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

Số 05
tháng 11/2017

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 11/2017

Tăng cường các giải pháp ngăn chặn, đẩy lùi thông tin xấu, độc trên Internet và mạng xã hội

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

Ngày nay, với sự phát triển như vũ bão của khoa học công nghệ - đặc biệt là công nghệ thông tin, cùng với sự phổ dụng của mạng Internet trong xu thế cuộc cách mạng công nghiệp lần thứ tư, có ngày càng nhiều thiết bị thông minh kết nối mạng giúp cho các tổ chức, cá nhân, địa phương đã và đang ứng dụng công nghệ thông tin vào mọi mặt của đời sống, góp phần nâng cao hiệu quả hoạt động, phục vụ phát triển kinh tế - xã hội, góp phần bảo đảm quốc phòng, an ninh của đất nước. Tuy nhiên, bên cạnh những mặt tích cực mà mạng Internet đem lại, thì trong thời gian gần đây, trên mạng Internet, nhất là mạng xã hội xuất hiện ngày càng nhiều thông tin xấu độc tuyên truyền, xuyên tạc chống phá Đảng, Nhà nước.

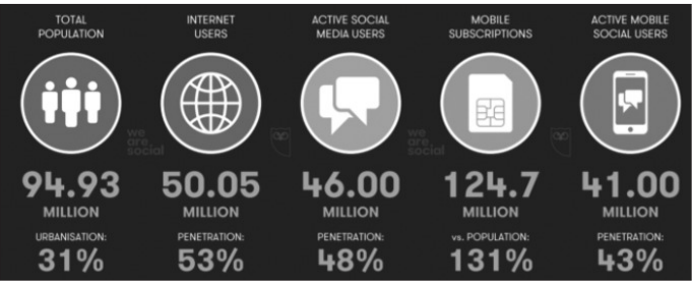
Tính hai mặt của mạng xã hội

Thông qua các phương thức giao tiếp có tính lan truyền nhanh trên môi trường mạng. Các thông tin, hình ảnh, clip có nội dung phản cảm liên quan đến mọi mặt của đời sống xã hội được các đối tượng có mục đích xấu cắt ghép, chỉnh sửa, kèm với các tiêu đề tên gọi mang tính "giật gân", "câu khách" nhằm gây sự chú ý và "lừa đảo" người dùng mạng xã hội. Các thông tin xấu độc tán phát trên internet và mạng xã hội là những thông tin bịa đặt, bóp méo sự thật, xuyên tạc vấn đề, "đổi trắng, thay đen", làm lẫn lộn đúng sai, thật giả; hoặc có một phần sự thật nhưng được đưa tin với dụng ý xấu, phân tích và định hướng dư luận bằng luận điệu sai trái, thù địch. Một số thông tin chưa được kiểm chứng, thông tin sai sự thật gây ảnh hưởng đến cá nhân, tổ chức; một số thông tin có những ngôn từ thô tục nội dung phản cảm, thậm chí soi mói, bình phẩm chủ quan chuyện đời tư của người khác, xúc phạm danh dự, nhân phẩm của nhiều cá nhân, gây bức xúc trong dư luận xã hội; vi phạm chuẩn mực đạo đức, văn hóa, thuần phong mỹ tục; kích động đồi trụy, bạo lực, bôi nhọ đời tư, vu khống...; Khá nhiều người lựa chọn mạng xã hội là nơi để bày tỏ quan điểm của cá nhân mình về người khác, nói xấu, công kích, miệt thị, người khác, thậm chí đưa thông tin sai lệch để vùi dập. Thông tin sai trái, độc hại có tính chất tội phạm như: Lừa đảo trên mạng, đánh cắp thông tin, mật khẩu, tán phát vi-rút...

Nguy hiểm và tinh vi hơn, gần đây, nhiều trang Facebook phản động đang giả dạng là những trang tin "tử tế" để tiếp cận người dùng, tăng số lượng người đăng ký theo dõi thường xuyên. Các trang này thường đưa những nội dung "câu view" nhằm "đánh lạc hướng" rồi đan cài những nội dung phục vụ ý đồ xấu của chúng. Người dùng phải thật hiểu biết mới phân biệt được thông tin xấu, độc này.

Theo thống kê của Bộ Thông tin và Truyền thông, tính đến 30/9/2017 tại Việt Nam, đối với 02 mạng xã hội Facebook và Youtube là 2 mạng

có đông người dùng Việt Nam sử dụng nhất, Facebook có khoảng 53 triệu thành viên, Youtube có khoảng 35 triệu thành viên tại Việt Nam. Trong đó theo nhận định của Bộ Trưởng Bộ Thông tin và Truyền thông thì: "Các thông tin tiêu cực như xuyên tạc, nói xấu, bôi nhọ, kêu gọi kích động biểu tình, chống phá nhà nước... chủ yếu tồn tại trên các mạng xã hội nước ngoài do nhận thức của người sử dụng cho rằng mạng xã hội là môi trường ảo nên có thể tự do phát ngôn mà không phải chịu trách nhiệm, gây ảnh hưởng đến tổ chức, cá nhân. Ngoài ra trước đây các trang mạng xã hội nước ngoài cung cấp dịch vụ tại Việt Nam nhưng gần như không bị điều chỉnh bởi các quy định của pháp luật Việt Nam dẫn đến tình trạng việc theo dõi, xử lý các thông tin vi phạm còn gặp khó khăn". Theo đó, Bộ Thông tin và Truyền thông đã phân loại thông tin độc hại gồm: *"Thông tin kích động chiến tranh, gây thù hằn dân tộc, đòi lật đổ chế độ. Thứ hai, thông tin độc hại xúc phạm nhân phẩm, danh dự cá nhân khi khai thác quá nhiều đời tư. Thứ ba, thông tin gây phương hại cho sức khỏe tính mạng, danh dự, nhân phẩm và tinh thần của con người".*



Thống kê hiện trạng sử dụng Internet tại Việt Nam (nguồn We Are Social - tháng 01/2017)

Tại phiên chất vấn của Quốc hội về lĩnh vực thông tin và truyền thông ngày 17/11/2017. Phó Thủ tướng Chính phủ Vũ Đức Đam đã phát biểu: "hiện trên thế giới có 7,5 tỷ người thì 52% dùng internet và 42% số đó dùng mạng xã hội; ở Việt Nam, con số lần lượt là gần 70% và 60%. Với số lượng người dùng lớn, thị trường internet ở Việt Nam lại gần như "của các công ty nước ngoài", với tỷ lệ từ trên 80% sử dụng dịch vụ của Google, Facebook, Yahoo...; chỉ riêng lĩnh vực trò chơi điện tử là các nhà cung cấp trong nước chiếm 60%".

Bên cạnh đó là các vấn đề liên quan đến an

Phó Thủ tướng Vũ Đức Đam phát biểu tại Quốc hội.

toàn thông tin trong tình hình hiện nay của Việt Nam: "Hiện về ứng dụng công nghệ thông tin thì Việt Nam đứng thứ 80 thế giới (mức trung bình), nhưng an toàn đứng trên 100 (trung bình yếu). Trong đó, chỉ số liên quan đến ý thức và hành vi của người dân thì Việt Nam thuộc nhóm yếu nhất trên thế giới. Trên thế giới cứ một giây có 176 sự cố liên quan đến an toàn an ninh thông tin, 3 cuộc tấn công mạng có chủ đích, có 4 mã độc được phát tán ra. Trong khi đó, Việt Nam đứng thứ trên 100 về an toàn thông tin nhưng một vài chỉ số đứng cuối cùng của thế giới. Đó là chỉ số tán phát thư rác từ Việt Nam. Cứ một giờ thì có 200 tỷ thư trên thế giới được phát đi, 53% trong số đó là thư rác, nhiều thư chứa mã độc. Và cứ 100 thư thì Việt Nam có 11,17%; Trung Quốc 12,4%; Mỹ 8,5%. Ở đây, nếu tính số người thì Việt Nam đứng số một, gấp 13,4 lần Trung Quốc và gần 8 lần Mỹ"

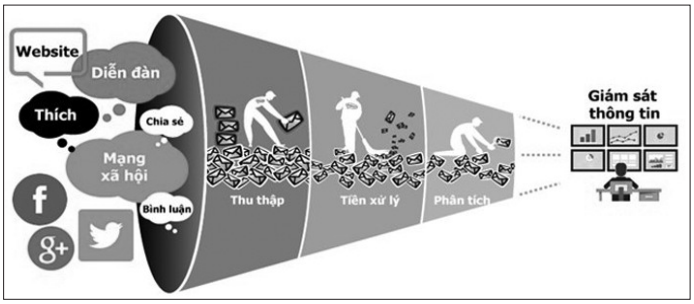
Những giải pháp ngăn chặn

Trong thời gian qua, Bộ TT&TT đã triển khai quyết liệt, đồng bộ các giải pháp nhằm tăng cường quản lý nội dung thông tin trên mạng, đấu tranh ngăn chặn các thông tin xấu độc, vi phạm pháp luật như: Tham mưu cho Quốc hội, Chính phủ ban hành, sửa đổi, bổ sung một số văn bản quy phạm pháp luật nhằm tăng cường quản lý Internet và thông tin trên mạng. Tăng cường xử lý các đối tượng có hành vi sai trái, phát ngôn thiếu chuẩn mực trên mạng xã hội.

Từ năm 2016 đến nay, Bộ TT&TT đã chỉ đạo các đơn vị chức năng tăng cường xử lý các đối tượng có hành vi sai phạm, phát ngôn thiếu chuẩn mực

trên mạng xã hội. Đối với trường hợp xác định được nhân thân của đối tượng vi phạm: tuỳ theo mức độ, Bộ TT&TT sẽ áp dụng hình thức xử lý kịp thời thông qua việc xử phạt vi phạm hành chính và biện pháp kỹ thuật, áp dụng theo quy định tại Nghị định số 174/2013/NĐ-CP ngày 13/11/2013 của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, công nghệ thông tin và tần số vô tuyến điện. Trường hợp vi phạm mức độ nhẹ thì nhắc nhở, rút kinh nghiệm, trường hợp vi phạm ở mức độ nặng có thể xem xét xử phạt vi phạm hành chính, thu hồi giấy phép, thu hồi tên miền...Trường hợp không xác định được nhân thân của tổ chức, cá nhân vi phạm, Bộ TT&TT yêu cầu các doanh nghiệp cung cấp dịch vụ như Google, YouTube, Facebook,... thực hiện các biện pháp ngăn chặn, gỡ bỏ theo quy định tại Thông tư số 38/2016/TT-BTTTT.

Ngoài ra, Bộ TT&TT cũng phối hợp chặt chẽ



Hệ thống kỹ thuật giám sát mạng xã hội.

với Bộ Công an để xác định hành vi, đối tượng và ngăn chặn, xử lý các trường hợp vi phạm ẩn danh tính hoặc đối tượng chống phá Đảng, Nhà nước. Tăng cường công tác thanh tra, kiểm tra và xử lý các hành vi vi phạm trên Internet và mạng xã hội. Chỉ đạo các cơ quan báo chí, truyền thông tăng cường tuyên truyền, nâng cao ý thức, trách nhiệm cho người sử dụng Internet và mạng xã hội.

Trong thời gian tới, Bộ trưởng Trương Minh Tuấn cho biết, Bộ sẽ tiếp tục hoàn thiện hệ thống văn bản pháp luật, đảm bảo môi trường pháp lý bình đẳng, minh bạch, kịp thời bổ sung, xây dựng các văn bản mới và xây dựng cơ chế chính sách về thông tin điện tử cho phù hợp với yêu cầu thực tiễn, đáp ứng hiệu quả quản lý, bổ sung các chế tài xử lý sai phạm nghiêm khắc hơn.

Nhận thức rõ vấn đề này, trong thời gian qua, với chức năng, nhiệm vụ được Chủ tịch UBND tỉnh, Giám đốc Sở Thông tin và Truyền thông giao cho Trung tâm Công nghệ thông tin và Truyền thông trong vai trò là cơ quan bảo đảm an toàn thông tin trên địa bàn tỉnh. Trung tâm đã tham mưu cho tỉnh triển khai các giải pháp nhằm hạn chế các nguy cơ gây mất an toàn thông tin nói chung cũng như chủ động ngăn chặn, đẩy lùi các thông tin xấu đốc trên môi trường mạng nói riêng, cụ thể như sau:

Một là: Để chủ động ngăn chặn, đẩy lùi thông tin xấu độc trên internet và mạng xã hội, đòi hỏi trước hết mỗi cán bộ công chức, viên chức, người lao động nói riêng và người dân tham gia mạng xã hội nói chung phải nhận biết được tính hai mặt của internet và mạng xã hội; nhận diện các thủ đoạn, nội dung thông tin xấu độc, tính chất nguy hại của nó đối với cá nhân và xã hội;

Hai là: Các cơ quan, ban ngành, đơn vị, địa phương cần tiếp tục chủ động, kịp thời cung cấp thông tin một cách đầy đủ, toàn diện cho người dân. Qua đó, trang bị kiến thức cần thiết để mỗi người có thể tự sàng lọc, tiếp nhận thông tin hữu ích, chính thống, đồng thời "miễn dịch" với những thông tin xấu độc làm nhiễu loạn môi trường xã hội.

Ba là: Cán bộ công chức, viên chức cần hạn chế việc sử dụng các tài khoản ứng dụng dùng chung như địa chỉ thư điện tử công vụ để đăng ký các dịch vụ trên mạng xã hội. Đồng thời, tăng cường công tác bảo đảm an toàn thông tin cho cá nhân và cơ quan, đơn vị như thực hiện nghiêm túc các biện pháp bảo đảm an toàn thông tin theo quy định; bảo vệ tài khoản thư điện tử, không để người khác sử dụng hộp thư cá nhân của mình; định kỳ thay đổi mật khẩu, bảo vệ thông tin cá nhân trên môi trường mạng,...

Bốn là: Triển khai đồng bộ các giải pháp kỹ thuật trong việc lắng nghe và phát hiện sớm các thông tin trên môi trường mạng, nhận biết các thông tin độc hại cũng như có các biện pháp phản ứng lại các thông tin đó. Qua đó giúp các cơ quan chức năng phát hiện thông tin theo từ khóa, để khoanh vùng đối tượng phát tán và hạn chế tối đa các thông tin lan truyền.

Kinh nghiệm triển khai các biện pháp đảm bảo an toàn thông tin mạng trên địa bàn tỉnh của Trung tâm CNTT&TT Sơn La

TRẦN THỊ LUYẾN
Giám đốc Trung tâm CNTT&TT Sơn La

Hiện nay cùng với việc đẩy mạnh ứng dụng CNTT, các nguy cơ về lộ, lọt, mất an toàn thông tin (ATTT) cũng ngày càng tăng và những hình thức tấn công trên mạng ngày càng đa dạng, tinh vi, nguy hiểm. ATTT đang là vấn đề nóng, và đang được nhiều nước trên thế giới, nhiều tổ chức và cộng đồng đặc biệt quan tâm. Theo thống kê của các chuyên gia CNTT cuối năm 2016 thì mỗi tháng ở Việt Nam có hơn 300 Website bị tấn công và 40% website có lỗ hổng bảo mật, và đó chỉ là bề nổi còn thực tế số lượng lớn hơn rất nhiều. Thống kê của VNCERT thì cho thấy chỉ trong nửa đầu năm 2016, tổng số sự cố an ninh mạng được VNCERT ghi nhận đã là 127.630 sự cố (gồm 8.758 sự cố Phishing, 77.160 sự cố Deface và 41.712 sự cố Malware), gấp hơn 4 lần so tổng sự cố an ninh mạng được trung tâm này ghi nhận trong năm 2015 và gấp gần 6,5 lần số sự cố diễn ra trong năm 2014.

Nhận thức được vấn đề này Trung tâm CNTT&TT tỉnh Sơn La, luôn coi việc đảm bảo ATTT, trong việc ứng dụng CNTT, là nhiệm vụ quan trọng ưu tiên hàng đầu, trong chiến lược phát triển CNTT và xây dựng chính quyền điện tử tại địa bàn tỉnh Sơn La.

Trong bối cảnh đó với vai trò là cơ quan chuyên ngành - Trung tâm CNTT&TT Sơn La, thường xuyên rà soát phối hợp với các đơn vị liên quan triển khai thực hiện các công tác đảm bảo ATTT trên địa bàn tỉnh. Trên cơ sở đó, những năm gần đây kết quả tình hình ATTT trên địa bàn tỉnh Sơn La tương đối ổn định. Cụ thể như sau:

Cổng thông tin điện tử Tỉnh Sơn La do Trung tâm CNTT&TT Sơn La phát triển và vận hành.

Về cơ chế pháp lý, chính sách

Ngày 21/6/2017, UBND tỉnh Sơn La đã ban hành "Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng Công nghệ thông tin của cơ quan nhà nước trên địa bàn tỉnh Sơn La". Trên cơ sở đó Trung tâm đã tham mưu cho Sở Thông tin và Truyền thông Sơn La ban hành "Quy định đảm bảo ATTT mạng trong hoạt động ứng dụng Công nghệ thông tin của Sở Thông tin và Truyền thông tỉnh Sơn La". Qua đó hoàn thiện nhằm tạo hành lang pháp lý, quy định cụ thể công tác đảm bảo ATTT mạng trong hoạt động ứng dụng CNTT tại các cơ quan, đơn vị.

Trung tâm tích hợp dữ liệu tỉnh Sơn La.

Hàng năm tổ chức đánh giá các tiêu chí đảm bảo an toàn thông tin, ứng dụng CNTT trong cải cách hành chính cho các sở ban ngành đơn vị trong tỉnh. Ban hành "Quy chế vận hành trung tâm tích hợp dữ liệu của tỉnh". Những quy chế này được ban hành nhằm hoàn chỉnh cơ sở pháp lý và hướng dẫn các cơ quan đơn vị thực hiện công tác đảm bảo an toàn, an ninh thông tin, phục vụ cho công tác điều hành quản lý nhà nước. Căn cứ những quy chế này các cơ quan, đơn vị trên địa bàn tỉnh triển khai, xây dựng quy chế nội bộ đảm bảo ATTT phù hợp với từng cơ quan đơn vị mình để áp dụng.

Mặt khác, với vai trò và chức năng nhiệm vụ được giao, Trung tâm luôn đảm bảo công tác tuyên truyền phổ biến các văn bản có liên quan về an toàn an ninh thông tin trong việc ứng dụng CNTT đến đúng đối tượng và kịp thời, nhằm giúp các cơ quan, đơn vị ứng phó đối với các sự cố mất ATTT.

Về giải pháp, biện pháp kỹ thuật.

Đối với hệ thống thông tin dùng chung của tỉnh bao gồm (Cổng thông tin điện tử, thư điện tử công vụ, một của điện tử) được xây dựng theo các tiêu chuẩn, quy chuẩn kỹ thuật và hướng dẫn của bộ Thông tin và Truyền thông. Hàng năm được xây dựng kế hoạch bảo dưỡng, nâng cấp nhằm cập nhật kỹ thuật kịp thời từng bước hoàn chỉnh theo tiêu chuẩn ATTT.

Về con người.

Trung tâm CNTT&TT luôn tâm niệm con người là yếu tố quan trọng nhất, luôn coi việc đào tạo, tập huấn, bồi dưỡng các cán bộ phụ trách về CNTT, tại các sở, ban, ngành về ATTT là ưu tiên. Sở Thông tin Truyền thông Sơn La cũng mở nhiều lớp tập huấn về bảo mật và ATTT, các kỹ năng cho cán bộ quản trị hệ thống.

Công tác hỗ trợ xử lý sự cố của Trung tâm CNTT&TT Sơn La.

Về công tác kiểm tra đánh giá.

Sở TTTT Sơn La chủ trì phối hợp các đơn vị liên quan tổ chức thường xuyên những cuộc kiểm tra đánh giá công tác đảm bảo ATTT, của các cơ quan, đơn vị. Mục tiêu nhằm kiểm tra tình hình đảm bảo ATTT tại các cơ quan, đơn vị, trên địa bàn như pháp lý, chính sách, biện pháp kỹ thuật. Từ kết quả đã kiểm tra Sở TTTT giao cho TTCNTT, hướng dẫn các cơ quan, đơn vị, giải pháp, biện pháp kỹ thuật triển khai nhằm từng bước hoàn thiện các vấn đề ATTT, cho hệ thống thông tin.

Gần đây, vấn đề các tin tặc liên tiếp tấn công vào các website Việt Nam, đặc biệt là các website có tên miền đuôi .gov.vn, nhằm chống phá và thực hiện các mục đích trính trị. Để đảm bảo an toàn các Website của tỉnh, Trung tâm CNTT&TT Sơn La thường xuyên rà soát các lỗ hổng bảo mật, các website cơ quan, đơn vị (tên miền sonla.gov.vn) trên địa bàn tỉnh. Kịp thời vá lỗi đảm bảo an toàn an ninh thông tin.

Các giải pháp kỹ thuật bảo đảm an toàn thông tin cho hệ thống mạng của các cơ quan, đơn vị trên địa bàn tỉnh

NGÔ PHƯƠNG
Trung tâm CNTT&TT Thanh Hóa

Ngày nay, an toàn thông tin có ý nghĩa hết sức quan trọng đối với người sử dụng công nghệ thông tin nói chung và cán bộ, công chức viên chức nói riêng. Các nguy cơ mất an toàn thông tin mạng không chỉ ảnh hưởng đến các cơ quan, tổ chức và cá nhân mà còn tác động mạnh mẽ đến sự phát triển và ổn định của xã hội.

Trong những năm qua, các cơ quan trên địa bàn tỉnh đã và đang tăng cường các biện pháp để đảm bảo an toàn thông tin (ATTT) cho các mạng công nghệ thông tin (CNTT) từ chính sách, quy trình kỹ thuật đến con người. Nhiều cơ quan, đơn vị đã trang bị nhiều thiết bị, công nghệ ATTT hiện đại như: Tường lửa (Firewall), mã hóa và mạng riêng ảo (VPN)... nhằm phòng chống và đối phó hiệu quả với các nguy cơ và hiểm họa mất ATTT đang ngày càng gia tăng. Tuy nhiên, cũng còn nhiều hệ thống CNTT tại các cơ quan, tổ chức và doanh nghiệp chưa được quan tâm trong công tác an toàn và bảo mật, dẫn đến các vụ việc mất an toàn thông tin, tồn tại nguy cơ bị phần tử xấu xâm nhập, khai thác, lấy cắp thông tin, bí mật nhà nước...

Đặc biệt trong thời gian qua, Trung tâm CNTT&TT qua công tác giám sát tình hình ATTT đã gửi các cảnh báo tới các cơ quan trên địa bàn tỉnh có hệ thống thông tin tham gia vào mạng máy tính ma Botnet. Tuy nhiên việc khắc phục và xác định những máy tính bị nhiễm mã độc trong hệ thống mạng của các cơ quan vẫn chưa được thực hiện một cách triệt để. Trước thực trạng trên đối với hệ thống CNTT của các cơ quan, tổ chức cần một giải pháp có khả năng thu thập, lưu trữ và xử lý các sự kiện để đưa ra các cảnh báo về các mối đe dọa mà họ đang phải đối mặt, từ đó xây dựng kế hoạch ngăn chặn và xử lý. Đó chính là các giải pháp thực hiện chức năng giám sát, cảnh bảo, phát hiện xâm nhập giúp đảm bảo an toàn thông tin cho hệ thống mạng LAN.

Bài viết này giới thiệu một số giải pháp dựa trên phần mềm nguồn mở thực hiện các chức năng hỗ trợ trong việc giám sát, phân tích và ngăn chặn các nguy cơ gây mất an toàn thông tin trong hệ thống thông tin của các cơ quan đơn vị trên địa bàn tỉnh.

1. Hệ thống giám sát hoạt động của các trang thiết bị trong hệ thống mạng

a. Mục tiêu

Một trong những công việc cơ bản của người quản trị là giám sát hạ tầng mạng CNTT. Giám sát mạng là kiểm tra tình trạng thông số dữ liệu của hệ thống hạ tầng mạng

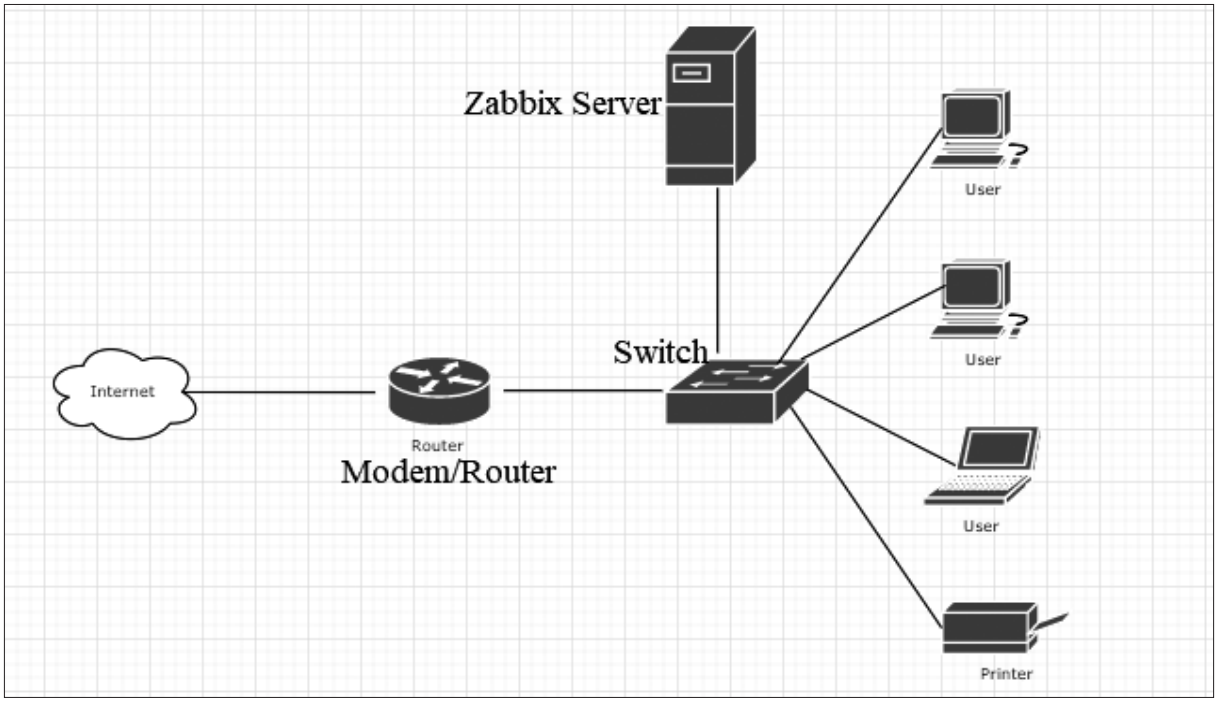
Phần mềm sử dụng các phương pháp cảnh báo linh hoạt, cho phép người quản lý cấu hình cảnh báo dựa trên email cho hầu hết các số liệu báo cáo, sự kiện xảy ra, cho phép chúng ta nắm bắt nhanh các sự cố xảy ra của thiết bị mạng (server, router, swich,...). Ngoài ra, còn hỗ trợ chức năng báo cáo, tổng hợp và dự đoán dữ liệu tốt dựa trên những dữ liệu có sẵn đã được lưu trữ.

Qua phần mềm giám sát này giúp lãnh đạo, người quản lý biết tất cả thông tin của hệ thống để nâng cấp và mở rộng hệ thống khi cần thiết; Giám sát được hầu hết các thiết bị mạng, các ứng dụng dịch vụ (SMTP, POP3,HTTP, FTP,...); Phát hiện sự cố, phát hiện tấn công nhanh chóng đưa ra cảnh báo cho người quản lý..

Hệ thống có thể tìm và giúp giải quyết việc lỗi trang web, hoạt động của người truy vấn và truyền tải file, nguyên nhân do quá tải, sự cố server, switch, firewall, kết nối mạng bị trễ hoặc các sự cố liên quan đến các thiết bị khác.

b. Triển khai

- Mô hình mạng khi triển khai:
- Yêu cầu:

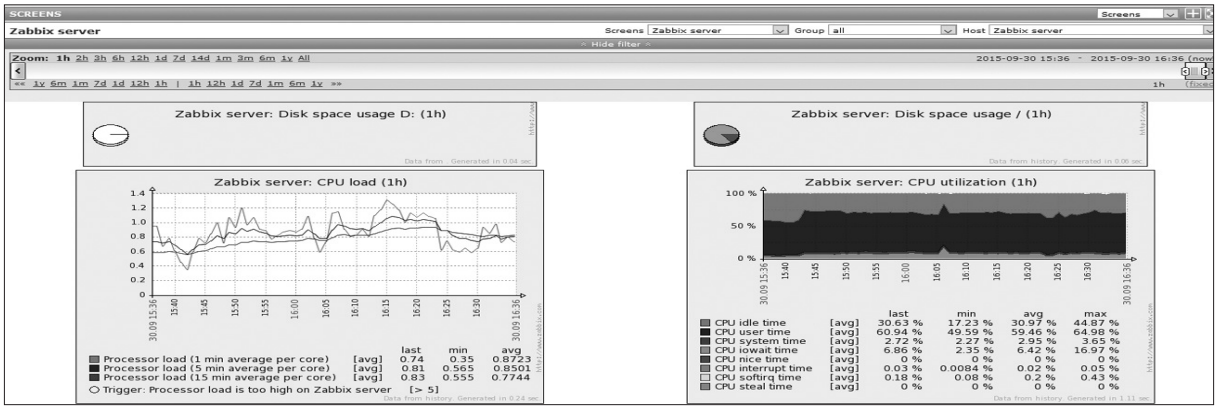


Zabbix Server: Máy chủ giám sát cài đặt phần mềm Zabbix
Switch, Server, firewall,PC, Laptop....: Thiết bị cần giám sát

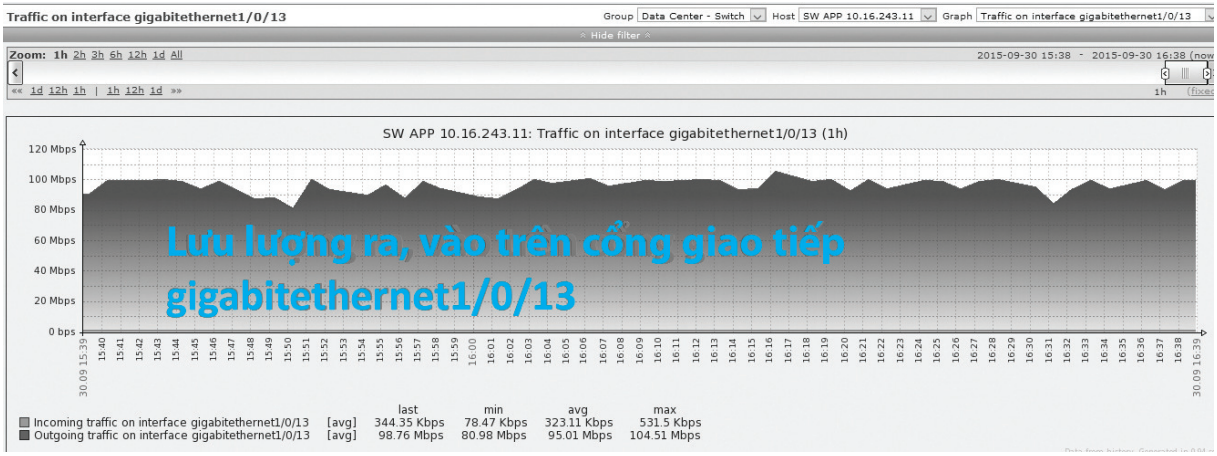
d. Kết quả:

- Giao diện đăng nhập phần mềm:

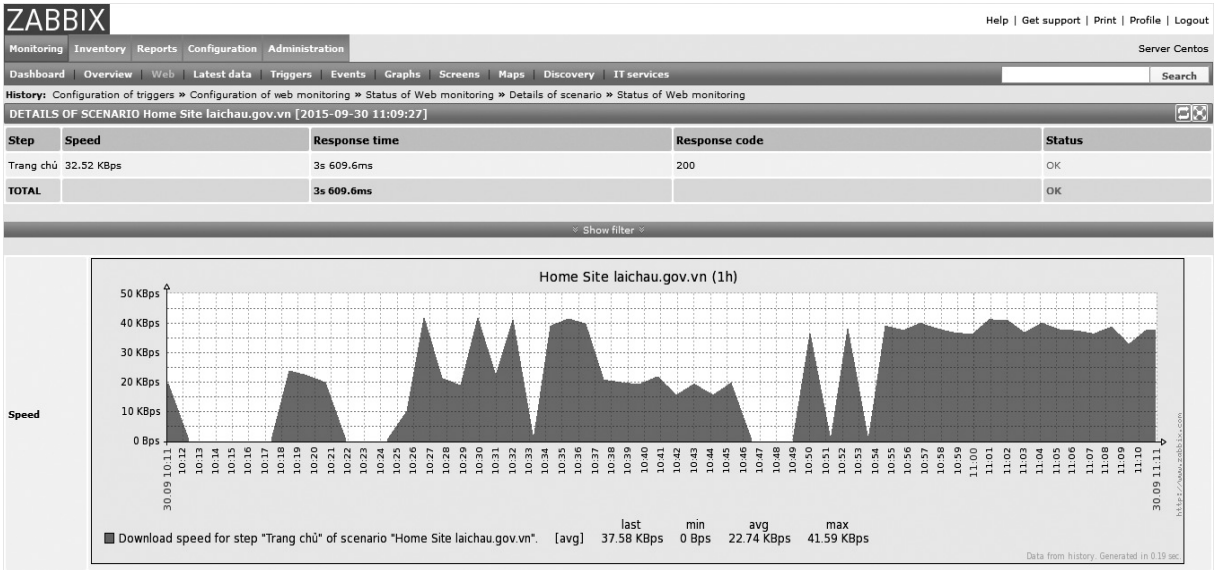
- Giám sát hoạt động của máy chủ: CPU, RAM, HDD, Network,....



- Giám sát băng thông mạng trên các thiết bị



- Giám sát hoạt động của Website



- Báo cáo

Host	Trigger	Severity	Number of status changes
Website laichau.gov.vn	Website laichau.gov.vn Trang chủ xảy ra sự cố	High	551
Zabbix server	Disk I/O is overloaded on Zabbix server	Warning	54
SW OFF 10.16.243.49	Operational status was changed on SW OFF 10.16.243.49 interface gigabitet	Information	32
mail.laichau.gov.vn	Processor load is too high on mail.laichau.gov.vn	Average	32
Website thongtindoingoai.laichau.gov.vn	Website thongtindoingoai.laichau.gov.vn không truy cập được	High	12
W_APP02 10.16.11.36	Zabbix agent on W_APP02 10.16.11.36 is unreachable for 5 minutes	Average	2
W_POT01 10.16.20.32	Free disk space is less than 20% on volume C:	Warning	1
W_POT01 10.16.20.32	Free disk space is less than 20% on volume D:	Warning	1
W_POT01 10.16.20.32	Host information was changed on W_POT01 10.16.20.32	Average	1

2. Hệ thống tường lửa ngăn chặn các truy cập vào hệ thống mạng

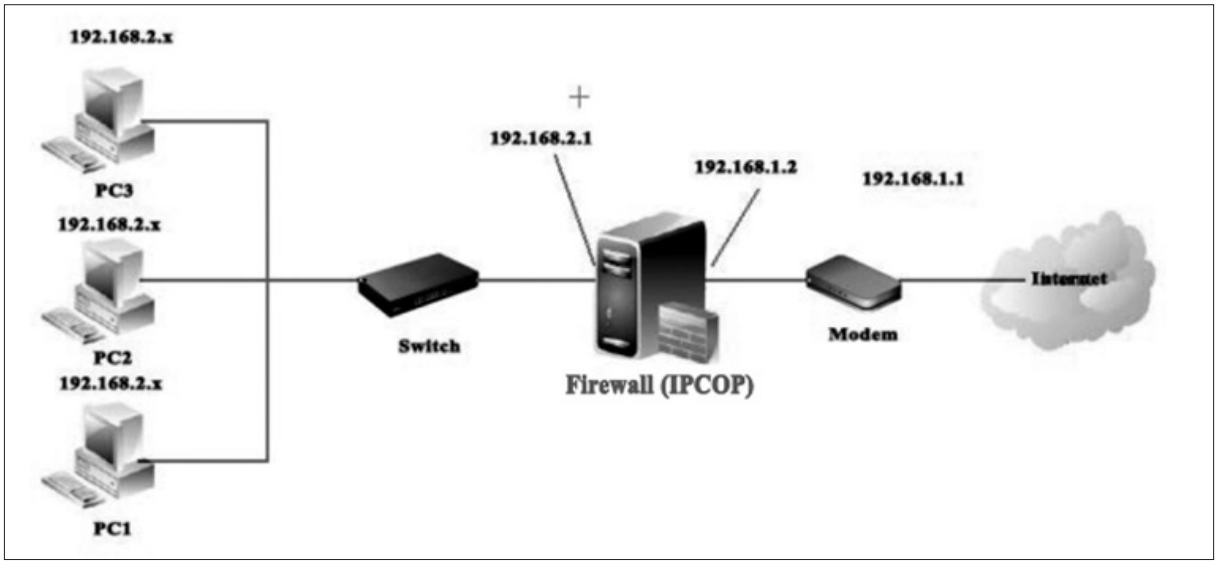
a. Mục tiêu

Trong trường hợp hệ thống mạng chưa có thiết bị Firewall cứng, các cơ quan, đơn vị có thể triển khai giải pháp nguồn mở trên 01 máy PC có cấu hình cơ bản để thực hiện các chức năng của một thiết bị ngăn chặn các kết nối đến các địa chỉ và IP xác định.

Thông qua chức năng nhật ký của hệ thống và danh sách các địa chỉ cần chặn, quản trị mạng có thể dễ dàng xác định và cô lập được máy trạm trong hệ thống mạng của đơn vị đang bị lây nhiễm mã độc và kết nối đến mạng máy tính ma botnet.

b. Triển khai

- Mô hình mạng khi triển khai:

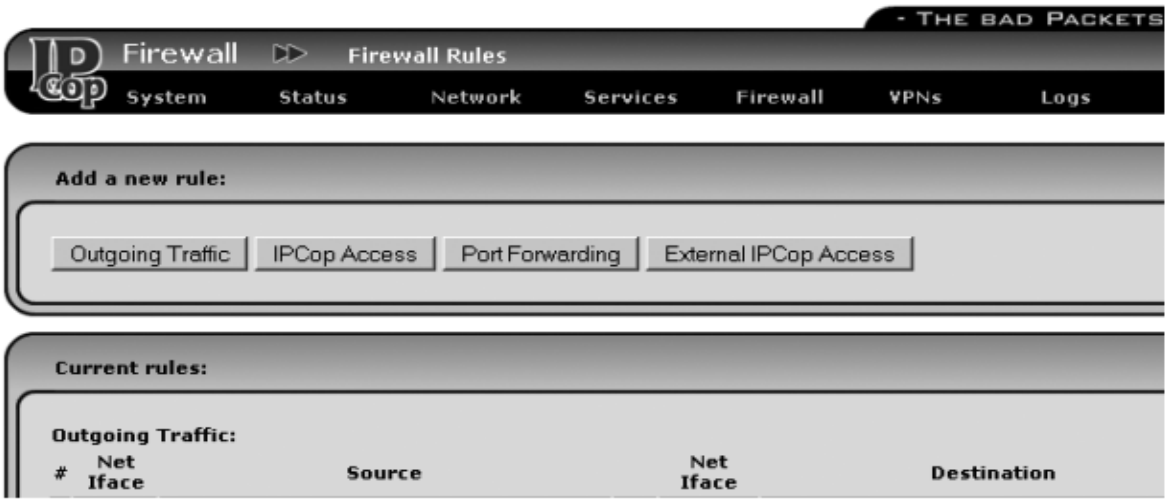


- Yêu cầu

01 máy PC có cấu hình thông thường, có 02 card mạng cài đặt phần mềm nguồn mở IPCOP thực hiện chức năng như một thiết bị Firewall.

c. Kết quả:

- Chặn địa chỉ liên kết đến hacker hoặc mạng máy tính ma thông qua địa chỉ IP hoặc tên miền



- Khoanh vùng và xác định máy bị nhiễm mã độc

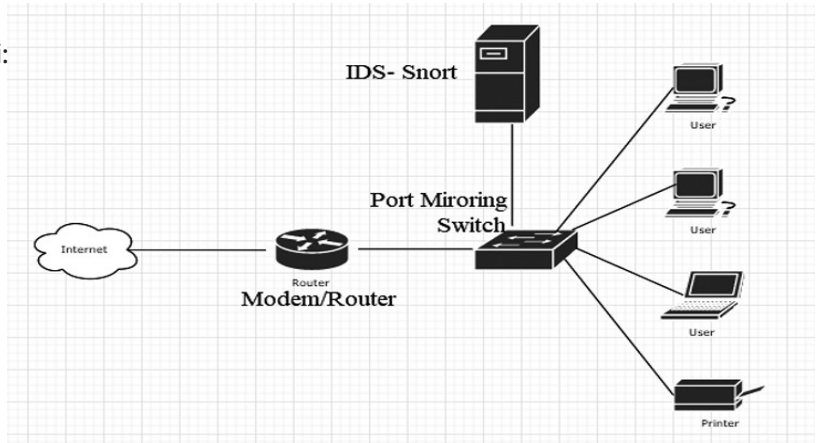
12:48:41	RED DROP	wan-1	IGMP	192.168.1.1	-	90:f6:52:a3:19:b8	224.0.0.1
12:50:46	RED DROP	wan-1	IGMP	192.168.1.1	-	90:f6:52:a3:19:b8	224.0.0.1
12:52:51	RED DROP	wan-1	IGMP	192.168.1.1	-	90:f6:52:a3:19:b8	224.0.0.1
12:54:34	GREEN DROP	lan-1	ICMP	192.168.2.174	-	00:0c:29:9e:f4:65	203.210.142.132
12:54:40	GREEN DROP	lan-1	ICMP	192.168.2.174	-	00:0c:29:9e:f4:65	203.210.142.132
12:54:45	GREEN DROP	lan-1	ICMP	192.168.2.174	-	00:0c:29:9e:f4:65	203.210.142.132
12:54:51	GREEN DROP	lan-1	ICMP	192.168.2.174	-	00:0c:29:9e:f4:65	203.210.142.132
12:54:56	RED DROP	wan-1	IGMP	192.168.1.1	-	90:f6:52:a3:19:b8	224.0.0.1
12:54:56	GREEN DROP	lan-1	ICMP	192.168.2.174	-	00:0c:29:9e:f4:65	203.210.142.132
12:55:02	GREEN DROP	lan-1	ICMP	192.168.2.174	-	00:0c:29:9e:f4:65	203.210.142.132
12:55:07	GREEN DROP	lan-1	ICMP	192.168.2.174	-	00:0c:29:9e:f4:65	203.210.142.132
12:57:01	RED DROP	wan-1	IGMP	192.168.1.1	-	90:f6:52:a3:19:b8	224.0.0.1
12:59:06	RED DROP	wan-1	IGMP	192.168.1.1	-	90:f6:52:a3:19:b8	224.0.0.1

3. Hệ thống phát hiện và ngăn chặn tấn công vào hệ thống mạng

Hệ thống giám sát phát hiện xâm nhập (IDS-Intrusion Detection System) là một phương pháp bảo mật có khả năng phát hiện các kiểu tấn công mới. Trên thị trường hiện nay, có rất nhiều thiết bị IDS/IPS tuy nhiên các thiết bị này có giá thành khá cao và chi phí duy trì bản quyền hàng năm rất tốn kém. Một trong những phần mềm IDS phổ biến hiện nay là Snort. Đây là một sản phẩm NIDS (Network-based IDS) mã nguồn mở với hệ thống signature database (được gọi là rule database) được cập nhật thường xuyên bởi nhiều thành viên trong cộng đồng Internet. Hệ thống IDS-SNORT thu thập các thông tin trên các thành phần của hệ thống, phân tích các thông tin, dấu hiệu nhằm đánh giá và đưa ra các cảnh báo sớm cho người quản trị hệ thống.

b. Triển khai

- Mô hình mạng khi triển khai:



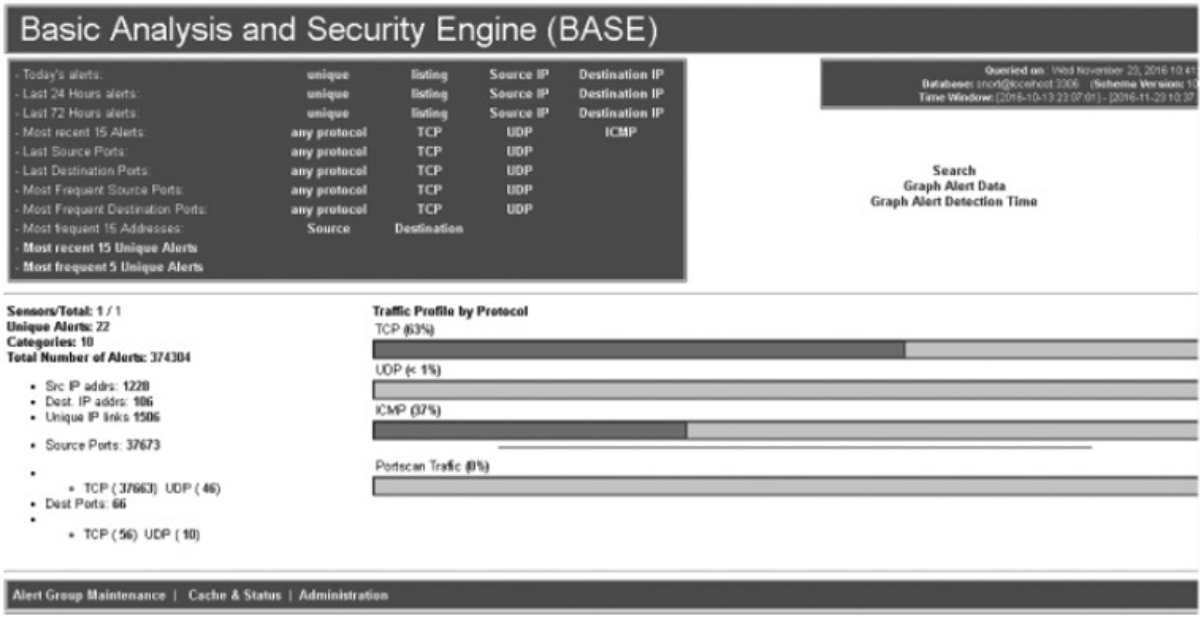
- Yêu cầu

01 máy PC có cấu hình mạnh, cài đặt phần mềm nguồn mở Snort thực hiện chức năng như một thiết bị IDS

+ Thiết bị chuyển mạch (Switch) có hỗ trợ cổng Miroring giám sát lưu lượng vào/ra trên hệ thống mạng.

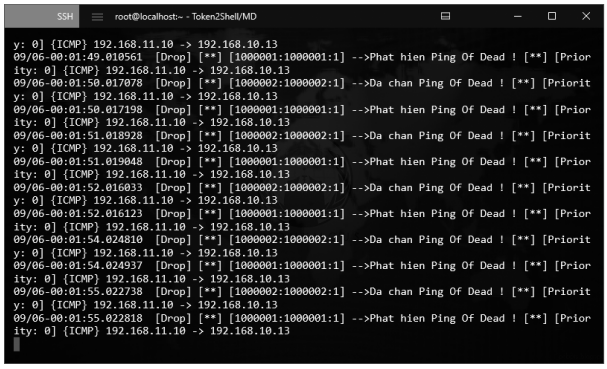
c. Kết quả:

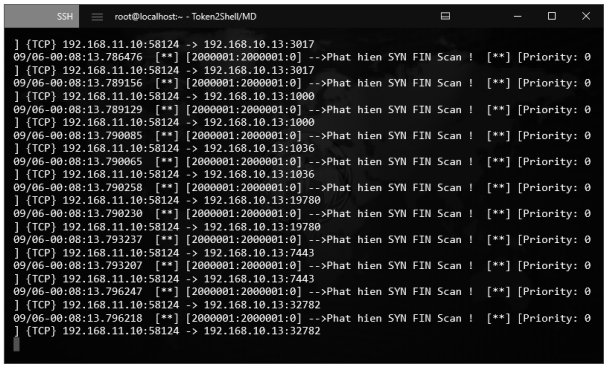
- Giao diện đăng nhập trên phần mềm



- Giám sát lưu lượng truy cập

- Phát hiện cảnh báo truy cập, tấn công dựa theo các luật được thiết lập sẵn





Trên đây là một số giải pháp kỹ thuật nhằm mục đích tăng cường khả năng bảo đảm an toàn thông tin trên hệ thống mạng của các cơ quan, đơn vị trên địa bàn tỉnh. Trong quá trình triển khai, áp dụng tại các cơ quan, đơn vị tùy thuộc vào mô hình mạng và mục đích của từng cơ quan, vui lòng liên hệ với Tổ Ứng cứu sự cố của Trung tâm CNTT&TT để được hỗ trợ.

Thông tin liên hệ:
Điện thoại: (0237) 3718699;
Fax (0237) 3718299.
Email: ungcuusuco@thanhhoa.gov.vn

HƯỚNG DẪN PHÁT HIỆN VÀ XỬ LÝ WEBSITE BỊ TẤN CÔNG

LÊ VĂN HUYÊN
Phó Trưởng phòng Quản lý Viễn thông
Sở Thông tin và Truyền thông Thanh Hóa

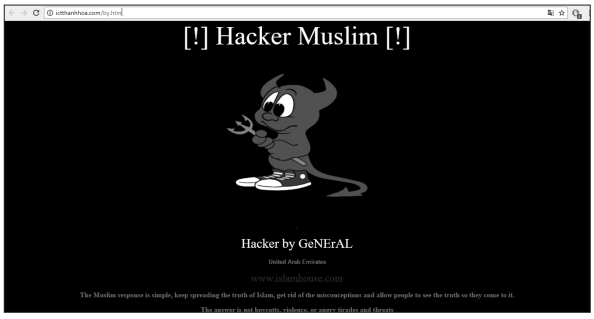
Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) ghi nhận đã có 9964 sự cố tấn công vào hệ thống mạng tại Việt Nam trong 9 tháng vừa qua. Các cuộc tấn công bao gồm cả 3 loại hình Phishing, Malware và Deface. Trong đó, tấn công bằng mã độc (malware) phát tán chiếm nhiều nhất với 4595 lần, tức hơn 46% tổng số các cuộc tấn công. Trong số các nạn nhân của loại hình malware này có 16 website có tên miền "gov.vn."

Trong tháng 11/2017, Trung tâm VNCERT ghi nhận 597 sự cố tấn công mạng vào các website tại Việt Nam, gồm 248 sự cố Phishing (tấn công lừa đảo), 232 sự cố Deface (tấn công thay đổi giao diện) và 117 sự cố Malware (cài mã độc).

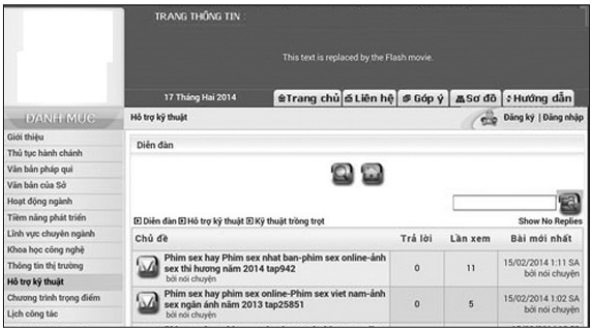
Đây là vấn đề nghiêm trọng và cần có phương án giải quyết triệt để. Rất nhiều website bị tấn công cho đến nay vẫn chưa khắc phục hoặc có những website bị tấn công mà quản trị không biết. Dưới đây là một số hướng dẫn cho các quản trị website nhằm phát hiện sớm nhất tình trạng website của mình đã hoặc đang bị tấn công để đưa ra phương án khắc phục kịp thời và triệt để.

Những dấu hiệu khi website bị tấn công

(1) Website bị thay đổi giao diện "Trang chủ" hoặc một đường dẫn tới một trang con của website bị tin tặc thay đổi giao diện. Xuất hiện nhiều dòng chữ được hacker chèn vào website, kiểu như: "**hacked by...**", "**God verify...**", "**security is low**"... Điều đó thể hiện website đã bị tin tặc hack thành công và chiếm hoàn toàn quyền điều khiển. Một mẹo nhỏ để phát hiện các đường dẫn mà tin tặc gửi lên là bạn có thể tìm kiếm trên Google theo cú pháp như sau: "**site.gov.vn hacked**" (với **site.gov.vn** là tên miền website của bạn).

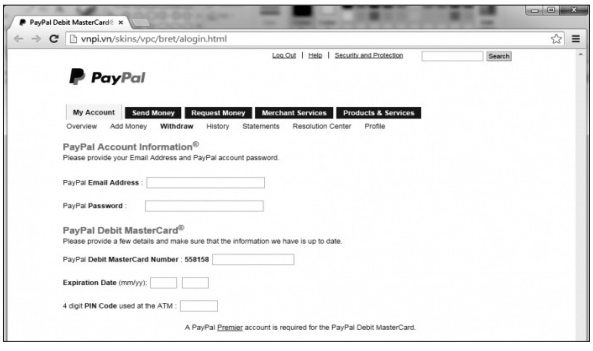


(2) Website bị chèn các đường dẫn tới các website khác mà bạn không biết, chèn các đoạn mã HTML để tăng truy cập cho các website khác, tồn tại nhiều đường dẫn tới các website chứa nội dung do tin tặc thiết lập...



Nên thường xuyên và định kỳ kiểm tra các backlink (đường dẫn tới website khác) trên website của mình hoặc thực hiện viewsource của website (Ấn chuột phải trên trang web / chọn viewpage source / Rà soát nội dung nguồn HTML của website để phát hiện đường dẫn lạ).

(3) Website bị chèn các đường dẫn giả mạo các website danh tiếng khác (giả mạo website của ngân hàng, giả mạo website giao dịch trực tuyến, giả mạo website Facebook, Gmail...). Các đường dẫn này được sử dụng để lừa đảo và chiếm tài khoản của người dùng.



(4) Trang web bị tự động đăng các tin tức Spam, các tin tức trái phép lên website.

(5) Các hệ thống hay các module giám sát thông báo rằng nhiều tệp tin trên website đã bị thay đổi nội dung.

(6) Phát hiện website của mình thường xuyên gửi các yêu cầu HTTP đến các website khác...

(7) Phát hiện các tệp tin, đoạn mã độc hại trên website, các tệp tin có chữ nhiều đoạn mã đã được mã hóa.

(8) Bị cảnh báo blacklist bởi Google, Bing, McAfee; Cảnh báo trong kết quả search Google

Xử lý khi website bị tấn công

(a) Xác định nguyên nhân

Để xác định được rõ nguyên nhân thì cần điều tra cụ thể trong từng trường hợp, nhưng website bị hack thông thường do những nguyên nhân sau:

- Đặt mật khẩu quản trị quá yếu, thiếu cơ chế chống brute force khiến kẻ tấn công có thể dò password admin, hoặc để lộ mật khẩu trong quá trình sử dụng

- Cài đặt các theme, module, plugin, extension,... không rõ nguồn gốc, kém an toàn

- Dùng mã nguồn phiên bản cũ với nhiều lỗi bảo mật, hacker có thể tấn công và khai thác lỗi

- Tấn công local attack tại các server share hosting

(b) Kiểm tra và xử lý

Bước 1: Cách ly, cô lập website

Trước tiên cần sao lưu (backup) lại trạng thái của website để phục vụ các bước điều tra sau này. Bạn hãy liên hệ ngay với nhà cung cấp để được hỗ trợ kiểm tra, cung cấp các bản backup.

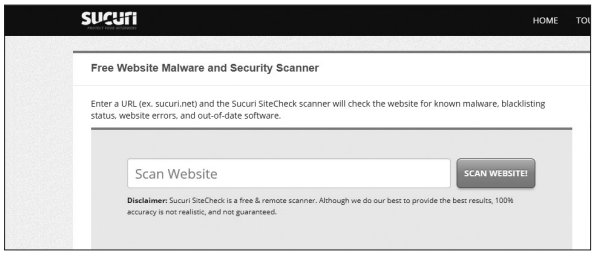
Có thể thay thế trang chủ bởi nội dung *"Website đang được bảo trì và nâng cấp, Xin vui lòng quay lại sau!"* hoặc chặn tất cả các kết nối đến website sử dụng firewall hoặc .htaccess.

Tiếp đó cần kiểm tra lại các tài khoản trên hệ thống xem hacker có tạo mới tài khoản không, nếu có thì xóa các tài khoản đó đi, đồng thời thực hiện thay đổi tất cả các thông tin tài khoản hiện tại bao gồm: tài khoản website, tài khoản kết nối CSDL, phpmyadmin, tài khoản quản lý hosting, FTP, encryption key...

Bước 2: Khôi phục lại hoạt động của website bị tấn công

Trong trường hợp có bản sao lưu của mã nguồn hoàn chỉnh, có thể tải bản mới lên bản mã nguồn mới cho website, trong trường hợp không có cần thực hiện xóa bỏ các dấu hiệu mà hacker đã để lại.

Có thể sử dụng công cụ của ***Sucuri*** để phát hiện các mã độc mà hacker đã chèn vào wesite của, tại đây. (*https://sitecheck.sucuri.net/*)



Bước 3: Tìm và loại bỏ các mã độc, backup, webshell đang tồn tại trên hệ thống

Hacker thường để lại mã độc trên website của bạn theo 03 hình thức sau:

- Chèn code mã độc vào các tệp tin trên website bị tấn công.

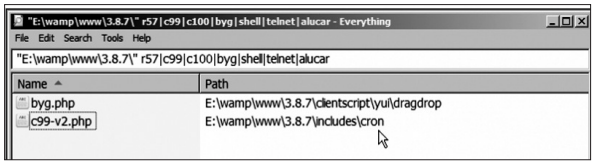
- Tải các tệp tin webshell, backdoor lên website để có thể kiểm soát website thông qua backdoor này.

- Cài đặt chương trình độc hại chạy ngầm, mở cổng để hacker truy cập vào trong lần sau.

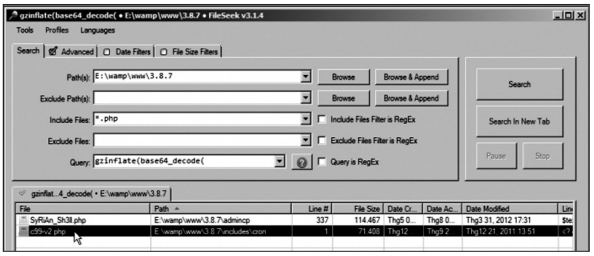
Để phát hiện các webshell, backdoor cần tìm và quét toàn bộ thư mục web của mình để phát hiện. Có thể sử dụng một số công cụ tìm kiếm: FileSeek, Everything, Webshell Detector...

Các file backdoors hacker để lại thường có tên gần giống với mã nguồn của website và nếu là mã nguồn php thì thường chứa các hàm PHP sau:

base64	passthru
base64_decode	create_function
gzinflate(base64_decode,	system
eval(gzinflate(base64_decode,	assert
eval(base64_decode	show_source
gzuncompress	proc_open
eval	stripslashes
exec	preg_replace (with /e/)
shell_exec	move_uploaded_file
pcntl_exec	



Để phát hiện các mã độc hại được nhúng và mã nguồn website, cần tìm và kiểm tra tất cả các



tệp tin có ngày thay đổi (date modified) xung quanh thời điểm tấn công. Rất có thể hacker đã chèn các mã độc vào các tệp tin bình thường của hệ thống.

Ngoài ra có thể đọc trong Log access để biết các backdoor mà hacker đã truy cập vào trước thời gian mà website bị tấn công.

Với các tiến trình mã độc trên website, cần thực hiện một cuộc điều tra về các tiến trình đang hoạt động, các tiến trình cho phép khởi động cùng hệ điều hành, các tiến trình được cài đặt để chạy theo lịch trong Crontab. Từ đó phát hiện ra các tiến trình độc hại trên máy chủ.

Bước 4: Điều tra nguyên nhân website bị hack

Trước tiên cần biết ai là người đã tấn công. Hacker đã tấn công như thế nào, hacker đã làm gì trên website, hacker còn cài đặt, ẩn giấu mã độc gì trên website?

Đây là bước khó nhất, nó đòi hỏi kinh nghiệm và kiến thức để có thể kiểm tra chính xác nguyên nhân và cách khắc phục. Bài viết này chỉ cung cấp một số bước cơ bản để kiểm tra và xác định nguyên nhân:

- Kiểm tra lưu lượng mạng để xác định các kết nối lưu lượng bất thường

- Kiểm tra trong access_log hay error_log tìm kiếm tất cả các thông tin liên quan đến việc website bị tấn công.

- Kiểm tra lại mã nguồn đang dùng có đang tồn tại lỗ hổng bảo mật nào không, các module, plugin được cài lên website có an toàn không, bạn cũng có thể sử dụng các công cụ bảo mật Acunetix, Nikto, OpenVAS để kiểm tra lại các lỗ hổng của website.

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

Bảo đảm an toàn thông tin khi sử dụng mạng xã hội

Mạng xã hội là một dạng xã hội ảo, mục đích kết nối các thành viên cùng môi trường, công việc, sở thích trên mạng với nhau. Cho phép người dùng chia sẻ và giao lưu thông tin một cách hiệu quả.

Mạng xã hội có những tính năng như chát, e-mail, phim ảnh, chia sẻ file, blog và xã luận. Những dịch vụ này có nhiều phương cách để các thành viên tìm kiếm bạn bè, đối tác: dựa theo nhóm (ví dụ như tên trường hoặc tên thành phố), dựa trên thông tin cá nhân (như địa chỉ e-mail hoặc tên tài khoản), hoặc dựa trên sở thích cá nhân (như thể thao, phim ảnh, sách báo, hoặc ca nhạc), lĩnh vực quan tâm: kinh doanh, mua bán...

Hiện nay thế giới có hàng trăm mạng xã hội khác nhau, như MySpace và Facebook nổi tiếng nhất trong thị trường Bắc Mỹ và Tây Âu; Orkut và Hi¬5 tại Nam Mỹ; Friendster tại Châu Á và các đảo quốc Thái Bình Dương. Mạng xã hội khác gặt hái được thành công đáng kể theo vùng miền như Bebo tại Anh Quốc, CyWorld tại Hàn Quốc, Mixi tại Nhật Bản và tại Việt Nam xuất hiện rất nhiều các mạng xã hội như: ZingMe, YuMe, Tamtay...

Các trang mạng xã hội đều được sở hữu bởi các hãng thương mại tư nhân và họ kiếm tiền bằng thu thập thông tin dữ liệu về cá nhân và bán thông tin này cho các đơn vị quảng cáo. Khi gia nhập một mạng xã hội, người dùng đang rời bỏ sự tự do của mạng Internet và bước vào mạng kết nối chịu sự chi phối và điều khiển bởi tổ chức sở hữu mạng này. Các thiết lập cài đặt bảo mật sự riêng tư chỉ có nghĩa là sự riêng tư của người dùng được bảo vệ khỏi các thành viên khác trong mạng chứ không bảo vệ thông tin khỏi chính nhà cung cấp dịch vụ mạng xã hội này. Thực tế người

dùng đang tin tưởng trao toàn bộ thông tin dữ liệu bản thân của mình cho nhà cung cấp mạng xã hội.

1. Mạng xã hội có an toàn không?

Như xã hội thực tế, không một mạng xã hội trên Internet, thế giới ảo hay trò chơi trực tuyến nào đảm bảo được 100% an toàn cho người sử dụng.

Trong khi mạng xã hội được xem là phương tiện giao tiếp tốt với mọi người thì nó cũng trở thành mục đích cho tội phạm mạng. Các hãng bảo mật lớn đã quan sát được làn sóng đe dọa trực tuyến ngày càng tăng lợi dụng mạng xã hội để đánh cắp thông tin sử dụng cho mục đích kiếm tiền. Những đe dọa này ngày càng phức tạp hơn, khó phát hiện hơn và thường nhằm vào lối sống "kết bạn trực tuyến" của mọi người.

2. Các rủi ro khi sử dụng mạng xã hội

Mạng xã hội hoạt động trên nguyên tắc kết nối và chia sẻ thông tin. Do đó, các mạng xã hội sẽ bắt buộc người sử dụng phải cung cấp một số nhất định các thông tin cá nhân. Càng nhiều thông tin mà người sử dụng cung cấp lên mạng xã hội, càng làm tăng nguy cơ bị kẻ xấu lợi dụng, làm ảnh hưởng tới hình ảnh, uy tín của bản thân. Sử dụng các thông tin đưa lên mạng xã hội như: vị trí địa lý, sở thích cá nhân, danh sách bạn bè, kẻ xấu có thể khai thác thêm các thông tin cá nhân khác hoặc các dữ liệu tài chính, ngân hàng của người dùng.

3. Làm sao để bảo vệ bản thân trên mạng xã hội?

Internet là một mạng công cộng được kết nối toàn cầu, chỉ đưa những thông tin lên mạng khi mình thấy thoải mái cho mọi người có thể đọc, xem được những thông tin này. Khi công khai thông tin cá nhân của mình trên mạng xã hội, người sử dụng cần xác định những thành viên khác trên mạng xã hội và Internet đều có thể lấy được những thông tin này, kể cả trường hợp những thông tin này đã được xóa, chỉnh sửa thì các bản lưu có thể tồn tại ở máy tính người sử dụng khác.

Do vậy, người sử dụng cần giới hạn lượng thông tin cá nhân mà mình cung cấp lên mạng xã hội, cố gắng hạn chế công khai các thông tin có tính liên kết, xâu chuỗi với nhau.

4. Bảo mật thông tin cá nhân trên mạng

- Không tiết lộ số điện thoại, địa chỉ thực tế, lịch công tác, thông tin liên quan tới công việc của mình tại cơ quan... Đặt chế độ cá nhân hoặc chỉ bạn bè thân thiết và tin cậy mới có thể xem để tránh trường hợp kẻ xấu có thể lợi dụng những thông tin đó uy hiếp, đe dọa.

- Sử dụng mật khẩu khó dò tìm, khó đoán và luôn giữ bí mật mật khẩu, tuyệt đối không chia sẻ cho ai khác.

5. Tạo dựng uy tín bản thân trên mạng

- Xin phép bạn bè mình trước khi đăng tải những bức ảnh và các câu chuyện của họ. Tôn trọng người khác trong cộng đồng mạng.

- Suy nghĩ và cân nhắc kỹ về những gì viết và đăng trên mạng.

- Thể hiện sự tôn trọng người khác trong giao tiếp, ứng xử trên mạng.

- Đăng ảnh phù hợp lên mạng. Không đưa những hình ảnh hở hang, mang tính khiêu dâm hoặc mang tính chất bạo lực lên mạng. Kẻ xấu có thể sử dụng những bức hình đó cho những mục đích không tốt đẹp.

Mạng xã hội **NÊN**:

✔ Sử dụng các trình duyệt web phổ biến và đã được cập nhật để truy cập mạng xã hội và Internet, thường xuyên theo dõi lịch sử truy cập để phát hiện các truy cập bất thường.

✔ Chỉ kết bạn với những người thân, quen biết ở ngoài đời. Xác minh với bạn bè, người thân qua điện thoại hoặc gặp mặt trước khi kết bạn trên mạng xã hội.

✔ Thường xuyên kiểm tra cơ chế bảo vệ thông tin cá nhân của mạng xã hội đối với tài khoản của mình. Kiểm tra các thông tin của tài khoản mà bạn bè, người lạ có thể thấy khi truy cập vào tài khoản của mình.

Mạng xã hội **KHÔNG NÊN**:

✕ Đăng tải hoặc tag ảnh cá nhân hoặc người thân trong gia đình ở góc gần, chính diện.

✕ Sử dụng cơ chế tự động đăng tải ảnh trên máy điện thoại di động, cho phép gắn vị trí địa lý vào các ảnh đã chụp.

✕ Sử dụng ảnh chân dung, ảnh cá nhân làm hình đại diện trên mạng xã hội, thay vào đó, nên sử dụng hình ảnh hoạt hình hoặc các biểu tượng, ảnh minh họa khác.

6. Hướng dẫn thiết lập chế độ an toàn cho tài khoản Facebook

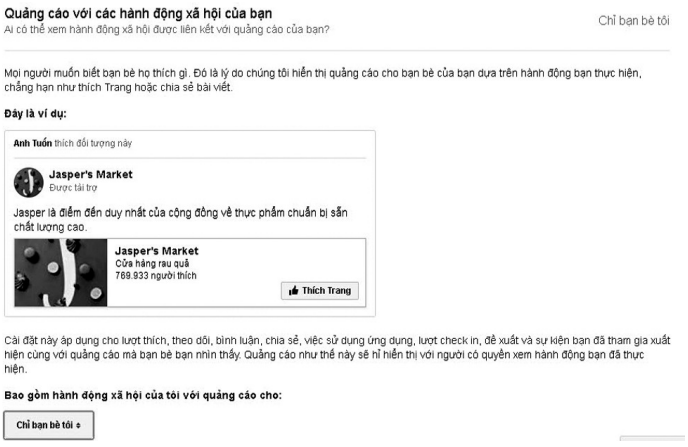
Các mục (1) Quyền riêng tư, (2) Dòng thời gian và gắn thẻ, (3) Bảo mật, (4) Quảng cáo đều chứa các tủy chỉnh liên quan tới thông tin cá nhân. Sử dụng các tùy chỉnh này để tăng cường an toàn cho tài khoản Facebook

(1) Trong phần Quyền riêng tư, giới hạn người xem cho các bài viết trong tương lai tại phần "Ai có thể thấy các bài đăng sau này của bạn?". Kiểm tra các hoạt động của tài khoản Facebook tại mục "Sử dụng nhật ký hoạt động". Ẩn các bài viết cá nhân tại dòng thời gian hoặc thiết lập chế độ chỉ cho phép Bạn bè đọc.

(2) Click vào Dòng thời gian và gắn thẻ "Xem với tư cách là" để thấy được những thông tin cá nhân của mình hiển thị với Bạn bè, người lạ trên Facebook như thế nào.

(3) Truy cập Bảo mật "Địa điểm bạn đã đăng nhập" để xem xét các truy cập đối với tài khoản Facebook của mình. Khi xuất hiện các truy cập bất thường, click vào "Kết thúc hoạt động" để ngăn chặn.

(4) Thiết lập "Quảng cáo với hoạt động xã hội của tôi" tại mục "Quảng cáo" về chế độ "chỉ bạn bè tôi"



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

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

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

1. Các website Việt Nam gặp gần 600 sự cố tấn công trong tháng 11/2017

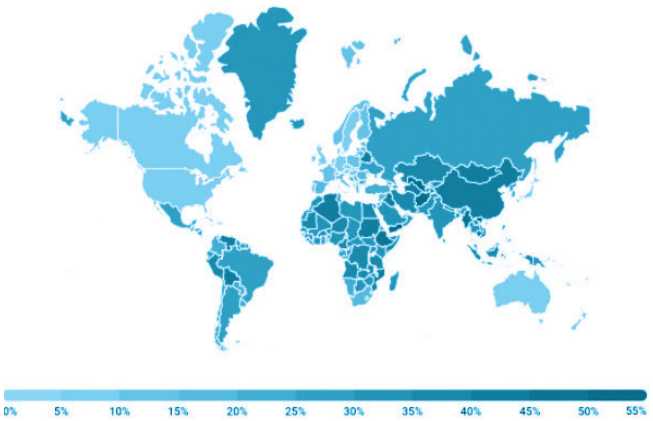
Trong tháng 11/2017, Trung tâm VNCERT thuộc Bộ Thông tin và Truyền thông ghi nhận 597 sự cố tấn công mạng vào các website tại Việt Nam, gồm 248 sự cố Phishing (tấn công lừa đảo), 232 sự cố Deface (tấn công thay đổi giao diện) và 117 sự cố Malware (cài mã độc).

Trong gần 600 sự cố tấn công mạng vào các website tại Việt Nam trong tháng 11 vừa qua, không có website nào của các cơ quan nhà nước có tên miền ".gov.vn"

2. Việt Nam đứng thứ 2 thế giới về tỉ lệ người dùng bị tấn công qua thiết bị lưu trữ

Theo công bố mới nhất của hãng bảo mật Kaspersky Lab, Việt Nam có tỉ lệ người dùng bị tấn công qua thiết bị lưu trữ đứng thứ hai thế giới trong quý 3 vừa qua.

Cụ thể, trong quý 3 năm 2017, 71,4% người dùng tại Việt Nam đã bị tấn công qua các thiết bị lưu trữ như: thẻ nhớ, ổ đĩa cứng, ổ đĩa di động, ổ đĩa USB, ổ đĩa quang (CD, DVD)... Con số này đã đưa Việt Nam đứng thứ 2 thế giới về tỉ lệ người dùng bị tấn công qua hình thức nêu trên.



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

3. Phát hiện hơn 11.000 cuộc tấn công mạng dưới nhiều hình thức

Bộ trưởng Bộ Thông tin và Truyền thông, Trương Minh Tuấn cho biết, tính đến hết tháng 10/2017, Việt Nam đã phát hiện 11.000 cuộc tấn công mạng dưới nhiều hình thức. Ngay trong hội nghị APEC có 27 cuộc tấn công mạng có chủ đích vào hệ thống trung tâm hội nghị cấp cao và trung tâm báo chí, 17 lỗ hổng được phát hiện và hàng nghìn cuộc có nguy cơ tấn công.

4. Mã độc mã hóa dữ liệu Bad Rabbit đang lan rộng

Một cuộc tấn công mã độc tống tiền kiểu mới đang phát tán nhanh chóng tại châu Âu và đã ảnh hưởng trên 200 tổ chức lớn ở Nga, Ukraine, Thổ Nhĩ Kì và Đức.

Mã độc mới có tên "Bad Rabbit" tương tự loại mã độc tống tiền có chủ đích Petya vào mạng của các doanh nghiệp, yêu cầu nạn nhân 0.05 bitcoin (~285 USD) tiền chuộc mở khóa hệ thống. Theo phân tích ban đầu của Kaspersky, Bad Rabbit được phát tán thông qua tấn công drive-by download, sử dụng cài đặt Adobe Flash player giả mạo nhằm đưa mã độc vào thiết bị người dùng.

Đến thời điểm hiện tại, nạn nhân là các kênh tin tức lớn như: Hãng thông tấn Interfax của Nga, hệ thống Kiev Metro của Ukraine, Sân bay Quốc tế Odessa và các bộ hạ tầng và tài chính của Ukraine.

Về cơ chế hoạt động do Bad Rabbit không khai thác lỗ hổng như hai loại mã độc mã hóa dữ liệu WannaCry và Petya nên phạm vi ảnh hưởng sẽ hẹp hơn, tốc độ lây lan chậm hơn. Bên cạnh đó, loại mã độc này nhắm vào đối tượng cụ thể nên mức độ ảnh hưởng cũng không lớn bằng WannaCry và Petya.

Thay vào đó, Bad Rabbit sử dụng các thông tin đăng nhập bị đánh cắp được mã hóa cứng thông qua SMB, trước tiên là từ xa ăn cắp mật khẩu từ máy tính bị nhiễm thông qua công cụ khai thác mật khẩu Mimikatz và sử dụng một danh sách tên người dùng/mật khẩu được mã hóa cứng trong mã nhị phân.

Để phòng ngừa nguy cơ mã độc tấn công, khuyến cáo người dùng nên sao lưu dữ liệu thường xuyên, cập nhật bản vá cho hệ điều hành, đồng thời chỉ mở các file văn bản nhận từ Internet trong môi trường cách ly Safe Run. Người

dùng cũng cần cài phần mềm diệt virus thường trực trên máy tính để được bảo vệ tự động.

5. Lỗ hổng zero-day trong Microsoft Office và DNS

Microsoft mới phát hành bản cập nhật Patch Tuesday tháng 10, vá các lỗ hổng trong mọi phiên bản Windows, cũng như Edge, IE, Skype cho Doanh nghiệp và Office. Trong đó, người dùng cần đặc biệt chú ý tới lỗ hổng zero-day trong Office và DNS.

Lỗ hổng zero-day trong Office có tên CVE-2017-11826, xuất hiện do phần mềm không xử lý chuẩn các đối tượng trong bộ nhớ. Để khai thác, tin tặc thực hiện tấn công phishing lừa người dùng mở tệp tin độc hại. Lỗ hổng ảnh hưởng đến mọi phiên bản của Microsoft Office và đã được sử dụng trong các cuộc tấn công thực tế.

Lỗ hổng này tồn tại trong Microsoft Office khi phần mềm không thể xử lý các đối tượng trong bộ nhớ. Khai thác thành công lỗ hổng, tin tặc có thể chạy mã tùy ý với vai trò người dùng hiện tại. Nếu người dùng đăng nhập với quyền quản trị, tin tặc có thể kiểm soát hệ thống bị ảnh hưởng, sau đó cài đặt các chương trình; xem, thay đổi hoặc xóa dữ liệu; hoặc tạo tài khoản mới với quyền người dùng đầy đủ. Người dùng được cấu hình với ít quyền trên hệ thống sẽ ít bị ảnh hưởng hơn người dùng có quyền quản trị.

Lỗ hổng thực thi mã từ xa trong dịch vụ phân giải tên miền (DNS), có thể cho phép tin tặc kiểm soát hoàn toàn máy tính hoặc máy chủ mục tiêu, từ đó truy cập vào hệ thống của người dùng. Lỗ hổng ảnh hưởng đến các máy tính chạy Windows 8.1, Windows 10, Windows Server 2012 đến 2016.

Lỗ hổng thực thi mã từ xa tồn tại trong DNSAPI của Windows DNS khi xử lý các gói tin DNS. Lỗ hổng cho phép tin tặc giành quyền thực thi mã tùy ý trên máy nạn nhân.

Để tránh nguy cơ bị tấn công, người dùng cần cập nhật bản mới nhất của Microsoft Office. Đồng thời người dùng nên tránh xa các mạng wifi công cộng, hoặc sử dụng VPN khi kết nối đến wifi công cộng.

6. Máy chủ DNS của CoinHive bị tấn công, hàng nghìn website bị lợi dụng để đào tiền ảo

Cuối tháng 10 máy chủ DNS của CoinHive - website cung cấp dịch vụ khai thác tiền ảo đã bị tấn công. CoinHive đã thu hút sự quan tâm sau khi trang web tải torrent nổi tiếng thế giới, The Pirate Bay, bị phát hiện là bí mật sử dụng dịch vụ này để đào tiền ảo trên trang web của họ.

Ngay sau đó hàng nghìn trang web khác cũng bắt đầu sử dụng CoinHive làm mô hình kiếm tiền bằng cách tận dụng sức mạnh xử lý CPU của khách truy cập để khai thác các loại tiền số. Ngay cả hacker cũng đang sử dụng các dịch vụ giống như CoinHive để kiếm tiền từ các trang web bị xâm nhập bằng cách tiêm script một cách bí mật

Người dùng được khuyến cáo nên cài đặt No Coin hoặc minerBlock, các trình mở rộng mã nguồn mở (plug-ins) có chức năng chặn các dịch vụ đào tiền ảo để tránh bị kẻ xấu lợi dụng.

7. Lổ hổng bảo mật nghiêm trọng của giao thức WPA2 ảnh hưởng hàng tỷ người dùng wifi toàn cầu

Ngày 16 tháng 10 trên trang web của nhà nghiên cứu bảo mật Mathy Vanhoef (www.krack-attacks.com) đã công bố một nhóm lỗ hổng trong giao thức WPA/WPA2, một giao thức được coi là an toàn nhất cho mạng không dây (Wi-Fi) hiện nay cho phép thực hiện kỹ thuật tấn công KRACKs (Key Reinstallation Attacks). Cụ thể, đối tượng tấn công có thể nghe lén, giải mã giao thức mã hóa và đọc được nội dung của các gói tin mà trước đây được cho là an toàn. Lỗ hổng này có thể bị lợi dụng để đánh cắp các thông tin cá nhân, thông tin nhạy cảm như tài khoản ngân hàng, thẻ tín dụng, tài khoản mạng xã hội, tài khoản trực tuyến, thông tin riêng, nội dung chat, thư điện tử, hình ảnh, video .v.v... được truyền qua mạng không dây.

Lỗ hổng này tồn tại trong chính nội tại của giao thức mạng không dây Wi-Fi chứ không liên quan đến các sản phẩm hay cách thức triển khai mô hình mạng, bất cứ thiết bị mạng không dây nào sử dụng giao thức mã hóa WPA/WPA2 đều có thể là mục tiêu của hình thức tấn công. Theo đánh giá, các thiết bị Android, Linux, Apple, Windows, OpenBSD, MediaTek, Linksys và nhiều thiết bị khác cũng có thể bị tấn công bằng việc điều chỉnh cách thức tấn công KRACKs cho phù hợp.

Hình thức tấn công này ảnh hưởng đến tất cả các thiết bị phát sóng Wi-Fi sử dụng giao thức WPA/WPA2. Và tùy thuộc vào cấu hình của hệ thống mạng, đối tượng tấn công thậm chí còn có thể thay đổi nội dung gói tin, hay đính kèm mã

độc tống tiền, mã độc gián điệp vào các gói tin và để người dùng tự lây nhiễm.

Ngày 16/10/2017, Cục An toàn thông tin, Bộ Thông tin và Truyền thông đã có Công văn số 541/CATTT-TĐQLGS cảnh báo về lỗ hổng trên.

8. Bluetooth bị hack ảnh hưởng 20 triệu thiết bị Amazon Echo và Google Home

Armis, công ty bảo mật IoT phát hiện ra lỗ hổng, ước tính có khoảng 20 triệu thiết bị Amazon Echo và Google Home có khả năng bị tấn công leo thang bởi các lỗ hổng BlueBorne.

BlueBorne là phương thức tấn công tinh vi khai thác tám lỗ hổng khi bật Bluetooth và cho phép kẻ tấn công chạy mã độc, ăn cắp thông tin nhạy cảm, kiểm soát hoàn toàn và thực hiện tấn công man-in-the-middle trên các thiết bị mục tiêu.

Điều tồi tệ hơn là việc khai thác BlueBorne không yêu cầu nạn nhân nhấp vào bất kỳ liên kết hoặc mở bất kỳ tập tin nào - hay nói cách khác không cần bất kỳ tương tác nào từ người dùng. Ngoài ra, hầu hết các sản phẩm an ninh có thể sẽ không phát hiện được việc tấn công. Đồng thời, sau khi kiểm soát được một thiết bị bật Bluetooth, kẻ tấn công có thể lây nhiễm bất kỳ hoặc tất cả các thiết bị trong cùng một mạng.

9. Cảnh báo nhóm 7 lỗ hổng trong phần mềm mã nguồn mở DNSmasq

Ngày 02 tháng 10 năm 2017, nhóm các chuyên gia bảo mật của Google đã công bố một nhóm gồm 07 lỗ hổng bảo mật trong phần mềm nguồn mở Dnsmasq (trong đó: 03 lỗ hổng cho phép đối tượng tấn công thực thi mã lệnh từ xa, 01 lỗ hổng để lộ thông tin, 03 lỗ hổng cho phép thực hiện tấn công từ chối dịch vụ) bằng cách gửi các gói tin yêu cầu truy vấn của giao thức DNS/DHCP tới thiết bị có cài đặt phần mềm.

Dnsmasq được cài đặt trên các máy tính sử dụng hệ điều hành Linux, thiết bị Home router, và cả thiết bị IoT để cung cấp chức năng phục vụ yêu cầu DNS, DHCP, quảng bá bộ định tuyến và khởi tạo mạng nên số lượng các thiết bị tại Việt Nam bị ảnh hưởng có thể là tương đối lớn. Hơn nữa nhiều thiết bị không chỉ sử dụng trong môi trường mạng LAN mà sử dụng cả trên Internet, nên đối tượng tấn công hoàn toàn có thể tìm kiếm các thiết bị và khai thác lỗ hổng mà không gặp khó khăn gì.

Hiện tại một số hãng sử dụng Dnsmasq trên các sản phẩm cũng đã xác nhận và đưa ra bản vá cho sản phẩm gồm: Google (Android), Slackware, Redhat, Debian...

Ngày 05/10/2017, Cục An toàn thông tin, Bộ Thông tin và Truyền thông đã có Công văn số 519/CATT-TTĐQLGS cảnh báo về lỗ hổng trên.

10. Hàng triệu thiết bị có nguy cơ bị tấn công qua lỗ hổng nghiêm trọng trong bộ vi xử lý của Intel

Ngày 20/11/2017, Intel đã phát hành bản vá INTEL-SA-00086 cho các điểm yếu an toàn thông tin trên firmware của các thiết bị sử dụng bộ vi xử lý của Intel. Các điểm yếu CVE-2017-5708, CVE-2017-5705, CVE-2017-5711, CVE-2017-5712, CVE-2017-5706, CVE-2017-5709, CVE-2017-5710, CVE-2017-5707 được đánh giá là các điểm yếu nghiêm trọng, có khả năng ảnh hưởng tới nhiều thiết bị mạng bao gồm cả các máy tính cá nhân, máy chủ và các thiết bị IoT.

Đây là điểm yếu an toàn thông tin cho phép đối tượng tấn công cài đặt mã độc và chiếm quyền điều khiển hệ thống. Để giúp người dùng xác định lỗ hổng trên thiết bị và cập nhật bản vá phù hợp. Nhà sản xuất phát hành công cụ kiểm tra tại địa chỉ: https://downloadcenter.intel.com/download/27150

Cục An toàn thông tin, Bộ Thông tin và Truyền thông khuyến nghị các đơn vị kiểm tra và cập nhật ngay bản vá cho các thiết bị bị ảnh hưởng để giảm nguy cơ tấn công mạng lợi dụng lỗ hổng này.

11. Cảnh báo mã độc nguy hiểm "đào" tiền ảo ẩn mình trong các website

Trung tâm Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) thuộc Bộ Thông tin và Truyền thông vừa đưa ra cảnh báo số 383/VNCERT-ĐPƯC ngày 15/11/2017 về mã độc khai thác tiền ảo Coinhive ẩn mình trên các website có thể gây ra nhiều tổn thất cho người dùng máy tính.

Theo VNCERT, đơn vị này đã ghi nhận được rất nhiều sự cố an toàn thông tin về mã độc khai thác tiền ảo Coinhive ẩn mình trên các website.

Khi người dùng truy cập vào trang web, thư viện mã Coinhive sẽ tự động chạy trên máy tính người dùng dưới dạng tiện ích mở rộng hoặc trực tiếp trong trình duyệt nhằm mục đích "đào" tiền ảo Bitcoin, Monero... bằng cách sử dụng trái phép

tài nguyên của người dùng (CPU, ổ cứng, bộ nhớ...) và gửi về ví điện tử của tin tặc.

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

1. Thống kê danh sách các cơ quan trên địa bàn tỉnh có địa chỉ IP truy vấn đến các tên miền/IP độc hại

Tên cơ quan	Domain/IP
UBND Quan Sơn	46.101.184.102 bhongircollege.com 69.195.140.124:9675 rukgan.com
UBND Thường Xuân	eleonuccorini.com kukutrustnet.info samayer.net bhongircollege.com www.ceylanogullari.com amsamex.com www.3pindia.in tn69abi.com 69.195.129.66 46.101.184.102
UBND Nga Sơn	69.195.140.124:9674 www.eleonuccorini.com www.3pindia.in tn69abi.com bhongircollege.com 46.101.184.102
UBND Cẩm Thủy	69.195.140.124:9675 smokin-tr.com a.sobea.in hzmksreiuojy.biz
UBND Lang Chánh	brucegarrod.com 69.195.140.124:9674 bhongircollege.com www.eleonuccorini.com 46.101.184.102
UBND Vĩnh Lộc	www.ceylanogullari.com ygiudewsqhct.in apadanapub.com 69.195.140.124:9674 Active
Sở Giao thông vận tải	69.195.140.124:9674 www.eleonuccorini.com a.sobea.in www.ceylanogullari.com 46.101.184.102
Sở Ngoại vụ	69.195.140.124:9674 Active ygiudewsqhct.in ceyueaeiogooemgq.org gmgigoiogeosyawm.org 69.195.140.124:1028 Inactive 96.43.141.190
Ban Dân tộc	a.sobea.in hzmksreiuojy.biz bhongircollege.com 69.195.140.124:9674 Active www.ceylanogullari.com 46.101.184.102
Ban Quản lý KKT Nghi Sơn và các KCN	69.195.140.124:9674 vitinhduycuong.com brucegarrod.com apadanapub.com www.eleonuccorini.com www.ceylanogullari.com smokin-tr.com chihuahuaupinghome.com hzmksreiuojy.biz a.sobea.in 46.101.184.102

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

Trong 02 tháng 10-11/2017, 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 41 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 thời gian từ **01/10-30/11** ghi nhận có **188** cuộc tấn công vào khai thác lỗ hổng ứng dụng Web và **28** cuộc tấn công chiếm đoạt quyền quản trị vào các dịch vụ đang hoạt động tại Trung tâm.

3. Công văn an toàn thông tin

- Ngày 16/10/2017, Cục An toàn Thông tin, Bộ Thông tin và Truyền thông ban hành công văn số 541/CATTT-TĐQLGS cảnh báo nguy cơ mất an toàn thông tin trên các thiết bị sử dụng mạng wifi

gửi tới cơ quan, tổ chức và người sử dụng.

- Ngày 05/10/2017, Cục An toàn thông tin, Bộ Thông tin và Truyền thông ban hành Công văn số 519/CATTTTĐQLGS gửi các cơ quan, tổ chức, doanh nghiệp cảnh báo về nhốm 07 lỗ hổng bảo mật trong phần mềm nguồn mở Dnsmasq.

- Ngày 15/11/2017 Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) ban hành công văn số 383/VNCERT-ĐPƯC về việc Phát hiện ngăn chặn mã độc "đào" tiền ảo bất hợp pháp.

- Ngày 01/11/2017 UBND tỉnh Thanh Hóa ban hành công văn số 818/VP-CNTT về việc Thực hiện các biện pháp đảm bảo an toàn thông tin phục vụ sự kiện APEC 2017

- Trung tâm CNTT&TT Thanh Hóa ban hành công văn số 194/TTCNTT&TT-QTHT, 197/TTC-NTT&TT-QTHT, 201/TTCNTT&TT-QTHT về việc Cảnh báo Hệ thống thông tin lây nhiễm mã độc tham gia mạng bonet cho hơn 30 cơ quan, đơn vị trên địa bàn tỉnh

- Ngày 23/10/2017 Trung tâm CNTT&TT Thanh Hóa ban hành công văn số 193/TTCNTT&TT-QTHT về việc thông báo Website bị tin tặc tấn công cho Công ty Cổ phần Bia Thanh Hóa.

- Ngày 10/8/2017 UBND tỉnh ban hành công văn số 9449/UBND-CNTT về việc giao triển khai thực hiện các quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia.

TIN HOẠT ĐỘNG

Cán bộ Trung tâm CNTT&TT tham gia lớp đào tạo CCNA tại Thanh Hóa

Sáng ngày 13/11 Sở TT&TT tỉnh Thanh Hóa phối hợp với Cục Tin học hóa thuộc Bộ TT&TT tổ chức một lớp đào tạo chứng chỉ CCNA. Tới dự lễ khai giảng có ông Trần Duy Bình - Giám đốc Sở TT&TT; đại diện Lãnh đạo Cục Tin học hóa và ông Nguyễn Công Trung - Phó Giám đốc Trung tâm đào tạo CNTT, Học viên BKACAD.

Lớp học nhằm hỗ trợ cho các cơ quan Nhà nước tỉnh Thanh Hóa trong việc đào tạo nâng cao trình độ cho các cán bộ chuyên trách CNTT về khả năng thiết kế, triển khai, quản trị hệ thống mạng theo các tiêu chuẩn quốc tế.

CCNA là chứng chỉ quốc tế do hãng sản xuất thiết bị mạng hàng đầu thế giới Cisco cấp. Những kỹ sư, chuyên viên mạng được nhận chứng chỉ CCNA sẽ được công nhận trên toàn thế giới. Khoá học CCNA này được tổ chức nhằm trang bị cho học viên các kỹ năng và những kiến thức cần thiết để có thể thiết lập, vận hành và xử lý sự cố cho những môi trường mạng văn phòng nhỏ và vừa; Khóa học giúp học viên có thể cấu hình các thiết bị SWITCH, ROUTER, có thể thiết lập các kết nối ra môi trường mạng diện rộng (WAN), và triển khai bảo mật trên môi trường mạng; Trang bị cho học viên toàn diện và đầy đủ các kiến thức và kỹ năng về hệ thống mạng; Chuẩn bị điều kiện cho kỳ thi lấy Chứng chỉ Quốc tế CCNA được công nhận trên toàn thế giới... Thời gian của khóa đào tạo sẽ được học liên tục trong 12 ngày (kể cả Thứ 7 và CN). Kết thúc khóa đào tạo sẽ có 10 học viên được lựa chọn đi Hà Nội thi chứng chỉ quốc tế CCNA.

Tham gia lớp bồi dưỡng có 15 học viên là cán bộ chuyên trách CNTT thuộc các Sở: Tài chính, Kế hoạch & Đầu tư, Giáo dục & Đào tạo, Y tế, Tài nguyên & Môi trường, Nông nghiệp và Phát triển nông thôn, Lao động - Thương binh và Xã hội và TT&TT. Trong đó, Trung tâm CNTT&TT cử 04 cán bộ kỹ thuật tham gia khóa học để củng cố lại kiến thức và kỹ năng về hệ thống mạng trong việc quản trị và vận hành Trung tâm An ninh mạng và An toàn dữ liệu của tỉnh.

NGÔ PHƯƠNG

Cán bộ Trung tâm CNTT&TT tham dự các khóa đào tạo ngắn hạn về An toàn thông tin năm 2017 theo đề án 99

Thực hiện theo Quyết định số 99/QĐ-TTg ngày 14/01/2014 của Thủ tướng Chính phủ về "Đào tạo và phát triển nguồn nhân lực An ninh, An toàn thông tin đến năm 2020". Mục tiêu chính của Đề án này là nhanh chóng đào tạo đội ngũ chuyên gia an toàn, an ninh thông tin đủ năng lực, trình độ đáp ứng yêu cầu của các cơ quan, tổ chức, doanh nghiệp về bảo đảm an toàn, an ninh thông tin trong các ngành, lĩnh vực trọng yếu của đất nước. Một trong những chỉ tiêu cụ thể của Đề án 99 là đến năm 2020 tập huấn, đào tạo ngắn hạn nâng cao kiến thức, kỹ năng về an toàn, an ninh thông tin cho 10.000 lượt cán bộ làm về an toàn, an ninh thông tin và CNTT tại các cơ quan nhà nước.

Trong năm 2017, Bộ Thông tin và Truyền thông tổ chức các khóa đào tạo với các nội dung liên quan đến công tác an toàn thông tin cho các đối tượng là cán bộ quản lý, kỹ thuật của các Bộ, ngành và địa phương.

Trên cơ sở các công văn mời tham dự khóa đào tạo, Trung tâm CNTT&TT đã cử các cán bộ lãnh đạo, kỹ thuật với nòng cốt là các thành viên trong Tổ Ứng cứu sự cố tham dự 04 khóa đào tạo với mục đích nâng cao năng lực về An toàn An

ninh thông tin; tăng cường khả năng phòng chống các nguy cơ tấn công, xâm nhập vào hệ thống thông tin trọng yếu quốc gia; khắc phục kịp thời các sự cố An toàn thông tin.

Các khóa học được Cục An toàn thông tin, Bộ Thông tin và Truyền thông tổ chức trong thời gian 01 tuần với sự tham gia giảng dạy là các giảng viên có kinh nghiệm trong việc triển khai các công tác về an toàn thông tin. Kết thúc khóa học các học viên của Trung tâm được Cục An toàn thông tin và đơn vị tổ chức khóa đào tạo cấp giấy chứng nhận hoàn thành khóa học.

HOÀNG ANH TUẤN

Trung tâm Công nghệ thông tin và truyền thông tham gia đoàn kiểm tra công tác bảo đảm An toàn thông tin tại Cảng Hàng không Thọ Xuân

Sáng ngày 08 tháng 11 năm 2017, tại Cảng Hàng không Thọ Xuân, đoàn công tác của Sở Thông tin và Truyền thông đã đến kiểm tra và có buổi làm việc với Cảng Hàng không Thọ Xuân về đảm bảo an toàn, an ninh thông tin cho các hoạt động APEC 2017 theo kế hoạch.

Tham gia đoàn công tác do đ/c Trần Duy Bình, Giám đốc Sở là Trưởng đoàn có các đ/c đại diện cho các phòng của Sở và Trung tâm CNTT&TT.

Báo cáo với đoàn công tác, đại diện lãnh đạo Cảng Hàng không Thọ Xuân đã trình bày các nội dung liên quan đến Công tác bảo vệ bí mật của đơn vị và đảm bảo an toàn, an ninh thông tin trong việc vận hành hệ thống thông tin phục vụ công tác nghiệp vụ của Cảng Hàng không. Đồng thời, đề xuất với đoàn công tác các nội dung phối hợp, hỗ trợ của Sở Thông tin và Truyền thông với Cảng Hàng không Thọ Xuân trong việc bảo đảm an toàn thông tin nói chung.

Thay mặt đoàn công tác, đ/c Trần Duy Bình đã đánh giá cao công tác chuẩn bị của Cảng Hàng không Thọ Xuân về đảm bảo an toàn, an ninh thông tin nói chung và phục vụ cho các hoạt động APEC 2017 trong thời gian qua. Đồng thời, nêu rõ tầm quan trọng trong việc triển khai các giải pháp bảo đảm an toàn thông tin tại các đơn vị, đặc biệt là tại Cảng Hàng không Thọ Xuân trong bối cảnh tình hình mất an toàn thông tin hiện nay.

Trong buổi làm việc, các đ/c trong đoàn đã có những đánh giá, góp ý về các biện pháp tăng cường hơn nữa công tác bảo đảm an toàn thông tin nói chung và hệ thống thông tin cho Cảng Hàng không.

LÊ VĂN TUẤN

Trung tâm CNTT&TT Thanh Hóa tổ chức thi cấp Chứng chỉ ứng dụng Công nghệ thông tin đợt 5 năm 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 08 tháng 10 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 5năm 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 5 năm 2017, có 15 thí sinh đăng ký dự thi và 15 thí sinh đã vượt qua 2 phần thicủa mình là phần thi trắc nghiệm lý thuyết trực tuyến trên phần mềm và phần thi thực hành kỹ năng trên máy tính; toàn bộ hồ sơ về kỳ thi đã được gửi Sở Giáo dục và đào tạo tỉnh để tiến hành cấp chứng chỉ, phôi chứng chỉ được Bộ Giáo dục và Đào tạo cấp theo số lượng thí sinh thi đậu, được Sở 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 31/2017/TT-BTTTT Quy định hoạt động giám sát an toàn hệ thống thông tin

Theo quy định tại Thông tư 31, hoạt động giám sát an toàn HTTT phải đảm bảo các nguyên tắc: được thực hiện thường xuyên, liên tục; chủ động theo dõi, phân tích, phòng ngừa để kịp thời phát hiện, ngăn chặn rủi ro, sự cố ATTT mạng; đảm bảo hoạt động ổn định, bí mật cho thông tin được cung cấp, trao đổi trong quá trình giám sát.

Đồng thời, đảm bảo có sự điều phối, kết hợp chặt chẽ, hiệu quả giữa hoạt động giám sát của Bộ TT&TT và hoạt động giám sát của chủ quản HTTT; từng bước xây dựng khả năng liên thông giữa hệ thống giám sát Bộ TT&TT và hệ thống giám sát của chủ quản HTTT trên phạm vi toàn quốc.

Hoạt động giám sát an toàn HTTT được thực hiện qua phương thức giám sát trực tiếp hoặc gián tiếp. Chủ quản HTTT có thể trực tiếp triển khai hoặc thuê dịch vụ giám sát. Trường hợp cần thiết, căn cứ vào năng lực, tình hình và nguồn lực thực tế, chủ quản HTTT đề nghị các đơn vị chức năng liên quan của Bộ TT&TT hỗ trợ giám sát phù hợp với nguồn lực thực tế.

Cùng với việc quy định cụ thể yêu cầu giám sát trực tiếp đối với chủ quản HTTT, Thông tư 31 của Bộ TT&TT cũng quy định rõ về hoạt động giám sát của doanh nghiệp. Cụ thể, doanh nghiệp viễn thông, doanh nghiệp cung cấp dịch vụ CNTT, doanh nghiệp cung cấp dịch vụ ATTT mạng có trách nhiệm phối hợp với chủ quản HTTT trong việc giám sát theo yêu cầu của Bộ TT&TT; cung cấp các thông tin về hạ tầng, kỹ thuật, hệ thống mạng và thực hiện các hỗ trợ kỹ thuật theo yêu cầu của Bộ TT&TT phục vụ cho hoạt động giám sát của Bộ TT&TT; đồng thời thực hiện các nhiệm vụ giám sát theo quy định tại Điều 7 Quyết định 05 ngày 16/3/2017 của Thủ tướng Chính phủ về hệ thống phương án ứng cứu khẩn cấp bảo đảm ATTT mạng quốc gia.

Theo quy định tại Thông tư 31, các hoạt động nâng cao năng lực giám sát HTTT gồm có: tổ chức giao ban, hội thảo định kỳ về hoạt động giám sát; bồi dưỡng, huấn luyện, diễn tập nhằm nâng cao năng lực giám sát; đôn đốc, kiểm tra việc thực hiện hoạt động giám sát, cảnh báo của các bộ phận chuyên trách về ATTT mạng; chia sẻ kiến thức, kinh nghiệm về giám sát, cảnh báo, ứng cứu sự cố; nghiên cứu, xây dựng các công cụ hỗ trợ hoạt động phối hợp, trao đổi thông tin trong công tác giám sát, cảnh báo, ứng cứu sự cố; phát triển các sản phẩm, dịch vụ giám sát, phân tích, cảnh báo chuyên sâu cho từng đối tượng giám sát cụ thể; thúc đẩy xây dựng các thỏa thuận hợp tác song phương, đa phương giữa bộ phận chuyên trách về ATTT mạng nhằm nâng cao năng lực giám sát, cảnh báo; tăng cường hợp tác quốc tế trong công tác giám sát, cảnh báo, ứng cứu sự cố.

Thông tư có hiệu lực thi hành kể từ ngày 15/01/2018./.

Ngày 25 tháng 10 năm 2017, Thủ tướng Chính phủ ban hành Quyết định số 1622/QĐ-TTg Phê duyệt Đề án đẩy mạnh hoạt động của mạng lưới ứng cứu sự cố, tăng cường năng lực cho các cán bộ, bộ phận chuyên trách ứng cứu sự cố an toàn thông tin mạng trên toàn quốc đến 2020, định hướng đến 2025

Theo đó, tại Quyết định 1622/QĐ-TTg, Chính phủ đặt ra mục tiêu cụ thể đến 2020 như sau:

Một là, nâng cao năng lực của Cơ quan điều phối quốc gia thông qua việc xây dựng các quy trình, nghiệp vụ quản lý, điều phối; đầu tư các hệ thống nhằm chủ động theo dõi, thu thập thông tin sự cố; hệ thống tiếp nhận, lưu giữ và xử lý thông tin sự cố; tăng cường khả năng điều hành và chia sẻ thông tin sự cố.

Hai là, đẩy mạnh các hoạt động của mạng lưới ứng cứu sự cố và các đơn vị chuyên trách, cơ quan chỉ đạo, điều hành ứng cứu sự cố an toàn thông tin mạng.

Ba là, nâng cao năng lực theo dõi, thu thập, phân tích, phát hiện sự cố và điều phối, ứng cứu sự cố trên toàn mạng lưới.

Bốn là, đẩy mạnh bồi dưỡng, đào tạo, phát triển đội ngũ nhân lực ứng cứu sự cố bảo đảm an toàn thông tin mạng.

Năm là, nâng cao nhận thức và tăng cường phổ biến kiến thức về các nguy cơ, sự cố mạng, công tác điều phối, ứng cứu sự cố, bảo đảm an toàn thông tin mạng.

Sáu là, đẩy mạnh hợp tác quốc tế, trao đổi chia sẻ thông tin, kinh nghiệm tăng cường khả năng phối hợp với các cơ quan, tổ chức an toàn thông tin mạng, ứng cứu sự cố (CERT) của các nước.

Đặc biệt, một trong số các nhiệm vụ chủ yếu trong thời gian tới mà Chính phủ đã đặt ra, đó là xây dựng, áp dụng các tiêu chuẩn quốc tế nhằm chuẩn hóa quy trình, dự phòng rủi ro, bảo vệ an toàn thông tin mạng.

Cụ thể, công tác xây dựng, áp dụng và đánh giá chuẩn quy trình quản lý rủi ro, bảo đảm an toàn thông tin mạng theo bộ chuẩn ISO/IEC 27xxx và các tiêu chuẩn khác về an toàn thông tin cho các thành viên mạng lưới ứng cứu sự cố và các đơn vị quản lý, vận hành các Trung tâm dữ liệu và Hệ thống thông tin quan trọng thuộc các bộ, cơ quan ngang bộ, UBND cấp tỉnh, doanh nghiệp viễn thông, internet, trung tâm dữ liệu, tổ chức tài chính, ngân hàng, chủ quản hệ thống thông tin quan trọng quốc gia. Hỗ trợ tổ chức các khóa đào tạo, tập huấn về bộ tiêu chuẩn ISO/IEC 27xxx và các tiêu chuẩn khác về an toàn thông tin mạng cho lực lượng ứng cứu sự cố, các cán bộ quản lý, vận hành các Trung tâm dữ liệu và hệ thống thông tin quan trọng nêu trên.

Bên cạnh đó, Cơ quan điều phối quốc gia sẽ được nâng cao năng lực hoạt động; tăng cường hiệu quả hoạt động của Mạng lưới ứng cứu sự cố. Hoạt động thu thập, phân tích, xác minh và cảnh báo, điều phối, ứng cứu sự cố an toàn thông tin mạng của cơ quan điều phối quốc gia, các đơn vị, tổ chức thành viên của mạng lưới cũng sẽ được tăng cường.

Hàng năm, Chính phủ sẽ tổ chức 01 chương trình diễn tập cấp quốc gia và 03 chương trình diễn tập theo vùng, miền hoặc theo ngành, lĩnh vực. 3-5 cuộc diễn tập quốc tế sẽ được triển khai hàng năm. Chính phủ giao cho cấp bộ, tỉnh, thành phố mỗi năm phải tổ chức ít nhất 01 cuộc diễn tập chuyên đề an toàn thông tin, ứng cứu sự cố mạng trong phạm vi của bộ, ngành, địa phương mình. Đồng thời phối hợp, tham gia các cuộc diễn tập quốc gia và quốc tế. Đội ngũ nhân lực ứng cứu sự cố, bảo đảm an toàn thông tin mạng sẽ được phát triển và nâng cao năng lực qua các chương trình huấn luyện, đào tạo, sát hạch cũng như bồi dưỡng, đào tạo. Bên cạnh đó, phát triển đội ngũ nhân lực thuê ngoài, ban hành các cơ chế, chính sách ưu đãi nhằm thu hút, nâng cao năng lực đội ngũ nhân sự trong lĩnh vực này.

Nguồn vốn để thực hiện Đề án là Ngân sách trung ương, ngân sách địa phương, Quỹ Dịch vụ viễn thông công ích Việt Nam, nguồn thu của các cơ quan, đơn vị được phép để lại sử dụng theo quy định, nguồn vốn, viện trợ không hoàn lại và các nguồn kinh phí hợp pháp khác.

NGUYỄN PHƯƠNG