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

Số 07
tháng 3/2018

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 3/2018

Tăng cường triển khai công tác bảo đảm an toàn thông tin mạng trong tình hình mới

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

Trong thời gian qua, tình hình mất an toàn, an ninh thông tin mạng có nhiều diễn biến phức tạp, tiềm ẩn nguy cơ về mất an toàn thông tin và những mối đe dọa nghiêm trọng đến chủ quyền không gian mạng, ảnh hưởng tiêu cực đến an ninh quốc gia, trật tự an toàn xã hội.

Trong năm 2017, tình hình mất an toàn, an ninh thông tin mạng diễn ra hết sức nghiêm trọng, trước bối cảnh ngày càng gia tăng các cuộc tấn công mạng nhằm vào các cơ quan trọng yếu của Đảng, nhà nước các doanh nghiệp tài chính ngân hàng đặc biệt là các thế lực thù địch, tội phạm mạng gia tăng hoạt động tấn công mạng nhằm thu thập thông tin, bí mật nhà nước, bí mật nội bộ, chiếm quyền điều khiển, phá hoại hệ thống mạng thông tin; sử dụng Internet, nhất là các trang mạng xã hội với nhiều phương thức, thủ đoạn tinh vi, xảo quyệt nhằm gây chia rẽ nội bộ, xâm phạm lợi ích, an ninh quốc gia. Hoạt động tuyên truyền phá hoại tư tưởng, phá hoại nội bộ trên không gian mạng của các thế lực thù địch diễn ra với quy mô, cường độ ngày càng lớn, có trọng tâm, trọng điểm; sử dụng các trang mạng, blog liên tục đăng tải các bài viết có nội dung xấu, độc hại; tổ chức các chiến dịch công kích, bôi nhọ nhằm hạ uy tín của lãnh đạo Đảng, Nhà nước... Bên cạnh đó, việc tội phạm mạng đã và đang đầu tư, tập trung nhiều nguồn lực hơn vào các cuộc tấn công có chủ đích (APT), đặc biệt là tấn công vào các hệ thống thông tin quan trọng. Cụ thể như tại Việt Nam, theo ghi nhận của Cục An toàn thông tin - Bộ Thông tin và Truyền thông đã xuất hiện một số cuộc tấn công có chủ đích nhằm vào một số doanh nghiệp, tập đoàn, tổng công ty nhà nước cũng như nhằm vào một số bộ, ngành và đã gây ra hậu quả. Qua đó, Cục An toàn thông tin đã phát hiện và bóc gỡ khoảng trên dưới 10 phần mềm độc hại tấn công có chủ đích APT khác nhau nằm vùng trong các hệ thống của các cơ quan, tổ chức nhà nước.

Mặt khác, qua công tác theo dõi, giám sát tình hình an toàn mạng quốc gia, Cục An toàn thông tin mạng đã ghi nhận trong năm 2017, có hơn 17 triệu lượt truy vấn từ các địa chỉ IP của Việt Nam đến các tên miền hoặc IP phát tán/điều khiển mã độc trên thế giới, chủ yếu là các kết nối tới các mạng botnet lớn như conficker, mirai, ramnit, sality, cutwai, zeroaccess... trong năm nay, đã có trên 19.000 lượt địa chỉ máy chủ web tại Việt Nam bị tấn công; trên 3 triệu địa chỉ IP Việt Nam thường xuyên nằm trong danh sách đen (black list) của các tổ chức quốc tế; và có hơn 100.000 camera IP đang được công khai trên Internet của Việt Nam (trên tổng số 307.201 camera IP) tồn tại các điểm yếu và lỗ hổng bảo mật có thể bị khai thác lợi dụng. Theo báo cáo, ghi nhận của Trung tâm VNCERT, năm 2017 đã có 13.382 sự cố tấn công mạng vào Việt Nam cả 03 loại hình Phishing, malware và deface, trong đó: tấn công mã độc (malware) là 6.400 trường hợp; và tấn công thay đổi giao diện (deface) là 4.377 trường hợp, và tấn công lừa đảo (phishing) là 2.605 trường hợp.

Như vậy có thể thấy mức độ nguy hiểm cũng như trình độ tấn công của kẻ tấn công vào hệ thống thông tin của chúng ta đã có những thay đổi căn bản thay đổi về chất so với những năm trước mặt khác với khả năng kết nối vô hạn của mạng thông tin toàn cầu thì các cuộc tấn công mạng sẽ ngày càng gia tăng không chỉ dừng lại ở mục đích phá hoại tư tưởng, thu thập thông tin tình báo mà còn nhằm phá hoại cơ sở hạ tầng thông tin gây thiệt hại lớn về kinh tế...

Về công tác triển khai đảm bảo an toàn an ninh thông tin mạng trong các cơ quan nhà nước

Đ/c Trần Duy Bình, Giám đốc Sở TT&TT trao giấy khen của Giám đốc Sở cho các tập thể hoàn thành xuất sắc nhiệm vụ năm 2017.

trên địa bàn tỉnh trong năm 2017, đã được các cơ quan đơn vị trên địa bàn tỉnh triển khai thực hiện tương đối đầy đủ kịp thời các văn bản chỉ đạo của Trung ương như chỉ thị số 28-CT/TW ngày 16 tháng 9 năm 2013 của Ban Bí thư về tăng cường công tác bảo đảm an toàn thông tin mạng; Chỉ thị số 15/CT-TTg ngày 17 tháng 6 năm 2014 của Thủ tướng Chính phủ về tăng cường công tác bảo đảm an ninh và an toàn thông tin mạng trong tình hình mới; Chỉ thị số 22/CT-UBND ngày 19/10/2015 của Chủ tịch UBND tỉnh về việc tăng cường đảm bảo an ninh và an toàn thông tin mạng trong các cơ quan nhà nước trên địa bàn tỉnh Thanh Hóa; Quyết định số 1293/2017/QĐ-UBND ngày 25/4/2017 của UBND tỉnh Thanh Hóa về việc Ban hành Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan quản lý nhà nước tỉnh Thanh Hóa và các văn bản hướng dẫn nghiệp vụ của Sở Thông tin và Truyền thông như ban hành các quy định, kế hoạch... về an toàn an ninh thông tin mạng. Qua đó, các cơ quan, đơn vị đã chủ động xây dựng áp dụng các giải pháp bảo mật an toàn thông tin đối với các hệ thống thông tin tại cơ quan đơn vị mình do đó chưa xảy ra các sự cố nghiêm trọng, chưa phát hiện các hoạt động xâm nhập trái phép nghiêm trọng vào hệ thống thông tin của các cơ quan đơn vị đặc biệt là tại trung tâm dữ liệu đặt tại VPUBND tỉnh và Sở Thông tin và Truyền thông.

Hoạt động ứng dụng và phát triển công nghệ thông tin trong các cơ quan nhà nước từ cấp tỉnh đến cấp xã trong năm 2017 cũng mang lại nhiều hiệu quả tích cực tạo tiền đề để tiếp tục phát triển trong năm 2018 và những năm tiếp theo. Các Sở, ban, ngành và UBND cấp huyện đã chủ động đầu tư nâng cấp hạ tầng công nghệ thông tin đẩy mạnh ứng dụng CNTT phục vụ công tác chỉ đạo điều hành cải cách hành chính có hiệu quả. Trong khối các cơ quan Đảng và Nhà nước

từ cấp tỉnh đến cấp huyện đều có mạng LAN, hạ tầng kết nối Internet cả tỉnh đạt 100%, tỷ lệ máy tính trong các cơ quan nhà nước đạt trên 96%; 100% xã có máy tính (từ 03 đến 05 máy); 100% cơ quan đơn vị cấp tỉnh, cấp huyện và đến cấp xã (đạt 43%) đã được triển khai ứng dụng chữ ký số. Ứng dụng phần mềm quản lý văn bản và hồ sơ công việc để trao đổi văn bản điện tử đã được triển khai đồng bộ sử dụng trong tất cả các Sở, ban, ngành và UBND cấp huyện (đạt 100%) và 253 UBND cấp xã trên phần mềm cũng đã được tích hợp chữ ký số chuyên dùng và kết nối liên thông để truyền nhận trao đổi thông tin văn bản trên môi trường mạng.

Cùng với việc đẩy mạnh ứng dụng CNTT trong hoạt động của các cơ quan hành chính nhà nước, nhằm thực hiện mục tiêu thành công 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", đề án "Xây dựng Khu CNTT tập trung phát triển phần mềm và nội dung số", Kiến trúc chính quyền điện tử tỉnh Thanh Hóa, hướng tới xây dựng Thanh Hóa trở thành thành phố văn minh, hiện đại, một trong những nhiệm vụ quan trọng được tỉnh quan tâm là công tác đảm bảo an toàn, an ninh thông tin.

Để thực hiện mục tiêu đó, bên cạnh việc ban hành các cơ chế chính sách về CNTT, tỉnh Thanh Hóa tập trung đầu tư phát triển hạ tầng CNTT: Hệ thống mạng WAN nội tỉnh kết nối tới các cơ quan, ban, ngành từ cấp tỉnh đến cấp xã; các sở, ban, ngành, UBND cấp huyện và cấp xã đều được kết nối mạng truyền số liệu chuyên dùng. 100% cơ quan nhà nước cấp tỉnh, huyện và hầu hết cấp xã đã kết nối mạng LAN. Đặc biệt, đầu tư nâng cấp Trung tâm An ninh mạng và An toàn dữ liệu của tỉnh để trở thành Trung tâm điều hành an ninh mạng đảm bảo an toàn, an ninh mạng cho hệ thống cơ sở dữ liệu lớn tập trung (Big Data) của tỉnh đảm bảo các quy chuẩn, tiêu chuẩn của Kiến trúc Chính quyền điện tử tỉnh Thanh Hóa để quản lý, lưu trữ các hệ thống phần mềm, CSDL của sở, ban, ngành; UBND cấp huyện, cấp xã và lưu trữ các hệ thống thông tin, dịch vụ thành phố thông minh của một số lĩnh vực tỉnh đang triển khai. Đồng thời triển khai hệ thống giám sát thông tin điện tử đảm bảo lưu trữ, kết nối các dịch vụ thành phố thông minh của tỉnh, kết nối tương tác với các Trung tâm an toàn, an ninh thông tin của Bộ Thông tin và Truyền thông và các Bộ, ngành liên quan để thực hiện nhiệm vụ giám sát, cảnh báo, ứng cứu sự cố mạng, máy tính; xử lý xung đột thông tin, an toàn thông tin mạng cho tất cả các sở, ngành, UBND cấp huyện, cấp xã.

Một trong những nội dung quan trọng góp phần bảo đảm ATANTT mạng là công tác đào tạo, bồi dưỡng cho đội ngũ cán bộ quản lý, chuyên trách về ATANTT. Hiện nay, hầu hết các cơ quan, đơn vị trên địa bàn tỉnh đã bố trí được cán bộ chuyên trách về CNTT. Sở Thông tin và Truyền thông thường xuyên tổ chức tập huấn về CNTT, đặc biệt là lĩnh vực an toàn mạng, chữ ký số cho các cán bộ chuyên trách về CNTT của các cơ quan hành chính nhà nước trên địa bàn tỉnh. Qua đó, cán bộ chuyên trách nắm vững những quy định của pháp luật trong lĩnh vực CNTT, an toàn thông tin; chứng thư số và hệ thống chứng thực chữ ký số chuyên dùng; nâng cao kỹ năng quản trị, vận hành hệ thống CNTT, đảm bảo ATANTT. Từ đó góp phần ứng dụng hệ thống CNTT tại cơ quan, đơn vị mình.

Hoạt động thông tin tuyên truyền, phổ biến, nâng cao nhận thức, trách nhiệm về an toàn thông tin trong năm 2017 theo Kế hoạch số 152/KH-UBND ngày 11/11/2015 của UBND tỉnh được tăng cường góp phần nâng cao nhận thức, ý thức cảnh giác mất an toàn thông tin mạng trong việc sử dụng, khai thác các ứng dụng CNTT trong các cơ quan nhà nước và của người dân.

Trước tình hình an toàn an ninh thông tin trên thế giới và ở Việt Nam tiếp tục diễn biến phức tạp để đảm bảo an toàn an ninh thông tin mạng trong năm 2018 trên địa bàn tỉnh, cần tập trung triển khai đồng bộ các giải pháp có ý nghĩa then chốt lâu dài cụ thể như sau:

Một là, tổ chức thực hiện những nhiệm vụ giải pháp đảm bảo an toàn an ninh thông tin mạng theo chỉ đạo của Trung ương cũng như tiếp tục triển khai thực hiện tốt các nội dung về công tác bảo đảm an toàn thông tin theo kế hoạch của UBND tỉnh. Đặc biệt là nâng cao vai trò, trách nhiệm của người đứng đầu trong công tác chỉ đạo, điều hành quyết liệt việc ứng dụng CNTT phục vụ cải cách hành chính nói chung và công

tác bảo đảm an toàn thông tin mạng tại cơ quan, đơn vị mình nói riêng.

Hai là, tiếp tục tăng cường công tác tuyên truyền giáo dục làm cho cán bộ, công chức, viên chức và nhân dân nhận thức rõ tầm quan trọng của công tác bảo đảm an toàn an ninh thông tin mạng coi đây là nhiệm vụ quan trọng cấp bách thường xuyên lâu dài của cả hệ thống chính trị. Đồng thời, dành kinh phí đầu tư các thiết bị, phần mềm bảo mật nhằm phòng chống các nguy cơ mất an toàn thông tin mạng ngăn chặn tình trạng lộ lọt thông tin kịp thời ứng phó với những nguy cơ đến từ thông tin mạng trong thời gian tới.

Ba là, tăng cường công tác thanh tra, kiểm tra chuyên ngành Thông tin và Truyền thông, đặc biệt là đánh giá cấp độ bảo đảm an toàn thông tin mạng đối với các hệ thống thông tin lớn của tỉnh như cổng thông tin điện tử của tỉnh, hệ thống thư điện tử công vụ, hệ thống một cửa điện tử liên thông... Đồng thời, nâng cao hiệu lực hiệu quả quản lý nhà nước trong công tác kiểm tra hoạt động báo chí, các trang thông tin điện tử; phát tán tin nhắn rác; tin nhắn lừa đảo, thuê bao di động trả trước, internet,... phối hợp với công an tỉnh, các ngành, các địa phương thực hiện tốt công tác đảm bảo an toàn hạ tầng thông tin, quản lý thông tin trên mạng internet, hạn chế những thông tin xấu tiêu cực gây ảnh hưởng đến trật tự an toàn xã hội, xử lý kịp thời các hành vi vi phạm theo quy định của pháp luật.

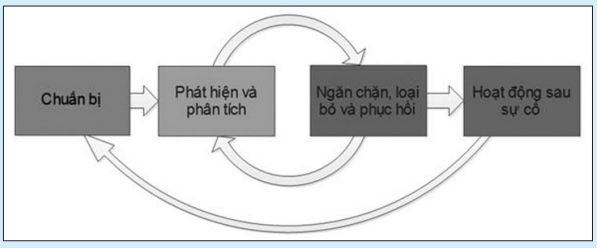
Bốn là, thường xuyên tổ chức đào tạo bồi dưỡng kiến thức an toàn an ninh thông tin cho cán bộ công chức, viên chức tại các cơ quan, đơn vị từ cấp tỉnh đến cấp xã nhằm đủ năng lực trình độ đáp ứng yêu cầu về bảo đảm an toàn thông tin đối với các hệ thống thông tin của cơ quan

Năm là, đẩy mạnh công tác phối hợp giữa các Sở, ban, ngành và UBND cấp huyện với các cơ quan chức năng trong bảo an toàn an ninh thông tin mạng qua đó kịp thời phát hiện các lỗ hổng bảo mật dấu hiệu tấn công xâm nhập cơ sở hạ tầng thông tin để phối hợp ngăn chặn khắc phục điều tra xử lý./.

Công tác điều phối, ứng cứu sự cố và đảm bảo an toàn thông tin mạng trên địa bàn tỉnh năm 2017

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

Trong những năm qua, tình hình an toàn thông tin trong nước có nhiều diễn biến rất phức tạp, các loại sự cố xảy ra với mạng máy tính trong nước đã tăng gấp nhiều lần so với cùng kỳ các năm trước đây. Các hình thức tấn công mạng đối với doanh nghiệp, người dùng cũng như các cơ quan và tổ chức trên toàn quốc như lừa đảo chiếm đoạt tài khoản trên mạng xã hội, thông tin cá nhân, mã hóa dữ liệu người dùng... ngày càng gia tăng. Đặc biệt, trong năm qua đã ghi nhận các hình thức tấn công mới của tội phạm mạng như tấn công thiết bị IoT như Router Wi-Fi, Camera IP... mà điển hình là sự bùng nổ các biến thể mới của mã độc Mirai, trong đó có biến thể nhắm mục tiêu đến Việt Nam. Năm 2017 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. Gần đây nhất, mã độc lây qua Facebook bùng phát từ ngày 19/12 và làm "náo loạn" Internet tại Việt Nam. Thống kê từ hệ thống giám sát virus của Bkav, đã có hơn 23.000 máy tính tại Việt Nam nhiễm loại mã độc này.



Sơ đồ quy trình ứng cứu sự cố.

Nhận thức rõ vấn đề này, từ nhiều năm qua, Sở Thông tin và Truyền thông đã tham mưu cho UBND tỉnh triển khai nhiều giải pháp để đối phó với các nguy cơ gây mất an toàn, an ninh thông tin nói chung và công tác ứng cứu xử lý sự cố máy tính nói riêng. Với chức năng, nhiệm vụ được Chủ tịch UBND tỉnh, Giám đốc Sở Thông tin và Truyền thông giao trong vai trò là đầu mối tiếp nhận và xử lý ứng cứu sự cố máy tính nói chung và an toàn thông tin nói riêng; Trung tâm CNTT&TT (Trung tâm) luôn đề cao và triển khai tốt công tác phối hợp điều phối và cảnh báo sớm sự cố tới các cơ quan, tổ chức trên địa bàn tỉnh. Bên cạnh các hình thức hỗ trợ gián tiếp qua số điện thoại đường dây nóng, qua phần mềm hỗ trợ công tác ứng cứu từ xa. Trung tâm đã chủ động xây dựng kế hoạch từ đầu năm để triển khai trực tiếp hỗ trợ tại các các cơ quan, tổ chức, doanh nghiệp thực hiện các hoạt động phòng ngừa, ngăn chặn, ứng cứu, khôi phục nhằm đối phó với các loại tấn công phá hoạt trên môi trường mạng cho các hệ thống thông tin của tỉnh, cụ thể như sau:

Tổ ứng cứu sự cố phối hợp với các cơ quan chức năng trong việc bảo đảm an toàn, an ninh thông tin mạng (nguồn: TTV)

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

- Trên cơ sở thành lập Tổ ứng cứu xử lý sự cố của Trung tâm trong năm 2016, Trung tâm đánh giá kết quả hoạt động của Tổ để qua đó điều chỉnh, kiện toàn nhân sự nhằm nâng cao hiệu quả công tác an toàn thông tin mạng, nâng cao năng lực, đảm bảo chủ động sẵn sàng ứng phó, xử lý sự cố, giảm thiểu nguy cơ gây mất an toàn thông tin mạng trong cơ quan nhà nước trên địa bàn tỉnh, đúng theo quy định tại Thông tư số 20/2017/TT-BTTTT, ngày 12/09/2017 của Bộ Thông tin và Truyền thông Quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc. Đồng thời, Trung tâm cũng đã rà soát, ban hành lại các Quy định, phương án, quy trình về công tác ứng cứu, xử lý sự cố. Qua đó, giúp cho hoạt động ứng cứu sự cố được triển khai khoa học và đảm bảo sự cố được xử lý nhanh chóng và kịp thời.

- Tại Trung tâm An ninh mạng và An toàn dữ liệu của tỉnh do Trung tâm quản lý và vận hành, đã triển khai nhiều giải pháp kỹ thuật, các phương án khắc phục và quy trình xử lý sự cố. Bên cạnh đó bổ sung các trang thiết bị, phần mềm an ninh một cách đồng bộ về giải pháp để chủ động trong việc giám sát và cảnh báo các dấu hiệu, nguy cơ gây mất an toàn thông tin trên các hệ thống thông tin trên địa bàn tỉnh cũng như với các ứng dụng dùng chung trên địa bàn như phần mềm Quản lý văn bản và hồ sơ công việc; các phần mềm chuyên ngành, các trang/cổng thông tin điện tử của các cơ quan, đơn vị... Đồng thời phân công cán bộ trực 24/24 trong ngày để sẵn sàng ứng cứu các sự cố máy tính, an toàn thông tin và an ninh mạng.

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

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

nhanh chóng và hiệu quả.

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

Hằng năm, bình quân Trung tâm thực hiện ứng cứu khoảng 600 lượt sự cố, ban hành 20 lượt văn bản cảnh báo sớm các sự cố gây mất an toàn thông tin. Trong năm 2017, Trung tâm đã thực hiện hỗ trợ ứng cứu 366 lượt sự cố liên quan đến các phần mềm dùng chung, hệ thống thông tin của các cơ quan, đơn vị trên địa bàn tỉnh; Ban hành 81 công văn cảnh báo địa chỉ IP nhiễm mã độc tham gia mạng Botnet, website bị tin tặc tấn công và mã độc thuộc loại Ransomware mã hóa dữ liệu để tống tiền, mã độc Petya, khắc phục các điểm yếu về ATTT khi sử dụng phần mềm TDoffice. Thông báo khẩn cấp về việc theo dõi, ngăn chặn kết nối máy chủ điều khiển mã độc WannaCry cho các đơn vị, tổ chức, doanh nghiệp... trên địa bàn tỉnh; thông qua đó đã từng bước nâng cao nhận thức, kỹ năng cho các CBCC, VC trong việc đảm bảo an toàn thông tin, dữ liệu của các đơn vị.

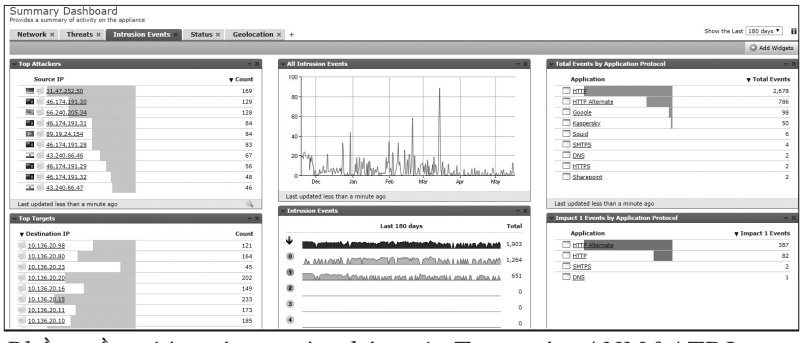
Trong năm 2018, Trung tâm sẽ tiếp tục triển khai đồng bộ các giải pháp nhằm tăng cường công tác đảm bảo an toàn thông tin và hỗ trợ ứng cứu sự cố cho các cơ quan, đơn vị trên địa bàn tỉnh, cụ thể như: Hỗ trợ đào tạo nâng cao nhận thức về an toàn thông tin cho cán bộ công chức, viên chức; Đào tạo cho cán bộ đầu mối làm nhiệm vụ đảm bảo an toàn thông tin trong việc xử lý và lập kế hoạch khắc phục sự cố; Kế hoạch phối hợp kiểm tra, rà soát, đánh giá đảm bảo an toàn thông tin cho các hệ thống thông tin và hỗ trợ ứng cứu xử lý sự cố; Xuất bản bản tin an toàn thông tin...

Qua đó, bước đầu đã có những chuyển biến tích cực trong việc giảm thiểu các rủi ro, nguy cơ gây mất an toàn thông tin tại các cơ quan, đơn vị trên địa bàn tỉnh. Tuy nhiên, với tình hình diễn biến phức tạp về mất an toàn thông tin hiện nay để hoạt động ứng cứu xử lý sự cố được triển khai hiệu quả hơn nữa, đề nghị các cơ quan, đơn vị cần thực hiện tốt một số nội dung sau:

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

Hai là, các cơ quan, đơn vị cần phối hợp liên kết chặt chẽ với các đơn vị khác để hình thành một mạng lưới ứng cứu khẩn cấp trên địa bàn tỉnh có sự gắn kết chặt chẽ theo theo quy định tại Thông tư số 20/2017/TT-BTTTT, ngày 12/09/2017 của Bộ Thông tin và Truyền thông. Đồng thời phải phối hợp, trao đổi thông tin giữa các đơn vị một cách thường xuyên, chủ động để cập nhập các thông tin cảnh báo, kỹ thuật, công nghệ mới để qua đó có được các phương án chiến lược phòng chống, ngăn chặn sự cố một cách nhanh chóng và hiệu quả hơn.

Ba là, cần quan tâm đầu tư trang thiết bị phục vụ công tác ứng cứu sự cố; xây dựng đội ngũ cán bộ chuyên trách công nghệ thông tin phụ trách về công tác đảm bảo về an toàn, an ninh thông tin đủ trình độ chuyên môn và kỹ thuật, nghiệp vụ; đặc biệt là nâng cao đạo đức công vụ trong việc quản lý thông tin nội bộ, bí mật nhà nước... Khi có sự cố hoặc nguy cơ gây mất an toàn thông tin, thủ trưởng đơn vị có trách nhiệm chỉ đạo kịp thời, áp dụng mọi biện pháp để khắc phục và hạn chế thấp nhất mức thiệt hại có thể xảy ra trong đơn vị mình, góp phần giữ vững ổn định chính trị, phát triển KT-XH của tỉnh trong thời gian tới./.



Phần mềm giám sát an toàn thông tin Trung tâm ANM&ATDL.

Tổng kết công tác đảm bảo ATTT tại Trung tâm tích hợp dữ liệu tỉnh Thanh Hóa trong năm 2017

PHẠM VĂN CƯỜNG
Phó Trưởng phòng Quản lý Cổng TTĐT&CNTT
Văn phòng UBND tỉnh Thanh Hóa

Trong năm 2017, công tác đảm bảo ATTT tại Trung tâm tích hợp dữ liệu tỉnh vẫn được duy trì hoạt động một cách an toàn, không để xảy ra sự cố hoặc các hoạt động xâm nhập trái phép gây mất an toàn thông tin; đảm bảo các hệ thống thông tin, các phần mềm ứng dụng dùng chung của tỉnh cài đặt tại Trung tâm tích hợp dữ liệu hoạt động ổn định, cụ thể như sau:

Hạ tầng kỹ thuật CNTT tại Trung tâm tích hợp dữ liệu của tỉnh đã được quan tâm đầu tư, nâng cấp với các máy chủ đủ mạnh, cùng các thiết bị đảm bảo an toàn thông tin như tường lửa, thiết bị phát hiện, cảnh báo và phòng chống xâm nhập trái phép, thiết bị chống thư rác, spam và quét virus; các bản quyền phần mềm vẫn được duy trì và mở rộng.

Cổng thông tin điện tử của tỉnh cung cấp nhiều thông tin liên quan đến chủ trương chính sách, các hoạt động của lãnh đạo tỉnh; cung cấp văn bản quy phạm pháp luật, văn bản chỉ đạo điều hành và các thủ tục hành chính; đăng tải toàn bộ Công báo điện tử của tỉnh, tích hợp và liên kết nhiều cơ sở dữ liệu, đa dạng hóa thông tin. Việc công khai số liệu giải quyết thủ tục hành chính, số liệu gửi nhận văn bản điện tử của các cơ quan quản lý nhà nước trên địa bàn tỉnh trên

HỆ THỐNG THEO DÕI VIỆC THỰC HIỆN NHIỆM VỤ CỦA ỦY BAN NHÂN DÂN TỈNH THANH HÓA

UBND TỈNH THANH HÓA
VĂN PHÒNG

BÁO CÁO TỔNG HỢP

TT	Tên đơn vị	Tổng số công việc được giao	Đã thực hiện và báo cáo			Đang thực hiện			Tỷ lệ so sánh	
			Tổng số	Chậm	Đúng thời gian quy định	Tổng số	Đang thực hiện trong hạn	Đang thực hiện đã quá hạn	Công việc đã thực hiện (%)	Đã thực hiện đúng hạn (%)
1	2	3	4	5	6	7	8	9	10	11
1	Ban Dân tộc	17	4	0	4	13	3	0	23	100
2	Ban Quản lý Khu kinh tế Nghi Sơn	65	25	0	10	40	5	0	38	100
3	Ban Tôn giáo	1	1	0	0	0	0	0	100	0
4	Ngân hàng Nhà nước	1	0	0	0	1	0	0	0	0
5	Sở Công Thương	71	30	0	15	41	4	0	42	100
6	Sở Giao thông Vận tải	55	26	0	12	29	3	0	47	100
7	Sở Giáo dục và Đào tạo	49	22	0	14	27	5	0	44	100
8	Sở Khoa học và Công nghệ	23	6	0	4	17	1	0	26	100

cổng thông tin điện tử Chính phủ và của tỉnh để người dân, doanh nghiệp giám sát được thực hiện thường xuyên. Hàng năm, cổng thông tin điện tử của tỉnh đã phục vụ hàng triệu lượt truy cập để khai thác thông tin.

Phần mềm theo dõi thực hiện nhiệm vụ của tỉnh đã được đưa vào sử dụng từ năm 2013, phần mềm giúp UBND tỉnh, Chủ tịch UBND tỉnh phát hành các văn bản giao việc cho các sở, ban, ngành và UBND các huyện, thị xã thành phố một cách nhanh chóng, kiểm soát được công việc đã giao; tránh tình trạng ách tắc, thiếu sót hoặc thực hiện không đầy đủ các chỉ đạo của UBND tỉnh, Chủ tịch UBND tỉnh làm ảnh hưởng đến hiệu quả chỉ đạo và điều hành. Để phát huy và nâng cao kỷ luật, kỷ cương hành chính trong việc thực thi các nhiệm vụ được giao, Văn phòng UBND tỉnh đã triển khai phần mềm theo dõi thực hiện nhiệm vụ đến tất cả các huyện, thị xã, thành phố trên địa bàn tỉnh nhằm theo dõi nhiệm vụ của UBND, Chủ tịch UBND cấp huyện giao cho các xã, phường, thị trấn và các các phòng ban chuyên môn trực thuộc UBND cấp huyện phục vụ công tác chỉ đạo, điều hành của các cấp.

Trung tâm tích hợp dữ liệu của tỉnh.

Hệ thống thư điện tử công vụ của tỉnh đã được đầu tư nâng cấp, đảm bảo, duy trì 100% cán bộ, công chức của các cơ quan quản lý hành chính nhà nước từ cấp tỉnh đến cấp xã có hộp thư điện tử và thường xuyên sử dụng trong công việc; tránh tình trạng sử dụng các hộp thư không chính thống như gmail, yahoo... theo chỉ đạo của Chính phủ, Bộ Thông tin và Truyền thông để trao đổi trong công việc./.

Tổng kết tình hình, sự kiện an toàn thông tin tiêu biểu trong năm 2017

BAN BIÊN TẬP

Năm 2017 đã đi qua với nhiều sự kiện về an toàn thông tin nổi bật cũng như bùng nổ các sự cố mất an toàn thông tin nghiêm trọng... Dưới đây, Bản tin An toàn thông tin điểm lại 10 tình hình, sự kiện an toàn thông tin tiêu biểu trong năm 2017 do Ban biên tập lựa chọn, tổng hợp và đánh giá.

1. Dự án Luật An ninh mạng

Dự thảo Luật An ninh mạng gồm 7 chương, 61 điều quy định về nguyên tắc, biện pháp, nội dung, hoạt động, điều kiện bảo đảm triển khai hoạt động bảo vệ an ninh mạng; trách nhiệm của cơ quan, tổ chức, cá nhân tham gia không gian mạng và có liên quan tới hoạt động bảo vệ an ninh mạng của nước Cộng hòa xã hội chủ nghĩa Việt Nam.

Tuy nhiên, do Luật An ninh mạng liên quan đến rất nhiều văn bản Luật đã ban hành như Bộ Luật hình sự, Luật An toàn thông tin mạng, Luật Cơ yếu, Luật Khoa học công nghệ, Luật Công nghệ thông tin... Vì vậy, Ban soạn thảo cần rà soát kỹ các quy định để tránh chồng chéo, trùng lặp với các Luật khác. Đồng thời, cần xác định rõ vai trò, chức năng, nhiệm vụ của các Bộ, ngành trong dự thảo Luật.

2. Dự án Luật Bảo vệ bí mật Nhà nước

Việc triển khai thực hiện Pháp lệnh Bảo vệ bí mật Nhà nước năm 2000 đã đạt nhiều kết quả quan trọng, nhưng đến nay đã bộc lộ những hạn chế, bất cập, chưa đáp ứng được yêu cầu bảo đảm an ninh, trật tự. Việc xây dựng Luật Bảo vệ bí mật Nhà nước là yêu cầu khách quan và cần thiết, góp phần cụ thể hóa các quy định của Hiến pháp năm 2013; tạo khuôn khổ pháp lý đầy đủ, vững chắc cho công tác bảo vệ bí mật Nhà nước, đáp ứng yêu cầu xây dựng và bảo vệ Tổ quốc trong tình hình mới; bảo đảm tốt các quyền con người, quyền công dân; phòng ngừa lộ, mất bí mật Nhà nước...

Dự thảo Luật Bảo vệ bí mật Nhà nước được bố cục thành 5 chương, 41 điều, trên cơ sở kế thừa và luật hóa những quy định phù hợp; sửa đổi, bổ sung những quy định còn thiếu, chưa khả thi của Pháp lệnh Bảo vệ bí mật Nhà nước

3. Triển lãm quốc gia về An toàn bảo mật 2017 (Security World)

Hội thảo diễn ra ngày 04/4/2017 tại Hà Nội với chủ đề "Bảo đảm an ninh mạng, an ninh thông tin trong thời kỳ cách mạng công nghiệp lần thứ 4". Tham dự Hội thảo có đại diện lãnh đạo các Ban, Bộ, ngành, hơn 400 chuyên gia, những người quan tâm về lĩnh vực ATTT.

Cuộc cách mạng công nghiệp lần thứ 4 có ảnh hưởng sâu sắc đến tất cả các lĩnh vực tại mọi quốc gia trên thế giới nói chung và Việt Nam nói riêng, đồng thời được dự báo sẽ tạo ra nhiều cơ hội và thách thức về ATTT. Điều đáng lo ngại nhất là người dùng Việt Nam vẫn chưa có ý thức và kiến thức đầy đủ để tự bảo vệ mình trước các rủi ro mất ATTT. Thực trạng trên đòi hỏi từng cơ quan, tổ

chức, doanh nghiệp và người dân cần nâng cao nhận thức và kỹ năng đảm bảo ATTT mạng, chủ động tăng cường các biện pháp tự bảo vệ, quản lý bảo mật và nghiên cứu tìm kiếm các giải pháp bảo vệ an toàn mạng. Security World 2017 có sự tham gia của các chuyên gia, lãnh đạo từ các cơ quan chính phủ, các tổ chức, doanh nghiệp trong và ngoài nước trong lĩnh vực bảo mật và an toàn thông tin. Song song với Hội thảo đã diễn ra Triển lãm công nghệ bảo mật 2017.

4. Ngày An toàn thông tin Việt Nam 2017

Ngày ATTT là sự kiện thường niên được tổ chức hàng năm và là một trong những hoạt động CNTT quan trọng trong năm được đông đảo cộng đồng ứng dụng và phát triển CNTT, ATTT, giới truyền thông và xã hội quan tâm. Năm 2017 là năm thứ 10 diễn ra sự kiện này.

Ngày ATTT Việt Nam năm 2017 gồm chuỗi các sự kiện về ATTT với trọng tâm là Hội thảo quốc tế được tổ chức tại Hà Nội ngày 01/12/2017, với chủ đề "An toàn thông minh trong thế giới kết nối mới". Tại Hội thảo, theo kết quả điều tra của VNISA, chỉ số ATTT năm 2017 của các tổ chức, doanh nghiệp Việt Nam là 54,2%. Chỉ số này vẫn còn thấp, đặc biệt là các doanh nghiệp vừa và nhỏ có nguy cơ mất ATTT rất cao; các khâu thiết lập và thực thi chính sách ATTT vẫn còn yếu; tốc độ phát triển ATTT tại Việt Nam vẫn còn chậm, sau 4 năm chỉ đạt mức trung bình về chỉ số, đặc biệt là lĩnh vực công nghiệp công nghệ ATTT.

5. Tấn công thiết bị IoT

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

Một nghiên cứu của Bkav cho thấy có tới 76% camera IP tại Việt Nam hiện vẫn dùng tài khoản và mật khẩu được nhà sản xuất cài đặt sẵn. Việc cập nhật bản vá cho lỗ hổng trên thiết bị IoT cũng không đơn giản như cập nhật cho phần

mềm, đòi hỏi sự can thiệp trực tiếp từ phía người dùng với kiến thức về mạng máy tính. Do đó, khả năng người dùng lơ là, không quan tâm đến lỗ hổng dù được cảnh báo là rất cao.

6. Thách thức đảm bảo an toàn trong công nghệ xác thực

Năm 2017, hàng loạt công nghệ sinh trắc học được đưa ra trong xác thực thông tin người dùng, đặc biệt là các công nghệ nhận diện hình ảnh. Tuy nhiên, các công nghệ này chưa đủ hoàn thiện và tồn tại lỗ hổng. Các chuyên gia đã chỉ ra công nghệ nhận diện mống mắt (Iris Scanner trên Galaxy S8 của Samsung) và công nghệ nhận diện khuôn mặt (Face ID trên iPhone X của Apple) không đảm bảo an toàn và có thể bị vượt qua dễ dàng.

Mật khẩu là giải pháp xác thực được sử dụng nhiều nhất hiện nay, nhưng ý thức sử dụng mật khẩu của người dùng tại Việt Nam chưa cao. Trong năm vừa qua, một số vụ mất tiền trong tài khoản ngân hàng tại Việt Nam cũng xuất phát từ nguyên nhân này. Theo thống kê của Bkav, cho tới nay vẫn còn tới 55% người dùng sử dụng chung một mật khẩu cho các tài khoản tại nhiều dịch vụ trực tuyến khác nhau.

7. Mã độc đào tiền ảo có dấu hiệu bùng nổ

Năm 2017 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.

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. Gần đây nhất, mã độc lây qua Facebook bùng phát từ ngày 19/12 và làm hơn 23.000 máy tính tại Việt Nam nhiễm loại mã độc này.

8. Mã độc tống tiền hoành hành trên khắp thế giới

Năm 2017 cũng chứng kiến sự bùng nổ của các ransomware lợi dụng lỗ hổng hệ điều hành để phát tán với tốc độ chóng mặt. Điển hình là ngày 12/5/2017, một loại mã độc có tên là WannaCry xuất hiện và lây lan tại hơn 100 quốc gia trên khắp các châu lục chỉ sau vài giờ xuất hiện, trong đó Châu Âu là nơi chịu ảnh hưởng nặng nề nhất. Việt Nam có hơn 1.900 máy tính bị lây nhiễm mã độc tống tiền này; trong đó, khoảng 1.600 máy tính được ghi nhận tại 243 cơ quan, doanh nghiệp và khoảng 300 máy tính là của cá nhân. Cuộc tấn công mã độc tống tiền WannaCry được xem là cuộc tấn công mạng lớn nhất từ trước đến nay, gây hậu quả nặng nề cho nhiều tổ chức, doanh nghiệp và cá nhân trên khắp thế giới.

Sau đó, đã xuất hiện họ mã độc tống tiền Petya/Petrwrap và một số dòng mã độc khác. Nguy hiểm hơn, mã độc tống tiền đã chuyển sang hướng tấn công smartphone. Số tiền chuộc khổng lồ hacker kiếm được chính là nguyên nhân dẫn tới sự bùng nổ của loại mã độc nguy hiểm này.

Để phòng ngừa nguy cơ mã độc tấn công, chuyên gia 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.

9. Tin tức giả mạo tràn lan mạng xã hội

Sự bùng nổ của tin tức giả mạo (tin bịa đặt, sai sự thật) mang lại không ít phiền toái cho người sử dụng mạng xã hội trong năm vừa qua. Tại Mỹ, tin tức giả mạo cũng tràn ngập Facebook, Google, Twitter... đặc biệt liên quan đến các sự kiện lớn. Tại Việt Nam, số liệu thống kê từ chương trình đánh giá an ninh mạng của Bkav cho thấy, 63% người dùng thường xuyên đọc được tin tức giả mạo trên Facebook, trong đó 40% là nạn nhân hằng ngày. Mặt khác, không chỉ khiến người đọc hoang mang, tin tức giả mạo còn tiềm ẩn nguy cơ gây bất ổn xã hội khi kẻ xấu cố tình đưa tin sai sự thật liên quan đến tình hình kinh tế, chính trị của đất nước.

Cùng với sự phát triển phổ biến của mạng xã hội đặc biệt là những trang mạng xã hội có đông người sử dụng như Facebook, nhiều đối tượng xấu đang sử dụng mạng xã hội làm nền tảng để lừa đảo trực tuyến hay phát tán những phần mềm độc hại, gây ra những rủi ro, mất an toàn thông tin cho người sử dụng.

10. Việt Nam giành giải Nhất cuộc thi WhiteHat Grand Prix 2017

Cuộc thi An ninh mạng toàn cầu với chủ đề "Di sản Việt Nam" diễn ra ngày 16/12, do Tập đoàn Bkav phối hợp với Cục ATTT, Bộ TT&TT tổ chức. Đây là năm thứ 5 liên tiếp WhiteHat Grand Prix diễn ra và là năm thứ 3 được mở rộng ra quy mô toàn cầu. Cuộc thi thu hút sự tham gia của 452 đội đến từ 62 quốc gia, vùng lãnh thổ trên thế giới như: Mỹ, Hàn Quốc, Đài Loan, Trung Quốc...

Trong 24 giờ thi đấu, các đội dự thi đã trải qua những phần thi trực tuyến với các chủ đề chính như: lỗ hổng web, khai thác lỗ hổng phần mềm, các hình thức tấn công, phòng thủ... Sau những nỗ lực bứt phá ở phút cuối, đội CLGTftMeePwn của Việt Nam đã giành giải Nhất, giải Nhì và Ba lần lượt thuộc về đội đến từ Đài Loan và Mỹ.

Tổng hợp các hình thức tấn công mạng phổ biến năm 2017 và xu hướng trong năm 2018

HOÀNG ANH TUẤN
Tổ phó Tổ Ứng cứu sự cố
Trung tâm CNTT&TT Thanh Hóa

Các vụ tấn công mạng tại Việt Nam ngày càng nghiêm trọng và phức tạp hơn. Trong 9 tháng đầu năm 2017, Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam VNCERT đã ghi nhận có 9.964 sự cố tấn công mạng trong nước. Trong đó có 1.762 sự cố website lừa đảo (Phishing), 4.595 sự cố về phát tán mã độc (Malware) và 3.607 sự cố tấn công thay đổi giao diện (Deface). Dưới đây là tổng hợp các hình thức tấn công mạng phổ biến trong năm 2017:

1. Tấn công vào trình duyệt (Browse Attacks)

Một trongcác hình thức tấn công mạngđiển hình nhất năm 2017 phải kể đến là tấn công vào trình duyệt. Các cuộc tấn công của trình duyệt thường được bắt đầu bằng những trang web hợp pháp nhưng dễ bị tổn thương. Kẻ tấn công có thể xâm nhập vào website và gây hại cho đối tượng bằng phần mềm độc hại.

Cụ thể, khi có khách truy cập mới thông qua trình duyệt web, trang web đó sẽ lập tức bị nhiễmmã độc. Từ đó, mã độc sẽ xâm nhập vào hệ thống của nạn nhân qua lỗ hổng của trình duyệt. Các trình duyệt web bị tin tặc tấn công chủ yếu năm 2017 là Microsoft Internet Explorer Edge, Google Chrome, Mozilla, Firefox, Apple Safari, Opera.

2. Tấn công vét cạn (Brute Force Attacks)

Brute force attacks làhình thức tấn công mạngsử dụng mật khẩu, tên người dùng... để tự động kết hợp chúng với nhau cho tới khi chính xác. Kiểu tấn công Brure attacks này có thể mất thời gian vì vậy tin tặc thường sử dụng phần mềm tự động hóa để nhập hàng trăm nghìn mật khẩu.

Để phòng tránh kiểu tấn công này, người quản trị website cần cấu hình module giới hạn số lần đăng nhập sai cho mỗi tài khoản, hoặc giới hạn số lần đăng nhập từ các địa chỉ IP.

3. Tấn công từ chối dịch vụ (Ddos Attacks)

Ddos attack hay còn gọi là tấn công từ chối dịch vụ - đứng thứ ba trong danh sáchcác cuộc tấn công mạng nổi bật năm 2017. Phương thức tấn công Ddos chủ yếu nhắm vào các mục tiêu

như: website, máy chủ trò chơi, máy chủ DNS..làm chậm, gián đoạn hoặc đánh sập hệ thống.

Theo khảo sát của Kaspersky, có tới 5.200 trường hợp bị tấn công từ chối dịch vụ Ddos tại 29 quốc gia khác nhau trong năm 2017 vừa qua.

4. Kiểu tấn công sử dụng sâu (Worm Attacks)

Worm là những chương trình có khả năng tự động khai thác, tấn công vào điểm đầu cuối hoặc những lỗ hổng đã có sẵn. Sau khi đã tận dụng các lỗ hổng thành công trong hệ thống, Worm sẽ tự động sao chép chương trình từ máy bị nhiễm rồi lây lan sang các máy khác.

Kiểu tấn công mạng Worm Attack thường yêu cầu người dùng tương tác trước để bắt đầu lây nhiễm. Worm attacks thường được tấn công thông qua tệp tải xuống chứa email độc hại, usb, đầu đọc thẻ.

Một trong ví dụ tiêu biểu của phương thức tấn công này làmã độc WannaCry đã lây nhiễm hơn 300.000 máy tínhchỉ sau một vài ngày. WannaCry nhắm vào mục tiêu lỗ hổng trên Windows, một khi máy bị nhiễm, phần mềm độc hại sẽ tự động quét hệ thống mạng kết nối với nhau, từ đó lây nhiễm sang các máy tính khác.

5. Tấn công bằng phần mềm độc hại

Các kiểu tấn công mạng thông qua phần mềm độc hại chủ yếu là:

Email phishings: Tin tặc thường lừa đảo người dùng bằng cách tạo ra những thông điệp để thu hút sự tò mò của người nhận. Nhưng thực chất, những tệp này sẽ chứa các phần mềm độc hại và phát tán ngay sau khi người dùng tải về máy.

Tấn công bằng website độc hại (malicious websites): Với cách thức này, kẻ tấn công thường tạo một trang web giả mạo có giao diện y hệt với giao diện của website gốc. Sau khi nạn nhân truy cập vào địa chỉ website đó, phần mềm độc hại sẽ từ từ thâm nhập vào hệ thống của họ. Điển hình cho ví dụ này là các vụ giả mạo website ngân hàng, website ngành hàng không vừa xảy ra trong năm 2016 - 2017.

Tấn công bằng quảng cáo chứa mã độc (Malvertising): Đối với một số kẻ tấn công thông minh, chúng sẽ tận dụng mạng lưới các quảng cáo để gắn mã độc vào đó. Khi click vào quảng cáo độc hại này, người dùng sẽ bị điều hướng tới một website khác có chứa phần mềm độc hại. Nguy hiểm hơn, trong một số trường hợp người dùng không click vào quảng cáo cũng có thể bị tấn công.

6. Tấn công website (Website Attacks)

Các dịch vụ tấn công công cộng chẳng hạn như thông qua ứng dụng website, cơ sở dữ liệu thường là đối tượng mục tiêu tấn công nhằm vào website.

Các cuộc tấn công mạng thông qua lỗ hổng website chủ yếu là lỗ hổng SQL Injection, XSS, và path Traversal.

7. Kiểu tấn công rà quét (Scan Attacks)

Thay vì sử dụng các hình thức tấn công toàn diện, Scan Attacks làkỹ thuật tấn công mạngrà quét lỗ hổng thông qua các dịch vụ, hệ thống máy tính, thiết bị, hạ tầng mạng của doanh nghiệp. Tin tặc sẽ sử dụng các công cụ để rà quét, nghe lén hệ thống mạng để tìm ra lỗ hổng sau đó thực thi tấn công.

8. Các kiểu tấn công mạng khác

Ngoài 7 kiểu tấn công mạng nổi bật nói trên, Hacker còn có thể xâm nhập vào bên trong hệ thống bằng cách:

+ Tấn công vật lý (Physical Attacks). Tin tặc sẽ cố gắng phá hủy, ăn cắp dữ liệu kiến trúc trong cùng một hệ thống mạng.

+ Tấn công nội bộ (Insider Attacks). Các cuộc tấn công nội bộ thường liên quan tới người trong cuộc. Các cuộc tấn công hệ thống mạng nội bộ có thể gây hại hoặc vô hại. Khi có tấn công mạng nội bộ xảy ra, thông tin dữ liệu của công ty có thể bị truy cập trái phép, thay đổi hoặc bán đổi.

1. Mã độc tống tiền

Mã độc tống tiền như WannaCry, Ransomware, Petya cũng là một trong những xu hướng tấn công mạng của Hacker trong năm 2018 tới đây. Ngoài ra, hình thức sử dụng mã độc tống tiền yêu cầu tiền chuộc bằng bitcoin sẽ được Hacker nhắm vào trong năm tới đây.

2. Thiết bị IoT và Big Data

Hình thức tấn công mạng như Phishing, Dos nhằm vào thiết bị IoT, Big Data dự báo tiếp tục gia tăng về số lượng, phức tạp hơn về kỹ thuật, rộng lớn hơn về quy mô. Theo ghi nhận cứ 02 phút lại có 01 thiết bị IoT bị tấn công

3. Tấn công thông qua bên thứ 3

Dự báo, hình thức tấn công mạng nhắm vào lỗ hổng phần mềm của bên thứ 3 sẽ nở rộ hơn năm nay. Nhìn lại năm 2017, các cuộc tấn công Shadowpad và ExPetya nhắm vào lỗ hổng phần mềm của bên thứ 3 cho thấy dạng phần mềm này có thể được sử dụng để xâm nhập vào doanh nghiệp. Tin tặc tận dụng lỗ hổng của phần mềm, cài backdoor vào đó và bắt đầu thu thập thông tin hoặc đánh cắp dữ liệu.

4. Tấn công thiết bị Router và Modem

Thiết bị mạng sẽ là điểm mấu chốt mà Hacker đã dự định từ lâu. Dự báo router và modem sẽ bị khai thác nhiều hơn. Kẻ xấu sẽ tận dụng kẽ hở của các thiết bị này để tiến hành các cuộc tấn công có chủ đích. Dựa vào điểm yếu của đường truyền mạng, Hacker sẽ chèn mã độc vào thiết bị.

5. Tấn công lừa đảo qua Email

Hình thức tấn công qua email sẽ luôn là xu hướng và mục đíchtấn công mạngcủa kẻ xấu. Hacker có thể gửi link, file chứa mã độc vào email sau đó yêu cầu người dùng click vào đường dẫn. Hacker có thể giả mạo thư email của google hoặc các tổ chức uy tín gửi mã độc tới email của bạn. Nguy hiểm hơn, chúng có thể tạo giả trang đăng nhập email của google để tống tiền người dùng.

6. Tấn công Website

Mục tiêu tấn công vào các website chắc chắn vẫn tiếp tục tăng vì đây là bộ mặt của doanh nghiệp và tổ chức. Để bảo mật cho người dùng, người sở hữu website cần bảo mật web ở chế độ cao nhất (cho cả người quản trị và người truy cập).

7. Lừa đảo qua Facebook

Tình trạng lừa đảo qua Facebook tiếp tục gia tăng và diễn biến khó lường. Một số hình thức lừa đảo cũ mà bạn cần phòng tránh là không click vào đường link giả mạo, cẩn thận với dạng tấn công phishing, không chấp nhận những yêu cầu liên quan tới tiền nong của người lạ mặt,...

Hoạt động triển khai đảm bảo an toàn thông tin trong thời gian trước trong và sau tết Nguyên đán Mậu Tuất 2018

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

Thực hiện Công văn số 4749/BTTTT-CATTT ngày 29/12/2017 của Bộ Thông tin và Truyền thông (TT&TT) về việc đôn đốc tăng cường bảo đảm an toàn thông tin trong dịp Tết Dương lịch và Tết Mậu Tuất 2018, Công văn số 26/VNCERT-ĐPƯC của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam về việc tăng cường công tác bảo đảm ATTT trong dịp nghỉ lễ Tết Nguyên đán Mậu Tuất 2018 và Kế hoạch số 87/STTTT-CNTT ngày 25/01/2018 của Giám đốc Sở Thông tin và Truyền thông về việc hướng dẫn tăng cường bảo đảm an toàn thông tin trong dịp tết Mậu Tuất 2018. Trung tâm Công nghệ thông tin và Truyền thông (trung tâm) đã xây dựng và triển khai Kế hoạch số 49/KH-TTCNTT&TT ngày 31/01/2018 của Giám đốc Trung tâm về việc Tổ chức đón tết Nguyên đán Mậu tuất năm 2018. Trong đó, tập trung nguồn lực của Trung tâm nhằm tăng cường công tác đảm bảo an toàn thông tin trong dịp nghỉ lễ tết Nguyên đán Mậu Tuất 2018 đến các Sở, ban, nghành cấp tỉnh; UBND các huyện, thị xã, thành phố trên địa bàn tỉnh.

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

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

Tăng cường phân công cán bộ tham gia trực tại Trung tâm An ninh mạng và An toàn dữ liệu của tỉnh để đảm bảo các hệ thống cơ sở dữ liệu và phần mềm dùng chung phục vụ công tác quản lý điều hành của phần lớn của các cơ quan, đơn vị trên địa bàn tỉnh được thông suốt, ổn định. Trong mỗi ca trực lãnh đạo Trung tâm đã chỉ đạo tăng từ 01 lên 02 cán bộ để đảm bảo thực hiện xử lý các sự cố khi có yêu cầu.

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

nguyên nhân gây ra sự cố.

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

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

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

Nhờ áp dụng triệt để biện pháp về tăng cường nhân lực kịp thời tiếp nhận, xử lý các sự cố, thực hiện nghiêm các quy trình rà soát, sao lưu mang tính kỹ thuật, trong thời giantrước, trong và sau tết Nguyên đán Mậu tuất 2018 tại Trung tâm An ninh mạng và An toàn dữ liệu của tỉnh, các dịch vụ trang/cổng thông tin điện tử, phần mềm, Cở sở dữ liệu chuyên ngành đang cung cấp tại trung tâm hoạt động đảm bảo, ổn định 24/24, không xảy ra hiện tượng mất an toàn an ninh thông tin. Cán bộ thường xuyên theo dõi và ghi nhận kịp thời các thông tin đăng tải trên mạng internet, không phát hiện có nội dung kích động và thông tin sai lệch nhằm ảnh hưởng đến trật tự, an toàn thông tin trên địa bàn tỉnh. Qua đó phục vụ tốt công tác lãnh đạo, chỉ đạo, điều hành trước, trong và sau tết Nguyên đán, của các cấp, ngành, chính quyền và truy cập thông tin của nhân dân trong tỉnh./.

Công tác tổ chức thi và cấp chứng chỉ ứng dụng CNTT theo chuẩn kỹ năng sử dụng công nghệ thông tin Thông tư số 03/2014/TT-BTTTT trong năm 2017 của Trung tâm

TRỊNH NGỌC QUỲNH

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

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

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

Với chức năng, nhiệm vụ được Chủ tịch UBND tỉnh giao, Trung tâm CNTT&TT Thanh Hóa đã chuẩn bị đầy đủ các điều kiện về cơ sở vật chất, trang thiết bị, nhân lực, giáo trình đào tạo, ngân hàng câu hỏi thi trắc nghiệm, phần mềm thi trắc nghiệm đảm bảo theo

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

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

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

Trong năm 2017, Trung tâm đã triển khai công tác tổ chức chiêu sinh, đào tạo, bồi dưỡng, tổ chức thi và cấp chứng chỉ 07 đợt cho hơn 220 thí sinh, trong đó đã cấp 210 chứng chỉ ứng dụng CNTT cơ bản.

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

Mọi chi tiết xin liên hệ: Phòng Đào tạo & Dịch vụ - Trung tâm CNTT&TT Thanh Hoá

- Địa chỉ: Số 73 Hàng Than, P. Lam Sơn - Tp Thanh Hoá
- Điện thoại: 02373.718.698
- Website:ict.thanhhoa.gov.vn.

Các cơ quan, đơn vị cử cán bộ đề nghị gửi danh sách đăng ký (theo mẫu đính kèm) về hòm thư: tuyensinhdaotaott03@gmail.com trước 03 ngày căn cứ theo lịch bồi dưỡng kiến thức hàng tháng.

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

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

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

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

- Thông tư liêntịch số 10/2015/TTLT-BYT- BNV, ngày 27/5/2015 giữa Bộ Nội vụvà Bộ Y tế về việc quy định mã số, tiêu chuẩn chức danh nghề nghiệp bác sĩ, bác sĩ y học dự phòng, y sĩ; Thông tư liên tịch số27/2015/TTLT-BYT-BNV, ngày 07/10/2015 về việc quy định mã số, tiêu chuẩn chức danh nghề nghiệp dược.

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

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

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

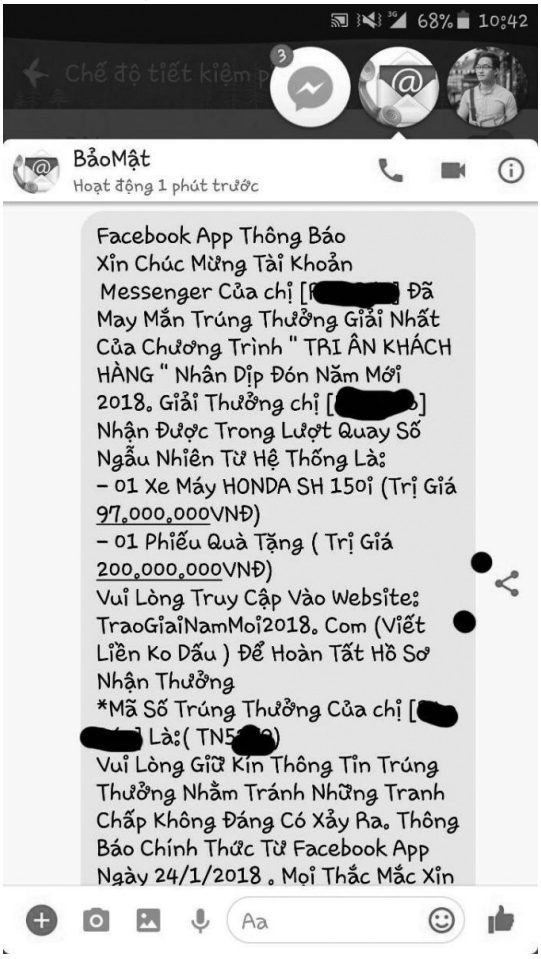
Cảnh báo các chiến dịch tấn công
LỪA ĐẢO QUA CHƯƠNG TRÌNH KHUYẾN MẠI, TRI ÂN KHÁCH HÀNG

TRẦN NGỌC HƯNG
Trung tâm CNTT&TT Thanh Hóa

Theo Cục An toàn thông tin - Bộ Thông tin và Truyền thông, lợi dụng thời điểm cuối năm, cận tết Âm lịch có nhiều chương trình khuyến mại, giảm giá, tri ân cho khách hàng, các đối tượng đang mở những chiến dịch tấn công lừa đảo nhắm vào người dùng Internet tại Việt Nam, nhất là người dùng Facebook.

Một số hình ảnh sử dụng trong chiến dịch tấn công lừa đảo (Phishing) của các đối tượng xấu.
(Nguồn: Cục An toàn thông tin)

Ngày 24/1/2018, Cục An toàn thông tin - Bộ TT&TT đã có công văn gửi đơn vị chuyên trách về CNTT các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ; Sở TT&TT các tỉnh, thành phố trực thuộc Trung ương; các Tập đoàn, Tổng công ty nhà nước; các Ngân hàng TMCP và các tổ chức tài chính để cảnh báo về các chiến dịch tấn công lừa đảo thông qua các chương trình khuyến mại, giảm giá, tặng quà tri ân cho khách hàng. Cục An toàn thông tin cho biết, qua công tác giám sát và theo dõi tình hình, Cục phát hiện đang có nhiều chiến dịch tấn công lừa đảo nhắm vào người sử dụng mạng Internet tại Việt Nam, đặc biệt là những người dùng mạng xã hội Facebook. Các chiến dịch lừa đảo này tạo ra hàng loạt trang web giả mạo các mạng xã hội, ngân hàng, nhà cung cấp dịch vụ lớn, các chương trình trúng thưởng để thu thập thông tin cá nhân, tài khoản mạng xã hội, tài khoản ngân hàng, thẻ tín dụng... của người sử dụng.



Theo phân tích của Cục An toàn thông tin, các đối tượng tấn công lợi dụng thời điểm cuối năm, thời gian cận tết Âm lịch có nhiều chương trình khuyến mại, giảm giá, tặng quà tri ân cho khách hàng; đồng thời tâm lý và thói quen mua sắm vội vàng cuối năm làm cho nhiều người dùng mất cảnh giác.

Các trang web lừa đảo được đối tượng tấn công lan truyền và quảng bá đến người dùng thông qua nhiều kênh khác nhau, trong đó kênh được sử dụng nhiều nhất hiện tại là Facebook Messenger. Để gia tăng sự tin tưởng của người dùng, các thông tin lừa đảo khi lan truyền còn được kèm theo các đoạn mã được quảng cáo là mã trúng thưởng. Cục An toàn thông tin đã phát hiện có ít nhất 700 tên miền được sử dụng để phục vụ cho các chiến dịch tấn công lừa đảo nói trên. Hầu hết các trang web đều sử dụng tên miền được đăng ký gợi mở đến chương trình trúng thưởng, trao giải như: hosofacebook.com; hosofb68669.com; hopqua2018.com; nhan-quatet2018.com; nhanthuong2018.com; trao-giainammoi2018.com; quacuoinam2018.com; mochathuongtet2018.com

Trước tình hình trên nhằm bảo đảm an toàn thông tin và phòng tránh nguy cơ bị tấn công lừa đảo, Trung tâm CNTT&TT khuyến nghị:

- Người dùng cần cảnh giác với những tin nhắn với các thông tin khuyến mãi, trúng thưởng, nhận thưởng. Không click vào bất cứ liên kết lạ nào được nhận từ tin nhắn trên facebook, kể cả từ các tài khoản bạn bè và người thân và các kênh tương tự như Zalo, Viber...

- Cảnh giác với những địa chỉ web lạ, gợi mở về việc nhận thưởng, trao giải. Trong trường hợp cần thiết, xin vui lòng liên hệ với chủ quản của nhãn hiệu đó để xác minh;

- Cập nhật mật khẩu tài khoản facebook, sử dụng các mật khẩu mạnh, chưa từng được sử dụng trước đó, bật tính năng xác thực 2 bước do facebook cung cấp;

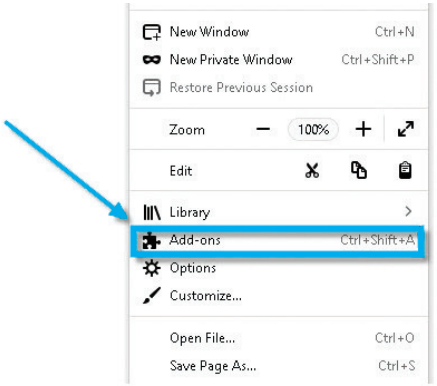
- Không cung cấp tài khoản mạng xã hội, tài khoản ngân hàng, thông tin cá nhân hay các thông tin riêng khác trên bất kỳ trang mạng không rõ nguồn gốc;

- Ngăn chặn trực tiếp danh sách các trang web lừa đảo ngay trên trình duyệt của người dùng bằng cách sử dụng các tiện ích trên các trình duyệt theo hướng dẫn như sau:

HƯỚNG DẪN CHẶN TRANG WEB TRONG FIREFOX

Bước 1: Truy cập trang add-ons của **Firefox**

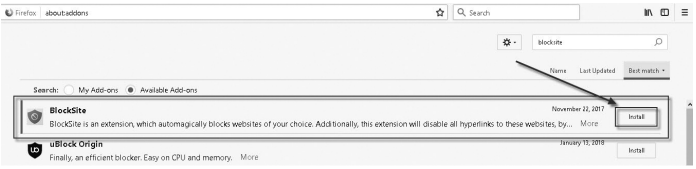
- Mở **Firefox** lên, click vào **Open menu** ở góc trên bên phải, chọn **Add-ons**



Bước 2: Cài đặt **BlockSite**

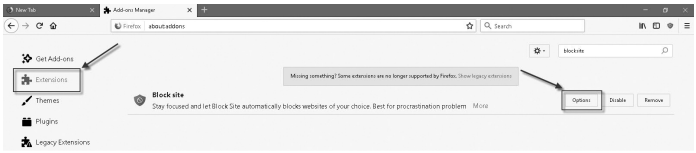
- Khi trang tiện ích mở ra, bạn gõ từ khóa **Blocksite** vào ô **Search** rồi ấn **Enter** để Firefox tìm chương trình Blocksite

- Sau đó danh sách tiện ích sẽ được liệt kê ở phía dưới, bạn click vào **Install** của add-ons **Blocksite** và đợi cho chương trình cài đặt xong.



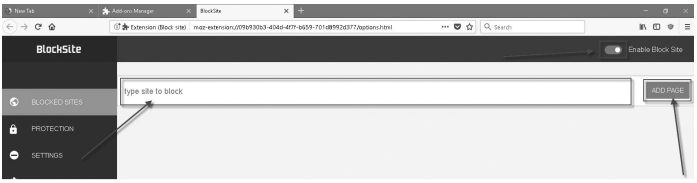
- Sau khi cài đặt xong, Firefox sẽ hiện ra thông báo yêu cầu bạn khởi động lại trình duyệt để có thể sử dụng add-on được. Click vào **Restart Now** để khởi động Firefox. Lưu ý phiên bản Firefox 58.0 mới nhất thì không cần Restart lại.

Bước 3: Sau khi Firefox khởi động lại, bạn click vào mục **Extension**, chọn mục **Options** của Blocksite



- Cửa sổ Blocksite hiện ra, **bật Enable Block Site** (trong trường hợp nó chưa được chọn trước,còn nếu được chọn rồi thì thôi) click vào ô trắng **type site to block** gõ địa chỉ website muốn chặn, tiếp theo click **ADD PAGE** để tiến hành thêm địa chỉ web cần chặn.

Để chặn theo danh sách các trang web kèm theo. Mở file phishing.txt vào copy/paste vào trong ô dưới đây.



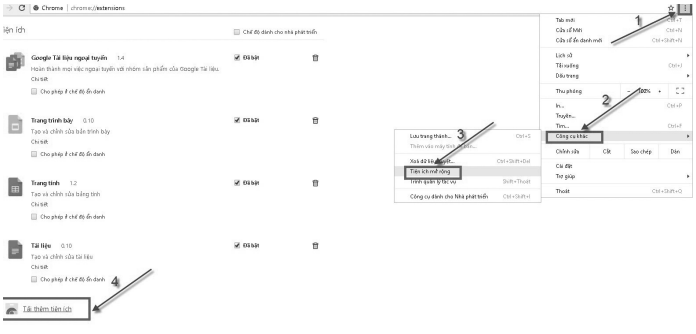
- Nếu muốn truy cập lại website vừa chặn, click vào biểu tượng thùng rác để xóa địa chỉ đã chặn.

Với những thao tác đã hướng dẫn ở trên người dùng có thể chặn các Website bất kỳ trên trình duyệt Firefox bằng tiện ích Blocksite, nhờ đó có thể ngăn người khác truy cập vào những website mà bạn không muốn trên máy tính của mình.

HƯỚNG DẪN CHẶN TRANG WEB TRONG GOOGLE CHROME

Bước 1: Truy cập trang add-ons của **Google Chrome**

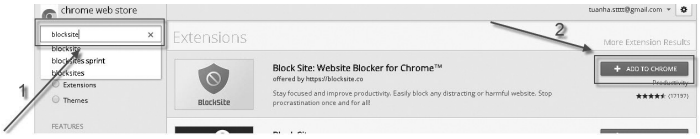
- Mở **Google Chrome** lên, click vào ⋮ **Tùy chỉnh và điều khiển Google Chrome** ở góc trên bên phải, chọn **Công cụ khác**, chọn **Tiện ích mở rộng**, tiếp theo chọn **Tải thêm tiện ích**



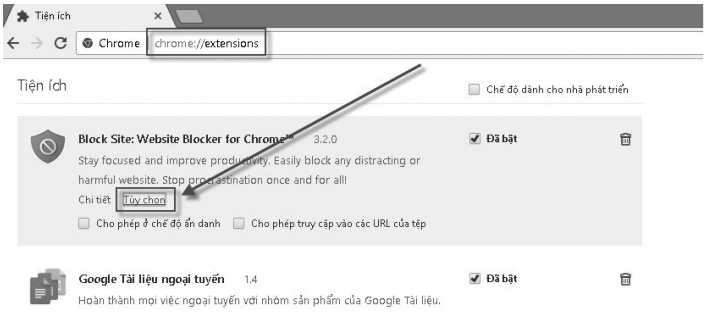
Bước 2: Cài đặt **BlockSite**

- Khi trang tiện ích mở ra, bạn gõ từ khóa **Blocksite** vào ô **Search** rồi ấn **Enter** để Google Chrome tìm chương trình Blocksite

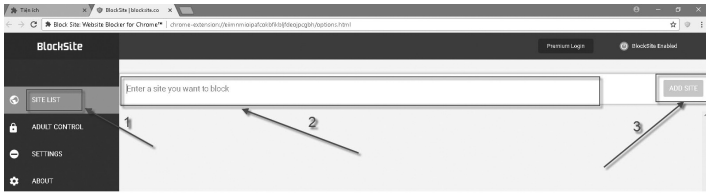
- Sau đó danh sách tiện ích sẽ được liệt kê ở phía bên, click vào **ADD TO CHROME** của add-ons **Blocksite** và đợi cho chương trình cài đặt xong.



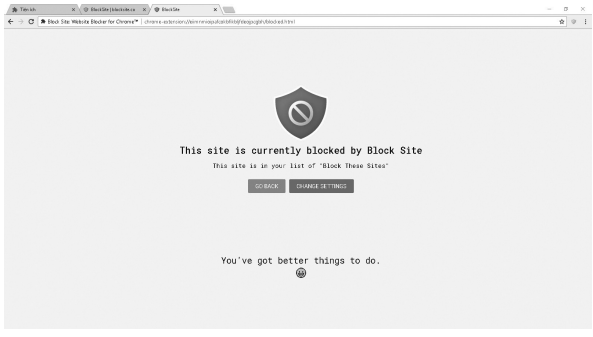
Bước 3: Sau khi cài đặt xong, quay trở lại **extensions**, click vào ô **Tùy chọn** của Blocksite



- Cửa sổ Blocksite hiện ra, bật **Enable Block Site** (trong trường hợp nó chưa được chọn trước, còn nếu được chọn rồi thì thôi) click vào ô trắng **Enter a site you want to block** gõ địa chỉ website muốn chặn, tiếp theo click **ADD PAGE** để tiến hành thêm địa chỉ web cần chặn



- Đây là thông báo sau khi truy cập vào trang web đã bị chặn



- Nếu muốn truy cập lại website vừa chặn, click vào biểu tượng thùng rác để xóa địa chỉ đã chặn.

Với những thao tác đã hướng dẫn ở trên người dùng có thể chặn các Website bất kỳ trên trình duyệt Google Chrome bằng tiện ích Blocksite, nhờ đó có thể ngăn người khác truy cập vào những website mà bạn không muốn trên máy tính của mình.

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 tấn công lừa đảo cần nhanh chóng thông tin về Tổ Ứng cứu sự cố của Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa theo địa chỉ dưới đây, để được hỗ trợ, xử lý kịp thời, hạn chế tối đa các nguy cơ mất an toàn thông tin mạng.

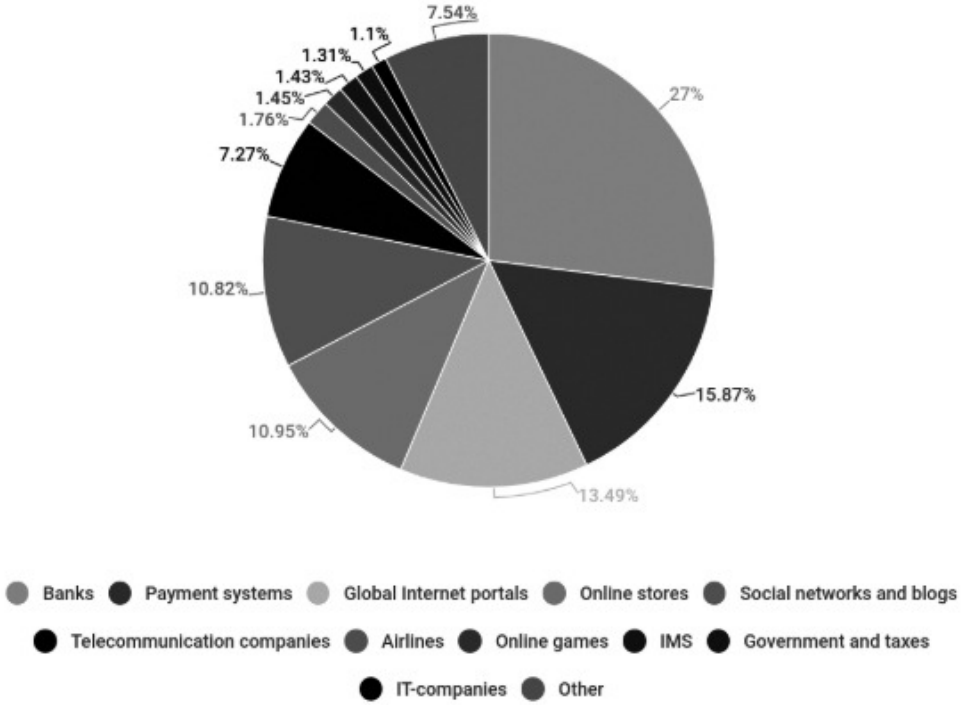
Thông tin liên hệ:
Điện thoại: (0237) 3718699;
Fax (0237) 3718299.
Email: ungcuusuco@thanhhoa.gov.vn

Phishing: Những con số năm 2017

Trong năm 2017, theo ghi nhận của Kaspersky ghi nhận 246.231.645 cuộc tấn công lừa đảo tới người dùng cuối so với 91.273.748 trong năm 2016. Trong đó 15,9% người dùng là mục tiêu xác định của kẻ lừa đảo.

Đồng thời các tổ chức được kẻ lừa đảo sử dụng để giả mạo nhiều nhất là ngân hàng (chiếm 27%), thứ hai là các hệ thống thanh toán (15,87%) và thứ 3 là các cửa hàng trực tuyến (10,95%).

Tại Việt Nam, theo ghi nhận của VNCERT thì tấn công lừa đảo (phishing) trong năm 2017 là 2.605 trường hợp.



THIẾT LẬP MÁY TÍNH AN TOÀN

Trong những năm qua, máy tính cá nhân đã trở nên phổ biến trên thị trường.
Khi sử dụng máy tính vừa mua hay vừa được cài đặt lại, các nguy cơ mất an toàn thông tin có thể ảnh hưởng đến người dùng.
Cần thiết có một số lưu ý để thiết lập máy tính mới an toàn.

Nguy cơ và hiểm họa

1 Các máy tính mới mua hay mới được cài đặt lại thường chưa được cập nhật các bản vá lỗi cũng như chưa được thực hiện các thiết lập an toàn cần thiết, kẻ xấu có thể lợi dụng các lỗ hổng để tấn công khai thác thông tin.

2 Việc truy cập trái phép vào máy tính có thể làm thất thoát thông tin cá nhân hoặc bị lợi dụng làm bước đệm để tấn công vào máy tính khác.

Thiết lập an toàn

- **Tạo mật khẩu mạnh** cho tài khoản của người dùng (bao gồm ký tự hoa, ký tự thường, ký tự chữ số, ký tự đặc biệt), giúp bảo vệ máy tính trong suốt quá trình sử dụng về sau.

- **Tháo bỏ các chương trình không cần thiết** như chương trình quảng cáo của nhà sản xuất, bản dùng thử các phần mềm đi kèm, sử dụng chức năng Programs and Futures trong Control Panel.

- **Kích hoạt chức năng tường lửa** bảo vệ cá nhân trên máy tính trước khi kết nối đến bất kỳ mạng máy tính nào, sử dụng chức năng Fire-wall trong Control Panel.

- **Nâng cấp các phần mềm và hệ điều hành Windows** để được cập nhật các bản vá lỗi bảo mật mới nhất, sử dụng chức năng Windows Update của Control Panel.

- **Cài đặt phần mềm diệt Virus**, bảo vệ người dùng khỏi mã độc và virus.

LỪA ĐẢO CHỈ BẰNG MỘT CÚ NHẤN CHUỘT

- Lừa đảo chỉ bằng một cú nhấn chuột là sự lừa gạt liên quan đến tiền bạc khi bạn sử dụng các dịch vụ hiển thị trên màn hình. Bạn bị yêu cầu phải thanh toán sau khi chạm vào một biểu tượng trên màn hình hoặc một video trên trang web nào đó.
- Gần đây, đã có những lừa đảo chỉ bằng một cú nhấn chuột thông qua các ứng dụng cho điện thoại thông minh và mạng xa hội như facebook, google+.
- Ngoài các trường hợp chỉ với một cú nhấn chuột, hóa đơn đòi thanh toán có thể hiện ra sau vài cú nhấn chuột, ví dụ sau khi kiểm tra thông tin cá nhân như tuổi, v.v. Trong một số trường hợp, kỹ thuật được dùng trở nên tinh vi và xảo quyệt hơn, ví dụ màn hình đòi thanh toán tiền không hề biến mất thậm chí kể cả sau khi tắt nguồn thiết bị và bật lại.

i | Nguy cơ và hiểm họa

1 Cú nhấn chuột vào các biểu tượng bắt mắt trên màn hình hoặc bật xem một băng hình có thể bị đòi thanh toán một cách phi lý hoặc mở đường dẫn đến các trang lừa đảo.

2 Có trường hợp hóa đơn đòi thanh toán có ghi các địa chỉ IP của thiết bị, cũng như các thông tin liên quan đến cá nhân nhằm khủng bố, bắt bạn phải thanh toán.

*3 – Địa chỉ IP là một số hiệu định danh được gán tự động cho các dụng cụ hoặc máy tính khi chúng được kết nối với internet.

? | Biện pháp đề phòng

- Chặn mọi hành vi tìm cách kết nối đến các trang mã độc thông qua việc sử dụng phần mềm lọc hay các phần mềm an ninh mới cập nhật. Chỉ tải các ứng dụng cho điện thoại thông minh từ những nguồn tin cậy.

- Khi sử dụng máy tính bạn cần biết rằng, một cú nhấn chuột không bao giờ xác định được danh tính của bạn, vì vậy đừng phản hồi lại các yêu cầu đòi thanh toán tiền. Tùy thuộc vào ứng dụng trên điện thoại thông minh, hãy lưu ý là thông tin lưu trong máy ví dụ như địa chỉ hay thông tin khác trong danh bạ có thể bị lộ.

- Nếu bạn chẳng may kết nối với một trang mã độc nào đó và liên tục nhận được hóa đơn hoặc nhắn tin thanh toán, hãy hỏi cơ quan có thẩm quyền (chính quyền hoặc tư vấn luật sư, v.v.) để được hướng dẫn.