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

Số 09
tháng 7/2018

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

BIÊN SOẠN
Cao Việt Cường; Trần Ngọc Hưng; Trịnh Ngọc Quỳnh; Trần Lê Phúc

THIẾT KẾ
Chung Nguyễn

TRUNG TÂM CÔNG NGHỆ THÔNG TIN & TRUYỀN THÔNG THANH HÓA
Địa chỉ: 73 Hàng Than, TP Thanh Hóa
Điện thoại: 02373.718.298
Fax: 02373.718.299
Website: ict.thanhhoa.gov.vn
Giấy phép xuất bản số: 10/GP-XBBT
Sở TTTT Thanh Hóa cấp ngày 12/02/2018

In 500 cuốn, khổ 19x27cm
Tại Công ty TNHH In & TBGD Thanh Huệ
In xong và nộp lưu chiểu tháng 7/2018

Bảo đảm an toàn thông tin cho hệ thống thông tin quan trọng

CAO VIỆT CƯỜNG
Trưởng phòng Tổng hợp - Hành chính
Trung tâm CNTT& TT Thanh Hóa

Triển khai Quyết định 632/QĐ-TTg của Chính phủ, Cục An toàn thông tin (Bộ TT&TT) tổ chức chuỗi hoạt động tập huấn, diễn tập đảm bảo an toàn thông tin cho các lĩnh vực quan trọng. Chương trình đảm bảo an toàn cho các hệ thống thông tin quan trọng của các lĩnh vực quan trọng đã diễn ra vào tổ chức chiều ngày 27/6 tại TP. Sầm Sơn, Thanh Hóa, với sự góp mặt của 17 cơ quan nhà nước, Tập đoàn kinh tế, Tổng công ty nhà nước và các tổ chức tài chính ngân hàng.

Tham dự buổi Diễn tập có ông Nguyễn Thành Hưng, Thứ trưởng Bộ TT&TT; ông Nguyễn Thanh Hải, Cục trưởng Cục ATTT, Bộ TT&TT; đại diện lãnh đạo tỉnh Thanh Hóa; cùng các cán bộ lãnh đạo, cán bộ quản lý, cán bộ kỹ thuật của 17 đơn vị tham gia chương trình, bao gồm: Bảo hiểm xã hội Việt Nam; Ủy ban Chứng khoán Nhà nước; Cục CNTT - Ngân hàng Nhà nước Việt Nam; Tập đoàn Điện lực Việt Nam; Tập đoàn Dầu khí Việt Nam; Tập đoàn Xăng dầu Việt Nam;...

Phát biểu khai mạc buổi Diễn tập, ông Nguyễn Thanh Hải cho biết, ATTT hiện nay đã trở thành vấn đề nóng, thu hút được sự quan tâm của các cấp, các ngành và cộng đồng xã hội. Công tác bảo đảm ATTT là công tác mang tính thường xuyên, liên tục, không ngừng chủ động phòng ngừa, diễn tập xử lý các tình huống đặt ra. Thực tiễn cho thấy, các cuộc tấn công mạng vào hệ thống thông tin quan trọng của các quốc gia trên thế giới đều là hình thức tấn công có chủ đích, tinh vi. Do đó, mặc dù hệ thống thông tin quan trọng được áp dụng nhiều giải pháp bảo đảm ATTT, thậm chí không kết nối Internet, được cô lập... nhưng vẫn bị tấn công mạng gây sự cố, thiệt hại. Nguyên nhân chủ yếu là do nhận thức và năng lực kỹ thuật của nhân lực phụ trách còn chưa tương xứng.

Ông Nguyễn Thanh Hải, Cục trưởng Cục An toàn thông tin - Bộ TT&TT phát biểu khai mạc buổi diễn tập (Ảnh: ICTnews)

Cũng theo nhận định của ông Nguyễn Thanh Hải, hoạt động bảo đảm ATTT của mỗi cơ quan, tổ chức ngoài việc phải tuân thủ nghiêm quy định của pháp luật còn cần tập trung vào 3 vấn đề gồm con người, công nghệ và quy trình xử lý sự cố. Trong đó, yếu tố con người là quan trọng nhất. Trong điều

Các đơn vị diễn tập nâng cao năng lực xử lý tình huống tấn công mạng vào hệ thống điều khiển công nghiệp và tài chính quan trọng.

kiện nguồn lực để đầu tư hạ tầng kỹ thuật hiện đại, tiên tiến nhằm bảo đảm ATTT còn khó khăn và chưa thể triển khai xong trong ngắn hạn, các cơ quan, tổ chức cần sớm tập trung hoàn thiện 2 yếu tố con người và quy trình. Yếu tố con người cần được quan tâm đào tạo đúng mức, nâng cao cả về nhân thức và năng lực kỹ thuật.

Thời gian qua, Cục ATTT và Trung tâm VNCERT thuộc Bộ TT&TT đã thường xuyên tổ chức các hoạt động diễn tập trong nước và quốc tế với nhiều chủ đề khác nhau. Tuy nhiên, đây là lần đầu tiên tổ chức diễn tập với chủ đề về các hệ thống điều khiển công nghiệp và tài chính, ngân hàng quan trọng tại Việt Nam. Chương trình diễn tập "Nâng cao năng lực xử lý tình huống tấn công mạng vào hệ thống công nghiệp và tài chính quan trọng" diễn ra trong thời gian 2 tiếng, 17 đơn vị tham gia theo 2 khu vực. Trong đó, 8 đơn vị diễn tập bảo đảm ATTT cho các hệ thống điều khiển công nghiệp và 10 đơn vị diễn tập về bảo đảm ATTT cho các hệ thống tài chính, ngân hàng. Trực tiếp hướng dẫn các đội diễn tập là 2 chuyên gia quốc tế đến từ Nga và Mỹ. Chương trình Diễn tập bao gồm 5 tình huống tập trung vào việc xử lý chỉ đạo, làm việc theo nhóm giúp các lãnh đạo, cán bộ quản lý, kỹ thuật viên chuyên trách về an toàn thông tin, CNTT của các cơ quan quản lý SCADA/ICS và hệ thống tài chính - ngân hàng quan trọng có thể thực hiện các biện pháp phòng chống, xử lý các tình huống tấn công mạng trong các kịch bản mô phỏng khi hệ thống vẫn được vận hành bình thường. Qua đó, giúp cán bộ có thêm nhận thức về các nguy cơ an toàn thông tin mới đối với hệ thống do mình quản lý và kinh nghiệm thực tế, nhanh nhạy, tự tin hơn khi xử lý các vấn đề an toàn thông tin chưa

Toàn cảnh Hội nghị "Bảo đảm ATTT cho hệ thống thông tin quan trọng".

biết trước khi vận hành hệ thống thông tin quan trọng của tổ chức mình.

Nối tiếp sự kiện, sáng ngày 28/6/2018, Cục ATTT, Bộ TT&TT đã chủ trì tổ chức Hội nghị "Bảo đảm ATTT cho hệ thống thông tin quan trọng" nhằm nâng cao nhận thức, kỹ năng và kinh nghiệm thực tế trong công tác bảo đảm ATTT, phòng, chống tấn công mạng vào các hệ thống thông tin quan trọng của 11 lĩnh vực, đặc biệt là các hệ thống SCADA/ICS và hệ thống thông tin quan trọng của các tổ chức tài chính - ngân hàng. Tham gia trình bày tham luận tại hội nghị là các chuyên gia hàng đầu trong lĩnh vực ATTT đến từ cơ quan chức năng thuộc Bộ TT&TT, các chuyên gia uy tín trong nước và quốc tế (đến từ Mỹ và Ấn Độ) về bảo đảm ATTT cho hệ thống SCADA/ICS và hệ thống tài chính - ngân hàng quan trọng.

Phát biểu tại Hội nghị, Thứ trưởng Nguyễn Thành Hưng nhấn mạnh, cần khẩn trương rà soát, hoàn thành việc xác định và xây dựng phương án bảo đảm ATTT cho các hệ thống thông tin cấp độ 4, cấp độ 5 trước tháng 11/2018 theo chỉ đạo của Thủ tướng Chính phủ. Trên cơ sở đó, rà soát, áp dụng các tiêu chuẩn, quy chuẩn kỹ thuật quốc gia và quốc tế. Các biện pháp bảo đảm ATTT cần tối thiểu đáp ứng yêu cầu của tiêu chuẩn quốc gia TCVN 11930 năm 2017.

Tại Hội nghị, các chuyên gia cùng các đại biểu khách mời đã tập trung vào thảo luận và chia sẻ các vấn đề có liên quan trong hoạt động bảo đảm ATTT cho hệ thống thông tin quan trọng; từ đó nghiên cứu, đề xuất và áp dụng các biện pháp, giải pháp nâng cao năng lực bảo đảm ATTT cho cơ quan, tổ chức của mình, góp phần vào công tác bảo đảm ATTT quốc gia nói chung.

Tham gia chương trình, các đơn vị được nâng cao kiến thức, kỹ năng về bảo đảm an toàn thông tin mạng. Đồng thời, các đơn vị được trải nghiệm thực tế các cuộc tấn công/phòng thủ mạng, từ đó được trang bị thêm kỹ năng và kinh nghiệm thực tiễn để triển khai công tác bảo đảm an toàn cho hệ thống thông tin quan trọng của quốc gia./.

Vai trò của Trung tâm điều hành an toàn thông tin trong việc triển khai chính quyền điện tử tỉnh Thanh Hóa

TRẦN NGỌC HƯNG
Phó Trưởng phòng Quản trị hệ thống
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, ngày càng có 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. Cùng với sự phát triển này, các đối tượng tấn công và hình thức tấn công mạng cũng ngày một đa dạng, phức tạp... Những cuộc tấn công này không chỉ gây đình trệ hệ thống, tiết lộ thông tin nhạy cảm, mà còn công khai nhiều tài liệu mật của các quốc gia gây tổn thất về chính trị, ngoại giao.

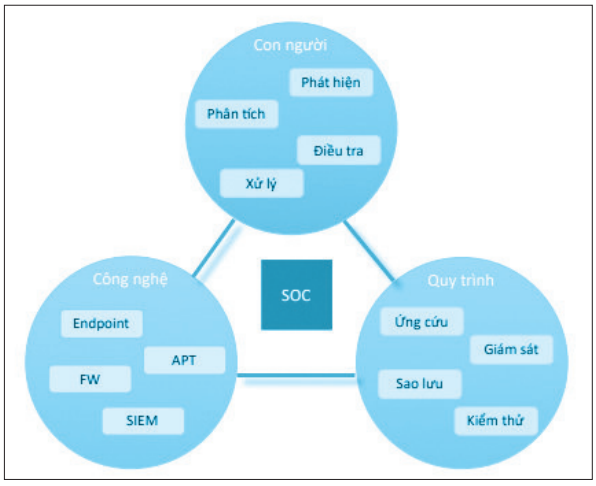
Trong thời gian qua, thực hiện chỉ đạo của Chính phủ trong việc xây dựng Chính phủ điện tử, tỉnh Thanh Hóa đã xây dựng Đề án "Xây dựng Chính quyền điện tử và phát triển các dịch vụ thành phố thông minh tỉnh Thanh Hóa giai đoạn 2017 - 2020" với các mục tiêu hướng tới xây dựng Chính quyền điện tử tỉnh Thanh Hóa. Việc triển khai xây dựng chính quyền điện tử thông qua thúc đẩy phát triển và ứng dụng CNTT sẽ xuất hiện những nguy cơ mới về mất an toàn thông tin và tiềm ẩn những mối đe dọa nghiêm trọng đến hoạt động của toàn bộ hệ thống. Bởi vậy, đã đặt ra nhiệm vụ đảm bảo an toàn thông tin mạng cho các hệ thống thông tin của các cơ quan, tổ chức trên địa bàn tỉnh nhằm tránh khỏi những hiểm họa mất an toàn thông tin trước những tấn công mạng có thể xảy ra. Để có thể làm việc này cần phải triển khai xây dựng Trung tâm điều hành an ninh mạng (SOC) của tỉnh, trong đó phải có một hệ thống giám sát an toàn mạng (GSATM) phù hợp nhằm kiểm soát, thu thập toàn bộ lưu lượng dữ liệu vào ra cho cả một hệ thống thông tin và đưa ra những cảnh báo chính xác tới người quản trị hệ thống khi có tấn công xảy ra.

Để bảo đảm an toàn thông tin cho các hệ thống thông tin các cơ quan, tổ chức đã trang bị nhiều thiết bị, công nghệ khác nhau để hỗ trợ việc đảm bảo an ninh thông tin hệ thống. Tuy nhiên, trên thực tế kể cả khi được cập nhật liên tục, các hệ thống bảo mật vẫn không thể theo kịp tốc độ xuất hiện của các loại hình tấn công mới. Do

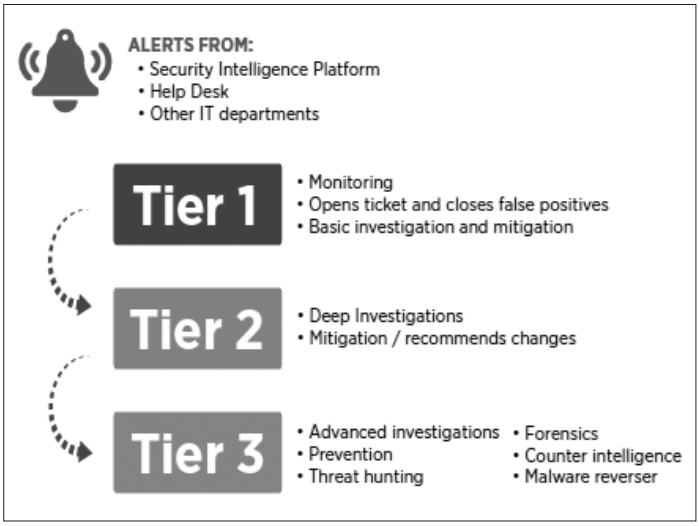
đó, đặt ra nhu cầu cần có những đơn vị tập trung để xử lý các vấn đề an ninh, có khả năng xử lý nhanh các sự cố và giám sát liên tục để phát hiện các bất thường dù là nhỏ nhất. Đồng thời là nơi xây dựng các giải pháp tổng thể nhằm ứng phó với các cuộc tấn công được lên kế hoạch kỹ lưỡng.

Mô hình Trung tâm Điều hành An toàn thông tin (SOC) sẽ cung cấp một giải pháp tổng thể cho vấn đề an ninh thông tin. Về cơ bản, nhiệm vụ của Trung tâm SOC bao gồm: Giám sát, phát hiện các bất thường trong hệ thống; kiện toàn hệ thống, ngăn ngừa các vụ việc mất an toàn thông tin; Phản ứng, điều tra, xử lý lại các sự cố, mối đe dọa; Kiểm soát và đánh giá mức độ tuân thủ của tổ chức. Bên cạnh đó, Trung tâm SOC còn có thể gián tiếp thực hiện các mục tiêu: Thu hẹp khoảng cách giữa việc vận hành CNTT và bảo đảm ATTT; Quản trị tập trung tất cả các công nghệ phòng thủ, giám sát, cảnh báo; Đánh giá mức độ hiệu quả trong công việc đầu tư bảo mật, vận hành hệ thống.

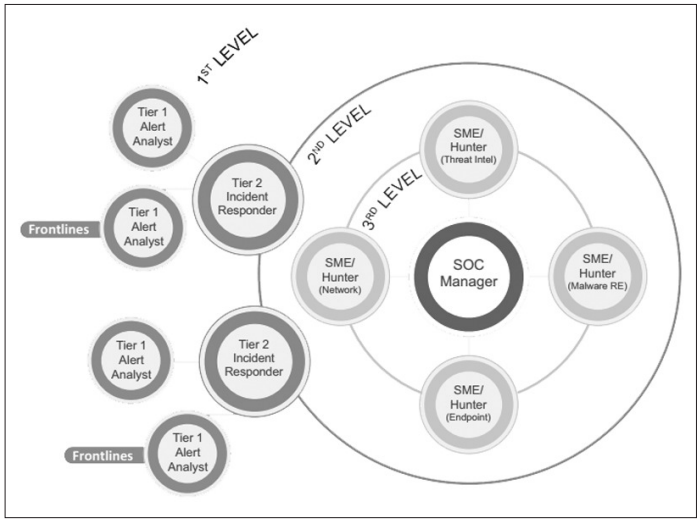
Trung tâm điều hành an ninh mạng (SOC) kết hợp giữa ba thành phần: Quy trình, Con người và Công nghệ. Các thành phần này thể hiện mối quan hệ như ở hình dưới đây. Ngoài các giải pháp công nghệ, những quy trình, chính sách chặt chẽ trong các khâu kết hợp với nguồn lực con người cũng đóng vai trò rất lớn trong đảm bảo an ninh.



- Quy trình: Là các quy định, quy trình, chính sách an ninh thông tin được triển khai trên hệ thống. Đây là bước mà các bộ phận phụ trách an ninh thông tin xác định những nguy cơ chính, thứ tự ưu tiên được mô hình hóa từ các dữ liệu thu thập và phân tích, từ đó đưa ra các biện pháp, cách thức được cách phát hiện và phòng chống, khắc phục. Các quy trình được thực hiện theo mô hình như ở hình dưới đây:



- Con người: Là những chuyên gia trong Trung tâm điều hành an ninh mạng, được phân công nhiệm vụ rõ ràng để phối hợp vận hành hệ thống. Mỗi vị trí đảm nhiệm một công việc trong hệ thống, tuân theo quy trình quy chuẩn của đơn vị; Bên cạnh đó cũng cần có sự hợp tác làm việc giữa các vị trí, các bộ phận để phát hiện, khắc phục sự cố. Sơ đồ phân tách các vị trí công việc gắn liền với nhân sự được thể hiện ở hình dưới đây:



Trong đó:

+ Alert Analyst: Những chuyên viên có nhiệm vụ theo dõi - giám sát, và cảnh báo từ hệ thống với thời gian 24/7; Khi có cảnh báo từ hệ thống, sẽ phân tích, đánh giá và chuyển tới Incident Responder hoặc SME/Hunter.

+ Incident Responder: Là những chuyên viên có nhiệm vụ tiếp nhận những cảnh báo từ Alert Analyst; Thực hiện ngăn chặn các sự cố được tiếp nhận.

+ SME/Hunter: Là những chuyên gia có kinh nghiệm làm việc, có chuyên môn cao. Trực tiếp xử lý các sự cố an ninh, điều tra, và đưa ra các điều lệnh ngăn chặn các sự cố.

+ SOC Manager: Là người quản lý hệ thống SOC. Tiếp nhận các thông tin báo cáo, phân tích từ các SME/Hunter; Người phát ngôn khi có sự cố xảy ra với hệ thống.

- Công nghệ: Một trong số các giải pháp công nghệ trọng tâm của Trung tâm SOC là hệ thống giám sát an toàn thông tin mạng (SIEM) đóng vai trò quan trọng trong việc đảm bảo an toàn thông tin cho toàn bộ Trung tâm. Hệ thống này cho phép thu thập, chuẩn hóa, lưu trữ và phân tích tương quan toàn bộ các sự kiện an toàn mạng được sinh ra trong hệ thống CNTT của tổ chức; Đây cũng chính là thành phần cốt lõi trong một Trung tâm SOC.

Hệ thống GSATM đóng vai trò rất quan trọng không thể thiếu trong hạ tầng CNTT. Thực hiện giám sát mọi hoạt động của hệ thống, tình trạng hoạt động của toàn bộ các thành phần tham gia như ứng dụng, thiết bị,... thu thập, chuẩn hóa, lưu trữ và phân tích tương quan toàn bộ các sự kiện an toàn mạng được sinh ra trong hệ thống thông tin của tổ chức. Qua đó, kịp thời phát hiện và đưa ra cảnh báo toàn diện vấn đề an toàn thông tin trong hệ thống.

Hệ thống GSATM đã phát triển qua các công nghệ: quản lý thông tin an toàn (Security infomation management - SIM), quản lý sự kiện an toàn (Security Event Management - SEM) và giải pháp quản lý phân tích sự kiện ATTT (Security Information and Event Management - SIEM).

- Hệ thống SIM tự động thu thập dữ liệu, ghi sự kiện từ các thiết bị an toàn, chẳng hạn như tường lửa, máy chủ, hệ thống phát hiện xâm nhập và phần mềm chống virus. Hệ thống dịch các dữ liệu, ghi vào các định dạng tương quan đơn giản; Do chưa có thành phần phân tích và xử lý sự kiện an ninh, nên SIM chỉ có thể phát hiện và xử lý được các biến cố đơn giản.

- Hệ thống SEM thu thập các dữ liệu sự kiện, nhật ký do các thành phần (thiết bị, ứng dụng) trong hệ thống tạo ra. Sau đó tập trung hóa việc lưu trữ và xử lý, phân tích các sự kiện, rồi lập báo cáo, đưa ra thông báo, cảnh báo liên quan đến vấn đề an ninh, an toàn của hệ thống; Hạn chế của SEM là không có khả năng lưu trữ nhật ký trong thời gian dài.

SIEM là một giải pháp hoàn chỉnh kết hợp từ SIM và SEM, cho phép các tổ chức thực hiện việc giám sát các sự kiện ATTT cho một hệ thống. Nó được xây dựng trên những ưu điểm của hai giải pháp SIM, SEM và bổ sung thêm các tính năng mới nhằm mục đích tăng cường hiệu quả trong việc giám sát an toàn mạng. Nguyên lý cơ bản của SIEM là thu thập các dữ liệu về các sự kiện an toàn từ nhiều thiết bị khác nhau, ở các vị trí khác nhau trong hệ thống. Từ đó giúp người quản trị có thể dễ dàng theo dõi tất cả các dữ liệu ở tại một vị trí duy nhất để phát hiện xu hướng và theo dõi các dấu hiệu bất thường, cũng như các dấu hiệu tấn công mạng có thể xảy ra. Một điểm mạnh nữa của SIEM là khả năng giám sát, quản lý người dùng và sự thay đổi cấu hình cho các hệ thống khác nhau, cung cấp khả năng kiểm soát đăng nhập, xem xét và ứng phó sự cố.

Về cơ bản hệ thống GSATM tuân thủ theo mô hình SIEM. Đây là mô hình chung cho hệ thống GSATM được sử dụng phổ biến hiện nay trên thế giới. Đối với hệ thống GSATM chức năng chính của nó là sẽ thu thập dữ liệu, phân tích và lưu trữ dữ liệu, cảnh báo.

Bài số sau, tác giả sẽ cung cấp thêm về việc triển khai mô hình giám sát tại các cơ quan, đơn vị trên địa bàn tỉnh Thanh Hóa trong việc giám sát an toàn thông tin mạng tập trung phục vụ xây dựng Chính quyền điện tử./.

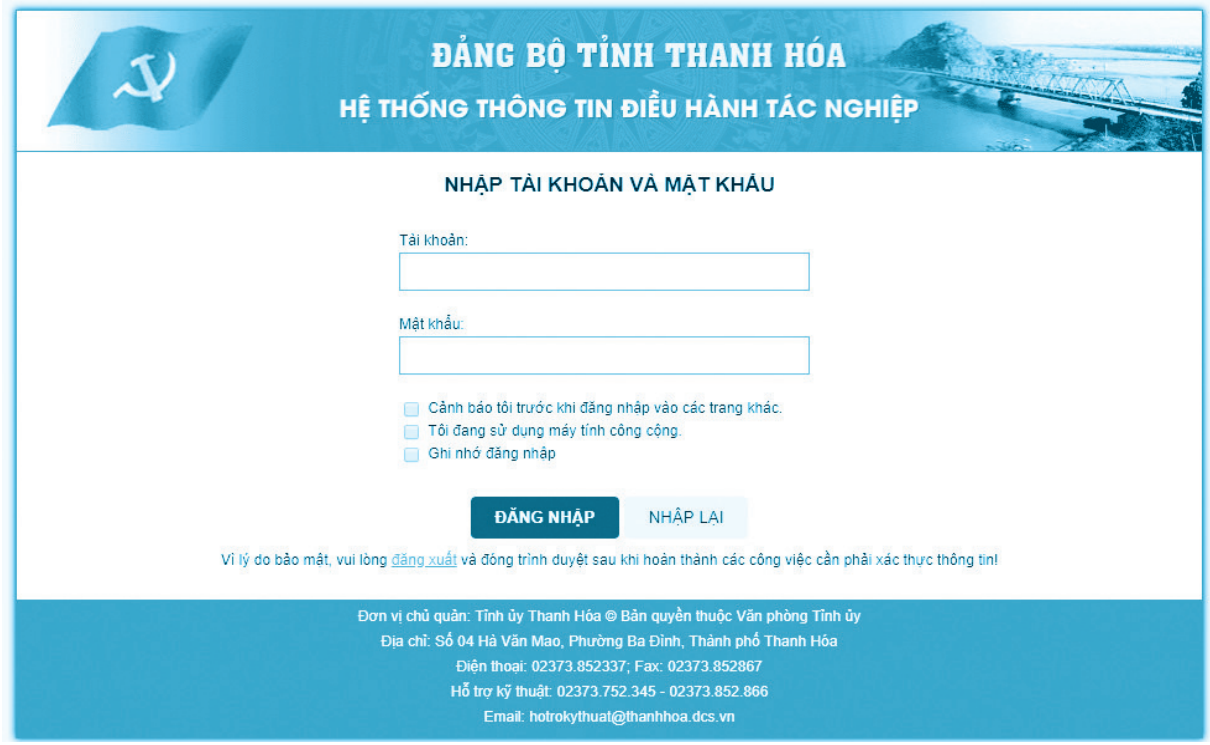
Công tác bảo đảm an toàn thông tin trong việc triển khai ứng dụng CNTT trong các cơ quan đảng tỉnh Thanh Hóa

LÊ TRUNG ANH
Phòng Cơ yếu - CNTT
Văn phòng Tỉnh ủy Thanh Hóa

Công nghệ thông tin (CNTT) là một trong những hạ tầng quan trọng của quốc gia, vừa là ngành kinh tế - kỹ thuật, vừa là ngành hạ tầng mềm phục vụ phát triển kinh tế - xã hội, đảm bảo an ninh quốc phòng và chủ quyền số. Tuy nhiên, cùng với quá trình đẩy mạnh ứng dụng CNTT, các nguy cơ về lộ lọt, mất an toàn thông tin cũng ngày càng tăng và những hình thức tấn công trên mạng ngày càng đa dạng, tinh vi, nguy hiểm. Ứng dụng Công nghệ thông tin đi đôi với an toàn, an ninh thông tin đang là vấn đề "nóng" và đang được nhiều quốc gia, nhiều tổ chức và cộng đồng đặc biệt quan tâm.

Thực hiện các Đề án tin học hóa hoạt động của cơ quan Đảng giai đoạn 2001 - 2005 (Đề án 47); giai đoạn 2006 - 2011 (Đề án 06), đến nay hạ tầng kỹ thuật về Công nghệ thông tin (CNTT) của các cơ quan Đảng tỉnh Thanh Hóa đã được đầu tư xây dựng, lắp đặt đưa vào sử dụng khá đồng bộ. Việc phát triển và ứng dụng CNTT của các cấp ủy đảng tỉnh Thanh Hóa đã có những chuyển biến cơ bản cả về nhận thức và hành động; công tác lãnh đạo, chỉ đạo ứng dụng CNTT gắn với cải cách hành chính và đổi mới phương thức lãnh đạo của Đảng đã góp phần nâng cao chất lượng, hiệu quả các mặt công tác, đổi mới lề lối tác phong làm việc; chất lượng, hiệu quả trong công tác chuyên môn từng bước được nâng lên rõ rệt. Phần lớn các văn bản đi/đến như các báo cáo định kỳ, đột xuất đã được thực hiện bằng mạng máy tính; nhiều đơn vị đã sử dụng các phần mềm để phục vụ điều hành tác nghiệp đi vào hoạt động có nền nếp. Các công tác quản lý về nghiệp vụ văn thư, lưu trữ, quản lý thẻ, hồ sơ đảng viên, xử lý đơn thư, khiếu tố, kế toán, quản lý tài sản thuận lợi và khoa học hơn.

Việc triển khai ứng dụng công nghệ thông tin phải gắn kết chặt chẽ với việc bảo đảm an toàn, an ninh và bảo mật thông tin. Công tác bảo đảm an ninh, an toàn mạng luôn được đề cao. Thực hiện nghiêm túc Chỉ thị số 28-CT/TW ngày 16/9/2013 của Ban Bí thư trung ương Đảng "về tăng cường công tác đảm bảo an toàn thông tin mạng"; Chỉ thị số 14/CT-TTg ngày 25/05/2018 của Thủ tướng Chính phủ "về việc nâng cao năng lực phòng, chống phần mềm độc hại"; các cảnh báo của Cục An toàn thông tin - Bộ thông tin và truyền thông về các phần mềm độc hại đang phát tán trên mạng Internet... Các cơ quan đảng trong tỉnh luôn tuân thủ theo quy chế quản lý, sử dụng và bảo vệ mạng thông tin diện rộng của Đảng, không kết nối mạng máy tính nội bộ với mạng Internet, triển khai hệ thống ATK (tường lửa mềm), các thiết bị tường lửa cứng (Firewall), thiết bị phát hiệm xâm nhập trái phép (IPS), thiết bị bảo mật ASA, định tuyến Router, phân vùng VLAN; hệ thống backup SAN, cài đặt hệ thống phòng, chống virus, hệ điều hành, phần mềm hệ thống có bản quyền. Các thiết bị tin học được các cơ quan chức năng kiểm tra an ninh trước khi đưa vào sử dụng; sử dụng các giải pháp bảo mật chứng thư số, chữ ký số, các thiết bị bảo



Hệ thống thông tin điều hành tác nghiệp trong các cơ quan Đảng.

mật truyền hình hội nghị trực tuyến,...

Ứng dụng các giải pháp bảo đảm an toàn, bảo mật của Ban Cơ yếu Chính phủ cho dữ liệu lưu trữ và trao đổi trên mạng như: bảo mật văn bản điện tử cấp độ "tuyệt mật, tối mật" gửi, nhận trên mạng, thiết bị bảo mật đường truyền hội nghị truyền hình trực tuyến; triển khai thiết bị nhớ an toàn. Triển khai hệ thống diệt virus thống nhất trên toàn bộ hệ thống mạng diện rộng của Đảng, được phân cấp và quản trị, cấu hình tập trung. Thường xuyên cập nhật, thông báo thông tin về nguy cơ, hiểm hoạ mất an toàn hệ thống, an ninh thông tin trong các hoạt động ứng dụng CNTT; quán triệt, nâng cao nhận thức, ý thức trách nhiệm và kỹ năng sử dụng cho người dùng về các biện pháp bảo đảm an toàn hệ thống và an ninh thông tin, bảo vệ bí mật của Đảng và Nhà nước trong hoạt động ứng dụng CNTT. Thực hiện các giải pháp kỹ thuật thực hiện quản lý người dùng tập trung trong mạng máy tính nội bộ (trong mỗi cơ quan và trong toàn bộ hệ thống các cơ quan đảng); kiểm soát, giám sát hoạt động truy nhập, khai thác thông tin trong mạng; sao lưu, bảo vệ dữ liệu hệ thống và các ứng dụng.

Thực hiện kế hoạch ứng dụng CNTT trong các cơ quan đảng giai đoạn 2015 - 2020 sẽ tích hợp các hệ thống cơ sở hạ tầng và hệ thống thông tin của cơ quan Đảng theo mô hình kiến trúc thống nhất của Trung ương; bảo đảm các ứng dụng CNTT đều thiết thực, hiệu quả, tiết kiệm và gắn kết chặt chẽ giữa tính tiện lợi với bảo đảm an toàn thông tin, bảo vệ bí mật của Đảng và Nhà nước; Các giao dịch giữa các cơ quan đảng được thực hiện trên môi trường mạng máy tính nội bộ và Internet có quản lý tập trung; góp phần đắc lực vào đổi mới phương thức, lề lối làm việc, cải cách thủ tục hành chính trong Đảng, tăng cường công tác cải tiến quy trình làm việc, chuẩn hoá quy trình, nghiệp vụ để ứng dụng CNTT đạt hiệu quả cao; phục vụ trực tiếp các cấp uỷ Đảng trong việc xây dựng các văn bản lãnh đạo, chỉ đạo.

Các cơ quan Đảng dần hoàn thiện cơ sở hạ tầng kỹ thuật và hệ thống bảo mật, an toàn thông tin: Hệ thống mạng thông tin diện rộng các cơ quan

Đảng kết nối với nhau qua mạng truyền số liệu chuyên dùng trên đường truyền chủ yếu là cáp quang, các đơn vị định tuyến thành mạng ngang hàng có thể truy cập trực tiếp sang vùng công cộng của nhau mà không cần hệ thống ủy quyền (Proxy). Đã xây dựng Trung tâm tích hợp dữ liệu (Data Center), cấu hình, cài đặt, tập trung các máy chủ, dữ liệu của các huyện, thị, thành phố, thuận lợi hơn trong công tác quản lý, cài đặt, triển khai, vận hành, bảo trì, bảo đảm an toàn, an ninh thông tin. Phòng họp trực tuyến đã được xây dựng và sử dụng thường xuyên giữa trung ương với tỉnh, tỉnh với các huyện mang lại hiệu quả, tiết kiệm thời gian, chi phí tổ chức hội nghị

Xuất phát từ yêu cầu cấp thiết phục vụ công việc, Văn phòng Tỉnh ủy đã chú trọng đầu tư xây dựng các hệ thống thông tin đặc thù và các hệ thống thông tin, hòm thư công vụ trên Internet theo tên miền do Văn phòng Trung ương Đảng cấp (.dcs.vn) sử dụng để trao đổi thông tin không mật. Tại các đảng ủy xã, phường, thị trấn trong tỉnh đã chuyển đổi sang sử dụng các ứng dụng và thư điện tử công vụ trên Internet để thuận tiện trong trao đổi thông tin, đáp ứng yêu cầu, đúng quy định, giảm chi phí đảm bảo an toàn.

Để công tác bảo đảm an toàn, an ninh thông tin có hiệu quả hơn, đồng thời đẩy mạnh ứng dụng công nghệ thông tin trong toàn đảng bộ, các cơ quan đảng, nhà nước, doanh nghiệp và người dân cần thực hiện tốt một số giải pháp sau:

Một là: Quán triệt, chỉ đạo thực hiện chấp hành nghiêm Luật An toàn thông tin mạng, Chỉ thị số 28-CT/TW ngày 16/9/2013 của Ban Bí thư trung ương Đảng ; Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ; Luật Cơ yếu, Pháp lệnh Bảo vệ bí mật Nhà nước và các nghị quyết, chỉ thị, văn bản chỉ đạo của Đảng, Nhà nước về công tác đảm bảo an toàn thông tin, bảo vệ bí mật Nhà nước.

Hai là: Đẩy mạnh tuyên truyền, giáo dục cho cán bộ, đảng viên và nhân dân nhận thức rõ tầm quan trọng của an toàn thông tin. Nâng cao ý thức, trách nhiệm, chấp hành pháp luật về an toàn thông tin.

Ba là: Ban hành quy định nội bộ về đảm bảo an toàn thông tin. Trang bị đầy đủ các kiến thức cơ bản về máy tính, mạng máy tính, bảo mật thông tin, các quy định của pháp luật về an toàn thông tin cho cán bộ, đảng viên, công chức, viên chức trong khai thác, sử dụng, vận hành các hệ thống thông tin.

Bốn là: Quan tâm bố trí, tuyển dụng, đào tạo cán bộ chuyên trách về CNTT có phẩm chất chính trị vững vàng, đủ năng lực, trình độ chuyên môn để trực tiếp quản lý, vận hành hệ thống mạng và các hệ thống thông tin của cơ quan, đơn vị, địa phương.

Năm là: Chủ động xây dựng và triển khai các biện pháp phòng ngừa, kế hoạch ứng phó sự cố an toàn thông tin, đấu tranh ngăn chặn, đẩy lùi thông tin xấu, độc hại trên mạng, đặc biệt là mạng xã hội. Thường xuyên tự kiểm tra, đánh giá công tác đảm bảo an toàn thông tin của cơ quan, đơn vị, địa phương./.

Thông tin chung về lỗ hổng bảo mật

- Lỗ hổng bảo mật là khiếm khuyết của các thành phần phần mềm, phần cứng hoặc của toàn bộ hệ thống có thể bị sử dụng để thực hiện các mối đe dọa an toàn thông tin (ATTT) của hệ thống. Bất kỳ hệ thống nào cũng đều có những lỗ hổng nhất định, chúng có thể được sinh ra trong mọi giai đoạn thuộc vòng đời của hệ thống.

- Lỗ hổng bảo mật Websitelà những điểm yếu nằm trong thiết kế và cấu hình của hệ thống, lỗi của lập trình viên hoặc sơ suất trong quá trình vận hành.

1. Lỗ hổng bảo mật Injection (Lỗi chèn mã độc): Injection là lỗ hổng xảy ra do sự thiếu sót trong việc lọc các dữ liệu đầu vào không đáng tin cậy. Khi bạn truyền các dữ liệu chưa được lọc tới Database (Ví dụ như lỗ hổngSQL injection), tới trình duyệt (lỗ hổng XSS), tới máy chủ LDAP (lỗ hổng LDAP Injection) hoặc tới bất cứ vị trí nào khác.

HÀ TUẤN ANH
Trung tâm CNTT - Sở Tài nguyên và Môi trường

Cách ngăn chặn lỗ hổng: Để chống lại lỗ hổng này chỉ "đơn giản" là vấn đề bạn đã lọc đầu vào đúng cách chưa hay việc bạn cân nhắc liệu một đầu vào có thể được tin cậy hay không. Về căn bản, tất cả các đầu vào đều phải được lọc và kiểm tra trừ trường hợp đầu vào đó chắc chắn đáng tin cậy. (Tuy nhiên, việc cẩn thận kiểm tra tất cả các đầu vào là luôn luôn cần thiết).

2. Broken Authentication: Đây là nhóm các vấn đề có thể xảy ra trong quá trình xác thực. Ví dụ như: URL có thể chứa Session ID và rò rỉ nó trong Referer Header của người dùng khác; Mật khẩu không được mã hóa hoặc dễ giải mã trong khi lưu trữ; Lỗ hổng Session Fixation; Tấn công Session Hijacking có thể xảy ra khi thời gian hết hạn của session không được triển khai đúng hoặc sử dụng HTTP (không bảo mật SSL)...

Cách ngăn chặn lỗ hổng: Cách đơn giản nhất để tránh lỗ hổng bảo mật web này là sử dụng một framework.

3. Lỗ hổng XSS (Cross Site Scripting): Đây là một lỗ hổng rất phổ biến. Kẻ tấn côngchèn các đoạn mã JavaScriptvào ứng dụng web. Khi đầu vào này không được lọc, chúng sẽ được thực thi mã độc trên trình duyệt của người dùng. Kẻ tấn công có thể lấy được cookie của người dùng trên hệ thông hoặc lừa người dùng đến các trang web độc hại.

Cách ngăn chặn lỗ hổng: Có một cách bảo mật web đơn giản đó là không trả lại thẻ HTML cho người dùng. Thông thường cách giải quyết đơn giản chỉ là Encode (chuyển đổi về dạng dữ liệu khác) tất cả các thẻ HTML. Ví dụ thẻ <script> được trả về dưới dạng <script&gt.

4. Lỗ hổng Insecure Direct Object References: Lỗ hổng này xảy ra khi chương trình cho phép người dùng truy cập các tài nguyên (dữ liệu, file, database). Nếu không thực hiện quá trình kiểm soát quyền hạn (hoặc quá trình này không hoàn chỉnh) kẻ tấn công có thể truy cập

một cách bất hợp pháp vào các dữ liệu nhạy cảm, quan trọng trên máy chủ.

Cách ngăn chặn lỗ hổng:

- Test cẩn thận: Nguyên nhân gây ra lỗi thường là do sự bất cẩn của developer. Tuy nhiên, nếu để sản phẩm bị lỗi thì đây là lỗi của tester. Đây là lỗi nằm trong code, do đó tester phải chịu trách nhiệm nếu để lỗi này xảy đến với người dùng.

- Bảo vệ dữ liệu "nhảy cảm": Với những dữ liệu như source code, config, database key, cần hạn chế truy cập. Cách tốt nhất là chỉ cho phép các IP nội bộ truy cập các dữ liệu này.

- Kiểm tra chặt chẽ quyền truy cập của người dùng.

5. Security Misconfiguration (Sai sót cấu hình an ninh): Do việc cấu hình an ninh lỏng lẻo tại các tầng trong kiến trúc web như nền tảng, OS, máy chủ ứng dụng, webserver, database,... khiến cho kẻ tấn công có thể khai thác vào các ứng dụng, ví dụ như sau: Chạy ứng dụng khi chế độ debug được bật; Directory listing; Sử dụng phần mềm lỗi thời (WordPress plugin, PhpMyAdmin cũ); Cài đặt các dịch vụ không cần thiết; Không thay đổi default key hoặc mật khẩu; Trả về lỗi xử lý thông tin cho kẻ tấn công lợi dụng để tấn công.

Cách ngăn chặn lỗ hổng: Có một quá trình "xây dựng và triển khai" tốt. Cần một quá trình audit chính xác bảo mật trên máy chủ trước khi triển khai.

6. Sensitive data exposure (Rò rỉ dữ liệu nhạy cảm): Các dữ liệu nhạy cảm không được lưu trữ và bảo vệ cẩn thận, dẫn đến khi bị kẻ tấn công khai thác gây ra những ảnh hưởng cho hệ thống máy chủ và khách hàng.

Cách ngăn chặn lỗ hổng:

- Sử dụng HTTPS có chứng chỉ phù hợp và PFS (Perfect Forward Secrecy). Không nhận bất cứ thông tin gì trên các kết nối không phải là HTTPS. Có cờ an toàn trên cookie.

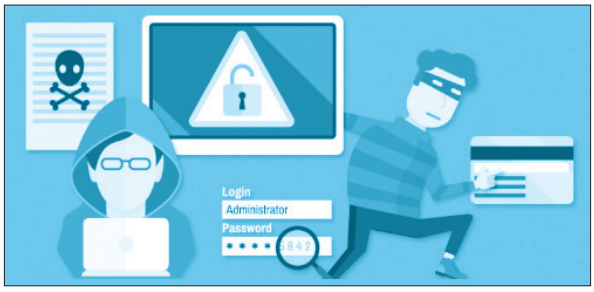
- Cần hạn chế các dữ liệu nhạy cảm có khả năng bị lộ của mình. Nếu bạn không cần những dữ liệu nhạy cảm này, hãy hủy nó.

- Nếu bạn có dữ liệu nhạy cảm mà bạn thực sự cần, lưu trữ mã hóa nó và đảm bảo rằng tất cả các mật khẩu được sử dụng hàm Hash để bảo vệ. Không lưu trữ các khóa mã hóa bên cạnh dữ liệu được bảo vệ.

7. Missing function level access control (lỗi phân quyền): Do thiếu các điều khoản trong việc phân quyền quản trị các mức, dẫn đến việc kẻ tấn công có thể lợi dụng và truy ra các điểm yếu trên hệ thống hay lợi dụng để leo thang đặc quyền.

Cách ngăn chặn lỗ hổng: Ở phía máy chủ, phải luôn được phân quyền một cách triệt để từ khâu thiết kế.

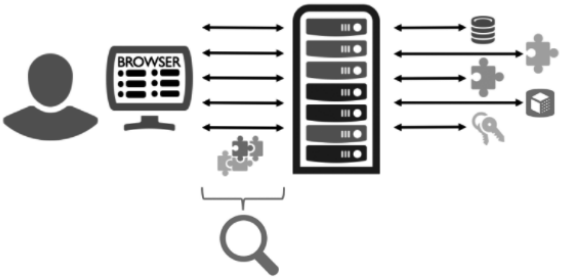
8. Cross Site Request Forgery (CSRF): Lợi dụng sơ hở của nạn nhân, kẻ tấn công có thể lừa nạn nhân thực hiện các hành động nguy hiểm mà nạn nhân không hề hay biết, ví dụ như chuyển tiền từ tài khoản nạn nhân sang tài khoản kẻ tấn công, thông qua các lỗ hổng XSS.



Cách ngăn chặn lỗ hổng: Lưu trữ một Token bí mật trong một trường form ẩn mà không thể truy cập được từ trang web của bên thứ ba. Tất nhiên bạn phải xác minh trường ẩn này. Một số trang web yêu cầu mật khẩu của bạn cũng như khi sửa đổi các cài đặt nhạy cảm.

9. Using component with known vulnerabilities: Do việc sử dụng mà không kiểm duyệt các thư viện, plugin, module, ứng dụng... có tồn tại các lỗ hổng đã được công khai, từ đó kẻ tấn

công có thể lợi dụng để tấn công vào hệ thống và thực hiện các mục đích xấu.



Cách ngăn chặn lỗ hổng: Chú ý cẩn thận khi sử dụng các thành phần của bên thứ 3. Kiểm tra cẩn thận các đoạn code quan trọng của bạn. Nếu các đoạn code này có lỗ hổng, tin tặc có thể đọc cơ sở dữ liệu, tệp tin cấu hình, mật khẩu... của bạn. Đảm bảo bạn đang sử dụng phiên bản mới nhất của tất cả mọi thứ và có kế hoạch cập nhật chúng thường xuyên.

10. Unvalidated redirects and forwards: Việc chuyển hướng không an toàn người dùng đến một đường dẫn bên ngoài có thể bị kẻ tấn công lợi dụng để chuyển hướng nạn nhân đến một trang đích được chuẩn bị sẵn của kẻ tấn công..

Cách ngăn chặn lỗ hổng:

- Không sử dụng chức năng chuyển hướng
- Có một danh sách tĩnh các vị trí hợp lệ để chuyển hướng đến.
- Có Whitelist tham số người dùng xác định.

Hướng dẫn ngăn chặn MÃ ĐỘC ĐÀO TIỀN ẢO TRÊN TRÌNH DUYỆT

NGUYỄN THỊ LIÊN
Trung tâm CNTT&TT Thanh Hóa

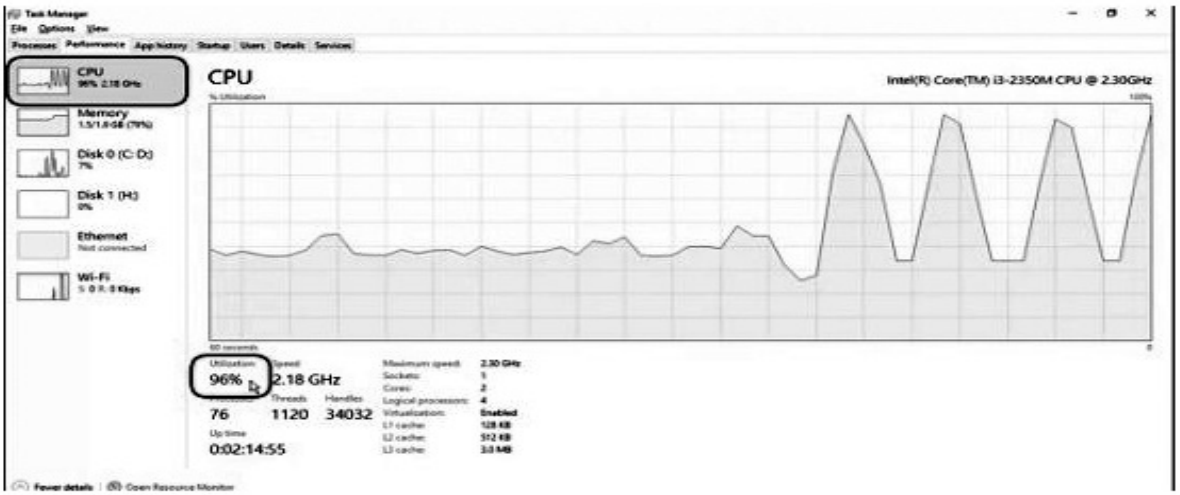
Thời gian qua, chứng kiến sự tăng giá chóng mặt của các đồng tiền ảo, tạo cơn sốt trên toàn cầu. Điều này cũng đã thúc đẩy hacker gia tăng mạng mẽ các hình thức tấn công nhằm biến máy tính người dùng thành công cụ đào tiền ảo. Hiện có 2 hình thức tấn công phổ biến nhất được hacker sử dụng là khai thác lỗ hổng website và lợi dụng mạng xã hội để phát tán virus.

Hacker thường chọn các website có nhiều người sử dụng để tấn công và cài mã độc có chức năng đào tiền ảo lên đó. Khi người dùng truy cập vào các website này, mã độc sẽ được kích hoạt. Với hơn 40% website tại Việt Nam tồn tại lỗ hổng có thể bị xâm nhập, khai thác, đây sẽ là đích nhắm của hacker trong việc phát tán mã độc đào tiền ảo.

Với hình thức thứ hai là hacker phát tán virus đào tiền ảo thông qua mạng xã hội. Sau khi lây nhiễm, mã độc sẽ âm thầm sử dụng tài nguyên của máy nạn nhân để chạy các chương trình đào tiền.

Đặc điểm chung của Mã độc đào tiền ảo sẽ khiến cho tốc độ xử lý của máy tính của người dùng trở nên chậm, có lúc gần như không thể chạy các phần mềm có yêu cầu tốc độ xử lý cao

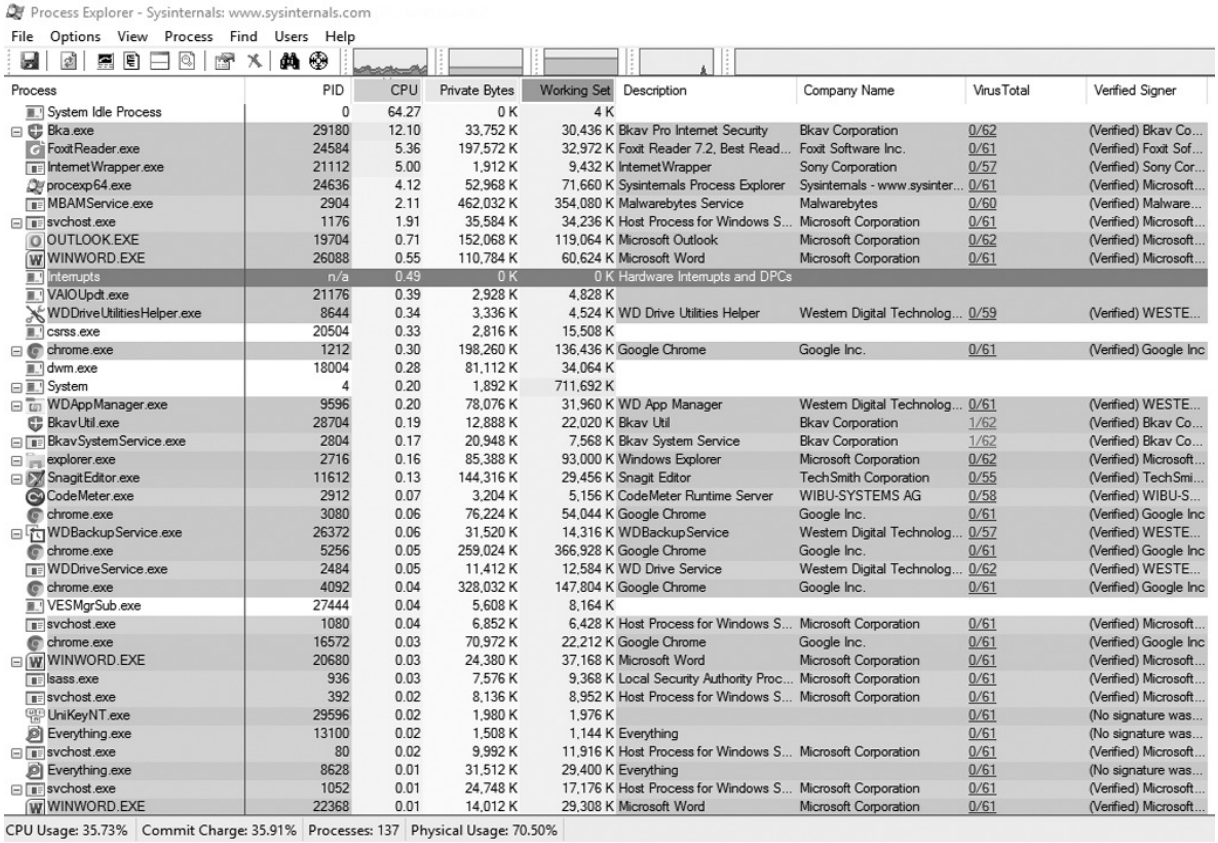
(chỉnh sửa ảnh hoặc video). Nếu người dùng chỉ sử dụng các phần mềm văn phòng bình thường sẽ không cảm nhận máy tính bị chậm, chỉ khi kết nối internet, dùng các phần mềm xử lý đồ họa, thiết kế mới thấy vấn đề này.



Cách thức ngăn chặn đào tiền ảo thông qua trình duyệt

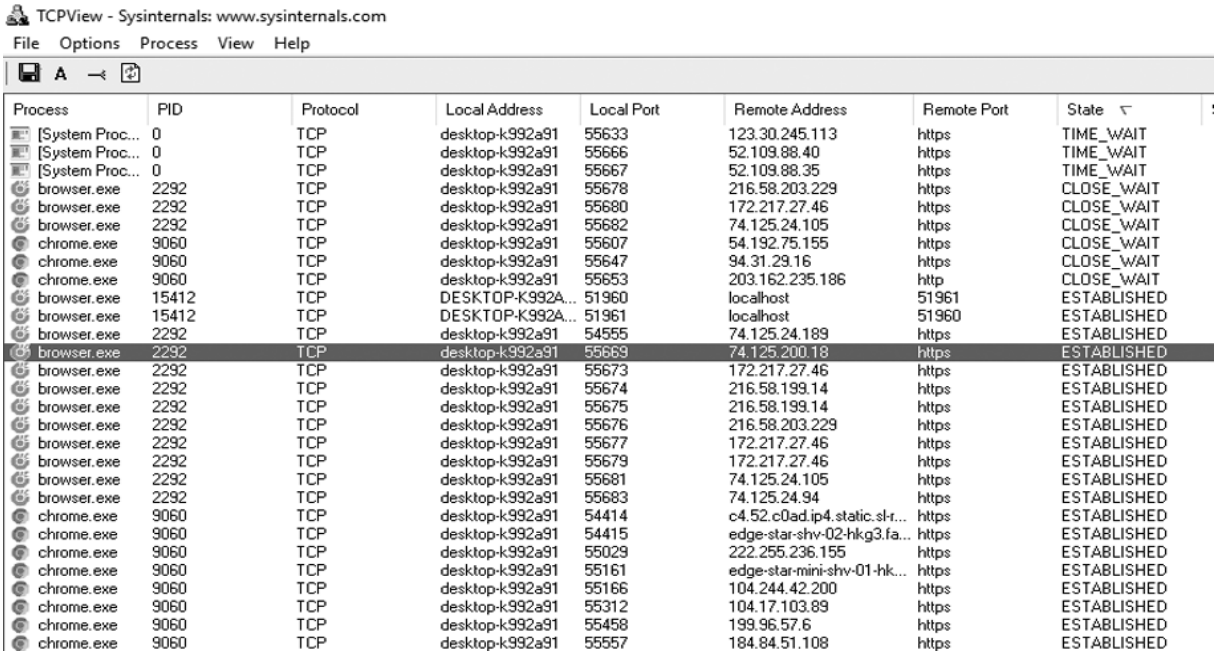
1. Kiểm tra hiệu năng máy tính và các kết nối

- 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.



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

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

No Coin Extension của Google Chrome được đánh khá khá hiệu quả khi chặn được các phần mềm như Coinhive. Nó có thể phát hiện ra các đoạn mã JavaScript sử dụng bởi miner và ngăn chặn trình duyệt truy cập vào website đó. Lưu ý extension này có thể khiến cho toàn bộ webpage không thể truy cập bằng các user khác.

- minerBlock (Chrome): https://chrome.google.com/webstore/detail/minerblock/emikbbbebcd-fohonlaifafnoanocnebl?hl=en

minerBlock là một extension có sẵn của Google Chrome có khả năng bảo vệ trình duyệt khỏi crypto jacking bằng hai phương thức khác nhau. Một là cách truyền thống chặn các request/scripts từ một danh sách blacklist thường được sử dụng bởi AdBlock và các phần mềm chặn miner. Cách thứ hai là phát hiện các hành vi đào tiền ảo tiềm tàng bên trong các đoạn script đã tải và xử lý ngay lập tức. Đây là ưu thế khiến minerBlock đem lại hiệu ứng tốt hơn với crypto jacking qua proxy.

- NoScript (Firefox): https://addons.mozilla.org/en-US/firefox/addon/noscript/

NoScripts là một Add-on chặn JavaScript cho Firefox, với quy định khá nghiêm ngặt. Nó sẽ vô hiệu

hóa hoàn toàn các nội dung JavaScript trên webpage, dẫn đến xử lý vô số website. NoScripts tích hợp hiệu quả với Tor Browser.

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

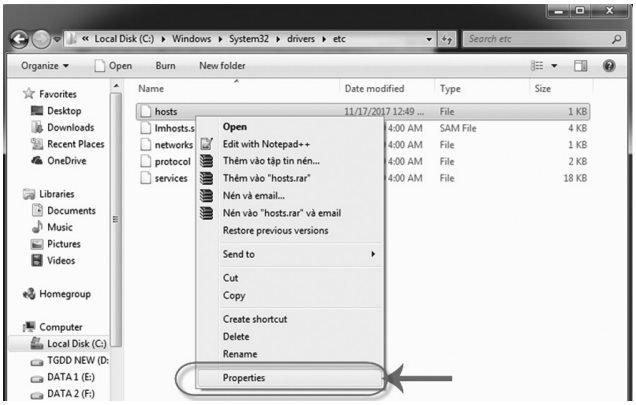
02 cách làm dưới đây giúp người dùng chặn kết nối đến các tên miền chứa mã độc đào tiền ảo mà không cần cài đặt bất kỳ phần mềm bên thứ 3. Tuy nhiên, hạn chế của cách thức này là cần phải xác định chi tiết danh sách tên miền cần chặn vì Hacker liên tục tạo mới danh sách các tên miền để điều khiển mã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

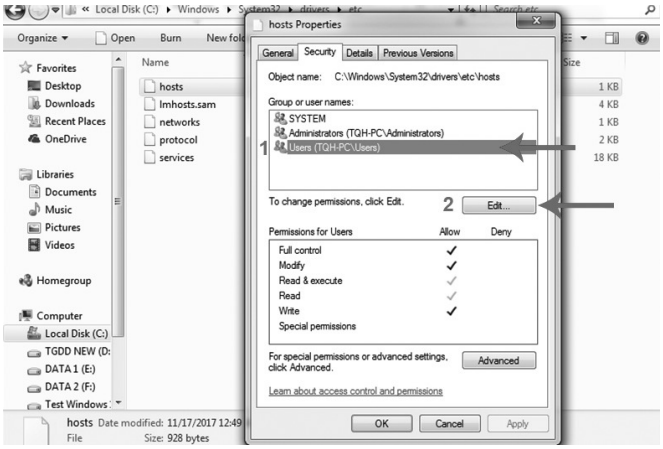
Cách 2: Sử dụng file host trên Windows để ngăn chặn quá trình phân giải tên miền cục bộ trên Windows.

Bước 1: Trên máy tính chạy Windows, bạn vào My Computer và truy cập đường dẫn sau:
C:\Windows\System32\drivers\etc.

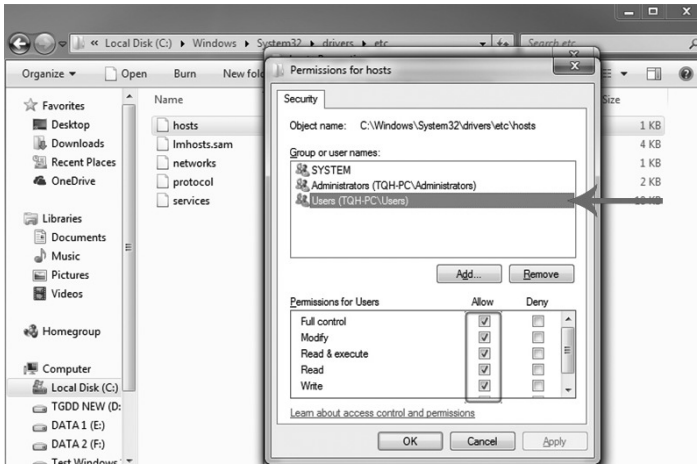
Bước 2: Click chuột phải vào tập tin **hosts** -> **Properties**...



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



...chọn tiếp vào mục **Users** -> Đánh dấu tích vào các ô tại mục **Allow**.



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

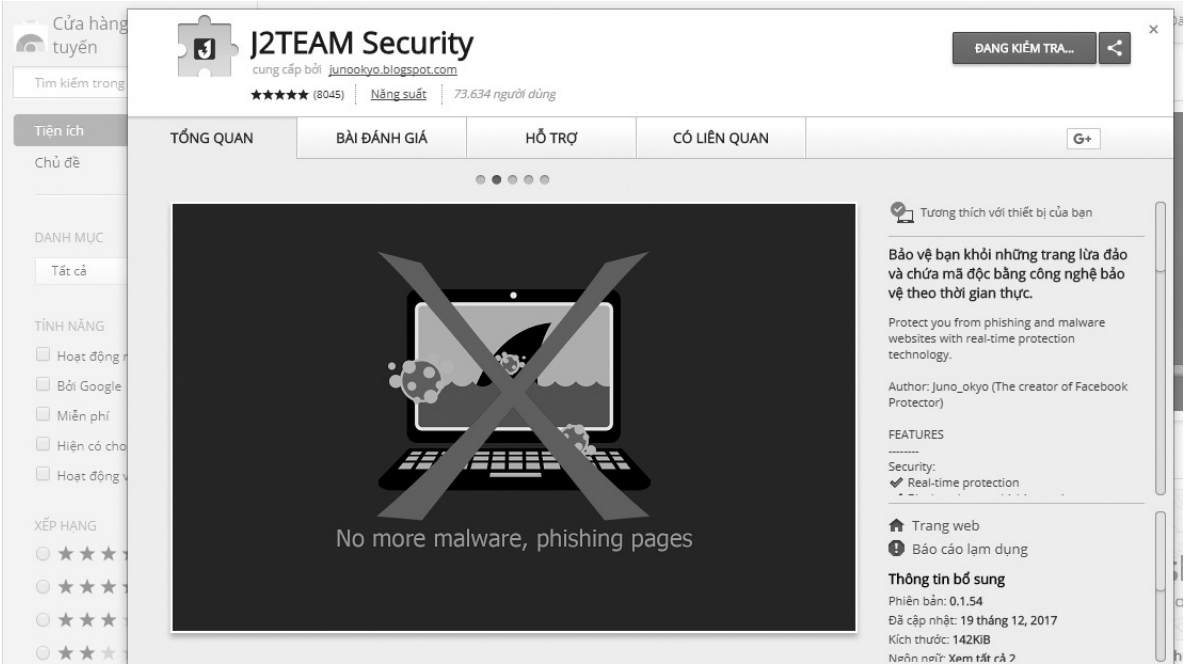
Bước 1: Sử dụng tiện ích trên trình duyệt

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.

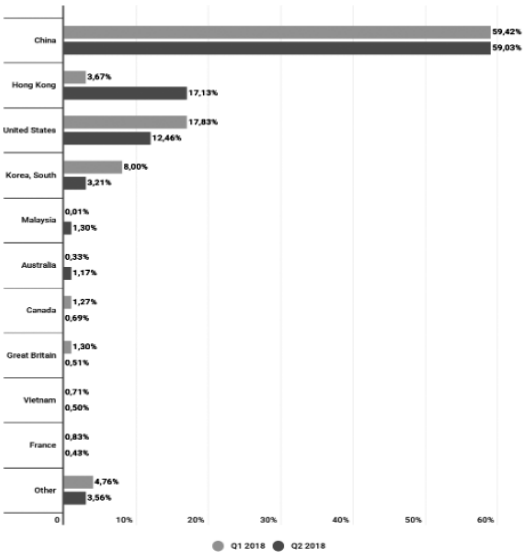
Thông tin liên hệ: Điện thoại: (0237) 3718699; Fax (0237) 3718299.

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

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

1. Tình hình tấn công DDoS

Theo báo cáo DDoS Intelligence mới nhất của Kaspersky Lab, trong quý II năm 2018, Trung Quốc là quốc gia đứng đầu danh sách hứng chịu các vụ tấn công DDoS, đứng thứ hai là Hồng Kông, thứ ba là Mỹ và ở vị trí thứ tư là Hàn Quốc. Trong số 10 quốc gia bị tấn công nhiều nhất, Việt Nam đứng thứ 9.



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

2. Thống kê danh sách các dịch vụ bị khai thác điểm yếu để tấn công

Theo tổng hợp của Kaspersky trong quý II/2018 danh sách các ứng dụng bị tội phạm mạng khai thác các điểm yếu/lỗ hổng để tấn công. Tỷ lệ khai thác của dịch vụ Telnet (75,4%) đứng ở vị trí số 1. Tiếp theo là khai thác thông qua dịch vụ SSH (11,59%) và HTTP (5,53%).

Trong số 10 quốc gia bị tấn công qua dịch vụ SSH đối với các thiết bị IoT thì Việt Nam đứng thứ 2 (11,38%). Đứng đầu là Trung Quốc (15,77%).

	Country	%*
1	China	15.77%
2	Vietnam	11.38%
3	USA	9.78%
4	France	5.45%
5	Russia	4.53%
6	Brazil	4.22%
7	Germany	4.01%
8	South Korea	3.39%
9	India	2.86%
10	Romania	2.23%

3. Tình hình tấn công bằng mã độc

Báo cáo tổng kết của Kaspersky Lab về tình hình mã độc hại trong quý II/2018 cho biết, Việt Nam đứng ở vị trí thứ 3 trong 10 nước bị tấn công bằng loại hình mã độc đòi tiền chuộc /mã hóa dữ liệu.

Thống kê danh sách các quốc gia có người dùng bị tấn công bằng mã độc đào tiền ảo. Theo đó, Việt Nam đứng ở vị trí thứ 8 (9,13%), vị trí số 1 về Ethiopia (17,84%), thứ 2 là Afghansitan (16,21%)

4. Tình hình Spam và tấn công Phishing

Báo cáo tổng kết của Kaspersky Lab về tình hình thư rác và lừa đảo trực tuyến trong quý II/2018 cho biết, Việt Nam tiếp tục nằm trong nhóm các quốc gia có nguồn phát tán thư rác đứng đầu với vị trí thứ 6 (3,98%), đứng thứ 1 là Trung Quốc (14,36%) và thứ 2 là Mỹ (12,11%).

Báo cáo của Kaspersky Lab về tình hình tấn công Phishing trên phạm vi toàn cầu trong quý II/2018. Dẫn đầu là Brazil với 15.51%, thứ 2 là Trung Quốc với 14.77%...

5. 5 loại mã độc đang lây nhiễm nhiều tại Việt Nam

Chia sẻ tại tọa đàm Nâng cao năng lực phòng, chống phần mềm độc hại theo Chỉ thị 14 Thủ tướng Chính phủ, được Cục An toàn thông tin - Bộ TT&TT phối hợp cùng Hiệp hội An toàn thông tin Việt Nam (VNISA) tổ chức chiều ngày 11/6, ông Vũ Ngọc Sơn, Phó chủ tịch phụ trách mảng Chống mã độc (Anti Malware) của Bkav cho biết, tỷ lệ lây nhiễm mã độc tại Việt Nam luôn ở mức rất cao; mỗi năm có trên 60 triệu lượt máy tính bị nhiễm mã độc.

Theo thống kê của Bkav, thiệt hại do virus máy tính gây ra cho người dùng Việt Nam đã liên tục tăng qua các năm, từ 8.500 tỷ đồng vào năm 2014 lên 8.700 tỷ đồng (năm 2015), 10.400 tỷ đồng (năm 2016) và năm ngoái là 12.300 tỷ đồng.

5 loại mã độc đang lây nhiễm nhiều tại Việt Nam bao gồm: Đào tiền ảo, mã hóa dữ liệu, phần mềm gián điệp, tấn công có chủ đích và qua thiết

bị USB.

Còn với virus đào tiền ảo - loại virus xuất hiện từ năm 2017 và thực sự bùng nổ trong năm nay, thống kê của Bkav cho thấy, 5 tháng đầu năm 2018, đã có trên 735.000 máy tính nhiễm mã độc đào tiền ảo, với con đường lây nhiễm chủ yếu là qua lỗ hổng phần mềm SMB (lỗ hổng virus Wanna Cry sử dụng). Cũng theo đại diện Bkav, hiện nay có tới trên dưới 40% số máy tính tại Việt Nam vẫn còn lỗ hổng SMB

Một loại virus cũng khá phổ biến, lây nhiễm nhiều ở Việt Nam thời gian qua là virus mã hóa dữ liệu. Theo thống kê của chuyên gia Bkav, trung bình cứ 10 email có 1 email chứa mã độc mã hóa dữ liệu.

Đối với virus qua USB, mỗi năm trung bình có 80% USB tại Việt Nam nhiễm virus ít nhất 1 lần trong năm. Điều này khiến cho 1,2 triệu máy tính nhiễm virus USB.

6. Hơn 145.000 Fiber Router ở Việt Nam tồn tại lỗ hổng cho phép hacker tấn công từ xa

Hơn 145.000 Fiber Router ở Việt Nam tồn tại lỗ hổng cho phép hacker tấn công từ xa vào hệ thống mạng. Các nhà nghiên cứu bảo mật tới từ vpnMentor đã tiết lộ hai lỗ hổng ảnh hưởng tới thiết bị mạng GPON home routers. Bằng việc khai thác hai lỗ hổng này, kẻ tấn công có thể thực thi bất kì mã thực thi từ xa nào.

Chỉ vài ngày sau khi những lỗ hổng này được công bố, chúng đã được sử dụng để khai thác kiểm soát các thiết bị bởi ít nhất 05 mạng botnet.

- Mạng botnet Mettle: Công cụ kiểm soát, điều khiển mã độc và rà quét mạng Internet được lưu trữ trên một máy chủ có địa chỉ tại Việt Nam. Mạng mã độc này sử dụng một modul tấn công mã nguồn mở có tên là Mettle để lây nhiễm mã độc lên các Home router tồn tại điểm yếu.

- Mạng botnet Muhstik: mạng botnet này mới được phát hiện khi đang khai thác lỗ hổng Drupal. Hiện tại mạng botnet này đã được cải tiến để khai thác lỗ hổng GPON, cùng với lỗi trong firmware JBOSS và DD-WRT.

- Mạng botnet Mirai: Mã khai thác GPON cũng đã được tích hợp vào trong một vài biến thể mới của mạng botnet IoT Mirai.

- Mạng botnet Hajime: Là một mạng botnet khác ít được biết đến, có mục tiêu thường là các thiết bị IoT, cũng đang sử dụng thêm mã khai thác GPON để kiểm soát các thiết bị Home Router.

- Mạng botnet Satori: Mạng botnet đã lây nhiễm hàng trăm nghìn thiết bị trong năm 2017, đã thêm mã khai thác GPON vào trong biến thể mới nhất.

Ngoài ra, mã khai thác chứng minh tính khả thi (PoC) cho các lỗ hổng GPON này được công bố rộng rãi trong cộng đồng, giúp cho những người không có kỹ năng cũng có thể dễ dàng thực hiện kịch bản tấn công.

7. Bản cập nhật tháng 6 của Microsoft vá 11 lỗ hổng nghiêm trọng

Ngày 12/6, Microsoft phát hành bản cập nhật an ninh cho hơn 50 lỗ hổng, 11 trong số đó được đánh giá là nghiêm trọng. Đây là các lỗi ảnh hưởng tới Windows, Internet Explorer, Edge, MS Office,... Khi bị khai thác thành công, hacker có thể tấn công chạy mã tùy ý trong mạng nội bộ hoặc tấn công từ xa. Người dùng được khuyến cáo cần ngay lập tức kiểm tra và cập nhật bản vá.

Lỗi nghiêm trọng nhất mà Microsoft vá trong tháng này là lỗ hổng thực thi mã từ xa (CVE-2018-8225) tồn tại trong DNSAPI.dll của Windows Domain Name (DNS), ảnh hưởng đến tất cả các phiên bản Windows từ 7 đến 10, cũng như các phiên bản Windows Server. Lỗ hổng này nằm ở cách Windows phân tích các truy vấn DNS, có thể bị khai thác tấn công bằng cách gửi các truy vấn DNS lỗi tới một hệ thống mục tiêu từ một máy chủ DNS độc hại bị hacker kiểm soát.

Một lỗi nghiêm trọng khác là lỗ hổng thực thi mã từ xa (CVE-2018-8231) trong chồng giao thức HTTP (HTTP.sys) của Windows 10 và Windows Server 2016, cho phép kẻ tấn công từ xa thực thi mã tùy ý và kiểm soát các hệ thống bị ảnh hưởng. Lỗ hổng này bắt nguồn khi HTTP.sys xử lý không đúng các đối tượng trong bộ nhớ, cho phép kẻ tấn công gửi một gói tin đặc biệt tới một hệ thống Windows bị ảnh hưởng để kích hoạt thực thi mã tùy ý.

Lỗ hổng thực thi mã từ xa nghiêm trọng tiếp theo (CVE-2018-8213) ảnh hưởng đến Windows 10 và Windows Server, tồn tại theo cách hệ điều hành xử lý các đối tượng trong bộ nhớ. Khai thác thành công có thể cho phép kẻ tấn công kiểm

soát máy tính Windows bị ảnh hưởng.

Nếu hệ thống tồn tại lỗ hổng, người dùng cần áp dụng các bản vá an ninh càng sớm càng tốt, bằng cách vào Cài đặt (Settings) -> Cập nhật & an ninh (Update & security) -> Cập nhật Windows (Windows Update) -> Kiểm tra (Check) các bản cập nhật hoặc cài đặt các cập nhật theo cách thủ công theo mã bản vá.

8. Lỗi Facebook khiến bài đăng riêng tư của 14 triệu người dùng hiển thị công khai

Tháng 6 vừa qua, Facebook đã gửi thông báo đến 14 triệu người dùng về một lỗi có thể khiến bài đăng riêng tư của họ vô tình hiện ở chế độ công khai. Không lâu sau đó, Facebook đã khắc phục được kịp thời lỗi không đáng có này.

Vấn đề xảy ra từ ngày 18/5, được Facebook khắc phục vào 22/5 tuy vậy phải đến 27/5 thì bài đăng bị lỗi mới được chỉnh lại quyền riêng tư mà người dùng thiết lập trước đó. Lỗi này xuất hiện khi nền tảng đang thử nghiệm tính năng làm nổi bật nội dung trong dòng thời gian người dùng. Các nội dung nổi bật sẽ được hiển thị công khai, nhưng Facebook đã vô tình làm công khai tất cả nội dung mới sau đó.

9. Phát hiện botnet khổng lồ gồm 500.000 router

Hơn nửa triệu thiết bị định tuyến và lưu trữ tại hàng chục quốc gia đã bị nhiễm một mã độc botnet phức tạp, có khả năng được thiết kế bởi nhóm hacker do Nga hậu thuẫn.

Bộ phận nghiên cứu tình báo mạng Talos của Cisco đã phát hiện một malware botnet các thiết bị IoT, có tên VPNFilter, được thiết kế với khả năng linh hoạt có thể thu thập thông tin tình báo, can thiệp vào quá trình liên lạc internet, cũng như tiến hành các hoạt động tấn công mạng phá hoại.

VPNFilter có thể đánh cắp thông tin đăng nhập của trang web và theo dõi các hệ thống điều khiển công nghiệp hoặc SCADA, như hệ thống lưới điện, cơ sở hạ tầng và nhà máy khác.

Các nhà nghiên cứu cho biết họ công bố những phát hiện của mình trước khi hoàn thành nghiên cứu, do lo ngại về một cuộc tấn công sắp tới có thể xảy ra tại Ukraine, vốn là nạn nhân của nhiều tấn công mạng từ Nga, bao gồm tấn công gây mất điện trên diện rộng và NotPetya.

Nếu router của bạn đã bị nhiễm malware này, hãy reset lại về chế độ mặc định ban đầu để diệt malware và cập nhật firmware càng sớm càng tốt. Để phòng chống lại các cuộc tấn công tương tự, bạn nên thay đổi thông tin đăng nhập mặc định trên thiết bị của mình. Nếu router của bạn có nguy cơ bị tấn công trong khi lại không thể cập nhật, đơn giản nhất là mua 1 router mới. Bảo mật và quyền riêng tư của bạn đáng giá hơn nhiều giá trị của một chiếc router.

10. Adobe tung bản vá cho lỗ hổng Zero-Day đang bị khai thác trên Flash Player

Adobe vừa phát hành bản vá bảo mật cho một lỗ hổng nghiêm trọng trong Flash Player đang bị các tin tặc khai thác để tấn công người dùng Windows. Được phát hiện độc lập bởi nhiều hãng bảo mật như ICEBRG, Qihoo 360 và Tencent, các cuộc tấn công qua lỗ hổng zero-day của Adobe Flash chủ yếu nhắm vào người dùng ở Trung Đông bằng cách sử dụng một bảng tính Excel đặc biệt. Khi mở tài liệu này, tất cả các mã khai thác và payload độc hại được phân phối thông qua các máy chủ từ xa. Lỗi tràn bộ nhớ đệm stack, được đặt tên là CVE-2018-5002, ảnh hưởng đến Adobe Flash Player 29.0.0.171 và các phiên bản cũ hơn trên Windows, MacOS và Linux, cũng như Adobe Flash Player trên Google Chrome và có thể bị khai thác để thực thi mã tùy ý trên các hệ thống mục tiêu.

Bên cạnh bản vá cho CVE-2018-5002, Adobe cũng tung ra các bản cập nhật bảo mật cho hai lỗ hổng "quan trọng", bao gồm lỗi tràn Integer (CVE-2018-5000) và lỗi đọc Out-of-bounds (CVE-2018-5001) cả hai lỗi trên đều dẫn đến việc lộ lọt thông tin. Vì vậy, người dùng được khuyến cáo ngay lập tức cập nhật Adobe Flash Player lên phiên bản 30.0.0.113 thông qua cơ chế cập nhật trong phần mềm hoặc bằng cách truy cập Trung tâm Download của Adobe Flash Player. Các chuyên gia khuyến cáo, người dùng nên gỡ bỏ Adobe Flash Player trên máy tính để tránh bị hacker khai thác. Trong trường hợp cần sử dụng phải cài đặt phiên bản 30.0.0.113 mới nhất để thay thế. Thông tin chi tiết về lỗ hổng và bản cập nhật, các bạn có thể xem và download tại đây:

https://helpx.adobe.com/security/products/flash-player/apsb18-19.html

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

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

Trong quý II, 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 95 lượt hỗ trợ, ban hành 03 công văn cảnh báo liên quan đến mã độc, Website và an toàn thông tin.

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

Theo ghi nhận của Trung tâm An ninh mạng và An toàn dữ liệu, trong thời gian từ 01/04-30/6 ghi nhận có 433 cuộc tấn công khai thác chiếm quyền quản trị; 231 cuộc tấn công bằng mã độc; 51 cuộc tấn công vào ứng dụng Website; 04 cuộc tấn công từ chối dịch vụ vào các dịch vụ đang hoạt động tại Trung tâm.

2. Công văn an toàn thông tin

- Ngày 20/4/2018 Sở Thông tin và Truyền thông ban hành công văn số 416/STTTT-CNTT về hướng dẫn, kiểm tra, rà soát, vá lỗ hổng bảo mật trên các thiết bị modem, router.

- Ngày 27/4/2018 Sở Thông tin và Truyền thông ban hành công văn số 460/STTTT-CNTT về Tăng cường đảm bảo an toàn thông tin kỳ nghỉ lễ 30/4 và 01/5/2018

- Ngày 24/4/2018 Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa ban hành công văn số 75/TTCNTT&TT-QTHT về cảnh báo lỗ hổng an toàn thông tin hệ quản trị nội dung Drupal.

- Ngày 03/5/2018 Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa ban hành công văn số 77/TTCNTT&TT-QTHT về việc cảnh báo lỗ hổng an toàn thông tin SA-CORE-2018-004 của hệ quản trị nội dung Drupal

- Ngày 9/5/2018 Sở Thông tin và Truyền thông ban hành công văn số 516/STTT-CNTT về việc đánh giá mức độ bảo đảm an toàn thông tin mạng

- Ngày 23/5/2018 Sở Thông tin và Truyền thông ban hành công văn số 619/STTT-CNTT về việc rà soát công tác đảm bảo an ninh, an toàn của hệ thống điều khiển công nghiệp và nguy cơ lộ lọt thông tin qua sử dụng mạng xã hội.

- Ngày 20/6/2018 Sở Thông tin và Truyền thông ban hành công văn số755/STTT-CNTT về việc báo cáo tổ chức Hội nghị bảo đảm ATTT cho các hệ thống thông tin quan trọng 2018.

- Ngày 20/6/2018 Sở Thông tin và Truyền thông ban hành công văn số 770/STTT-CNTT về việc xin góp ý cho dự thảo Kế hoạch ứng phó sự cố đảm bảo an toàn thông tin mạng.

TIN HOẠT ĐỘNG

Trung tâm CNTT&TT tổ chức vận hành các cuộc họp trên hệ thống Hội nghị trực tuyến của tỉnh

Dự án xây dựng hệ thống phòng họp trực truyến cho các cơ quan nhà nước tỉnh Thanh Hóa đặt tại 03 điểm cầu trung tâm là Văn phòng Tỉnh ủy, Văn phòng UBND tỉnh, Sở Thông tin và Truyền thông và 28 điểm cầu đầu cuối (27 huyện, thị xã, thành phố và Ban Quản lý Khu Kinh tế Nghi Sơn) do Sở Thông tin và Truyền thông làm chủ đầu tư. Sau khi dự án triển khai xong, đã giao cho Trung tâm CNTT&TT vận hành và tổ chức kỹ thuật các cuộc họp trên toàn hệ thống. Trong quý II/2018, Trung tâm đã tổ chức thành công cho 05 cuộc họp do Tỉnh ủy và UBND tỉnh chủ trì, cụ thể như sau:

- Ngày 02/4/2018, tại UBND tỉnh tổ chức Hội nghị trực tuyến bàn biện pháp đẩy nhanh tiến độ đầu tư công, tăng cường công tác QLNN về đấu thầu và QL đầu tư XD...

- Ngày 17/4/2018, tại UBND tỉnh tổ chức Hội nghị trực tuyến triển khai Kế hoạch chống thất thu thuế đối với hộ kinh doanh trên địa bàn tỉnh...

- Ngày 22/4/2018, tại Tỉnh ủy tổ chức Hội nghị trực tuyến triển khai học tập quán triệt các nghị quyết, chỉ thị, quy định văn bản của BCT, BBT Trung ương và BTV tỉnh ủy...

- Ngày 13/6/2018, tại UBND tỉnh tổ chức Hội nghị trực tuyến triển HNTT quán triệt, triển khai các luật mới gồm: Luật Quy hoạch, Luật Thủy sản, Luật Lâm nghiệp...

- Ngày 29/6/2018, tại Tỉnh ủy tổ chức Hội nghị trực tuyến học tập, quán triệt Nghị quyết Hội nghị trung ương 7 (khóa XII) của Đảng

Ngô Phương

Trung tâm CNTT&TT tham gia diễn tập quốc tế về an toàn thông tin ASEAN - JAPAN năm 2018

Ngày 23/5/2018, tại Hà Nội, Trung tâm CNTT&TT Thanh Hóa đã tham dự diễn tập quốc tế về an toàn thông tin ASEAN-JAPAN năm 2018 với chủ đề "Tấn công DoS/DDoS và hoạt động phối hợp ứng cứu, xử lý sự cố". Diễn tập do Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (Bộ TT&TT) đã chủ trì tổ chức cho các thành viên mạng lưới ứng cứu sự cố, các đơn vị CNTT của các Bộ, ngành, tỉnh/thành trên toàn quốc tham gia. Thứ trưởng Bộ TT&TT Nguyễn Thành Hưng đã đến tham dự và phát biểu khai mạc cuộc Diễn tập.

Theo đại diện VNCERT, mô hình diễn tập bao gồm 3 cấp: cơ quan điều phối quốc tế, cơ quan điều phối quốc gia và các đơn vị hạt nhân. Trong đó, các đơn vị hạt nhân là nơi cần được bảo vệ nhất, nơi mà có thể gặp phải tình huống bị tấn công mạng trực tiếp hoặc gián tiếp; và đồng thời cũng là đơn vị nên tham gia hỗ trợ ứng cứu sự cố tấn công mạng cho các đơn vị khác nhằm phòng tránh lây lan đến đơn vị mình. Mô hình diễn tập này chính là cấu trúc của liên minh phối hợp quốc tế trong ứng cứu sự cố máy tính trong khu vực đang được áp dụng hiện nay. Do đó, khác với diễn tập APCERT và diễn tập ASEAN tập trung vào phân tích các loại hình tấn công mạng thì diễn tập ASEAN - Nhật Bản tập trung vào tạo lập cơ chế phối hợp, vận hành nhanh và chính xác các công đoạn chuyển giao thông tin giữa tất cả các đơn vị có liên quan khi có tấn công mạng xảy ra.

Kịch bản Diễn tập quốc tế ASEAN - Nhật Bản 2018 giả định có các cuộc tấn công mạng từ một nhóm tin tặc và gồm 3 giai đoạn kéo dài trong 3 ngày. Ngày 1 là giai đoạn cảnh báo, Nhật Bản phát hiện việc truy cập website và trao đổi email bị chậm lại đồng thời có các cuộc tấn công DDoS nhỏ xuất hiện; Ngày 2 là giai đoạn tấn công: xuất hiện cảnh báo một cuộc tấn công diện rộng và sau đó các cuộc tấn công quy mô lớn gây ra tắc nghẽn việc truy cập website và ngừng trệ việc gửi nhận email của các đơn vị nạn nhân. Do vậy, việc liên lạc bằng điện thoại được sử dụng; Ngày 3 là giai đoạn đỉnh điểm: sau khi dịch vụ email được khôi phục thì các email giả mạo có chứa mã độc được gửi đến máy tính của quan chức các quốc gia thành viên ASEAN làm máy tính những người nhận này bị nhiễm mã độc. Các email lừa đảo tinh vi này sau đó làm bùng phát mã độc không chỉ trong các cơ quan, tổ chức chính phủ mà còn lây lan ra cộng đồng.

Yêu cầu đặt ra cấp quốc gia tham gia Diễn tập quốc tế ASEAN - Nhật Bản là bằng cách trao đổi các báo cáo tình huống về những gì đang diễn ra và cung cấp các thông tin cảnh báo có chứng cứ cùng với chiến lược giảm thiểu thiệt hại, đối phó với các cuộc tấn công, mỗi quốc gia cần làm cho cộng đồng nhận thức được mức độ nguy hại của tình huống đang diễn ra và có biện pháp đối phó kịp thời.

Cao Việt Cường

Diễn tập an toàn thông tin mạng trực tuyến WhiteHat Drill 05

WhiteHat Drill 05 là chương trình diễn tập trực tuyến với chủ đề "Điều tra, xử lý và phòng chống mã độc đào tiền ảo qua lỗ hổng phần mềm" được Cục An toàn thông tin (Bộ Thông tin và Truyền thông) và Tập đoàn công nghệ Bkav phối hợp tổ chức vào ngày 9-10/5/2018. Đây là chương trình diễn tập quy mô lớn nhất từ trước tới nay tại Việt Nam với sự tham gia của 150 đội đến từ các cơ quan quản lý nhà nước, ngân hàng, tập đoàn, doanh nghiệp... trên toàn quốc. Tham dự diễn

tập, Trung tâm CNTT&TT cử Tổ ứng cứu sự cố đăng ký tham dự các nội dung của buổi diễn tập.

Phát biểu tại Lễ khai mạc, ông Nguyễn Huy Dũng, Phó cục trưởng Cục An toàn thông tin (ảnh) cho biết: "Năng lực đảm bảo ATTT của tổ chức, quốc gia không đo bằng việc có bị tấn công mạng hay không, mà bằng tính chuyên nghiệp và chủ động khi xảy ra tấn công mạng. Cục An toàn Thông tin luôn đồng hành cùng các tổ chức, doanh nghiệp và cộng đồng để chúng ta chuyển từ tình thế bị động sang chủ động đối phó với mỗi cuộc tấn công mạng. Đây cũng là một trong những hợp tác hiệu quả giữa cơ quan nhà nước và doanh nghiệp trong công tác bảo đảm ATTT".

Chia sẻ về chủ đề của chương trình, ông Ngô Tuấn Anh, Phó chủ tịch phụ trách an ninh mạng của Bkav cho biết: "Thời gian gần đây, các cuộc tấn công phát tán mã độc nhằm thu lợi bất chính như mã độc tống tiền ransomware, đánh cắp tài khoản ngân hàng, mã độc đào tiền ảo... đã bùng nổ. Trong đó, mã độc đào tiền ảo được hacker ngày càng lựa chọn nhiều vì việc tấn công xảy ra âm thầm, nạn nhân khó nhận biết hơn để xử lý. Khi bị lây nhiễm, toàn bộ tài nguyên máy tính của nạn nhân bị huy động trái phép vào mục đích đào tiền ảo của hacker.WhiteHat Drill 05 là chương trình diễn tập an toàn thông tin mạng có số đội tham dự lớn nhất từ trước tới nay tại Việt Nam".

Theo kịch bản, hệ thống của các đội bị cài mã độc đào tiền ảo qua lỗ hổng phần mềm. Nhiệm vụ của từng đội là phải cô lập hiện trường, tránh mã độc lây lan rộng hơn, phân tích mã độc để xác định nguồn gốc cuộc tấn công. Tiếp đến, cần xác định chính xác lỗ hổng bị khai thác, vá lỗ hổng để tránh bị tấn công trở lại. Các đội thực hiện tổng cộng 5 Pha. Kết thúc phần thi, đội thi của Trung tâm đã hoàn thành các pha của diễn tập và xếp thứ 16/71 đội tham gia.

Lê Duy

Trung tâm CNTT&TT Thanh Hóa tổ chức thi cấp Chứng chỉ ứng dụng Công nghệ thông tin đợt8, 9 năm 2018

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

Trong hai tháng 5,6 năm 2018, Trung tâm Công nghệ thông tin và truyền thông Thanh Hóa tổ chức kỳ thi sát hạch cấp Chứng chỉ công nghệ thông tin chuẩn cơ bản,đợt 8,9năm 2018; Hội đồng thi được Sở Giáo dục và đào tạo thành lập bao gồm đầy đủ các Ban theo quy định về việc tổ chức thi và cấp chứng chỉ ứng dụng công nghệ thông tin tại Thông tư liên tịch số 17/2016/TTLT-BGDĐT-BTTT ngày 21 tháng 6 năm 2016 giữa Bộ Giáo dục và Đào tạo và Bộ Thông tin và Truyền thông.

Kỳ thi Đợt 8,9năm 2018, có 377 thí sinh đăng ký dự thi và tham dự 2 phần thicủa mình là phần thi trắc nghiệm lý thuyết trực tuyến trên phần mềm và phần thi thực hành kỹ năng trên máy tính; toàn bộ hồ sơ về kỳ thi đã được gửi Sở Giáo dục và đào tạo tỉnh để tiến hành cấp chứng chỉ, phôi chứng chỉ được Bộ Giáo dục và Đào tạo cấp theo số lượng thí sinh thi đậu, được Sở 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*

Đỗ Tiến