/2016, Bộ Giáo dục và Đào tạo - Bộ Thông tin và Truyền thông đã ban hành thông tư liên tịch số 17/TTLT-BGDĐT-BTTTT quy định về việc tổ chức thi và cấp chứng chỉ ứng dụng CNTT, như vậy chỉ những đơn vị đảm bảo đủ điều kiện được quy định trong (Thông tư 17) thì mới được thẩm định và cấp phép cho tổ chức đào tạo, thi và cấp chứng chỉ.

Với chức năng, nhiệm vụ được Chủ tịch UBND tỉnh giao, Trung tâm CNTT&TT Thanh Hóa đã chuẩn bị đầy đủ các điều kiện về cơ sở vật chất, trang thiết bị, nhân lực, ngân hàng câu hỏi thi

Tổ chức lớp đào tạo, tập huấn tại huyện Quan Sơn.

trắc nghiệm, phần mềm thi trắc nghiệm đảm bảo theo đúng quy định tại Thông tư liên tịch số 17/TTLT-BGDĐT-BTTTT, ngày 21/6/2016 giữa Bộ Giáo dục và Đào tạo - Bộ thông tin và Truyền thông. Đến nay Trung tâm CNTT&TT Thanh Hóa là đơn vị sự nghiệp đầu tiên trên địa bàn tỉnh Thanh Hóa được cấp phép đủ điều kiện bồi dưỡng ôn tập, tổ chức thi và cấp chứng chỉ ứng dụng CNTT theo chuẩn kỹ năng sử dụng công nghệ thông tin Thông tư số 03/2014/TT-BTTTT.

Là đơn vị sự nghiệp CNTT&TT của tỉnh. Trung tâm tích cực tuyên truyền, quảng bá, ban hành các quy chế, quy định và chuẩn bị các điều kiện về cơ sở vật chất, phương án theo phương châm đảm bảo chất lượng, hiệu quả trong công tác tổ chức ôn tập, bồi dưỡng, tổ chức thi và cấp chứng chỉ ứng dụng CNTT theo đúng quy định chuẩn kỹ năng sử dụng công nghệ thông tin tại Thông tư số 03/2014/TT-BTTTT.

Hàng tuần, Trung tâm nhận hồ sơ tuyển sinh và tổ chức ôn tập vào các buổi tối hoặc thứ 7, chủ nhật; hoặc theo lịch đăng ký của các cơ quan đơn vị và tổ chức thi vào các ngày thứ 7 và chủ nhật hàng tuần. Để tạo điều kiện thuận lợi cho các học viên tham gia các khóa học, ôn tập và thi sát hạch, Trung tâm sẽ lựa chọn địa điểm để tổ chức ôn tập, thi phù hợp nhất.

Chuẩn kỹ năng sử dụng công nghệ thông tin được áp dụng để đánh giá về trình độ, kỹ năng sử dụng CNTT của các cán bộ, công chức, viên chức, người lao động nhằm phục vụ cho công tác tuyển dụng, bố trí công tác, chuyển ngạch, nâng bậc và được quy định chuẩn kỹ năng, tiêu chuẩn chức danh nghề nghiệp đối với các cấp trong ngành giáo dục, ngành y tế, ngành khoa học và công nghệ, Công an và các hoạt động khác của các ngành có liên quan.

Mọi chi tiết xin liên hệ: Phòng Đào tạo & Dịch vụ - Trung tâm CNTT&TT Thanh Hoá - Địa chỉ: Số 73 Hàng Than, P. Lam Sơn - Tp Thanh Hoá - Điện thoại: 02373.718.698 - 0949253678 hoặc truy cập vào địa chỉ Website:ict.thanhhoa.gov.vn.

Các cơ quan, đơn vị cử cán bộ đề nghị gửi danh sách đăng ký về hòm thư: tuyensinhdao taott03@gmail.comtrước 03 ngày căn cứ theo lịch bồi dưỡng kiến thức hàng tháng./.

Trích dẫn các văn bản quy định của các lĩnh vực về tiêu chuẩn chức danh nghề nghiệp yêu cầu phải có chứng chỉ ứng dụng CNTT quy định tại TT 03/TT-BTTTT

- Thông tư liên tịch số 36/2014/TTLT-BGDĐT- BNV quy định mã số, tiêu chuẩn chức danh nghề nghiệp viên chức giảng dạy trong các trường đại học công lập;

- Thông tư liên tịch số 20, 21, 22, 23/2015/TTLT-BGDĐT-BNV ngày 16/9/2015 giữa Bộ Nội vụ và Bộ Giáo dục và Đào tạo quy định mã số, tiêu chuẩn chức danh nghề nghiệp giáo viên các cấp mầm non; tiểu học công lập; trung học cơ sở công lập; trung học phổ thông công lập;

- Thông tư số 11/2014/TT-BNV, ngày 09/10/2014 của Bộ Nội vụ Quy định chức danh, mã ngạch và tiêu chuẩn nghiệp vụ chuyên môn các ngạch công chức hành chính;

- Thông tư liên tịch số 10/2015/TTLT-BYT-BNV, ngày 27/5/2015 giữa Bộ Nội vụvà Bộ Y tế về việc quy định mã số, tiêu chuẩn chức danh nghề nghiệp bác sĩ, bác sĩ y học dự phòng, y sĩ; Thông tư liên tịch số 27/2015/TTLT-BYT-BNV, ngày 07/10/2015 về việc quy định mã số, tiêu chuẩn chức danh nghề nghiệp dược.

- Thông tư liên tịch số 24/2014/TTLT-BKHCN-BNV, ngày 01/10/2014 giữa Bộ Nội vụ và Bộ Khoa học và Công nghệ về việc Quy định mã số và tiêu chuẩn chức danh nghề nghiệp viên chức chuyên ngành khoa học và công nghệ.

- Thông tư số 18/2016/TT-BCA, ngày 01/6/2016 của Bộ trưởng Bộ Công an ban hành (Thông tư 18) quy định tiêu chuẩn chức danh cán bộ lãnh đạo, chỉ huy trong Công an nhân dân.

- Văn bản lĩnh vực lao động, lưu trữ, Nông nghiệp, Tài nguyên môi trường, Văn hóa, thể thao và du lịch...

CÁC BƯỚC THIẾT LẬP MÁY TÍNH MỚI AN TOÀN

• Các nguy cơ mất an toàn thông tin có thể lập tức ảnh hưởng đến chúng ta ngay sau khi sử dụng máy tính vừa mua hoặc vừa cài đặt lại.

• Do đó cần có một số lưu ý để thiết lập máy tính mới an toàn chống lại các nguy cơ bị tấn công như sau:

Bước 1: Tạo các mật khẩu mạnh.

Ngay trong các bước đầu tiên của việc thiết lập cấu hình máy tính. Các tài khoản của người sử dụng cần được tạo ra với mật khẩu có độ phức tạp nhất định.

Các mật khẩu dễ nhớ như "123456", "abcedf"... tuyệt đối không được sử dụng vì đây là các mật khẩu yếu rất dễ đoán.

Một mật khẩu an toàn thường bao gồm các loại ký tự sau:

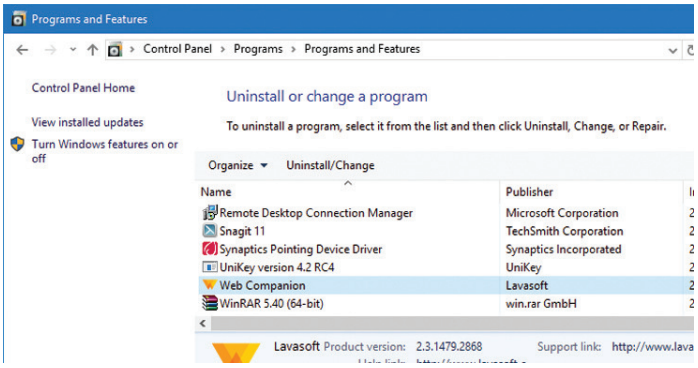
- Ký tự hoa, ký tự thường
- Ký tự chữ số
- Ký tự đặc biệt ($#%"#%)

Mật khẩu mạnh sẽ giúp bảo về máy tính trong suốt quá trình sử dụng về sau.

Bước 2: Tháo gỡ các chương trình không cần thiết.

Các máy tính mới thường được nhà sản xuất cài đặt sẵn các chương trình quảng cáo, giới thiệu hoặc bản dùng thử của các phần mềm. Các phần mềm này có thể chứa sẵn các nguy cơ mất an toàn thông tin.

Do đó, người dùng cần tháo bỏ các chương trình không cần thiết trên máy tính của mình ngay trong quá trình thiết lập ban đầu.

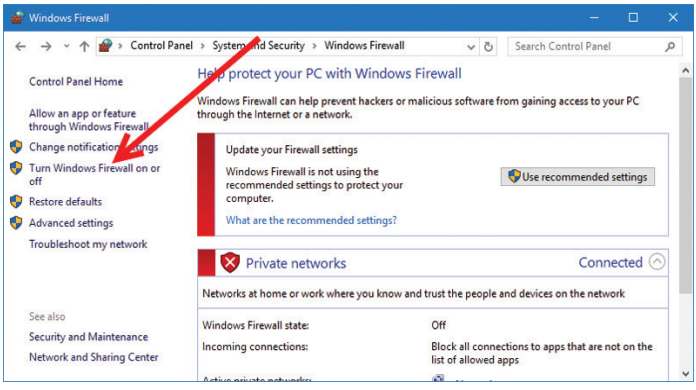


*(Sử dụng Chức năng **Program and Features** để liệt kê các phần mềm đã được cài sẵn trong các máy mới)*

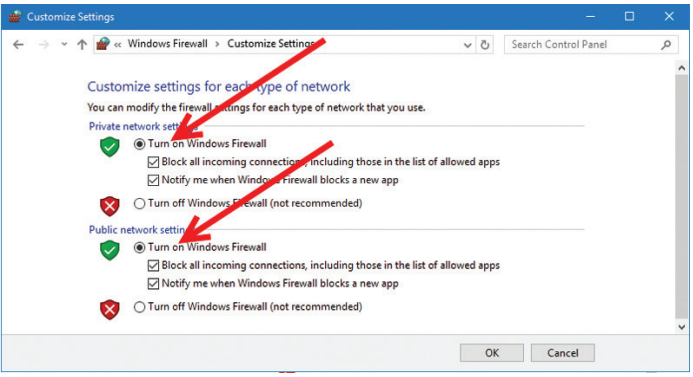
Bước 3: Kích hoạt chức năng tường lửa bảo vệ cá nhân trên máy tính.

Các hệ điều hành hiện nay hầu hết đều tích hợp các tường lửa nhằm bảo vệ người sử dụng khỏi tấn công cơ bản. Hãy kích hoạt phần mềm tường lửa trước khi kết nối đến bất kỳ mạng máy tính nào (Internet/Wifi/LAN...).

Trên hệ điều hành Windows, có thể kích hoạt tường lửa bằng cách truy cập chức năng Firewall trong Control Panel:



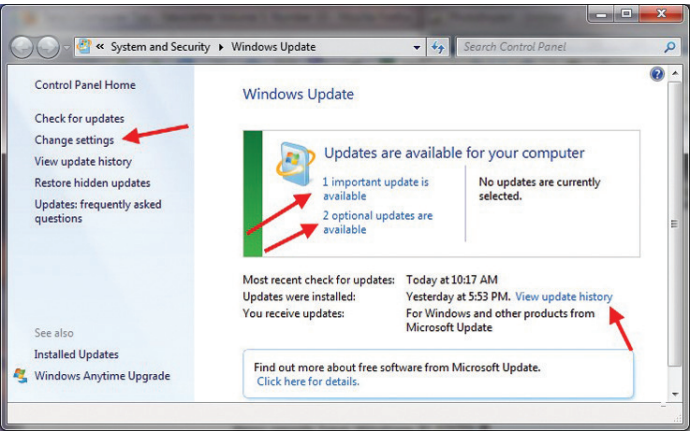
Tiếp tục lựa chọn ***"Turn Windows Firewall on or off"*** để thực hiện việc kích hoạt



Tiếp tục chọn các lựa chọn ***"Turn on..."*** và tùy chọn bên dưới để kích hoạt.

Bước 4: Nâng cấp các phần mềm và hệ điều hành Windows.

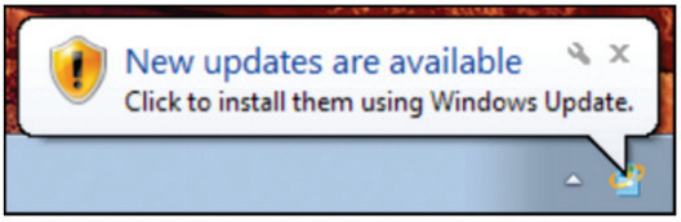
Hệ điều hành của máy tính lúc vừa cài đặt có thể là phiên bản cũ chưa được vá các lỗi bảo mật. Do đó, người sử dụng cần thiết lập chế độ tự động nâng cấp và thực hiện nâng cấp cho hệ điều hành và các phần mềm khác.



Trong phần ***Windows update*** của Control Panel, sử dụng tùy chọn ***"change settings"*** để thiết lập việc tự động cập nhật.

Trong các tùy chọn về nâng cấp, người sử dụng có thể tùy chọn theo nhu cầu của mình. Tuy nhiên, có thể tùy chọn việc tự quyết định thực hiện nâng cấp theo yêu cầu của người sử dụng để đảm bảo không bị gián đoạn công việc do quá trình nâng cấp.

Sau đó, sẽ thông báo đến người sử dụng khi có bản cập nhật mới. Người sử dụng sẽ click vào thông báo để thực hiện việc cập nhật



Bước 5: Cài đặt phần mềm diệt virus.

Phần mềm diệt virus là lớp lá chắn quan trọng bảo vệ người sử dụng khỏi các mã độc và virus. Do đó, cần có chương trình diệt virus để bảo vệ người dùng ngay trong các hoạt động đầu tiên của người sử dụng trên máy tính.

Trên thị trường có nhiều hãng cung cấp giải pháp diệt virus, người sử dụng có thể lựa chọn giải pháp miễn phí hoặc các bản thương mại.

Ngoài ra người dùng có thể cân nhắc sử dụng các phần mềm diệt virus của Việt Nam sản xuất như BKAV hay CMC

Các phần mềm này đều có các phiên bản miễn phí với chức năng hạn chế cho người sử dụng./.

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

BẢO VỆ THÔNG TIN CÁ NHÂN
ĐƯỢC PHÁP LUẬT QUY ĐỊNH TẠI LUẬT AN TOÀN THÔNG TIN MẠNG

NGUYỄN XUÂN ĐỒNG
Phòng quản lý CNTT, Sở TT&TT

Thông tin trên mạng đã trở thành tài sản có giá trị đặc biệt của mỗi cá nhân, tổ chức và cả quốc gia. Nhiều cá nhân, tổ chức có giá trị tài sản trên mạng còn lớn hơn nhiều so với các tài sản hữu hình khác. Các doanh nghiệp sẽ không thể tồn tại và phát triển nếu các thông tin hoặc hệ thống thông tin bị đánh cắp hay bị phá hoại. Các cơ quan nhà nước thì không thể phục vụ người dân, doanh nghiệp nhanh chóng và thuận tiện nếu các website hoạt động không bình thường. Cải cách hành chính, chính phủ điện tử, thương mại điện tử và hàng loạt chương trình lớn khác sẽ không thể thực hiện được nếu an toàn thông tin không được đảm bảo.

Thời gian vừa qua, nhiều website của các doanh nghiệp và cơ quan nhà nước bị tấn công, phá hoại, trong đó có một số hệ thống thương mại điện tử, một số tờ báo điện tử lớn có hàng triệu người đang sử dụng dịch vụ. Tin tặc không loại trừ một quốc gia, một tổ chức hay cá nhân nào, ngay cả nước Mỹ, một trong những nước phát triển nhất trên thế giới về CNTT, cũng gặp không ít rắc rối.

Bên cạnh đó, hằng ngày chúng ta vẫn sử dụng các giao dịch trực tuyến, thương mại điện tử, ngân hàng điện tử... Khi sử dụng các dịch vụ trên mạng này, người sử dụng sẽ phải kê khai các thông tin cá nhân như: Tên, ngày sinh, địa chỉ liên hệ, số điện thoại hay số CMND. Những thông tin này gắn với việc xác định rõ ràng danh tính, nhân thân của một con người cụ thể, nhằm phân biệt người này với người khác. Ngày càng có nhiều thông tin cá nhân của người sử dụng được lưu trữ ở trên mạng. Nếu những thông tin này không được bảo vệ một cách thích hợp, kẻ xấu có thể thu thập, khai thác trái phép. Đây là một trong những nguyên nhân gây ra hiện tượng phát tán thông tin cá nhân trên mạng, gây bức xúc dư luận trong những năm gần đây.

Luật An toàn thông tin mạng đã có hiệu lực thi hành từ ngày 01/7/2016, trong đó quy định rõ trách nhiệm của chính người dùng và trách nhiệm của cơ quan quản lý nhà nước trong việc bảo vệ thông tin cá nhân trên mạng.

Trước hết, nguyên tắc chung là mỗi người phải có trách nhiệm *"tự bảo vệ thông tin cá nhân và tự chịu trách nhiệm khi cung cấp những thông tin đó trên mạng"*, vì vậy, người sử dụng phải tự ý thức bảo vệ thông tin cá nhân của mình, cũng như thận trọng khi cung cấp thông tin cá nhân của mình lên mạng Internet; cơ quan quản lý nhà nước có trách nhiệm thiết lập kênh thông tin trực tuyến để tiếp nhận kiến nghị, xử lý và tổ chức thanh tra, kiểm tra các phản ánh của tổ chức, cá nhân liên quan đến các vấn đề bảo vệ thông tin cá nhân trên mạng.

Tại Điều 17, Luật An toàn thông tin mạng quy định rõ tổ chức, cá nhân xử lý thông tin cá nhân có trách nhiệm thu thập và sử dụng thông tin cá nhân sau khi có sự đồng ý của chủ thể thông tin cá nhân về phạm vi và mục đích của việc thu thập thông tin đó, trường hợp sử dụng vào mục đích khác mục đích ban đầu phải có sự đồng ý của chủ thể thông tin cá nhân; không được cung cấp, chia sẻ, phát tán thông tin cá nhân đã thu thập cho bên thứ ba mà chưa có sự đồng ý của chủ thể thông tin cá nhân hoặc theo yêu cầu của cơ quan nhà nước có thẩm quyền; cung cấp thông tin cá nhân theo yêu cầu của chủ thể thông tin cá nhân.

Về chế tài xử phạt đối với các hành vi phát tán, chia sẻ thông tin cá nhân, tùy theo mức độ, hành vi thì tổ chức, cá nhân vi phạm sẽ bị xử lý vi phạm hành chính hoặc xử lý trách nhiệm hình sự theo các quy định pháp luật hiện hành.

Về việc cập nhật, sửa đổi và hủy bỏ thông tin cá nhân, Luật đã quy định rõ, chủ thể thông tin cá nhân có quyền yêu cầu tổ chức, cá nhân xử lý thông tin cá nhân cập nhật, sửa đổi, hủy bỏ thông tin cá nhân của mình mà tổ chức, cá nhân đó đã thu thập, lưu trữ, hoặc ngừng cung cấp thông tin cá nhân của mình cho bên thứ ba.

Ngay khi nhận được yêu cầu của chủ thể thông tin cá nhân về việc cập nhật, sửa đổi, hủy bỏ thông tin cá nhân hoặc đề nghị ngừng cung cấp thông tin cá nhân cho bên thứ ba, tổ chức, cá nhân xử lý thông tin cá nhân có trách nhiệm thực hiện yêu cầu và thông báo lại cho chủ thể thông tin cá nhân hoặc cung cấp cho chủ thể thông tin cá nhân quyền tiếp cận để tự cập nhật, sửa đổi, hủy bỏ thông tin cá nhân của mình do tổ chức, cá nhân xử lý thông tin cá nhân đang lưu trữ. Áp dụng các biện pháp phù hợp để bảo vệ thông tin cá nhân, thông báo lại cho chủ thể thông tin cá nhân đó trong trường hợp chưa thực hiện được yêu cầu do yếu tố kỹ thuật hoặc yếu tố khác.

Luật An toàn thông tin mạng cũng quy định tổ chức, cá nhân xử lý thông tin cá nhân phải hủy bỏ thông tin cá nhân đã được lưu trữ khi đã hoàn thành mục đích sử dụng hoặc hết thời hạn lưu trữ và thông báo cho chủ thể thông tin cá nhân biết, trừ trường hợp pháp luật có quy định khác.

Luật An toàn thông tin mạng kết hợp cùng Bộ luật Dân sự, Luật Bảo vệ người tiêu dùng và các văn bản pháp luật chuyên ngành khác như Luật Viễn thông, Luật Công nghệ thông tin, Luật Giao dịch điện tử... sẽ tạo thành hệ thống pháp luật đồng bộ, đầy đủ cho công tác bảo vệ thông tin cá nhân của người sử dụng trong kỷ nguyên Internet hiện nay, góp phần thúc đẩy hơn nữa hoạt động giao dịch điện tử phục vụ phát triển KT-XH./.