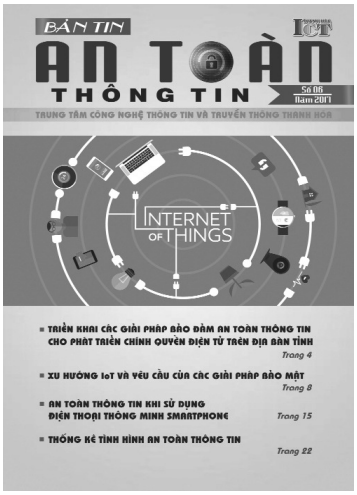
BẢN TIN
AN TOÀN THÔNG TIN
TRUNG TÂM CÔNG NGHỆ THÔNG TIN & TRUYỀN THÔNG THANH HÓA

Số 06
tháng 12/2017



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

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

THIẾT KẾ
Chung Nguyễn

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

In 500 cuốn, khổ 19x27cm
Tại Công ty TNHH In&TBGD Thanh Huệ
In xong và nộp lưu chiểu tháng 12/2017

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".

Triển khai các giải pháp bảo đảm an toàn thông tin cho phát triển chính quyền điện tử trên địa bàn tỉnh

ThS. TRẦN DUY BÌNH
Giám đốc Sở Thông tin và Truyền thông

Trong bối cảnh công nghệ thông tin phát triển rộng khắp như hiện nay thì cũng tiềm ẩn nguy cơ về mất an toàn thông tin và những mối đe dọa nghiêm trọng đến chủ quyền không gian mạng, các vấn đề về mất an toàn thông tin (ATTT), vấn nạn thư rác, tấn công xâm nhập hệ thống công nghệ thông tin (CNTT) đang gia tăng ở mức báo động. Các tổ chức tin tặc đã thực hiện nhiều cuộc tấn công với hình thức ngày càng tinh vi vào các cơ quan chính phủ của nhiều quốc gia và gây ra hậu quả rất nghiêm trọng. Hoạt động tin tặc ngày càng có quy mô và có tổ chức hơn. Theo các chuyên gia, tình hình an toàn, an ninh thông tin mạng tại Việt Nam vẫn diễn biến theo chiều hướng phức tạp. Kết quả theo dõi, giám sát tình hình an toàn thông tin mạng của các cơ quan thuộc khối an toàn thông tin của Bộ Thông tin và Truyền thông trong năm 2017 ghi nhận khoảng 14.000 cuộc tấn công mạng vào các hệ thống thông tin của Việt Nam, bao gồm gần 3.000 cuộc tấn công lừa đảo, 6.500 tấn công cài phần mềm độc hại và 4.500 tấn công thay đổi giao diện. Bởi vậy, tại Việt Nam, việc đảm bảo ATTT cho Chính phủ điện tử được đặt ra rất cấp bách.

Thời gian qua, được sự quan tâm của Bộ

Thông tin và Truyền thông và các Bộ, ngành, cơ quan Trung ương, hoạt động ứng dụng và phát triển CNTT, xây dựng chính quyền điện tử trên địa bàn tỉnh Thanh Hóa có nhiều chuyển biến và đạt được kết quả quan trọng. Nhận thức được vai trò to lớn của CNTT đối với sự phát triển kinh tế - xã hội, trong hơn 10 năm qua, triển khai Nghị Quyết số 03-NQ/TU ngày 17/4/2007 của Ban Thường vụ Tỉnh ủy; Thanh hóa đã ban hành nhiều chủ trương, chính sách, kế hoạch để triển khai thực hiện tập trung đẩy mạnh ứng dụng và phát triển CNTT, xây dựng chính quyền điện tử trên địa bàn tỉnh Thanh Hóa. Đó là việc đầu tư trang bị cơ sở hạ tầng CNTT trong các cơ quan nhà nước đã cơ bản đáp ứng được nhu cầu để ứng dụng CNTT; việc ứng dụng và phát triển CNTT phục vụ công tác chỉ đạo điều hành, cung cấp các dịch vụ công trực tuyến đến các tổ chức, doanh nghiệp, người dân được chú trọng thực hiện, đã góp phần đẩy mạnh cải cách hành chính, cải thiện môi trường đầu tư kinh doanh, năng lực cạnh tranh cấp tỉnh, chỉ số hiệu quả quản trị và hành chính công, chỉ số hội nhập kinh tế quốc tế tăng cao và nằm trong nhóm các tỉnh dẫn đầu của cả nước.

Tuy nhiên, sau hơn 10 năm ứng dụng và phát triển CNTT, xây dựng chính quyền điện tử vẫn còn tồn tại những khó khăn bất cập như: Hạ tầng CNTT-TT chưa đồng bộ; Các ứng dụng CNTT, cơ sở dữ liệu dùng chung còn ít; Nguồn nhân lực CNTT còn mỏng, trình độ chưa cao phải tiếp tục được tập huấn, bồi dưỡng; Công tác đảm bảo an toàn thông tin mạng còn nhiều khó khăn; Chưa có điều kiện triển khai các hệ thống thông minh trên các lĩnh vực để tiến đến hình thành và phát triển đô thị thông minh.

Thực hiện Nghị quyết số 36-NQ/TW ngày 01/7/2014 của Bộ Chính trị về "Đẩy mạnh ứng dụng, phát triển CNTT đáp ứng yêu cầu phát triển bền vững và hội nhập quốc tế", Nghị quyết số 36a/NQ-CP ngày 14/10/2015 của Chính phủ về Chính phủ điện tử, đặc biệt là trong xu thế cuộc Cách mạng công nghiệp 4.0 đang phát triển mạnh mẽ, Sở Thông tin và Truyền thông được giao chủ trì, đã tham mưu cho Ban Thường vụ Tỉnh ủy và UBND tỉnh Thanh Hóa phê duyệt Đề án "Xây dựng chính quyền điện tử và phát triển các dịch vụ thành phố thông minh tỉnh Thanh Hóa giai đoạn 2017 - 2020", tham mưu UBND tỉnh Ban hành Khung kiến trúc chính quyền điện tử tỉnh Thanh Hóa giai đoạn 2017 - 2020 và định hướng đến 2030.

Với mục tiêu đẩy mạnh việc ứng dụng và phát triển CNTT trong các cơ quan nhà nước xây dựng Chính quyền điện tử theo Nghị quyết 36a của Chính phủ phù hợp Khung Kiến trúc Chính phủ điện tử Việt Nam nhằm ứng dụng CNTT, tự động hóa và trí tuệ nhân tạo nâng cao năng lực chỉ đạo, điều hành, đẩy mạnh cải cách hành chính phục vụ các doanh nghiệp và người dân ngày càng hiệu quả tốt hơn; góp phần cải thiện môi trường đầu tư kinh doanh và nâng cao chỉ số cạnh tranh cấp tỉnh; Lựa chọn triển khai một số lĩnh vực thí điểm phát triển các dịch vụ thành phố thông minh tỉnh Thanh Hóa giai đoạn 2017 - 2020, để tạo điều kiện nâng cao khả năng tiếp cận với cuộc Cách mạng công nghiệp 4.0. Theo đó, Đề án có các mục tiêu như sau:

Một là, xây dựng Chính quyền điện tử theo Nghị quyết 36a của Chính phủ và Khung Kiến trúc Chính phủ điện tử Việt Nam nhằm nâng cao năng lực chỉ đạo, điều hành, đẩy mạnh cải cách hành chính phục vụ các doanh nghiệp và người dân ngày càng hiệu quả; góp phần cải thiện môi trường đầu tư kinh doanh và nâng cao chỉ số cạnh tranh cấp tỉnh.

Hai là, xây dựng Trung tâm đào tạo, chuyển giao công nghệ nhằm đào tạo và phát triển nguồn nhân lực quản lý và ứng dụng CNTT của tỉnh; đồng thời tạo môi trường thuận lợi để khởi tạo doanh nghiệp công nghiệp phần mềm, nội dung số và hỗ trợ các doanh nghiệp trên địa bàn tỉnh ứng dụng CNTT trong hoạt động sản xuất, kinh doanh phục vụ hội nhập và phát triển. Đặc biệt đây cũng là nơi để bồi dưỡng, cập nhật trình độ cùng với các trường Đại học của tỉnh và khu vực để đáp ứng nguồn nhân lực có đủ trình độ để tiếp cận với cuộc Cách mạng công nghiệp 4.0

Ba là, ứng dụng và phát triển các dịch vụ thành phố thông minh trên cơ sở ứng dụng CNTT, tự động hóa và trí tuệ nhân tạo trong một số lĩnh vực nhằm nâng cao chất lượng công tác quản lý, các hoạt động chuyên môn, nghiệp vụ của các ngành, các cấp, cung cấp các dịch vụ chất

lượng cao phục vụ nhu cầu và nâng cao chất lượng cuộc sống và tạo ra môi trường sống thân thiện, tiện lợi nhất cho người dân, góp phần cải thiện môi trường đầu tư kinh doanh và hội nhập quốc tế của tỉnh.

Do đó, để bảo đảm tuyệt đối an toàn cho hạ tầng và ứng dụng CNTT trong việc triển khai thành công Đề án nói chung và xây dựng Chính quyền điện tử trên địa bàn tỉnh nói riêng. Mặt khác 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 tuyên truyền, phổ biến:

Tổ chức 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 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.

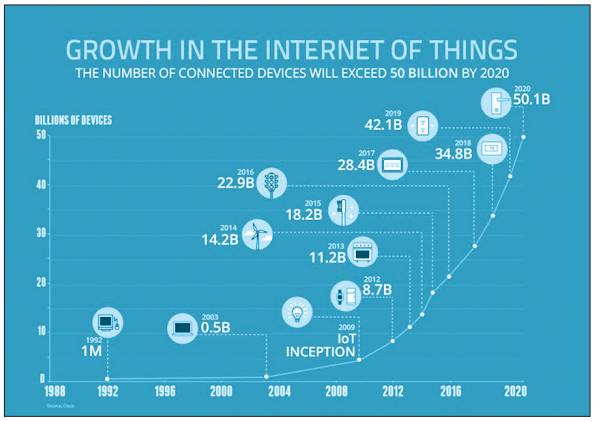
5. Về đẩy mạnh phối hợp trong công tác đảm bảo an toàn, an ninh thông tin:

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 an toàn an ninh thông tin cũng như khắc phục sự cố về an toàn thông tin mạng./.

Xu hướng IoT và yêu cầu của các giải pháp bảo mật

NGUYỄN TIẾN QUỲNH
Phó Giám đốc Học viện NetPro

Dự kiến, cuộc cách mạng Internet of Things (IoT - Internet của Vạn vật) sẽ chứng kiến gần 50 tỷ thiết bị được kết nối với Internet vào năm 2020 - tương đương với 6 thiết bị cho mỗi người trên hành tinh.



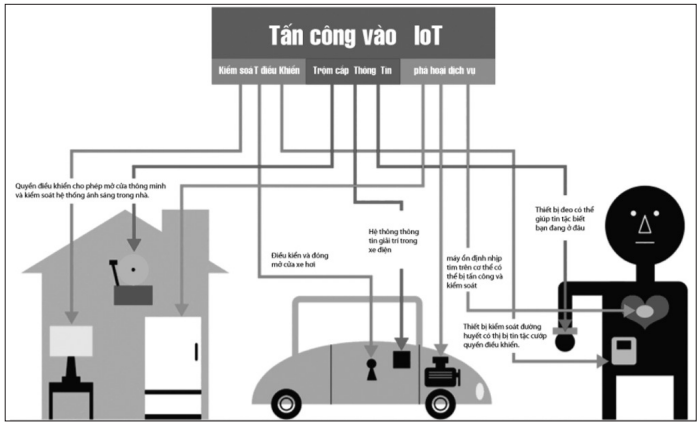
Thế giới đang ở trên đỉnh của một cuộc cách mạng chuyển đổi công nghệ, mà như lời của tạp chí công nghệ WIRED thì: "các vật dụng nhàm chán nhất trong cuộc sống của chúng ta có thể tự nói chuyện với nhau qua kết nối không dây, thực hiện nhiệm vụ theo mệnh lệnh, cung cấp dữ liệu cho chúng ta theo cách chưa từng có trước đây".

Trong thời gian vừa qua, thế giới đã chứng kiến những cuộc tấn công mạng dưới hình thức mới - tấn công từ các thiết bị IoT với quy mô tác động rất lớn. Một vài vụ tấn công theo hình thức này cũng đã có mặt tại Việt Nam:

- Cuối tháng 9/2016, một công ty lưu trữ của Pháp đã nhận hai cuộc tấn công đồng thời với băng thông đạt gần 1Tbps, một trong hai cuộc tấn công đạt đỉnh điểm là 799 Gbps. Vụ tấn công này được tạo thành từ 145.607 máy quay video kỹ thuật số và camera IP đã bị chiếm quyền.

- Ngày 21/10, thông qua hàng trăm ngàn thiết bị IoT như camera, thiết bị giám sát em bé và router gia đình, tin tặc đã lây nhiễm mã độc cho các thiết bị này, làm "ngập lụt" những trang web dịch vụ của Mỹ bằng lưu lượng giao tiếp khổng lồ. Vụ tấn công đã khiến một nửa dân số Mỹ không truy cập được internet trong nhiều giờ.

- Tại Việt Nam, VNPT Net - đơn vị quản lý vận hành toàn bộ mạng lưới của VNPT cho biết, trong quá trình vận hành khai thác mạng lưới, đơn vị này đã phát hiện những cuộc tấn công DDoS với hình thức tương tự - sử dụng các thiết bị IoT để tấn công. Trung tâm An ninh mạngcủa VNPT Net đã tìm ra được danh sách gần 11.000 khách hàng của VNPT có khả năng bị nhiễm mã độc và tham gia các mạng botnet này.



Thách thức mới cho bảo mật trong thời đại IoT

Internet of Thing tạo ra các thách thức mới trong vấn đề bảo mật vì các lý do sau:

Đầu tiên, ở khía cạnh trung tâm của Internet, các sản phẩm và dịch vụ thường xuyên truyền lượng lớn thông tin.

Thứ hai, số lượng thiết bị IoT kết nối vào internet là rất lớn, đến hàng tỷ, hàng chục tỷ thiết bị.

Thứ ba, lỗ hổng bảo mật trong các sản phẩm thông minh hiện nay rất nhiều, mở ra một cơ hội lớn cho tin tặc xây dựng hệ thống botnet và các

dạng tội phạm mạng theo đó nảy nở rất nhanh.

Thứ tư, trong thời đại IoT không thể xác định rõ phạm vi thiết bị cần bảo vệ khỏi các cuộc tấn công.

Cuối cùng, phải đảm bảo duy trì sự riêng tư trong khi trao đổi chia sẻ dữ liệu với thiết bị của khách hàng là cá nhân hay với đối tác.

Bảo mật cho các thiết bị IoT là rất khó khăn vì những lý do về kỹ thuật, công nghệ và thậm chí cả nền văn hóa. Đối với người dùng thông thường, đã là rất khó để khiến họ cập nhật những bản vá mới nhất trên máy tính xách tay, điện thoại thông minh. Ngày nay trong một thế giới thiết bị nào cũng có kết nối Internet, thiết bị nào cũng có thể có những lỗ hổng bảo mật, khi nhà sản xuất muốn nâng cấp firmware hay cài bản vá cho những thiết bị này sẽ rất phiền phức. Do đó, không có gì là ngạc nhiên khi bảo mật trong kỷ nguyên IoT đang trở thành đề tài nóng trên mọi diễn đàn lớn nhỏ trên thế giới. Tốc độ ứng dụng các thiết bị IoT càng cao thì khả năng xảy ra rủi ro về bảo mật càng lớn. Theo dự báo của hãng Gartner, thế giới sẽ chi 547 triệu đô la cho việc bảo mật IoT trong năm 2018, tăng gần 200% so với khoản chi của năm 2015. Đến năm 2020, hơn 25% các vụ tấn công sẽ liên quan đến IoT. Đặc biệt, riêng từ năm 2020 trở đi, thị trường bảo mật IoT sẽ tăng với tốc độ chóng mặt.

Giải pháp bảo mật cho các đơn vị thời IoT

Trong thời đại của Internet of Things, một giải pháp an ninh đáng tin cậy phải áp dụng một cách tiếp cận mới về cơ bản, trong đó tập trung vào bốn yếu tố trung tâm như trong danh sách dưới đây:

Yếu tố #1: Đảm bảo an ninh của thiết bị hoạt động trong Mạng.

Để đảm bảo an ninh cho các thiết bị, có nghĩa phải bảo đảm rằng chỉ thiết bị được uỷ quyền có thể truyền hoặc nhận dữ liệu liên quan với một dịch vụ IOT.

Các thuộc tính cần thiết của an ninh cho thiết bị bao gồm:

- Xác thực mạnh (điều khiển truy cập) cho cả thiết bị mạng mới và thiết bị mạng truyền thống, đảm bảo dữ liệu thực sự bắt nguồn từ một thiết bị hợp pháp và không phải là một sự gian lận.
- Khả năng mở rộng quy mô, để đảm bảo hiệu quả và tiết kiệm chi phí cho các nhà cung cấp dịch vụ với hàng triệu thiết bị IoT.

Yếu tố #2: Bảo vệ dữ liệu với mã hóa liên tục để đảm bảo an toàn cả trong khi hoạt động và nghỉ ngơi

Nguyên tắc trung tâm trong một giải pháp bảo mật để bảo vệ các dữ liệu là mã hóa mạnh mẽ, biến dữ liệu thành một chuỗi ngẫu nhiên các con số và chữ cái (ciphertext) đó là vô nghĩa cho bất cứ ai ngoại trừ những người dùng có đúng mã (key) để mở khóa. Trong một môi trường IoT, một khối lượng lớn dữ liệu được truyền qua lại giữa hàng triệu thiết bị. Một giải pháp bảo mật dữ liệu phải sử dụng mã hóa mạnh mẽ cho cả dữ liệu đang được truyền qua lại và phần chưa được truyền. Với mã hóa, dữ liệu được chuyển đổi thành mã vô nghĩa, mà nghĩa đen có thể đi bất cứ nơi nào và được lưu trữ bất cứ nơi nào, mà không sợ bị tổn hại an ninh: Nói một các đơn giản, với mã hóa thông tin ẩn giấu ngay trước mắt.

Yếu tố #3: Cho phép quản lý cả vòng đời của các thiết bị IoT

Giải pháp bảo mật IoT cần phải có khả năng thích nghi cao, từ khi được đưa vào sử dụng. Qua thời gian, các dịch vụ IoT được bảo vệ chắc chắn sẽ được tăng cường với các tính năng mới. Do đó, một giải pháp bảo mật ngay từ đầu phải thể hiện một cơ chế thích ứng trong suốt vòng đời của một sản phẩm hoặc dịch vụ IoT.

Yếu tố #4: Triển khai các giải pháp bảo mật nhưng không ảnh hưởng tới thiết bị và quy trình làm việc bình thường

Các giải pháp an ninh sẽ có hiệu quả nhất khi chúng không ảnh hưởng tới hoạt động của thiết bị và luồng công việc. Các giải pháp đó có thể làm việc với bất kỳ loại thiết bị nào và có chức năng như là một add-on cho bất kỳ công việc nào.

Trong kỷ nguyên Internet of Things, một giải pháp an ninh đáng tin cậy phải áp dụng cách tiếp cận tập trung vào bốn yếu tố trung tâm như đã nói, nhưng phải theo cả hai cách suy nghĩ là về vấn đề an ninh và vấn đề công nghệ mới./.

Cảnh báo nguy cơ
MẤT AN TOÀN THÔNG TIN khi sử dụng Camera IP

PHẠM VĂN THI
Phó Giám đốc Công ty HITECH

Trong những năm gần đây việc sử dụng Camera IP được sử dụng rất rộng rãi trong nhiều cơ quan, doanh nghiệp, hộ gia đình. Việc sử dụng Camera IP đem lại nhiều lợi ích to lớn trong việc giám sát các hoạt động như: kinh doanh, an ninh...

Tại Việt Nam hiện có rất nhiều dòng sản phẩm Camera IP của nhiều hãng khác nhau từ cao cấp đến rẻ tiền như: PANASONIC, HIKVISION, YOOSEE... Đặc biệt rất nhiều sản phẩm Camera IP rẻ tiền của Trung Quốc với nhiều tính năng vượt trội được sử dụng rộng rãi, đặc biệt trong các hộ gia đình... Hầu hết các đầu ghi hình Camera và Camera IP hiện nay đều tích hợp công nghệ đám mây (Cloud) để truy cập, quan sát từ xa môi trường mạng Internet. Việc cài đặt, thiết lập thiết bị qua cloud và đăng nhập tài khoản để sử dụng rất dễ dàng. Khi kết nối vào mạng Internet thì Camera được cấp một địa chỉ IP và mở các cổng truy cập (port) mặc định (80, 4567...) và hoạt động trong hệ thống mạng LAN như một máy tính hay điện thoại thông minh...

Việc sử dụng Camera IP đem lại nhiều lợi ích to lớn tuy nhiên camera IP cũng có nhiều lỗ hổng an toàn thông tin rất nghiêm trọng, cụ thể như sau:

Theo báo cáo tình hình an ninh mạng quý 3-2016 của Tập đoàn công nghệ Bkav, người sử dụng camera IP ở Việt Nam đang phải đối mặt nguy cơ bị truy cập trái phép từ Internet. Cụ thể, kết quả khảo sát cho thấy có tới 76% camera IP tại Việt Nam hiện vẫn dùng tài khoản và mật khẩu mặc định của nhà sản xuất. Bkav cho biết, tài khoản quản trị và mật khẩu mặc định của các camera IP là thông số được nhà sản xuất công bố rộng rãi mà ai cũng có thể biết. Việc người sử dụng vẫn dùng mật khẩu mặc định có nguyên nhân không nhỏ đến từ các nhà sản xuất và cung cấp dịch vụ lắp đặt camera IP khi họ không khuyến cáo khách hàng đổi các thông số mặc định của thiết bị trước khi đưa vào sử dụng. "Khi camera IP vẫn đặt mật khẩu mặc định, kẻ xấu có thể dễ dàng truy cập, chiếm được quyền điều khiển thiết bị và theo dõi người dùng", đại diện Bkav cho hay.

Tình hình mất an toàn thông tin trên các thiết bị IoT nói chung và camera giám sát (CCTV) nói riêng tại Việt Nam ngày một gia tăng, nhiều thiết bị có thể đã bị kiểm soát để thực hiện các cuộc tấn công mạng nguy hiểm. Trong tháng 11/2017, hệ thống của Cục An toàn thông tin, Bộ Thông tin và Truyền thông đã phát hiện ở Việt Nam có ít nhất 307.201 camera tại nhiều địa điểm như các chương trình hội nghị, phân xưởng, nhà trẻ .v.v... bị khai thác và đối tượng tấn công có thể dễ dàng công bố công khai hình ảnh các camera này giám sát được lên mạng internet.

Theo trang web *Insecam.com*, một trang web cho phép người dùng xem trực tiếp hàng nghìn các camera camera giám sát, camera an ninh theo chuẩn CCTV và Camera IP đơn giản trên toàn thế giới. Đáng chú ý là trang web này đang liệt kê có hàng trăm camera quan sát tại Việt Nam. Sau khi truy cập, người dùng có thể nhận thấy các camera này còn được phân chia thành các khu vực (Hà Nội, Hải Phòng, TP.HCM...) đồng thời còn hiện rõ cả vị trí tính theo Kinh độ, Vĩ độ, nhà sản xuất và mật khẩu mặc định để truy cập vào Camera này. Tuy nhiên, trang web này chỉ tập hợp các Camera với một số mẫu mã và khu vực nhất định. Nếu mở rộng phạm vi thống kê với nhiều khu vực và mẫu mã camera hơn, thì con số camera bị mất an toàn sẽ lớn hơn nhiều.

Nguy cơ mất an toàn thông tin khi sử dụng Camera IP

Trước tình hình mất an toàn thông tin trong việc sử dụng các hệ thống giám sát bằng camera, có thể nhận thấy các nguy cơ thường trực như sau:

- Camera bị tấn công từ chối dịch vụ (DDoS - Distributed Denial Of Service) làm cho hệ thống mạng tại các cơ quan, đơn vị bị tê liệt, làm ảnh hưởng đến các hoạt động ứng dụng công nghệ thông tin khác gây thiệt hại về kinh tế hoặc tin tặc lợi dụng các lỗi bảo mật trên các hệ thống Camera IP để tạo thành một mạng máy tính ma (botnet) làm bàn đạp tấn công vào các hệ thống máy chủ khác.

- Tài khoản đăng nhập Camera bị đánh cắp: Nếu tài khoản Camera bị đánh cắp, chiếm quyền sử dụng và kiểm soát hệ thống Camera, tin tặc có thể thu thập trái phép các hình ảnh từ Camera như ví dụ nêu ở trên. Xa hơn nữa, nếu chiếm quyền điều khiển cao nhất (root) của Camera, tin tặc có thể kiểm soát toàn bộ hoạt động của nó, kể cả việc thay đổi hình ảnh Camera cung cấp.

Hầu hết người dùng (nhất là các hộ gia đình) chưa quan tâm quản lý tài khoản đăng nhập Camera IP, đầu ghi hình, mật khẩu đăng nhập thường để mặc định của hãng sản xuất. Trong khi đó, tài khoản mặc định của các hãng sản xuất (đầu ghi hình và Camera thông minh) rất đơn giản, dễ đoán (user: admin, pass: admin; user: admin, pass: 123). Mặt khác, các Camera thông minh hiện nay sử dụng công nghệ P2P - Peer two Peer (sử dụng thuật toán điện toán đám mây cho phép các máy tính kết nối với nhau, các máy này vừa được coi là máy chủ, vừa là máy khách nên băng thông và khả năng lưu giữ là do tất cả các máy này đóng góp lại) nên thiết bị điện thoại thông minh dễ dàng kết nối với Camera IP qua Internet. Do đó, cài đặt phần mềm kết nối Camera và dò tìm, đánh cắp tài khoản và tấn công chiếm quyền kiểm soát các hệ thống Camera hiên nay dễ thực hiện.

Một số biện pháp đảm bảo an toàn và bảo mật thông tin

Để đảm bảo an toàn và bảo mật thông tin khi lắp đặt, sử dụng Camera quan sát, cần tiến hành một số biện pháp sau:

- Chọn mua các hãng sản xuất đầu ghi hình, Camera IP có thương hiệu uy tín trên thị trường. Có cam kết dịch vụ đi kèm phải được đảm bảo, rõ ràng.

- Cài đặt, cấu hình hệ thống Camera (đầu ghi hình Camera, Camera IP...) trong vùng mạng an toàn (vùng mạng có các thiết bị bảo mật mạng firewall). Tắt tính năng cho phép truy cập camera IP từ mạng Internet bên ngoài nếu thấy không cần thiết.

- Đối với các hệ thống Camera an ninh như: Camera phục vụ cho ngành giao thông, Camera an ninh quan sát các nơi có tính chất phức tạp và nhạy cảm cần có giải pháp mã hóa dữ liệu trước khi truyền - nhận dữ liệu qua môi trường mạng.

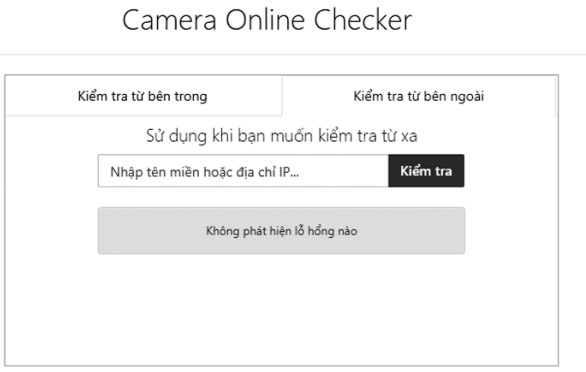
- Thiết lập lại mật khẩu mạnh (mật khẩu khó đoán, khó dò tìm) ngay sau khi đưa hệ thống Camera vào sử dụng.

- Thường xuyên nâng cấp, cập nhật chương trình phần mềm của đầu ghi hình, Camera thông minh để khắc phục các lỗi bảo mật.

- Đảm bảo an toàn và bảo mật thông tin đối với thiết bị (smartphone, tablet...) dùng để truy cập xem Camera, đầu ghi hình để tránh trường hợp bị tấn công leo thang đặc quyền.

- Trong trường hợp chưa bảo đảm về an toàn thông tin trong việc sử dụng Camera, người dùng không nên đặt Camera quan sát những nơi nhạy cảm.

Bên cạnh đó, người dùng có thể sử dụng công cụ trực tuyến của BKAV để kiểm tra độ an toàn thông tin trong việc sử dụng hệ thống Camera của mình tại địa chỉ sau: *http://tools.whitehat.vn/online/10*



Đảm bảo an toàn thông tin trên hệ thống phần mềm quản lý văn bản và hồ sơ công việc

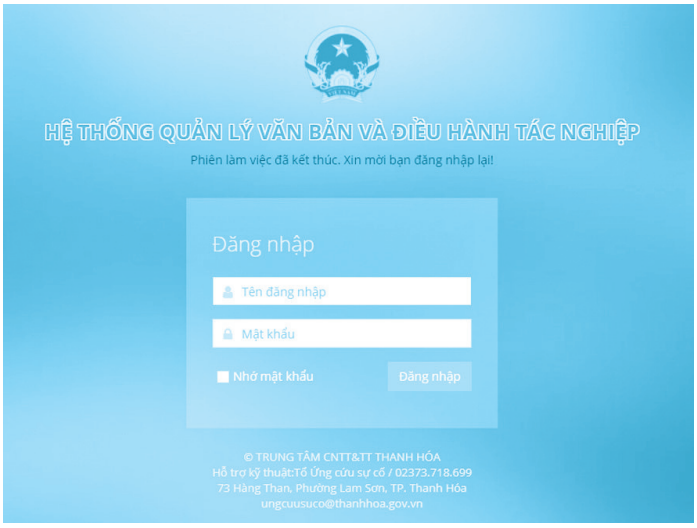
LÊ VĂN HOÀNG
Phó Giám đốc Công ty CP tin học Tân Dân

Thực hiện Quyết định số 3401/QĐ-UBND ngày 29/10/2008 của Chủ tịch UBND tỉnh về việc phê duyệt Báo cáo kinh tế - kỹ thuật công trình: "Hoàn thiện một số hệ thống thông tin số phục vụ sự chỉ đạo, điều hành và quản lý của tỉnh". Trong đó, phê duyệt việc triển khai cài đặt phần mềm Quản lý văn bản và hồ sơ công việc (sau đây gọi tắt là phần mềm TDOffice) cho 48 cơ quan, đơn vị là các sở, ban, ngành cấp tỉnh và UBND cấp huyện. Sau một thời gian đưa vào khai thác và sử dụng, phần mềm TDOffice đã phát huy được hiệu quả và đáp ứng về yêu cầu trao đổi, thực hiện nhiệm vụ của cán bộ công chức trên môi trường mạng, công tác chỉ đạo, điều hành của các đơn vị. Giúp cho các cơ quan, đơn vị xây dựng được hệ thống kho văn bản điện tử tập trung, khắc phục tình trạng tản mạn, thất lạc, sai lệch thông tin, đảm bảo việc gửi nhận văn bản giữa các đơn vị; hỗ trợ công tác lưu trữ, quản lý hồ sơ công việc; nhanh chóng cung cấp thông tin về văn bản và hồ sơ công việc phục vụ yêu cầu của lãnh đạo, cán bộ quản lý và cán bộ chuyên môn một cách chính xác, đầy đủ; người dùng có thể truy cập vào hệ thống và làm việc mọi lúc, mọi nơi;...;

Thống kê tổng hợp gửi nhận văn bản điện tử trên môi trường mạng tại địa chỉ: http://qlvb.thanhhoaict.gov.vn

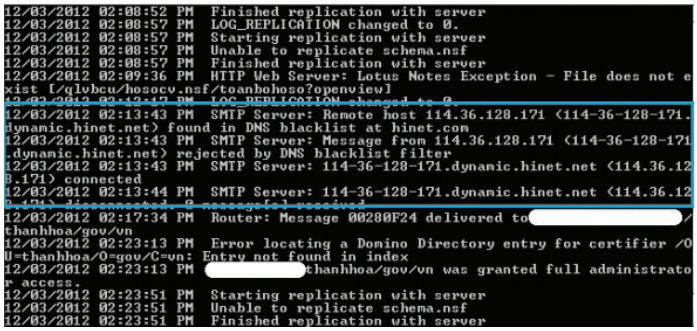
Việc triển khai ứng dụng phần mềm vào xử lý công việc sẽ tạo môi trường làm việc hiện đại gắn với cải cách hành chính, góp phần đẩy mạnh cải cách hành chính, nâng cao hiệu quả hoạt động của các cơ quan, đơn vị trên địa bàn tỉnh. Với những ưu điểm trên, trong thời gian qua phần mềm tiếp tục được triển khai mới tại các cơ quan khác và các tổ chức chính trị xã hội trên địa bàn tỉnh với hơn 50 đơn vị đang tham gia liên thông trao đổi văn bản trong mạng diện rộng của tỉnh. Bên cạnh đó phần mềm được triển khai nhân rộng xuống hơn 300 UBND cấp xã trên địa bàn tỉnh nhằm đáp ứng việc triển khai kết nối, liên thông văn bản điện tử từ cấp tỉnh đến cấp huyện, cấp xã trong việc thực hiện Kế hoạch số 01/KH-UBND ngày 04/01/2016 để tổ chức thực hiện

Nghị quyết số 36a/NQ-CP ngày 14/10/2015 của Chính phủ về Chính phủ điện tử.



Giao diện đăng nhập phần mềm trên trình duyệt web và trên Mobile.

Trong thời gian qua, Trung tâm đã được Chủ tịch UBND tỉnh, Sở Thông tin và Truyền thông giao trong việc hỗ trợ xử lý và khắc phục sự cố trên các phần mềm ứng dụng dùng chung trên địa bàn tỉnh, trong đó có phần mềm TDOffice cho các cơ quan, đơn vị đảm bảo hoạt động thông suốt trong quá trình sử dụng. Qua đó, theo ghi nhận về tình hình an toàn thông tin trên địa bàn tỉnh của Trung tâm, trong thời gian qua liên tục có những đợt tấn công mạnh vào các hệ thống chạy phần mềm TDOffice của các đơn vị đang sử dụng. Với việc tấn công vào các điểm yếu, lỗ hổng của các hệ thống này giúp cho các tin tặc có thể chiếm quyền và làm thay đổi phương thức hoạt động cũng như nội dung của phần mềm. Dẫn đến việc làm lộ, lọt thông tin bí mật của các cơ quan, đơn vị trong quá trình sử dụng phần mềm.



Trường hợp hệ thống phần mềm của cơ quan bị tấn công theo hình thức Spam Mail

Nhằm tăng cường bảo đảm an toàn thông tin trong việc vận hành, sử dụng và khai thác phần mềm TDOfice. Đồng thời hạn chế các nguy cơ, rủi ro như trên, cần triển khai các biện pháp như sau:

1. Đối với các cơ quan, đơn vị

- Triển khai và áp dụng Quy chế quản lý, vận hành và khai thác sử dụng phần mềm quản lý văn bản và hồ sơ công việc trong các cơ quan hành chính nhà nước tỉnh Thanh Hóa theo Quyết định số 4764/2017/QĐ-UBND của Ủy ban nhân dân tỉnh ngày 11/12/2017.

- Rà soát danh sách cán bộ công chức, viên chức, người lao động trên hệ thống phần mềm TDOffice tại các các đơn vị. Đối với những tài khoản người dùng không tham gia sử dụng trên phần mềm cần được gỡ bỏ hoàn toàn khỏi cơ sở dữ liệu trên hệ thống.

- Quán triệt yêu cầu cán bộ công chức, viên chức, người lao động thiết lập và bảo quản mật khẩu đăng nhập trên phần mềm. Mật khẩu phải có độ phức tạp và khó đoán biết. Định kỳ phải thường xuyên thay đổi mật khẩu.

- Nâng cấp và cập nhật bản vá lỗ hổng bảo mật cho phần mềm của đơn vị theo khuyến cáo của Trung tâm.

- Rà soát và kiểm tra các quyền truy cập của các tài khoản trên các chức năng chính của phần mềm như chức năng Văn bản đi/đến và Hồ sơ công việc...Đảm bảo quyền truy cập của người dùng được phân cấp đúng chức năng trên phần mềm.

- Áp dụng các bước hướng dẫn bảo đảm an toàn, an ninh thông tin cho máy chủ chạy phần mềm TDOffice tại Công văn số 10/TTCNTT&TT-QTHT ngày 05/3/2013 của Trung tâm CNTT&TT Thanh Hóa và theo tài liệu kỹ thuật *"Hướng dẫn một số biện pháp kỹ thuật cơ bản đảm bảo an toàn thông tin trên phần mềm TDOffice"*

- Thực hiện việc sao lưu dữ liệu thường xuyên trên phần mềm. Dữ liệu sao lưu được đặt ở các vị trí khác nhau. Không đặt bản sao lưu trên cùng máy chủ chạy phần mềm.

- Triển khai hiệu quả ứng dụng chữ ký số chuyên dùng của cơ quan, đơn vị trên phần mềm nhằm bảo đảm các đặc tính về an toàn thông tin trong việc gửi nhận văn bản trên môi trường mạng.

- Thường xuyên thực hiện việc theo dõi, giám sát hoạt động của phần mềm để kịp thời phát hiện các sự cố và dấu hiệu bất thường gây mất an toàn thông tin. Có phương án kiểm tra, đánh giá đảm bảo an toàn thông tin trên hệ thống phần mềm cũng như xây dựng các phương án dự phòng, đối phó khi có sự cố xảy ra.

2. Đối với người sử dụng trên phần mềm

- Để giúp người sử dụng có thể truy cập vào phần mềm theo đúng tên đơn vị đã được thiết lập nhằm hạn chế việc nhập sai địa chỉ hoặc bấm vào địa chỉ được tin tặc gửi đến nhằm đánh cắp thông tin tài khoản. Người dùng truy cập vào địa chỉ duy nhất trên môi trường mạng là: ***http://qlvb.thanhhoaict.gov.vn***

Tổng hợp địa chỉ truy cập trên môi trường mạng và hướng dẫn sử dụng cho người dùng tại địa chỉ: http://qlvb.thanhhoaict.gov.vn

- Thay đổi mật khẩu được cấp và bảo vệ mật khẩu sử dụng phần mềm.

- Không truy nhập vào tài khoản của người khác và không cung cấp tài khoản cá nhân cho người khác để sử dụng phần mềm.

- Không sử dụng chế độ tự động lưu thông tin tài khoản/mật khẩu khi sử dụng trình duyệt.

- Đăng xuất ngay sau khi kết thúc phiên làm việc trên phần mềm; không nên thoát khỏi trình duyệt mà không sử dụng nút "Thoát" để tránh các lỗi không đáng có.

- Sử dụng các trình duyệt cập nhật mới nhất có chế độ bảo mật tiêu chuẩn hoặc chế độ cao để truy cập vào phần mềm.

- Chỉ đăng nhập qua các thiết bị đáng tin cậy, không đăng nhập qua thiết bị công cộng/dùng chung, không sử dụng các mạng wifi công cộng để sử dụng phần mềm.

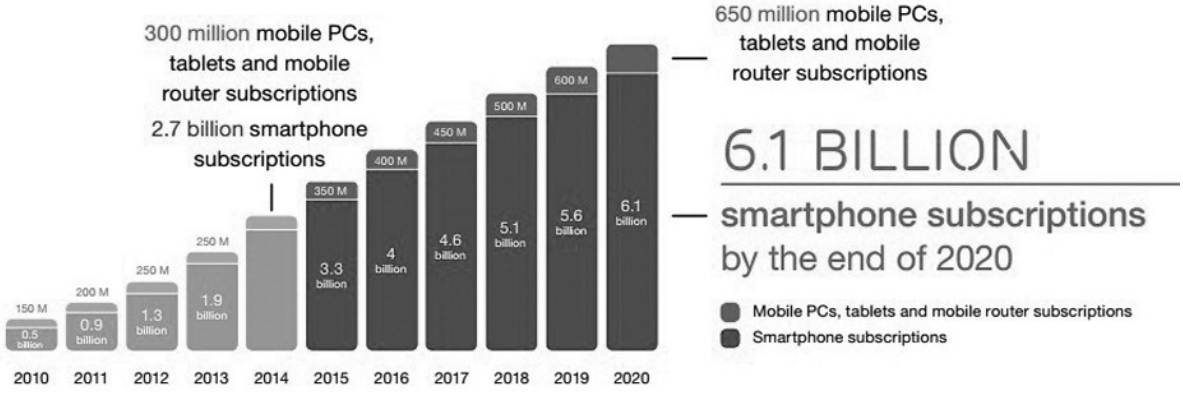
An toàn thông tin khi sử dụng điện thoại thông minh Smartphone

TRẦN NGỌC HƯNG
Trung tâm CNTT&TT Thanh Hóa

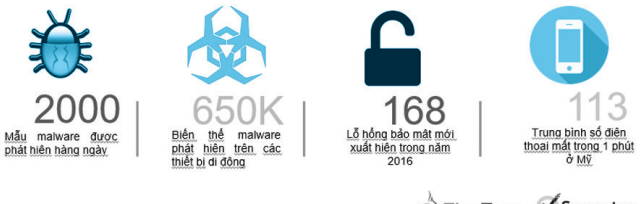
Các thiết bị di động như điện thoại thông minh và máy tính bảng không chỉ ngày càng có nhiều tính năng sử dụng thông minh hơn, mà còn được sử dụng phổ biến hơn, đã khiến cho khối lượng dữ liệu mà chúng tạo ra đang tiếp tục tăng theo cấp số nhân. Sự tăng trưởng này mang đến những thách thức mới cho người sử dụng và cả những cơ hội mới cho tin tặc và những kẻ lừa đảo trên mạng.

Điện thoại thông minh đóng vai trò ngày càng quan trọng trong cuộc sống hiện đại. Một số lượng lớn người dùng cũng như thông tin được lưu trữ trên thiết bị này và đang không ngừng gia tăng. Thêm vào đó, xu hướng mang thiết bị riêng đi làm (BYOD) đang dần phổ biến, những chiếc smartphone còn được dùng để lưu trữ dữ liệu trong công việc. Do đó, điện thoại thông minh là mối đe dọa an ninh lớn nhất không chỉ cho các cá nhân mà còn cả các doanh nghiệp.

Theo ước tính của eMarketer, số người sử dụng điện thoại thông minh trên toàn thế giới năm 2016 sẽ vượt 2 tỷ. Năm 2015, khoảng 1/4 dân số thế giới sử dụng smartphone và đến năm 2018, sẽ là khoảng 1/3 dân số thế giới, tương đương 2,56 tỷ người. Số lượng này còn tiếp tục tăng khi một nghiên cứu mới đây của Ericsson dự báo, đến năm 2020, số lượng người dùng smartphone trên toàn cầu sẽ đạt mức kỷ lục chiếm 70% dân số trên toàn thế giới, với 6,1 tỷ người.



Smartphone có thể không an toàn, thậm chí gây nguy hiểm cho bạn khi nói đến vấn đề bảo mật dữ liệu riêng tư của người dùng. Theo một nghiên cứu gần đây, có hơn 48% người sử dụng smartphone không sử dụng mật mã để khóa thiết bị của họ. Bất cứ ai kiểm soát được điện thoại của người khác cũng kiểm soát nhận dạng ảo của người đó, do đó hãy cố gắng tự bảo vệ mình ngay từ bây giờ.



Báo cáo tình hình mất an toàn thông tin trên Smartphone năm 2016

Những rủi ro thông tin trên smartphone

Theo xếp hạng của ENISA, Cơ quan an ninh châu Âu về an toàn thông tin mạng, những rủi ro về an toàn bảo mật trên các thiết bị di động smartphone và máy tính bảng được phân theo theo từng cấp độ như sau:

#1. Nghe lén thông tin

Các thiết bị di động khi bị tấn công có thể bị:

- Ghi âm thông qua microphone
- Ghi âm cuộc gọi
- Đọc các tin nhắn
- Đọc lịch sử cuộc gọi
- Tra cứu địa điểm
- Xem trộm hình ảnh
- ...

#2. Giả mạo thông tin

Gửi các tin nhắn lừa đảo đến các số trong danh bạ, chuyển hướng các tin nhắn đến các đầu số khác...

Sử dụng các ứng dụng email để gửi các email mạo danh, lừa đảo đến danh bạ email...

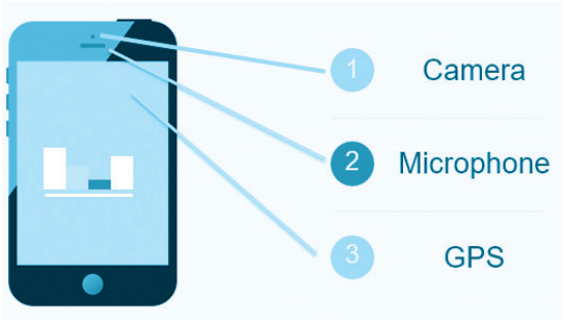
Tự động đăng thông tin lên các trang mạng xã hội đã được thiết lập sẵn trong thiết bị di động...

#3. Đánh cắp dữ liệu

- Các tài khoản ngân hàng, tín dụng, an sinh xã hội lưu trên thiết bị...
- Những thông tin như danh bạ, số điện thoại, nhật ký cuộc gọi trong thiết bị có thể được sử dụng để tạo ra những danh sách khách hàng...
- Những thông tin về thiết bị như IMEI, Version OS, kernel...
- Những thông tin cá nhân khác của chủ thiết bị như hình ảnh, email, video, voice call...

#4. Tấn công tài chính

Gọi đến các đầu số trả phí



Những phần mềm gián điệp có thể lợi dụng quyền sử dụng cuộc gọi và tin nhắn để âm thầm kết nối, nhắn tin đến những đầu số trả phí

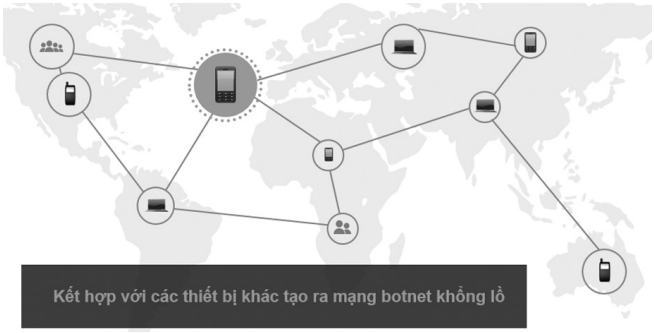
Xem trộm mã OTP

Những phần mềm gián điệp có thể trở thành công cụ tiếp tay cho việc đánh cắp tiền từ tài khoản ngân hàng bằng cách tự động lấy mã OTP và xóa nó để người dùng không phát hiện

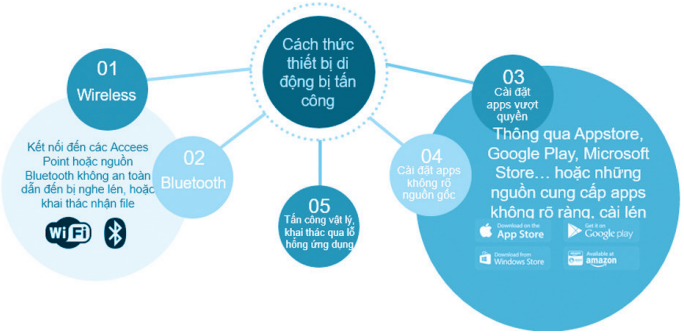
Mã hóa dữ liệu tống tiền

Mã độc cũng có thể mã hóa các file dữ liệu quan trọng bằng những khóa riêng và yêu cầu trả tiền để được giải mã.

#5. Tấn công thiết bị khác

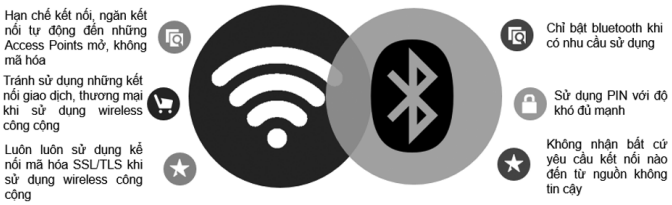


Cách thức thiết bị di động bị tấn công



Bảo đảm An toàn thông tin cho các thiết bị di động

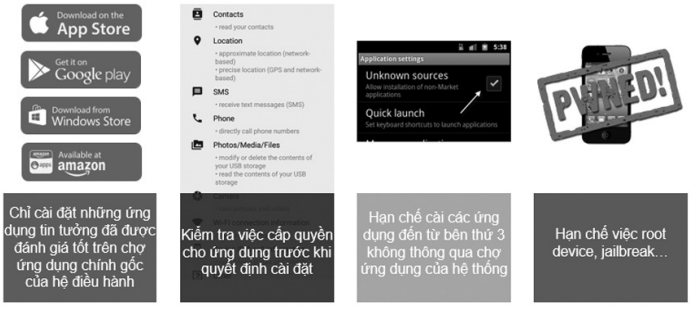
1. Luôn luôn thận trọng khi mở các kết nối mạng hay bluetooth ở những nơi công cộng



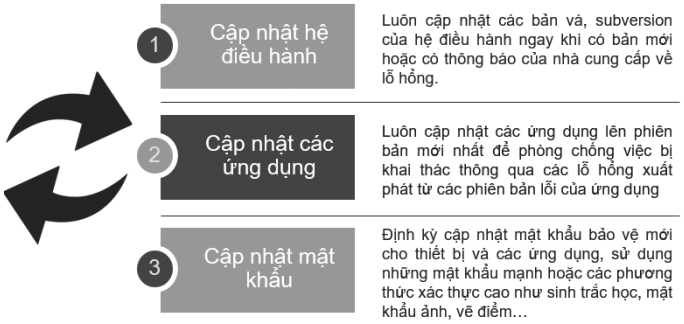
2. Sử dụng các phần mềm bảo mật

Thường xuyên sử dụng các phần mềm bảo mật để quét, phát hiện mã độc trên hệ thống, kiểm tra hành vi sử dụng tài nguyên trái phép, các kết nối kém bảo mật...

3. Quản lý Ứng dụng



4. Cập nhật trên điện thoại



5. Phòng chống việc mất an toàn thông qua tấn công vật lý với thiết bị di động

6. Nguồn gốc và xuất xứ điện thoại

- Nên mua điện thoại của những nhà sản xuất có uy tín và từ những nhà phân phối chính thức hoặc cửa hàng lớn (Do hiện nay nhiều dòng điện thoại giá rẻ, phần lớn xuất xứ không rõ ràng trà trộn vào thị trường, cài đặt sẵn mã độc từ lúc xuất xưởng để thu thập thông tin người dùng, tự động nhắn tin đến đầu số dịch vụ để trộm tiền trong tài khoản điện thoại của người dùng).

- Nếu mua lại điện thoại cũ hoặc được tặng điện thoại: nên khôi phục về cài đặt gốc (reset factory), đổi mật khẩu đồng bộ dữ liệu lên Cloud (Apple iCloud,...) trước khi sử dụng để đảm bảo điện thoại không bị cài đặt sẵn phần mềm gián điệp từ trước đó, đảm bảo dữ liệu không đồng bộ lên tài khoản Cloud của người chủ cũ.

7. Sao lưu dữ liệu an toàn

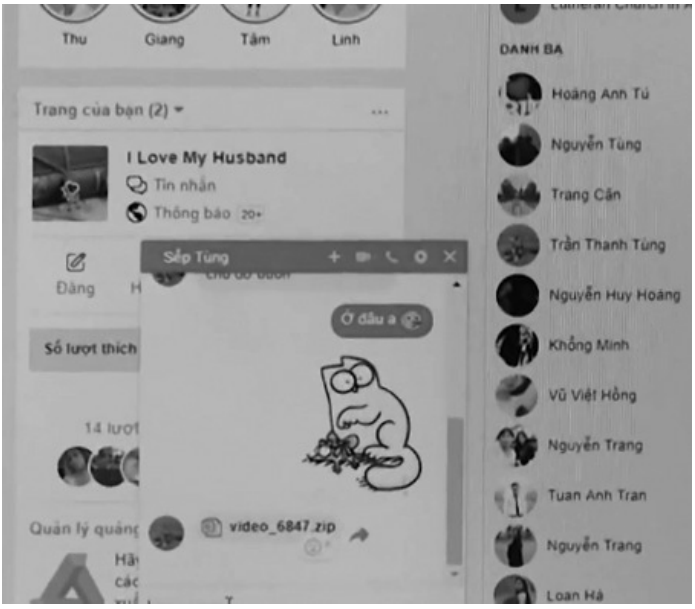
Nên sử dụng các phần mềm sao lưu, đồng bộ dữ liệu mặc định của thiết bị, không nên sử dụng các phần mềm sao lưu, đồng bộ của các nhà sản xuất không có uy tín, vì như vậy vô tình bạn lại tự đẩy dữ liệu cá nhân của mình lên một nơi chưa đảm bảo an toàn.

Phát hiện, ngăn chặn mã độc "đào tiền ảo"

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

Tình hình mã độc "đào" tiền ảo đang diễn biến rất phức tạp. Mới đây nhất, nhiều người dùng Facebook trên máy tính tại Việt Nam đã bị dính một loại mã độc mới làm cho máy tính của họ chạy chậm lại hay không thể sử dụng được. Mã độc này lây lan bằng cách gửi cho nạn nhân những tin nhắn của bạn bè dưới dạng tập tin nén zip (có tên dạng "video_" + 4 số ngẫu nhiên) trong khung trò chuyện của Facebook hay ứng dụng web Messenger. Nếu nạn nhân nhấp tiếp vào tập tin giả mạo này, máy tính của họ sẽ bị nhiễm mã độc. Trường hợp máy tính nạn nhân dùng trình duyệt web Google Chrome, mã độc sẽ cài đặt một extension (tiện ích mở rộng) để tiếp tục phát tán tập tin zip qua Facebook Messenger tới danh sách bạn bè của nạn nhân. Mục đích của đợt phát tán mã độc này nhằm chiếm quyền điều khiển máy tính của nạn nhân, từ đó lợi dụng máy tính của nạn nhân để đào tiền ảo, khiến cho máy tính của nạn nhân luôn trong tình trạng hoạt động chậm và gần như không thể sử dụng được.

Thống kê từ hệ thống giám sát virus của Bkav, tính tới 14 giờ chiều 21-12, đã có hơn 12.600 máy



tính tại Việt Nam nhiễm mã độc đào tiền ảo lây qua Facebook. Điều đáng ngại theo Bkav ghi nhận cứ 10 phút, hacker lại tung lên mạng một biến thể virus mới nhằm tránh bị phát hiện bởi các phần mềm an ninh. Theo chuyên gia của Bkav, số máy tính bị nhiễm mã độc còn tiếp tục gia tăng mạnh. Bên cạnh đó tin tặc đã lập trình để sinh tự động biến thể mới nhằm qua mặt các phần mềm an ninh. Tính tới thời điểm hiện tại đã có khoảng hơn 500 biến thể của mã độc đào tiền ảo được tung lên mạng và chưa có dấu hiệu dừng lại.

Mới đây, Trung tâm ứng cứu khẩn cấp máy tính Việt Nam VNCERT cũng đã gửi công văn điều phối số 383/VNCERT-ĐPƯC ngày 15/11/2017 về việc yêu cầu tăng cường phát hiện, ngăn chặn mã độc khai thác tiền ảo Coinhive ẩn mình trên các website. Các website cũng có thể bị chèn các mã độc khai thác thể hiện qua những từ khóa trong mã nguồn website như "coinhive.com", "coinhive", "coin-hive", "coinhive.rnin.js", "authedr-nine.com", "authedrnine.rnin.js", "coinhive.min.js", "authedmine.com", "authedmine.min.js".

Khi người dùng truy cập vào những trang web bị chèn mã độc, thư viện mã Coinhive sẽ tự động chạy trên máy tính người dùng dưới dạng tiện ích mở rộng hay trực tiếp trong trình duyệt web nhằm mục đích "đào" tiền ảo Bitcoin, Monero... bằng cách sử dụng trái phép tài nguyên của người dùng như: CPU, ổ cứng, bộ nhớ... và gửi về ví điện tử của tin tặc.

Giới thiệu về mã độc đào tiền ảo

Nguyên nhân của vấn đề trên xuất phát từ giá trị của đồng tiền ảo đang tăng chóng mặt, và mọi người mọi nhà đang tìm cách khai thác chúng. Tuy nhiên, rất nhiều thủ đoạn mang tính tiêu cực đang được các hacker lén sử dụng để trục lợi. Phổ biến nhất trong số đó là cài mã độc lên website (tính cả trường hợp chủ website tự cài lên trang web của mình), nếu bạn hay một ai đó truy cập vào trang web bị nhiễm mã độc để làm việc, xem tin tức, xem phim, nghe nhạc... thì ngay lập tức tính năng "đào tiền lén" sẽ được kích hoạt.

Tuy nhiên, người dùng sẽ không được hưởng bất kỳ lợi gì từ đồng tiền ảo này, mà ngược lại toàn bộ hiệu năng của máy tính sẽ được tận dụng tối đa để khai thác tiền ảo. Từ đó hiệu năng máy tính bị nhiễm sẽ giảm xuống rõ rệt và đáng kể. Mặt khác mã độc còn thực hiện các hành vi thu thập thông tin tài khoản của người dùng và chiếm quyền sử dụng máy tính để phát tán mã độc.

Phát hiện, ngăn chặn mã độc "đào tiền ảo"

#1: Đối với các cổng/trang thông tin điện tử

Đề nghị phối hợp với các đơn vị đã xây dựng cổng/trang thông tin điện tử cho cơ quan, đơn vị kiểm tra, rà soát mã nguồn để phát hiện các mã được chèn vào. Dấu hiệu nhận biết gồm các từ khóa trong mã nguồn website "coinhive.com", "coinhive", "coin-hive", "coinhive.min,js", "authed-mine.com", "authedmine.min.js".

Nếu phát hiện cổng/trang thông tin điện tử bị chèn các mã khai thác như nêu trên, cần rà soát và kiểm tra lại lỗ hổng trên máy chủ, lỗ hổng trên cổng/trang thông tin điện tử, kiểm tra các tài khoản bị lộ lọt có quyền thay đổi mã nguồn, nhằm khắc phục lỗ hổng bị lợi dụng.

#2: Đối với các hệ thống mạng trong các cơ quan, đơn vị

Thực hiện giám sát và bóc gỡ, xử lý trên các máy tính trong mạng nội bộ có xuất hiện các kết nối đến các địa chỉ tên miền sau: afminer.com, coin-have.com, coinerra.com, coinhive.com, coin-nebula.com, crypto-loot.com, hashforcash.com.us, jescoin.com, ppoi.org, au-thedmine.com.

Sử dụng tường lửa để ngăn chặn các kết nối

ra các địa chỉ sau: afminer.com, coin-have.com, coinerra.com, coinhive.com, coinnebula.com, crypto-loot.com, hashforcash.us, jescoin.com, ppoi.org, authedmine.com.

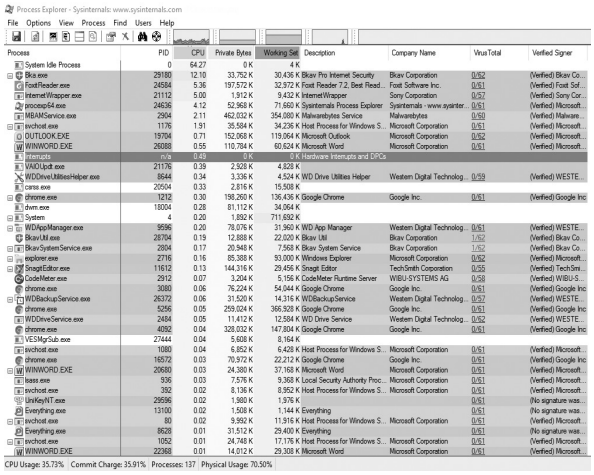
Thường xuyên kiểm tra và quét các lỗ hổng tồn tại trên hệ thống để phát hiện kịp thời sự xuất hiện của các đoạn mã độc hại. Trong trường hợp phát hiện ra các lỗ hổng, lập tức triển khai các biện pháp khắc phục, cập nhật các bản vá bổ sung và loại bỏ các chương trình độc hại đã bị tin tặc chèn vào.

#3: Đối với người dùng

1. Kiểm tra hiệu năng máy tính và các kết nối

- Sử dụng phần mềm miễn phí có tên "Process Explorer" của Microsoft tại địa chỉ https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer để kiểm tra danh sách các tiến trình đang chạy và tài nguyên sử dụng trên máy tính.

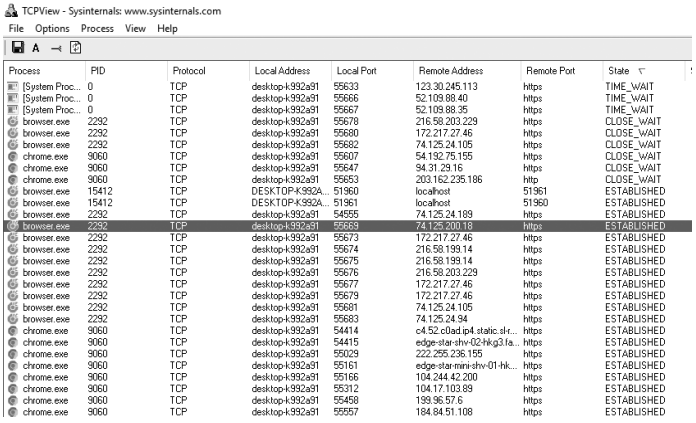
- Bằng cách kiểm tra tài nguyên của các tiến



trình đang sử dụng, ta phát hiện được sự gia tăng đột ngột trong việc sử dụng hiệu năng của máy tính để qua đó đặt nghi vấn về việc lây nhiễm các loại mã độc đào tiền ảo.

- Sử dụng công cụ khác cũng của Microsoft là TCPview tại địa chỉ https://docs.microsoft.com/en-us/sysinternals/downloads/tcpview. Công cụ này cho phép nhanh chóng xem chính xác quá trình kết nối với các địa chỉ bên ngoài internet, và thậm chí cho phép bạn kết thúc quá trình, đóng kết nối. Thông qua công cụ này, người dùng có thể kiểm tra danh sách các tên miền mà mã độc kết nối đến như ở trên có xuất hiện trên máy tính của mình hay không.

2. Ngăn chặn mã độc đào tiền ảo trên Chrome,



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
[System Proc...	0	TCP	desktop-k992a91	55633	123.30.245.113	https	TIME_WAIT
[System Proc...	0	TCP	desktop-k992a91	55666	52.109.88.40	https	TIME_WAIT
[System Proc...	0	TCP	desktop-k992a91	55667	52.109.88.35	https	TIME_WAIT
browser.exe	2292	TCP	desktop-k992a91	55678	216.58.203.229	https	CLOSE_WAIT
browser.exe	2292	TCP	desktop-k992a91	55680	172.217.27.46	https	CLOSE_WAIT
browser.exe	2292	TCP	desktop-k992a91	55682	74.125.24.105	https	CLOSE_WAIT
chrome.exe	9060	TCP	desktop-k992a91	55607	54.192.75.155	https	CLOSE_WAIT
chrome.exe	9060	TCP	desktop-k992a91	55647	94.31.29.16	https	CLOSE_WAIT
chrome.exe	9060	TCP	desktop-k992a91	55653	203.162.235.186	http	CLOSE_WAIT
browser.exe	15412	TCP	DESKTOP-K992A...	51960	localhost	51961	ESTABLISHED
browser.exe	15412	TCP	DESKTOP-K992A...	51961	localhost	51960	ESTABLISHED
browser.exe	2292	TCP	desktop-k992a91	54555	74.125.24.189	https	ESTABLISHED
browser.exe	2292	TCP	desktop-k992a91	55669	74.125.200.18	https	ESTABLISHED
browser.exe	2292	TCP	desktop-k992a91	55673	172.217.27.46	https	ESTABLISHED
browser.exe	2292	TCP	desktop-k992a91	55674	216.58.199.14	https	ESTABLISHED
browser.exe	2292	TCP	desktop-k992a91	55675	216.58.199.14	https	ESTABLISHED
browser.exe	2292	TCP	desktop-k992a91	55676	216.58.203.229	https	ESTABLISHED
browser.exe	2292	TCP	desktop-k992a91	55677	172.217.27.46	https	ESTABLISHED
browser.exe	2292	TCP	desktop-k992a91	55679	172.217.27.46	https	ESTABLISHED
browser.exe	2292	TCP	desktop-k992a91	55681	74.125.24.105	https	ESTABLISHED
browser.exe	2292	TCP	desktop-k992a91	55683	74.125.24.94	https	ESTABLISHED
chrome.exe	9060	TCP	desktop-k992a91	54414	c4.52.c0ad.ip4.static.sl-r...	https	ESTABLISHED
chrome.exe	9060	TCP	desktop-k992a91	54415	edge-star-shv-02-hkg3.fa...	https	ESTABLISHED
chrome.exe	9060	TCP	desktop-k992a91	55029	222.255.236.155	https	ESTABLISHED
chrome.exe	9060	TCP	desktop-k992a91	55161	edge-star-mini-shv-01-hk...	https	ESTABLISHED
chrome.exe	9060	TCP	desktop-k992a91	55166	104.244.42.200	https	ESTABLISHED
chrome.exe	9060	TCP	desktop-k992a91	55312	104.17.103.89	https	ESTABLISHED
chrome.exe	9060	TCP	desktop-k992a91	55458	199.96.57.6	https	ESTABLISHED
chrome.exe	9060	TCP	desktop-k992a91	55557	184.84.51.108	https	ESTABLISHED

Firefox

Sử dụng tiện ích trên trình duyệt: ***No Coin, minerBlock*** và ***NoScript*** là tiện ích mở rộng được phát triển để phát hiện và ngăn chặn vấn nạn đào tiền ảo lén khi người dùng duyệt web. Cách sử dụng rất đơn giản, người dùng có thể tham khảo như sau:

Bước 1: Tải về theo đường dẫn sau.

No Coin (Chrome):

https://chrome.google.com/webstore/detail/no-coin-block-miners-on-t/gojamcfopckidlocpkbelmpjcgmbgjcl?hl=en

minerBlock (Chrome):

https://chrome.google.com/webstore/detail/minerblock/emikbbbebcdfohonlaifafnoanocnebl?hl=en

NoScript (Firefox):

https://addons.mozilla.org/en-US/firefox/addon/noscript/

Bước 2: Nhấn vào Add to Chrome (đối với trình duyệt Chrome) hoặc Add to Firefox (đối với trình duyệt Firefox) -> Thêm tiện ích để cài đặt. Lúc này

trình duyệt của bạn đã được bảo vệ trước mã độc đào tiền ảo.

3. Chặn kết nối đến tên miền khai thác tiền ảo trên Windows

02 cách làm dưới đây giúp người dùng chặn kết nối đến các tên miền chứa mã độc đào tiền ảo mà không cần cài đặt bất kỳ phần mềm bên thứ 3. Tuy nhiên, hạn chế của cách thức này là cần phải xác định chi tiết danh sách tên miền cần chặn vì Hacker liên tục tạo mới danh sách các tên miền để điều khiển mã độc.

Cách 1: Sử dụng Firewall được cung cấp trên Windows, tạo các luật để chặn các kết nối đến các tên miền theo danh sách trên.

Cách 2: Sử dụng file host trên Windows để ngăn chặn quá trình phân giải tên miền cục bộ trên Windows.

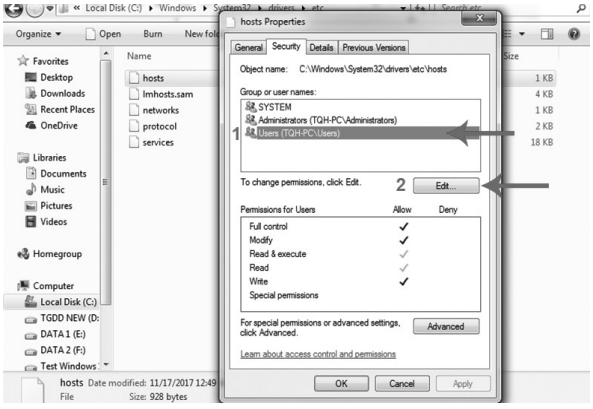
Bước 1: Trên máy tính chạy Windows, bạn vào My Computer và truy cập đường dẫn sau:

C:\Windows\System32\drivers\etc.

Bước 2: Click chuột phải vào tập tin hosts -> Properties...

...chọn tiếp vào Security -> Chọn vào mục có trên máy tính của bạn (thông thường là dòng có chữ Users) -> Edit...

..chọn tiếp vào mụcUsers -> Đánh dấu tích vào



các ô tại mụcAllow.

Bước 3: Quay trở lại C:\Windows\System32\drivers\etc -> Mở tập tin hosts -> Chọn vào Notepad nếu máy tính yêu cầu -> Thêm vào cuối văn bản đoạn mã sau:

0.0.0.0 afminer.com0.0.0.0 coin-have.com0.0.0.0 coinerra.com0.0.0.0 coinhive.com0.0.0.0 coinnebula.com0.0.0.0 crypto-loot.com0.0.0.0 hashforcash.us0.0.0.0 jescoin.com0.0.0.0 ppoi.org0.0.0.0 authedmine.com

Bước 4: Nhấn vào File -> Save để lưu kết quả.

4. Ngăn chặn mã độc đào tiền ảo trên facebook

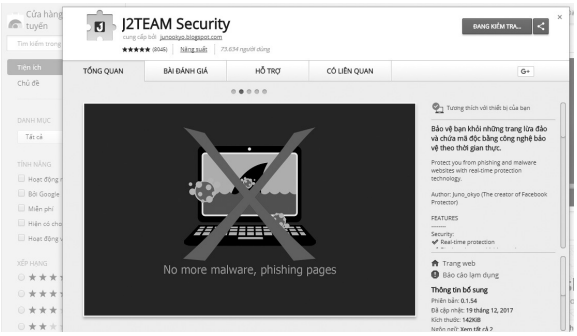
Bước 1: Sử dụng tiện ích trên trình duyệt

Để ngăn chặn các loại mã độc đào tiền ảo gửi qua Facebook, bạn có thể sử dụng phần mềm J2TEAM Security. Về cơ bản, J2TEAM Security sẽ giúp hạn chế tình trạng lừa đảo trên Facebook, ngăn chặn các trang web độc hại, kiểm tra xem ai là người nhắn tin với bạn nhiều nhất trên Facebook... Mới đây, nhà phát triển tiện ích vừa cập nhật thêm tính năng giúp ngăn chặn các đoạn mã (script) để đào Bitcoin bất hợp pháp khi chưa được người dùng đồng ý.

Đầu tiên, bạn hãy cài đặt J2TEAM Security cho trình duyệt Chrome tại địa chỉ: https://chrome.google.com/webstore/detail/j2team-security/hmlcjjclebjnfohgmgikjfnbmfkigocc

Khi hoàn tất, người dùng chỉ cần bấm vào biểu tượng của tiện ích ở góc phải trình duyệt và chọn Block Cryptocurrency mining script. Kể từ lúc này, mỗi khi truy cập vào các trang web có chèn script để đào Bitcoin, tiện ích sẽ tự động ngăn chặn và hiển thị thông báo trên màn hình.

Bước 2: Nâng cao nhận thức và xử lý khi bị lây nhiễm



- Cảnh giác và không mở các tập tin hay đường dẫn lạ được gửi qua Facebook Messenger hay bất kỳ ứng dụng truyền thông nào khác (ví dụ: Viber, Zalo, thư điện tử,...).

- Nếu nhận được các thông tin (tập tin hoặc đường dẫn) lạ, có thể thông báo hoặc gửi thông tin về Tổ Ứng cứu sự cố của Trung tâm để tổng hợp và phân tích, cảnh báo khi có những dấu hiệu, nguy cơ tấn công mạng mới.

- Đối với người dùng đã bị lây nhiễm cần cài đặt và cập nhật các phần mềm phòng, chống mã độc, virus để phát hiện và ngăn chặn, loại bỏ mã độc.

- Ngay lập tức đổi mật khẩu cho tài khoản đăng nhập trên trình duyệt của mình nếu đã lỡ mở file nén đính kèm.

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 mã độc đào tiền ảo 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.
Email: ungcuusuco@thanhhoa.gov.vn

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

I. Tình hình An toàn thông tin trong nước và quốc tế

1. Gần 13.000 máy tính tại Việt Nam nhiễm mã độc đào tiền ảo lây qua Facebook Messenger

Thống kê từ hệ thống giám sát virus của Bkav, tính tới ngày 21/12, đã có hơn 12.600 máy tính tại Việt Nam nhiễm mã độc đào tiền ảo lây qua ứng dụng Facebook Messenger.

Công ty Bkav ghi nhận cứ 10 phút, hacker lại tung lên mạng một biến thể mới của mã độc đào tiền ảo được phát tán mạnh qua Facebook Messenger nhằm tránh bị phát hiện bởi các phần mềm an ninh. Hiện nay, đã có khoảng hơn 500 biến thể của mã độc đào tiền ảo được tung lên mạng và chưa có dấu hiệu dừng lại.

2. Các hệ thống thông tin tại Việt Nam nhận khoảng 14.000 cuộc tấn công mạng trong năm 2017

Năm 2017, các cơ quan thuộc khối an toàn thông tin của Bộ Thông tin và Truyền thông đã ghi nhận khoảng 14.000 cuộc tấn công mạng vào các hệ thống thông tin của Việt Nam, bao gồm gần 3.000 cuộc tấn công lừa đảo, 6.500 tấn công cài phần mềm độc hại và 4.500 tấn công thay đổi giao diện.

Cục An toàn thông tin, Bộ Thông tin và Truyền thông đã ghi nhận trong năm 2017, có hơn 17 triệu lượt truy vấn từ các địa chỉ IP của Việt Nam đến các tên miền hoặc IP phát tán/điều khiển mã độc trên thế giới, chủ yếu là các kết nối tới các mạng botnet lớn như conficker, mirai, ramnit, sality, cutwai, zeroaccess... đã có trên 19.000 lượt địa chỉ máy chủ web tại Việt Nam bị tấn công; trên 3 triệu địa chỉ IP Việt Nam thường xuyên nằm trong danh sách đen (black list) của các tổ chức quốc tế; và có hơn 100.000 camera IP đang được công khai trên Internet của Việt Nam (trên tổng số 307.201 camera IP) tồn tại các điểm yếu và lỗ hổng bảo mật có thể bị khai thác lợi dụng.

3. 1,5 triệu IP Việt Nam nằm trong các mạng botnet

Theo Cục An toàn thông tin, tại Việt Nam vẫn có tới 1,5 triệu IP khác nhau nằm trong các mạng botnet quốc tế. Theo số liệu thống kê được đại diện Cục ATTT đưa ra tại sự kiện, đến tháng 10/2017, có hơn 8 triệu lượt IP việt Nam (trong đó có tới 1,5 triệu IP khác nhau) nằm trong các mạng botnet.

Ngoài ra, đại diện Cục ATTT cho hay trong tổng số 307.000 IP camera có hơn 100.000 IP camera còn tồn tại những lỗ hổng bảo mật và có thể dễ dàng trở thành một trong những botnet trong các cuộc tấn công Ddos.

4. Dữ liệu rò rỉ liên quan đến ít nhất 1.800 tài khoản thư điện tử của các cơ quan, tổ chức tại Việt Nam

Đầu tháng 12/2017, thông qua hệ thống của Cục An toàn thông tin (Cục ATTT) và một số kênh

thông tin, Cục ATTT đã phát hiện thông tin về việc lộ, lọt 41 GB dữ liệu liên quan đến các tài khoản thư điện tử. Đây là nguồn dữ liệu chứa thông tin tài khoản thư điện tử bị lộ, lọt lớn nhất từ trước đến nay, bao gồm cả những dữ liệu đã lộ, lọt trước đây.

Qua các biện pháp kỹ thuật ban đầu, Cục An toàn thông tin đã phát hiện và xác định có rất nhiều thông tin tài khoản thư điện tử của nhiều cơ quan tổ chức tại Việt Nam bao gồm: có 473.770 thông tin tài khoản thư điện tử của Việt Nam trong đó có1056 tài khoản tên miền .gov.vn; 806 tài khoản của các ngân hàng

Qua kiểm tra sơ bộ, Cục ATTT nhận thấy đây là những tài khoản có thể là tài khoản thư điện tử đang được sử dụng, tài khoản đăng ký trên các ứng dụng mạng xã hội, tài khoản ngân hàng .v.v... Đặc biệt, do thói quen người dùng thường dùng chung tên đăng nhập và mật khẩu trên các ứng dụng khác nhau bao gồm thư điện tử, mạng xã hội, tài khoản ngân hàng nên nguy cơ mất an toàn thông tin là rất lớn.

5. Nhiều laptop HP dính lỗi keylogger theo dõi bàn phím

HP thừa nhận 460 mẫu laptop của hãng chứa lỗi có thể bí mật ghi lại tất cả mọi thứ người dùng gõ trên bàn phím.

Một nhà nghiên cứu bảo mật vừa phát hiện ra lỗ hổng trong đoạn phần mềm được cài trên nhiều laptop khác nhau. Nó nằm ở phần mềm Synaptics, điều khiển đầu vào trackpad và bàn phím trên 460 mẫu laptop HP, bao gồm cả các phiên bản Pavilion, EliteBook và ProBook. Keylogger này có khả năng ghi lại mọi thứ bạn gõ trên máy tính (keystroke). Keylogger nếu nằm trong tay của hacker sẽ vô cùng nguy hiểm vì nó ghi và gửi keystroke có nguy cơ tiết lộ thông tin nhạy cảm của bạn như mật khẩu. Tuy nhiên là keylogger trong phần mềm Synaptics trên laptop HP mặc định vô hiệu hóa và hacker phải có quyền truy cập cấp quản trị viên mới kích hoạt được, đồng nghĩa hacker phải tiếp cận về mặt vật lý đối với một laptop.

Trên trang hỗ trợ khách hàng, HP khẳng định cả Synaptics và HP đều không truy cập dữ liệu khách hàng. Dù vậy, nếu đang dùng laptop HP, bạn vẫn nên lưu tâm đến vấn đề này. HP đã cung cấp danh sách tất cả mẫu máy bị ảnh hưởng cũng như bản vá lỗi để tải về. Nếu không biết máy đang dùng là mẫu nào, bạn có thể kiểm tra sticker dán trên máy có chứa mã số.

6. Tấn công mạng bằng mã độc đào tiền ảo sẽ bùng nổ trong năm 2018

Nhận định tấn công mạng thông qua các thiết bị IoT là một xu thế tất yếu và đã được minh chứng rõ qua thực trạng an ninh mạng năm nay, các chuyên gia Bkav cũng đưa ra dự báo tấn công vào thiết bị IoT sẽ tiếp tục phát triển mạnh trong năm 2018 tới.

Trong năm 2017, thiết bị kết nối Internet (IoT) như Router Wi-Fi, Camera IP... đã trở thành đích nhắm của các hacker, điển hình là sự bùng nổ các biến thể mới của mã độc Mirai, trong đó có biến thể nhắm mục tiêu đến Việt Nam. Bên cạnh đó, lỗ hổng Blueborne trong công nghệ kết nối không dây Bluetooth đẩy 8,2 tỷ thiết bị IoT trên toàn cầu sử dụng công nghệ này rơi vào vòng nguy hiểm. Hay KRACK, lỗ hổng cho phép hacker xâm nhập vào hầu hết mạng Wi-Fi mà không cần mật khẩu, khiến các thiết bị IoT có kết nối Wi-Fi đối mặt với cuộc tấn công mạng quy mô lớn chưa từng có.

Cũng trong báo cáo tổng kết tình hình an ninh mạng năm 2017 và dự báo xu hướng năm 2018 vừa phát ra chiều ngày 26/12, Bkav dự báo, năm 2018 sẽ tiếp tục chứng kiến sự bùng nổ các cuộc tấn công phát tán mã độc nhằm thu lợi bất chính như mã độc mã hóa tống tiền Ransomware, mã độc đào tiền ảo...

7. Nỗi ám ảnh mang tên Ransomware

17% người dùng tham gia chương trình đánh giá an ninh mạng 2017 của Bkav cho biết gặp phải sự cố dữ liệu bị mã hóa do mã độc tống tiền ransomware gây ra. Thống kê từ hệ thống giám sát virus của Bkav cũng cho thấy, 11,22% lượng email lưu chuyển trong năm 2017 là email phát tán ransomware. Như vậy cứ trung bình 100 email nhận được thì người sử dụng sẽ gặp 11 email chứa ransomware. Con số này đã giảm so với năm 2016, song vẫn là tỷ lệ cao.

Năm 2017 cũng chứng kiến sự bùng nổ của các ransomware lợi dụng lỗ hổng hệ điều hành để phát tán với tốc độ chóng mặt. Điển hình là mã độc WannaCry, lây nhiễm trên hàng trăm máy tính tại hơn 90 nước chỉ trong vài giờ. Tại Việt Nam, hơn 1.900 máy tính có chứa WannaCry và

hơn 52% máy tính tồn tại lỗ hổng có thể bị tấn công bởi mã độc này. Sau đó là sự xuất hiện của mã độc tống tiền Petya làm tê liệt hàng loạt ngân hàng, sân bay, máy ATM và nhiều doanh nghiệp lớn tại châu Âu. Tương tự, mã độc Bad Rabbit đã lan rộng trong hệ thống của ít nhất 200 tổ chức trên thế giới. Số tiền chuộc khổng lồ hacker kiếm được chính là nguyên nhân dẫn tới sự bùng nổ của loại mã độc nguy hiểm này.

8. Bản vá tháng 12 của Microsoft khắc phục 19 lỗ hổng quan trọng trên trình duyệt

Bản cập nhật Patch Tuesday tháng 12 của Microsoft giải quyết hơn 30 lỗ hổng, gồm 19 lỗ hổng nghiêm trọng ảnh hưởng đến trình duyệt Internet Explorer và Edge. Các lỗ hổng quan trọng là vấn đề lỗi bộ nhớ có thể bị khai thác để thực thi mã từ xa trên máy tính mục tiêu. Các lỗ hổng an ninh - hầu hết có liên quan đến công cụ viết script của trình duyệt - có thể bị khai thác bằng cách lừa mục tiêu truy cập một trang web tự tạo đặc biệt hoặc một trang web có chứa các quảng cáo độc hại.

CVE-2017-11927, chỉ được đánh giá "quan trọng", là một lỗi tiết lộ thông tin trong Windows "đưa chúng ta trở về những ngày đầu của Internet Explorer và các tập tin CHM". Vấn đề này ảnh hưởng đến bộ xử lý giao thức its:// của Windows - ITS, hoặc InfoTech Storage Format, định dạng lưu trữ được sử dụng trong các tệp CHM.

Theo Microsoft, chưa lỗ hổng nào bị khai thác trong thực tế hoặc được tiết lộ trước khi bản vá được phát hành.

9. 100 mật khẩu phổ biến nhất năm 2017

Theo thường niên, vào cuối năm công ty về dịch vụ bảo mật SplashData lại đưa ra danh sách top các mật khẩu phổ biến nhất. Dẫn đầu danh sách này là mật khẩu "123456" và đứng thứ hai là "Password". Đây là danh sách những mật khẩu phổ biến nhất vừa được thống kê từ hơn năm triệu mật khẩu đã bị rò rỉ trong năm 2017.

Mặc dù gặp phải việc mất dữ liệu thông qua các cuộc tấn công vào mật khẩu từ hacker trong nhiều năm. Nhưng năm 2016 và 2017, nhiều người dùng vẫn tiếp tục sử dụng mật khẩu yếu dễ dàng đoán ra để bảo vệ dữ liệu của mình. Ví dụ: "123456" và "Password" là hai mật khẩu phổ biến nhất mà SplashData đã đưa ra, bởi số lượng người sử dụng quá lớn.

Danh sách 100 mật khẩu phổ biến nhất trong năm 2017 được cung cấp tại địa chỉ sau: https://13639-presscdn-0-80-pagely.netdna-ssl.com/wp-content/uploads/2017/12/Top-100-Worst-Passwords-of-2017a.pdf

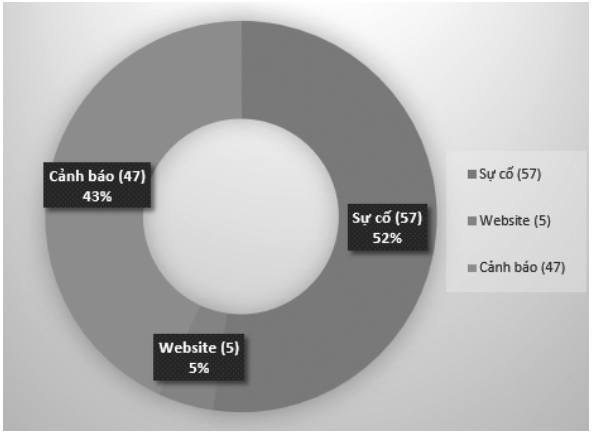
10. Chương trình quản lý mật khẩu trên Windows 10 dính lỗ hổng bảo mật do dùng plugin của bên thứ 3

Một nhà nghiên cứu tại Google có tên là Tavis Ormandy đã khám phá ra rằng bộ cài Windows 10 có đi kèm một trình quản lý mật khẩu bên thứ ba. Đó chính là Keeper, và nó có một lỗ hổng trên plugin trình duyệt, khiến cho các trang web độc hại có thể lấy trộm mật khẩu. Ormandy đã báo cáo lỗ hổng tới Keeper và hãng này đã phát hành bản vá 11.4 để khắc phục lỗi tại địa chỉ sau:

https://blog.keepersecurity.com/2017/12/15/update-for-keeper-browser-extension-v11-4/.

Keeper cũng cho biết họ chưa thấy có vụ tấn công thực tế nào.

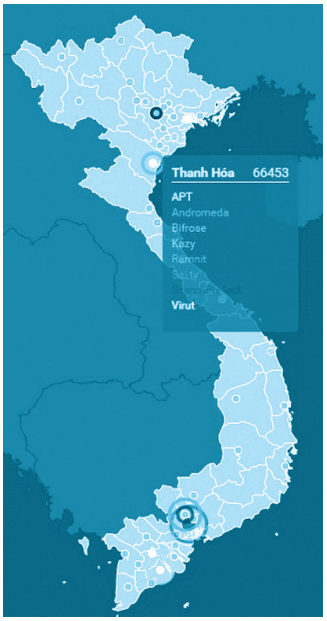
II. Tình hình An toàn thông tin trên địa bàn tỉnh



Trong quý IV, 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 62 lượt hỗ trợ, cảnh báo cho 47 đơn vị liên quan đến mã độc, Website và an toàn thông tin cho phần mềm dùng chung của tỉnh.

- Theo số liệu giám sát an toàn thông tin của nhà mạng Viettel, trên địa bàn tỉnh ghi nhận hơn 60.000 các lượt tấn công bao gồm các tấn công có chủ đích APT, các mã độc kết nối và tham gia vào mạng máy tính ma Botnet như Andromeda, Bifrose, Kazy, Ramnit, Sality... Trong số các địa phương, Thanh Hóa nằm trong số 10 tỉnh có tỉ lệ lây nhiễm mã độc cao nhất cả nước.

- Theo ghi nhận của Trung tâm An ninh mạng



và An toàn dữ liệu, trong quý 4 ghi nhận có 249 cuộc tấn công vào khai thác lỗ hổng ứng dụng Web và 35 cuộc tấn công chiếm đoạt quyền quản trị vào các dịch vụ đang hoạt động tại Trung tâm và 07 cuộc tấn công theo hình thức từ chối dịch vụ.

III. Công văn an toàn thông tin

- Ngày 19/12/2017, Cục An toàn Thông tin, Bộ Thông tin và Truyền thông ban hành công văn số683/CATTT-TĐQLGS về các biện pháp phòng, chống mã độc lây lan thông qua Facebook Messenger tại Việt Nam gửi tới cơ quan, tổ chức và người sử dụng.

- Ngày 26/12/2017 Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) ban hành công văn số 442/VNCERT-ĐPƯC về việc "lộ 1,4 tỷ tài khoản và mật khẩu từ các trang mạng xã hội, dịch vụ trực tuyến".

- Ngày 23/10/2017 Trung tâm CNTT&TT Thanh Hóa ban hành công văn số 216/TTCNTT&TT-QTHT về việc Cảnh báo Hệ thống thông tin lây nhiễm mã độc tham gia mạng bonet cho 06 cơ quan, đơn vị trên địa bàn tỉnh.

TIN HOẠT ĐỘNG

Trung tâm CNTT&TT Thanh Hóa tổ chức thi cấp Chứng chỉ ứng dụng Công nghệ thông tin đợt6năm 2017

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; Chứng chỉ được quy định tại Thông tư 03/2014/TT-2014 của Bộ Thông tin và Truyền thông.

Trong ngày 16 tháng 11 năm 2017, Trung tâm Công nghệ thông tin và truyền thông Thanh Hóa tổ chức kỳ thi sát hạch cấp Chứng chỉ công nghệ thông tin chuẩn cơ bản, đợt 6 năm 2017; Hội đồng thi được Sở Giáo dục và đào tạo thành lập gồm 14 người, bao gồm đầy đủ các Ban theo quy định về việc tổ chức thi và cấp chứng chỉ ứng dụng công nghệ thông tin tại Thông tư liên tịch số 17/2016/TTLT-BGDĐT-BTTT ngày 21 tháng 6 năm 2016 giữa Bộ Giáo dục và Đào tạo và Bộ Thông tin và Truyền thông.

Kỳ thi Đợt 6 năm 2017, có 55 thí sinh đăng ký dự thi và 55 thí sinh đã vượt qua 2 phần thi của mình là phần thi trắc nghiệm lý thuyết trực tuyến trên phần mềm và phần thi thực hành kỹ năng trên máy tính; toàn bộ hồ sơ về kỳ thi đã được gửi Sở 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 GDĐT 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

NGUYỄN TÌNH

VĂN BẢN MỚI

Ngày 15 tháng 11 năm 2017, Bộ Thông tin và Truyền thông ban hành Thông tư số 32/2017/TT-BTTTT Quy định về việc cung cấp dịch vụ công trực tuyến và bảo đảm khả năng và bảo đảm khả năng truy cập thuận tiện đối với trang thông tin điện tử hoặc cổng thông tin điện tử của cơ quan nhà nước

Theo đó, các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ; Tổng cục, Cục và cơ quan tương đương; UBND các tỉnh, thành phố trực thuộc Trung ương và các cơ quan chuyên môn trực thuộc; UBND các huyện, quận, thị xã, thành phố thuộc tỉnh khi xây dựng Cổng TTĐT hoặc Trang TTĐT phải đảm bảo những quy định về cung cấp dịch vụ công trực tuyến và bảo đảm khả năng truy cập thuận tiện đối với Cổng TTĐT hoặc Trang TTĐT của cơ quan Nhà nước.

Khi xây dựng Cổng TTĐT, Trang TTĐT và dịch vụ công trực tuyến của cơ quan Nhà nước phải định hướng theo nguyên tắc lấy người sử dụng làm trung tâm. Thực hiện các thủ tục hành chính nhanh gọn, giảm thiểu số lần mà người sử dụng phải đến cơ quan nhà nước trong một năm, bảo đảm thuận tiện cho người sử dụng.

Tại mục "Dịch vụ công trực tuyến" trên Cổng TTĐT của các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ; UBND các tỉnh, thành phố trực thuộc Trung ương phải thông báo đầy đủ, kịp thời toàn bộ danh sách dịch vụ công trực tuyến của cơ quan, của các đơn vị thuộc, trực thuộc. Các dịch vụ công trực tuyến phải tương ứng với toàn bộ các thủ tục hành chính của cơ quan và của các đơn vị thuộc, trực thuộc. Danh sách các dịch vụ công trực tuyến được phân loại theo ngành, theo lĩnh vực, theo cấp hành chính và thể hiện rõ mức độ của dịch vụ để thuận tiện cho việc tìm kiếm, sử dụng.

Dịch vụ công trực tuyến mức độ 3, mức độ 4 cần đạt được các yêu cầu chất lượng tối thiểu như: Dễ dàng tìm thấy dịch vụ sau tối đa 3 lần bấm chuột từ trang chủ của Cổng TTĐT; dễ dàng tìm được dịch vụ bằng các công cụ tìm kiếm phổ biến; tự động xác định các thông tin của người sử dụng, thông tin chuẩn của cơ quan Nhà nước; có hướng dẫn chi tiết cách sử dụng dịch vụ; bảo đảm thời gian xử lý, trao đổi dữ liệu nhanh dưới 10 giây; các dịch vụ công trực tuyến cần hoạt động liên tục 24 giờ trong tất cả các ngày;... Mỗi dịch vụ công trực tuyến mức độ 3, mức độ 4 phải cung cấp chức năng để người sử dụng có thể đánh giá sự hài lòng đối với dịch vụ sau khi sử dụng.

Ngoài ra, Thông tư cũng quy định rõ về điều kiện để đạt được các mức độ của dịch vụ công trực tuyến; quy định chung về thiết kế, xây dựng Cổng TTĐT, Trang TTĐT và dịch vụ công trực tuyến; giao diện, bố cục của Cổng TTĐT, Trang TTĐT; bảo đảm an toàn cho Cổng TTĐT, Trang TTĐT và dịch vụ công trực tuyến trong quá trình khai thác, vận hành;...

Thông tư có hiệu lực thi hành từ ngày 01/6/2018 và thay thế cho Thông tư số 26/2009/TT-BTTTT ngày 31/7/2019 của Bộ trưởng Bộ Thông tin và Truyền thông Quy định về việc cung cấp thông tin và bảo đảm khả năng truy cập thuận tiện đối với trang thông tin điện tử của cơ quan Nhà nước.

Ngày 11 tháng 12 năm 2017, Ủy ban nhân dân tỉnh Thanh Hóa ban hành Quyết định số 4764/QĐ-UBND về việc ban hành Quy chế quản lý, vận hành và khai thác sử dụng phần mềm quản lý văn bản và hồ sơ công việc trong các cơ quan hành chính nhà nước tỉnh Thanh Hóa

Theo đó, Quy chế được áp dụng cho các cơ quan hành chính nhà nước của tỉnh bao gồm UBND các cấp, các cơ quan chuyên môn trực thuộc UBND các cấp và cán bộ, công chức, viên chức trong các cơ quan hành chính nhà nước tham gia quản lý, vận hành và khai thác sử dụng phần mềm. Đồng thời, quy chế cũng áp dụng đối với các Cơ quan khác và các tổ chức chính trị xã hội trên địa bàn tỉnh Thanh Hóa được tham gia sử dụng phần mềm.

Hệ thống phần mềm quản lý văn bản và hồ sơ công việc là một thành phần trong hệ thống công nghệ thông tin tỉnh phục vụ công tác quản lý, điều hành tác nghiệp, trao đổi thông tin, chia sẻ dữ liệu trong nội bộ và giữa các cơ quan nhà nước trên địa bàn tỉnh với những chức năng cơ bản gồm: Quản lý văn bản đi, đến, chuyển nhận văn bản qua môi trường mạng; xử lý văn bản, giải quyết công việc thông qua hồ sơ công việc trên phần mềm; quản lý lịch công tác...

Văn bản đến do cơ quan, đơn vị khi tiếp nhận qua đường mạng và đường công văn khi cập nhật vào hệ thống gồm cả văn bản được số hóa bằng phương pháp quét (scan) và văn bản gốc của văn bản để thuận tiện trong quá trình khai thác, sử dụng, đồng thời phải sử dụng bộ mã tiếng Việt Unicode chuẩn TCVN 6909-2001 để trao đổi thông tin trong hệ thống. Văn bản do các cơ quan, đơn vị phát hành được trao đổi trên hệ thống phải đảm bảo tích hợp chữ ký số theo đúng các quy định tại Luật Giao dịch điện tử và các văn bản liên quan nhằm đảm bảo tính an toàn, bảo mật, tin cậy, xác thực của dữ liệu.

Quy chế cũng quy định rõ về quản lý phần mềm đối với Giám đốc các Sở; Trưởng các ban, ngành; Chủ tịch UBND cấp huyện; Chủ tịch UBND cấp xã và các đối tượng khác trong việc tham gia quản lý, vận hành và khai thác sử dụng phần mềm.

Quy chế có hiệu lực từ ngày 25/12/2017./.

NGUYỄN PHƯƠNG