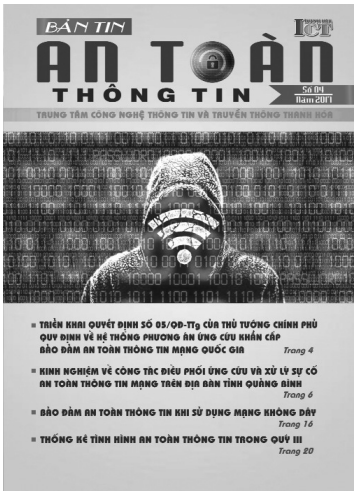
BẢN TIN
AN TOÀN THÔNG TIN
TRUNG TÂM CÔNG NGHỆ THÔNG TIN & TRUYỀN THÔNG THANH HÓA

Số 04
tháng 9/2017



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

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

THIẾT KẾ
Chung Nguyễn

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

In 500 cuốn, khổ 19x27cm
Tại Công ty TNHH In&TBGD Thanh Huệ
In xong và nộp lưu chiểu tháng 9/2017

Đ/c Phan Tâm, Thứ trưởng Bộ TT&TT phát biểu tại Hội nghị.

Triển khai Quyết định số 05/QĐ-TTg của Thủ tướng Chính phủ quy định về Hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng Quốc gia

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

Trong những năm gần đây, Chính phủ Việt Nam cùng các Bộ, ngành và địa phương đang rất nỗ lực xây dựng, hoàn thiện hệ thống văn bản quy phạm pháp luật trong lĩnh vực an toàn thông tin mạng nhằm tạo ra một hành lang pháp lý thuận lợi giúp các người dân, cơ quan quản lý và doanh nghiệp có môi trường sử dụng, kinh doanh và kết nối internet một cách an toàn và hiệu quả nhất. Ngày 16 tháng 03 năm 2017, Thủ tướng Chính phủ đã ký Quyết định số 05/2017/QĐ-TTg (Quyết định 05) ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia, trong đó giao các bộ, ngành, địa phương và các cơ quan, tổ chức liên quan thực hiện các nhiệm vụ để sẵn sàng ứng cứu sự cố, bảo đảm an toàn thông tin mạng Quốc gia.

Để phổ biến Quyết định của Thủ tướng, sáng ngày 18/5/2017 tại Hà Nội, Bộ Thông tin và Truyền thông đã tổ chức Hội nghị phổ biến

Quyết định 05. Tham dự Hội nghị có Thứ trưởng Bộ TT&TT Phan Tâm và các lãnh đạo, cán bộ đảm nhiệm công tác bảo đảm an toàn thông tin mạng của các Bộ, ngành, các Sở TT&TT các tỉnh, thành phố trực thuộc Trung ương.

Phát biểu tại Hội nghị, Thứ trưởng Phan Tâm chia sẻ: Từ năm 2011, Bộ TT&TT đã ban hành Thông tư số 27/2011/TT-BTTTT ngày 4/10/2011, quy định về điều phối các hoạt động ứng cứu sự cố mạng Internet Việt Nam. Sau 6 năm triển khai, đến nay mạng lưới ứng cứu sự cố an toàn mạng với hơn 130 đơn vị thành viên đã hình thành. Đây là một con số khá ấn tượng ngay cả với các bạn bè quốc tế. Tuy nhiên, mạng lưới này chưa thực sự hoạt động hiệu quả.

Thứ trưởng khẳng định: "Trong bối cảnh các cuộc tấn công mạng càng ngày càng tinh vi, phức tạp và có sự tổ chức bài bản và quy mô trên diện rộng, hậu quả ngày càng nặng nề, mạng lưới ứng cứu sự cố cần được xây dựng một cách chuyên nghiệp để có thể phối hợp ngăn chặn và phòng ngừa các nguy cơ tấn công mạng có thể xảy ra bất cứ lúc nào. Quyết định 05/2017/QĐ-TTg được ra đời để nhằm mục đích đó"

Để việc triển khai Quyết định 05/2017/QĐ-TTg đạt hiệu quả cao, ngày 26/7/2017 Bộ Thông tin và Truyền thông ban hành công văn số 2640/BTTTT-VNCERT hướng dẫn và đề nghị các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ và Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương (sau đây gọi tắt là các Bộ, Tỉnh) nghiên cứu nội dung Quyết định 05, chỉ đạo các cơ quan, tổ chức liên quan thực hiện các công việc để triển khai Quyết định này, bao gồm các nội dung cụ thể sau:

1. Kiện toàn và bổ sung chức năng nhiệm vụ cho Ban chỉ đạo ứng dụng công nghệ thông tin thuộc bộ, tỉnh đảm nhiệm chức năng Ban chỉ đạo ứng cứu khẩn cấp sự cố an toàn thông tin mạng trong phạm vi bộ, tỉnh mình, do 1 lãnh đạo bộ hoặc lãnh đạo UBND cấp tỉnh trực tiếp chỉ đạo (căn cứ theo Điều 5 của Quyết định 05); Trong trường hợp chưa có Ban chỉ đạo ứng dụng công nghệ thông tin hoặc điều kiện đặc thù cần thiết, các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân cấp tỉnh xem xét thành lập Ban chỉ đạo ứng cứu khẩn cấp sự cố an toàn thông tin mạng trong phạm vi bộ, tỉnh mình.

2. Giao cơ quan chuyên trách về công nghệ thông tin (hoặc cơ quan chuyên trách về an toàn thông tin nếu có) đảm nhiệm chức năng và nhiệm vụ là Đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng trong phạm vi bộ, tỉnh mình (căn cứ theo Điều 6 của Quyết định 05). Giao Đơn vị chuyên trách ứng cứu sự cố có trình kiện toàn tổ chức hoặc thành lập Đội ứng cứu sự cố và tổ chức hoạt động ứng cứu sự cố trong lĩnh vực, địa bàn, phạm vi mình quản lý.

3. Chỉ đạo các cơ quan, đơn vị trực thuộc là đơn vị có nghĩa vụ phải tham gia làm thành viên mạng lưới ứng cứu sự cố (căn cứ theo Điều 7 của Quyết định 05) điền đầy đủ thông tin vào Bản khai hồ sơ thành viên mạng lưới ứng cứu sự cố để hoàn tất thủ tục đăng ký tham gia mạng lưới và thực hiện các trách nhiệm, quyền hạn của thành viên mạng lưới theo quy định. Thông báo, khuyến khích và tạo điều kiện để các cơ quan, tổ chức, doanh nghiệp trực thuộc (không phải là thành viên bắt buộc) có Đơn đăng ký tham gia mạng lưới ứng cứu sự cố đăng ký tự nguyện tham gia mạng lưới ứng cứu để được chia sẻ thông tin, tham gia hỗ trợ, phối hợp trong điều phối, ứng cứu sự cố, bảo đảm an toàn thông tin mạng.

4. Lập kế hoạch và tổ chức, duy trì hoạt động của Ban chỉ đạo ứng cứu khẩn cấp sự cố an toàn thông tin mạng, Đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng, Đội ứng cứu sự cố; Tham gia hoạt động của Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia;

5. Tổ chức các đợt tập huấn, tuyên truyền, phổ biến, quán triệt thực hiện Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia, Thông tư của Bộ Thông tin và Truyền thông quy định về điều phối ứng cứu sự cố an toàn thông tin mạng, các văn bản pháp luật hướng dẫn triển khai Luật An toàn thông tin mạng và các văn bản pháp luật có liên quan.

6. Căn cứ theo Điều 16, 17 và Phụ lục II của Quyết định 05, các cơ quan, tổ chức xây dựng, trình phê duyệt và triển khai kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng bổ sung

năm 2017, kế hoạch 2018 và các năm tiếp theo, trong đó chú trọng các nội dung:

- Đánh giá tình hình thực hiện công tác phòng, chống, ứng phó sự cố, bảo đảm an toàn thông tin mạng thời gian qua; Đánh giá các nguy cơ, sự cố an toàn thông tin mạng đối với các hệ thống công nghệ thông tin thuộc phạm vi quản lý hoặc có trách nhiệm hỗ trợ ứng cứu sự cố;

- Xác định các nội dung, nhiệm vụ của kế hoạch thời gian tới, trong đó chú trọng: Các hoạt động liên quan thuộc trách nhiệm của cơ quan, đơn vị mình tại các Điều 7, 11, 12, 13, 14, 16 Quyết định 05; Tổ chức nghiên cứu, xây dựng các kịch bản tấn công, các nguy cơ, tình huống sự cố có khả năng xảy ra; Tổ chức xây dựng các phương án ứng cứu, đối phó, ngăn chặn theo kịch bản, tình huống dự kiến; Triển khai các giải pháp giám sát, phát hiện, cảnh báo sớm, kiểm tra, rà quét, đánh giá an toàn thông tin; phòng ngừa, dự phòng rủi ro; Triển khai hoạt động thường trực, điều phối, dự phòng ứng cứu, xử lý sự cố; Tổ chức đào tạo, huấn luyện, diễn tập và hoạt động của Đội ứng cứu sự cố; Xây dựng, phát triển đội ngũ nhân lực ứng cứu sự cố; Hỗ trợ xây dựng, áp dụng tiêu chuẩn và các quy trình, quy chế bảo đảm an toàn thông tin; Triển khai các hoạt động nghiệp vụ đặc thù bảo đảm an toàn thông tin mạng cho các hệ thống thông tin thuộc phạm vi quản lý; và các nội dung liên quan khác;

- Xác định cụ thể các nguồn lực đảm bảo, giải pháp tổ chức thực hiện và kinh phí để triển khai các nội dung của kế hoạch, đảm bảo khả thi, hiệu quả.

Theo đó, Ngày 04/4/2017, UBND tỉnh ban hành Công văn số 3479/UBND-CNTT về việc phổ biến, triển khai thực hiện Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ. Theo đó, UBND tỉnh giao Sở Thông tin và Truyền thông chủ trì phối hợp với các đơn vị có liên quan, nghiên cứu nội dung Quyết định số 05/2017/QĐ-TTg nêu trên của Thủ tướng để phổ biến, triển khai thực hiện trên địa bàn tỉnh; tham mưu, báo cáo Chủ tịch UBND tỉnh những vấn đề vượt thẩm quyền.

Kinh nghiệm về công tác điều phối ứng cứu và xử lý sự cố an toàn thông tin mạng trên địa bàn tỉnh Quảng Bình

NGUYỄN VĨNH HUẾ
Giám đốc Trung tâm CNTT&TT Quảng Bình

An toàn thông tin mạng (ATTT) là vấn đề ngày càng được xã hội, các tổ chức, cá nhân quan tâm bởi tầm quan trọng và tác động của nó đối với tất cả các lĩnh vực trong đời sống như: an ninh quốc phòng, kinh tế, chính trị, giáo dục... Bên cạnh việc xây dựng chính quyền ứng dụng công nghệ thông tin hiện đại, đáp ứng nhu cầu của người dân và doanh nghiệp thì việc đảm bảo cho hệ thống thông tin hoạt động ổn định và tin cậy, tránh bị phá hoại trái phép cũng quan trọng không kém.

Trong thời gian qua, nhận thức được vai trò quan trọng và cấp thiết của việc đảm bảo An toàn thông tin, UBND Quảng Bình đã ban hành nhiều văn bản quan trọng nhằm chỉ đạo đơn vị chuyên trách và các sở, ban, ngành, địa phương và doanh nghiệp trên địa bàn tỉnh. Đặc biệt, trong quý III/2016, UBND tỉnh đã ban hành Quyết định số 2654/QĐ-UBND, ngày 30/8/2016 quyết định thành lập Tổ ứng cứu sự cố máy tính của tỉnh. Tổ gồm 42 thành viên, trong đó Tổ trưởng là đồng chí Nguyễn Phi Khanh, Phó Giám đốc Sở Thông tin và Truyền thông Quảng Bình cùng các cán bộ quản trị mạng, phụ trách CNTT các Sở, ban, ngành, địa phương và doanh nghiệp. Quyết định của UBND tỉnh quy định rõ trách nhiệm của

Lễ ký kết thỏa thuận hợp tác về các hoạt động điều phối ứng cứu sự cố mạng máy tính trên địa bàn tỉnh Quảng Bình.

Tổ ứng cứu sự cố máy tính, cơ quan thường trực và các cơ quan, đơn vị liên quan. Trong đó, Tổ ứng cứu sự cố máy tính có nhiệm vụ chủ yếu là: Hỗ trợ các cơ quan đảng, đoàn thể chính trị - xã hội; các sở, ban ngành cấp tỉnh, các cơ quan trực thuộc Ủy ban nhân dân tỉnh; các cơ quan Trung ương đóng trên địa bàn tỉnh trong công tác đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin (CNTT) và tổ chức ứng cứu các sự cố máy tính, mạng máy tính, mạng Internet trên địa bàn tỉnh.

Trước khi thành lập Tổ, tình hình xử lý sự cố ATTT ở Quảng Bình gặp một số khó khăn nhất định, đặc biệt là sự không đồng bộ, chưa có tính kết nối giữa Sở Thông tin và Truyền thông - đơn vị chuyên trách về Công nghệ thông tin của tỉnh - và đầu mối quản trị mạng, phụ trách CNTT các sở, ban, ngành, địa phương và doanh nghiệp. Điều này gây khó khăn trong việc điều phối xử lý sự cố ATTT, chưa huy động được nguồn lực về nhân sự, tài chính của các doanh nghiệp CNTT và viễn thông trên địa bàn (VNPT, Viettel, Mobifone...) để cùng phối hợp xử lý sự cố.

Đặc biệt, trong các năm 2015, 2016, tình hình ATTT trong nước và quốc tế diễn biến phức tạp, trong tình hình đó, Lãnh đạo Sở Thông tin và Truyền thông đã có nhiều hoạt động như: Thành lập Phòng Ứng cứu sự cố máy tính, trực thuộc Trung tâm CNTT&TT Quảng Bình, có nhiệm vụ tiếp nhận, xử lý các sự cố máy tính tại các cơ quan, đơn vị trên địa bàn; Ký cam kết Thỏa thuận "Phối hợp công tác đảm bảo an toàn thông tin trên địa bàn tỉnh Quảng Bình giai đoạn 2016 - 2020" giữa Cục An toàn thông tin và Sở Thông tin và Truyền thông Quảng Bình vào ngày 29/7/2016; Phân công nhiệm vụ Xây dựng chuyên trang An toàn thông tin trên website Sở tại địa chỉ: stttt.quangbinh.gov.vn; Tăng cường các biện pháp an ninh tại Trung tâm dữ liệu điện tử của tỉnh (đặt tại Sở Thông tin và Truyền thông - STTTT); Khẩn trương ban hành các văn bản cảnh báo, hướng dẫn xử lý sự cố ATTT cho các Sở, ban, ngành, địa phương và doanh nghiệp trên địa bàn tỉnh... Chính nhờ các hoạt động kịp thời đó đã phần nào giảm bớt được các thiệt hại liên quan đến các sự cố về ATTT.

Sau khi Tổ ƯCSCMT được thành lập, các thành viên của Tổ đã tích cực kết nối, rà quét và ứng cứu xử lí nhiều trường hợp mất ATTT diễn ra trên địa bàn tỉnh: Xử lý mã hóa dữ liệu (Ransomware) tại máy chủ Sở Tài chính, Sở Giao thông Vận Tải, Sở Tài Nguyên và Môi trường, Trường Đại học Quảng Bình,...; Rà quét phát hiện và cảnh báo các website đang tồn tại các lỗ hổng bảo mật như Thư viện tỉnh Quảng Bình, các đơn vị trường học trên địa bàn tỉnh...; tìm và diệt các mã độc các webiste đang được lưu trữ tại máy chủ hosting trên địa bàn, ...; cảnh báo địa chỉ IP nhiễm mã độc tham gia mạng botnet cho các trường học, trung tâm ngoại ngữ của tỉnh và hỗ trợ ứng cứu sự cố cho một số cá nhân, đơn vị và doanh nghiệp khác.

Bộ phận chuyên trách của Tổ ƯCSCMT đã chủ trì xây dựng các quy trình ứng cứu và xử lý các sự cố máy tính có thể xảy ra đối với các hệ thống phần mềm dùng chung: quy trình xử lý sự cố hệ thống mạng, quy trình xử lý mã độc, bóc gỡ Botnet, quy trình xử lý sự cố website, email, hệ thống QLVB&ĐH,... Chuyên mục ATTT luôn cập nhật thông tin mới nhất về cảnh báo, hướng dẫn an toàn thông tin, phục vụ Lãnh đạo, cán bộ, người dân và doanh nghiệp trong toàn tỉnh. Chuyên mục cung cấp đầy đủ các nội dung về: quy trình Ứng cứu sự cố, cảnh báo An toàn thông tin, hướng dẫn An toàn thông tin, thủ thuật Công nghệ thông tin, văn bản pháp quy An toàn thông tin của Trung ương và địa phương...

Đ/c Giám đốc Trung tâm CNTT&TT Quảng Bình khai mạc Hội nghị tập huấn khai thác sử dụng phần mềm một cửa liên thông cho các cơ quan trên địa bàn tỉnh.

Nhận thức được ATTT là lĩnh vực khá mới mẻ, đòi hỏi phải có nhân lực trình độ cao về CNTT, Lãnh đạo Sở TTTT, Tổ ƯCSCMT thường xuyên quan tâm, cử cán bộ học tập, tập huấn về ATTT tại địa phương và các tỉnh thành khác. Thành viên của Tổ đã tham gia nhiều khóa học tại TP. Đà Nẵng như: khóa "Đào tạo ngắn hạn về An toàn thông tin năm 2016" của Bộ Thông tin và Truyền thông tổ chức, khóa đào tạo "Đảm bảo kỹ thuật An toàn thông tin" do Trung tâm ứng cứu khẩn cấp máy tính Việt Nam tổ chức; tập huấn "Triển khai IPV6 dành cho cơ quan Đảng, Nhà nước" do Trung tâm Internet Việt Nam (VNNIC) tổ chức cùng nhiều khóa đào tạo diễn ra tại Quảng Bình như: tập huấn "Kỹ năng về hoạt động điều phối ứng cứu sự cố máy tính" do Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam tổ chức; tập huấn "An toàn, an ninh mạng cho cán bộ chuyên trách Công nghệ thông tin" do các chuyên gia về mạng của Sở Thông tin và Truyền thông Quảng Bình phối hợp với Sở Thông tin và Truyền thông Đà Nẵng tổ chức... Cán bộ chuyên trách CNTT của Sở là thành viên của Tổ đã tổ chức các buổi diễn tập về ứng cứu sự cố máy tính cho các thành viên trong Tổ. Ngoài ra, Tổ ƯCSCMT cũng đã tham mưu ban hành các văn bảnvề nâng cao nhận thức và trách nhiệm về ATTT, thường xuyên trao đổi, học tập kinh nghiệm về xử lý sự cố ATTT từ các chuyên gia, các đơn vị ở trong và ngoài tỉnh.

Một trong những ghi nhận nổi bật thời gian qua, là nhờ có những điều phối, cảnh báo và hướng dẫn kịp thời từ các thành viên Tổ ƯCSCMT mà trên địa bàn tỉnh không ghi nhận các trường hợp lây nhiễm mã độc WannaCry, mã độc tống

tiền Ransomwave, biến thể mới của mã độc Ransomwave (mã độc Petya).

Để công tác đảm bảo ATTT đạt nhiều kết quả hơn nữa, trong thời gian tới Tổ ƯCSCMT sẽ tiếp tục phối hợp chặt chẽ với Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VNCERT), Cục An toàn thông tin - Bộ TTTT, Trung tâm an ninh mạng BKAV và các doanh nghiệp an ninh mạng trong toàn quốc tiến hành tiếp nhận, trao đổi thông tin và cùng phối hợp xử lý sự cố ATTT trên địa bàn tỉnh. Trước mắt, Tổ sẽ tiến hành phối hợp với Trung tâm ứng cứu khẩn cấp máy tính Việt Nam - Chi nhánh Đà Nẵng tập huấn ATTT cho các thành viên Tổ ứng cứu sự cố máy tính; tiếp tục tuyên truyền cho người dân, doanh nghiệp và cán bộ trong tỉnh nhận thức được vai trò quan trọng của ATTT thông qua website của Sở Thông tin và Truyền thông và chuyên mục ATTT phát trên Đài Phát thanh Truyền hình Quảng Bình...

Việc đảm bảo ATTT trong giai đoạn mới vô cùng phức tạp và nặng nề, chính vì vậy các thành viên của Tổ ƯCSCMT luôn quyết tâm và xác định được vai trò, trách nhiệm của mỗi cá nhân, cùng phối hợp chặt chẽ nhằm xây dựng chính quyền ứng dụng công nghệ thông tin hiện đại, ổn định và an toàn.

Ban hành Quy chế đảm bảo An toàn thông tin mạng trong hoạt động ứng dụng CNTT của các cơ quan quản lý nhà nước tỉnh Thanh Hóa

LƯƠNG THANH NGỌC
Phòng Quản lý CNTT, Sở TT&TT

Ngày 25/4/2017, UBND tỉnh Thanh Hóa đã ban hành Quy chế đảm bảo An toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin (CNTT) của các cơ quan quản lý nhà nước tỉnh tại Quyết định số 1293/2017/QĐ-UBND.

Đối tượng áp dụng của Quy chế là các sở, ban, ngành cấp tỉnh, các đơn vị sự nghiệp công lập trực thuộc UBND tỉnh; UBND các huyện, thị xã, thành phố, UBND xã, phường, thị trấn; các cán bộ, công chức, viên chức, người lao động và những tổ chức, cá nhân có liên quan tham gia vận hành, khai thác các hệ thống thông tin tại các cơ quan quản lý nhà nước; các doanh nghiệp cung cấp dịch vụ viễn thông, CNTT, Internet, các doanh nghiệp, tổ chức, cá nhân có tham gia vào các hoạt động ứng dụng CNTT của các cơ quan quản lý nhà nước. Quy chế cũng khuyến khích các cơ quan, đơn vị khác có hoạt động ứng dụng và phát triển CNTT trên địa bàn tỉnh áp dụng.

Quy chế quy định các nội dung về bảo vệ thông tin cá nhân, bảo vệ hệ thống thông tin, giám sát an toàn hệ thống thông tin và ngăn chặn xung đột thông tin trên mạng nhằm tuân thủ các quy định của Luật An toàn thông tin mạng và các văn bản pháp luật có liên quan để giúp các cơ quan quản lý nhà nước giảm thiểu tối đa các nguy cơ gây mất an toàn thông tin mạng trong hoạt động ứng dụng CNTT.

Một số quy định mới của Luật An toàn thông tin mạng và các văn bản pháp luật có liên quan được UBND tỉnh Thanh Hóa cập nhật, bổ sung quy định cụ thể tại Quy chế này như:

- Bảo vệ thông tin cá nhân, Quy chế quy định: Cán bộ, công chức có trách nhiệm tự bảo vệ thông tin cá nhân của mình và tuân thủ các quy định tại khoản 1, khoản 2 Điều 10; khoản 1, khoản 4 Điều 16; khoản 3 Điều 17; khoản 1 Điều 18 Luật An toàn thông tin mạng; cán bộ, công chức khi sử dụng, khai thác các hệ thống thông tin của cơ quan, đơn vị và các phần mềm ứng dụng dùng chung của tỉnh phải có trách nhiệm: Tự quản lý và tự chịu trách nhiệm về bảo vệ thông tin cá nhân đã được khai báo trong các hệ thống thông tin; không tiết lộ tài khoản đăng nhập, đấu nối, truy cập trái phép vào các phần mềm dùng chung của tỉnh; Ngay sau

Triển khai các hoạt động đảm bảo ATTT mạng hằng năm của Sở Thông tin và Truyền thông Thanh Hóa.

khi được cấp tài khoản truy cập vào các phần mềm dùng chung của tỉnh, cơ quan, đơn vị, cá nhân được cấp tài khoản phải thực hiện việc đổi mật khẩu; Khi khai thác, sử dụng các phần mềm dùng chung của tỉnh tại các điểm truy cập Internet công cộng, tuyệt đối không đặt chế độ lưu trữ mật khẩu trong quá trình sử dụng;...

- Bảo vệ hệ thống thông tin, quy chế quy định: các cơ quan, đơn vị thực hiện việc phân loại thông tin, phân loại cấp độ an toàn cho hệ thống thông tin thuộc quyền quản lý theo thuộc tính bí mật để có biện pháp bảo vệ phù hợp. Cụ thể: việc phân loại thông tin được thực hiện theo các quy định tại Điều 9 Luật An toàn thông tin mạng và khoản 1, Điều 6 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ; việc quản lý gửi thông tin trên mạng phải tuân thủ theo các nội dung quy định tại Điều 10 Luật An toàn thông tin mạng;...

- Giám sát an toàn hệ thống thông tin và ngăn chặn xung đột thông tin trên mạng cũng được Quy chế quy định cụ thể như: cơ quan, đơn vị phải thực hiện việc lưu trữ nhật ký tình trạng hoạt động của các hệ thống thông tin tại các máy chủ trong thời gian ít nhất là 30 ngày để phục vụ các công tác đảm bảo an toàn thông tin mạng; quản lý chặt chẽ các tài khoản đã cung cấp cho người dùng từng cơ quan, đơn vị; cán bộ, công chức của các cơ quan, đơn vị có trách nhiệm ngăn chặn xung đột thông tin trên mạng theo các nội dung quy định tại khoản 1 Điều 28 Luật An toàn thông tin mạng; khoản 1 Điều 7; các khoản 4, 5 Điều 12 và Điều 27 Nghị đinh số 142/2016/NĐ-CP ngày 14/10/2016 của Chính phủ;...

Đồng thời, Quy chế cũng quy định trách nhiệm của các cơ quan, đơn vị, cán bộ, công chức, viên chức và người lao động; các doanh nghiệp cung cấp dịch vụ viễn thông, CNTT, Internet, các doanh nghiệp, tổ chức, cá nhân có tham gia vào các hoạt động ứng dụng CNTT của các cơ quan quản lý nhà nước trong việc đảm bảo an toàn thông tin mạng.

UBND tỉnh Thanh Hóa giao Sở TT&TT chủ trì, phối hợp với các đơn vị có liên quan thành lập đoàn kiểm tra liên ngành và tổ chức kiểm tra, giám sát việc thực hiện đảm bảo an toàn thông tin mạng tại các cơ quan quản lý hành chính nhà nước của tỉnh, tại các doanh nghiệp cung cấp dịch vụ viễn thông, CNTT, Internet trên địa bàn tỉnh để kịp thời phát hiện, xử lý các hành vi vi phạm an toàn thông tin mạng.

BÙNG PHÁT MÃ ĐỘC TỐNG TIỀN VÀ DỰ ÁN "NO MORE RANSOMWARE"

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

Trong thời gian gần đây, một số loại mã độc tống tiền với hình thức lây nhiễm mới, có nhiều tính năng mới và nguy hiểm đã bị phát hiện. Theo các chuyên gia, đây là những biến thể mới, bước phát triển mới của mã độc tống tiền (Ransomware) đã gia tăng chóng mặt và trở thành một trong những mối đe dọa phổ biến trên Internet.

Dự báo về tình hình an ninh mạng trong thời gian tới, đặc biệt là vào cuối năm 2017, chuyên gia đến từ Công ty An ninh mạng BKAV cho rằng: mã độc mã hóa tống tiền sẽ diễn biến rất phức tạp với nhiều hành vi và thủ đoạn mới nhằm tăng khả năng lây nhiễm.

Bùng phát các phương thức lây nhiễm mã độc:

- Thông qua các Email độc hại

Email được xem như là phương thức tấn công truyền thống. Ngày nay, rất khó để có thể nhận biết được các email giả mạo mà tin tặc tạo ra, đặc biệt là nội dung trong email được đầu tư và nghiên cứu rất kỹ liên quan đến người nhận. Mục đích để người nhận được thư sẽ thực hiện theo mong muốn của tin tặc. Bên cạnh đó, các kỹ thuật giấu file chứa mã độc vào trong các file đính kèm ngày càng khó phát hiện, đặc biệt là với người dùng bình thường.

- Các trang web độc hại

Một cách phổ biến khác khiến người dùng bị lây nhiễm là thông qua các trang web bị tin tặc chiếm quyền điều khiển, kể các các trang web hợp pháp đã bị tiêm nhiễm các bộ công cụ khai thác người dùng như các plug-in trên trình duyệt như Java, Flash Player, Adobe Reader và Silverlight. Khi truy cập vào các trang web này thì tự động sẽ tải về các tập tin chứa mã độc về máy tính của người dùng mà không hề hay biết.

Bên cạnh đó, hiện nay còn ghi nhận các kỹ thuật tấn công ngày càng tinh vi và liên tục đổi mới của tin tặc bởi vì:

- Mã độc đã trở thành nghành công nghiệp với lợi nhuận lớn, chính vì thế mã độc dưới dạng dịch vụ (MaaS-Malware as a Service) khiến cho việc khởi động một cuộc tấn công trở nên đơn giản hơn, dễ dàng thành công ngay cả đối với các tội phạm mạng ít hiểu biết về công nghệ.

- Kỹ thuật lừa đảo (Socical Engineering) được sử dụng để lừa đảo dẫn dụ người dùng trong việc chạy các file, liên kết có chứa mã độc.

- Tin tặc hoạt động ngày càng theo một phương thức chuyên nghiệp, từ khi xác định đối tượng tấn công, đến cách thức tấn công và ẩn danh sau khi đã hoàn thành mục đích.

- Khai thác triệt để các lỗ hổng, điểm yếu bảo mật trong các cơ quan, cá nhân

- Thiếu công nghệ phòng chống tiên tiến: Các giải pháp bảo mật cần phải được thiết kế để chống lại các kỹ thuật Ransomware hiện nay.

Minh chứng cho sự bùng phát của mã độc tống tiền là sự xuất hiện của WannaCry vào ngày 12/5/2017. Đây là một biến thể của mã độc tống tiền và có tên gọi khác là WanaCrypt0r 2.0 hay Wcry. Chỉ sau 02 ngày xuất hiện, mã độc này đã gây ảnh hưởng đến 10.000 tổ chức, 200.000 cá

nhân trong khoảng 150 quốc gia trên thế giới. Tất cả các máy tính là nạn nhân đều bị WannaCry mã hóa dữ liệu và ra yêu cầu đòi tiền chuộc khoảng 300 USD. Số tiền này sẽ tăng gấp đôi nếu thời hạn quá 03 ngày và sẽ bị xóa mãi mãi nếu người dùng không trả tiền cho hacker thông qua hệ thống thanh toán bằng đồng tiền bitcoin. Tại Việt Nam theo thống kê từ hệ thống giám sát virus của BKAV, đã có hơn 1900 máy tính bị lây nhiễm mã độc tống tiền này, trong đó có khoảng 1.600 máy tính được ghi nhận ở 243 cơ quan, doanh nghiệp và khoảng 300 máy tính là người dùng cá nhân

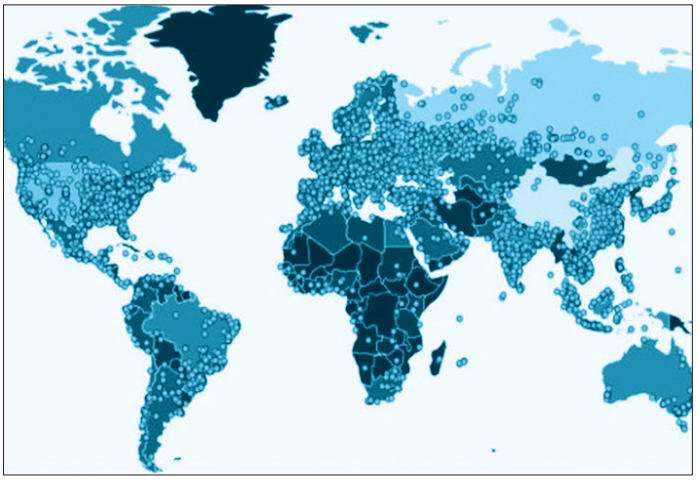
Cuộc tấn công của mã độc tống tiền WannaCry được xem là cuộc tấn công mạng lớn nhất từ trước đến nay và gây hậu quả nặng nề cho các tổ chức, doanh nghiệp và cá nhân trên toàn thế giới. Khi được cài đặt vào máy tính WannaCry sẽ tìm thấy các tập tin trong ổ cứng và mã hóa chúng và để lại cho chủ sở hữu một thông báo trả tiền chuộc nếu muốn giải mã dữ liệu.

Điểm đặc biệt làm cho WannaCry cực kỳ nguy hiểm là mã độc đã khai thác lỗ hổng MS17-010 có trên tất cả các Hệ Điều Hành Windows có sử dụng giao thức chia sẻ file SMBv1 để tự lây nhiễm. Lỗi bảo mật nghiêm trọng này chỉ mới được Microsoft phát hành các bản vá lỗi vào ngày 14/3/2017 và có rất nhiều máy tính còn chưa kịp thực hiện update. Từ công cụ khai thác lỗi MS17-010 đầu tiên là EternalBlue xuất hiện vào tháng 4/2017, đến nay đã có nhiều phiên bản mã khai thác được giới Hackers tinh chỉnh và sử dụng. Các mã khai thác lỗi này còn được tích hợp trong các bộ công cụ kiểm thử thông dụng như Metasploit, Empire.

Với mỗi nạn nhân bị lây nhiễm, WannaCry sẽ khởi tạo một cặp khoá RSA-2048. Mỗi tập tin được mã hoá bằng khóa ngẫu nhiên AES-128. Khóa private của mỗi nạn nhân mã hóa bởi public key của tin tặc. Sau đó, mã độc WannaCry sẽ tiến hành mã hóa và xóa bỏ tất cả các file tạm, thực thi phần tống tiền với phần mềm Tor và Bitcoin Wallet để nhận tiền chuộc dữ liệu mà không bị truy vết.

Khi các vụ tấn công mã độc tống tiền WannaCry chưa kết thúc, vào cuối tháng 6 vừa qua, mã độc mới xuất hiện Petya với mức độ còn nguy hiểm hơn WannaCry do hình thức mã hóa toàn bộ ổ cứng và có khả năng lây nhiễm rộng hơn trong mạng nội bộ. Petya đã làm tê liệt hàng loạt ngân hàng, sân bay, máy ATM và một số doanh nghiệp lớn tại Châu Âu.

Mã độc WannaCry đã khởi đầu cho một kỷ nguyên mới của các biến thể mã độc tống tiền tự phát thông qua lỗ hổng hệ thống. Petya tiếp nối khả năng đó bằng cách thêm vào các phương thức khác để vượt qua cơ chế kiểm soát đã được vá. Điều này làm dấy lên những lo ngại về các biến thể khác sử dụng các cơ chế tấn công tương tự nhưng phức tạp hơn trong tương lai gần.



Bản đồ thống kê các quốc gia trên thế giới bị lây nhiễm mã độc WannaCry.

Trước 02 đợt tấn công mã độc nói trên, Bộ Thông tin và Truyền thông đã kịp thời hướng dẫn các cơ quan, đơn vị, cá nhân các biện pháp phòng ngừa lây lan mã độc nói chung như sau:

+ Đối với cá nhân:

- Thực hiện cập nhật ngay các phiên bản hệ điều hành Windows đang sử dụng. Riêng đối với các máy tính sử dụng Windows XP sử dụng bản cập nhật mới nhất dành cho lỗ hổng này tại địa chỉ được cung cấp trên trang web của Microsoft.

- Cập nhật ngay các chương trình Antivirus đang sử dụng. Đối với các máy tính không có phần mềm Antivirus cần tiến hành cài đặt và sử dụng một phần mềm Antivirus có khả năng cập nhật.

- Cẩn trọng khi nhận được email có đính kèm đường link lạ được gửi trong email, trên các mạng xã hội, công cụ chat online,...

- Cần thận trọng khi mở các file đính kèm ngay cả khi nhận được từ những địa chỉ email quen thuộc. Sử dụng các công cụ kiểm tra phần mềm độc hại trực tuyến hoặc trên phần mềm diệt Virus có bản quyền trên máy tính với các file này trước khi mở ra.

- Không mở các đường dẫn có cấu trúc không rõ ràng, các đường dẫn link được rút gọn.

- Thực hiện các biện pháp sao lưu dữ liệu quan trọng ra thiết bị độc lập với máy tính hoặc sao lưu trực tuyến trên môi trường mạng.

+ Đối với các cơ quan, tổ chức:

- Theo dõi ngăn chặn kết nối đến các máy chủ điều khiển mã độc WannaCry để xác định được các máy tính bị nhiễm trong mạng để có biện pháp xử lý kịp thời; có giải pháp đảm bảo an toàn thông tin đang có sẵn trong tổ chức và cập nhật vào các hệ thống bảo vệ như IDS/IPS; Firewall,...

- Khẩn trương cập nhật bản vá, phiên bản mới nhất cho hệ điều hành máy chủ, máy trạm theo hướng dẫn của cơ quan chuyên môn

- Cập nhật phần mềm chống mã độc (Kapersky, Symantec, Avast, AVG, MSE, Bkav, CMC,...) cũng như thường xuyên quét Virus, mã độc, kiểm tra máy tính, ổ đĩa lưu trữ dữ liệu để phát hiện sớm mã độc xuất hiện trên thiết bị, máy tính...

- Thực hiện biện pháp lưu trữ dữ liệu quan trọng ngay.

- Cảnh báo tới người dùng trong tổ chức và thực hiện các biện pháp như nêu trên đối với người dùng...

Dự án "No More Ransom"

Sáng kiến "No More Ransom" tạm dịch là "không phải trả tiền chuộc" là Cổng thông tin trực tuyến nhằm mục đích thông báo cho cộng đồng về sự nguy hiểm của mã độc tống tiền và giúp đỡ nạn nhân cách thức để phục hồi lại dữ liệu mà không phải trả lại tiền chuộc cho tội phạm mạng. Đây là dự án được ra mắt lần đầu vào ngày 25/7/2016, mở đầu một cấp độ hợp tác mới giữa cơ quan hành pháp - cảnh sát quốc gia Hà Lan, Europol và khu vực tư nhân là các công ty an ninh mạng như Intel Security và Kapersky trong việc cùng nhau chống lại sự bùng nổ của mã độc tống tiền.

Dự án không chỉ cung cấp thông tin và các công cụ giải mã miễn phí mà còn cho phép các nạn nhân tải lên một tập tin bị mã hóa để qua đó xác định biến thể mã độc đã mã hóa dữ liệu tại địa chỉ của dự án là: www.nomoransom.org. Thông qua dự án này người dùng được cung cấp thêm các thông tin hữu ích liên quan đến Ransomware và cách thức để tự bảo vệ mình. Hiện tại, dự án đã hỗ trợ 27 ngôn ngữ và cung cấp tổng cộng 84 công cụ giải mã miễn phí.

Giao diện trang chủ của dự án.

Đến thời điểm hiện tại, dự án đã ghi nhận sự tham gia của nhiều đối tác mới như AVAST, CERT Polska và Eleven Paths... nâng tổng số đối tác liên kết là 07 thành viên và đối tác hỗ trợ tham gia chương trình hiện có thêm 30 thành viên mới, nâng tổng số thành viên lên mức 70. Chỉ sau hơn 02 tháng ra mắt, hơn 2.500 người dùng đã có thể giải mã được dữ liệu của mình mà không phải trả tiền cho tội phạm mạng bằng cách sử dụng các công cụ giải mã được cung cấp trên trang web của dự án.

Hiện dự án vẫn liên tục kêu gọi nâng cao nhận thức của người sử dụng cũng như sự ủng hộ của cộng đồng mạng để có thể hoàn thành tiêu chí đúng như tên gọi "No More Ransom" của mình.

Công cụ kiểm tra an toàn thông tin hệ thống của Microsoft

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

Trong thời gian qua, ghi nhận việc lây lan mạnh của các mã độc như WannaCry/ Petya... đối với các máy tính của người dùng xuất phát từ nguyên nhân chính từ cách thức khai thác và lây nhiễm của tin tặc hướng tới các lỗ hổng bảo mật chưa được người dùng cập nhật và khắc phục. Bên cạnh các nguy cơ khác như người dùng không sử dụng mật khẩu khi đăng nhập, không thực hiện cập nhật các bản vá bảo mật mới nhất cho Hệ điều hành và các phần mềm của Microsoft... Để giúp cho người dùng, đặc biệt là cán bộ phụ trách Công nghệ thông tin của các cơ quan, đơn vị dễ dàng kiểm soát các điểm yếu trên. Hãng công nghệ Microsoft đã cung cấp phiên bản miễn phí giúp rà quét và kiểm tra an toàn thông tin trên hệ điều hành Windows có tên là **Microsoft Baseline Security Analyzer (MBSA).**

1. Thông tin về công cụ

MBSA là công cụ kiểm tra "độ an toàn" cho các sản phẩm Microsoft theo khuyến nghị của Microsoft, được cung cấp miễn phí, thiết kế dành riêng cho các chuyên gia công nghệ thông tin và các doanh nghiệp vừa và nhỏ.

Các mục chính được MBSA kiểm tra:

- Các điểm yếu bảo mật của Windows: Tính năng tự động cập nhật, tính năng tự động đăng nhập, mật khẩu,...
- Các điểm yếu bảo mật của IIS (máy chủ web, nếu có)
- Các điểm yếu bảo mật của SQL (máy chủ CSDL, nếu có)
- Các cập nhật bảo mật của Windows, IS, Office,...

MBSA cho phép người quản trị có thể xác định được các lỗ hổng hoặc điểm yếu tồn tại trên một hoặc một nhóm các máy tính. MBSA thực hiện quét trên các máy tính được chọn và tạo ra bản báo cáo chi tiết cho từng máy tính về mức độ an toàn đã được thực hiện và đưa ra các gợi ý để khắc phục các điểm yếu tồn tại.

MBSA có thể kiểm tra các sai sót trong việc cấu hình có thể dẫn đến các vấn đề về mất an toàn trong hệ điều hành như cấu hình các dịch vụ: công cụ Microsoft Baseline Security Analyzer. Microsoft SQL Server, MSDE và IIS. Hiện tại phiên bản phát hành mới nhất của công cụ này là Microsoft Baseline Security Analyzer 2.3 được đăng tải trên website link của Microsoft.

2. Cài đặt Microsoft Baseline Security Analyzer

Yêu cầu chung

- Hệ điều hành: với WindowsServer, từ phiên bản WindowsServer™ 2003 trở lên, với Windows, từ phiên bản Windows 2000 Service Pack 3 trở lên.
- Trình duyệt: Internet Explorer5.01 hoặc mới hơn.
- Các dịch vụ cần được kích hoạt:

Đối với máy cài đặt MBSA: Workstation service, Server service;

Đối với máy thực hiện quét cục bộ: Workstation service, Client for Microsoft Networks

Đối với máy thực hiện quét từ xa: Server service, Remote Registry service, File and Print Sharing.

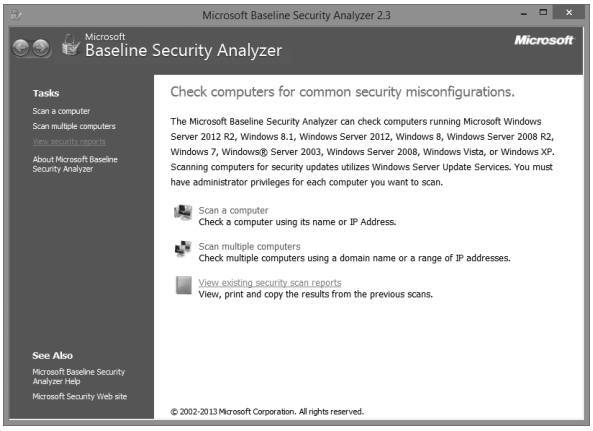
Ngoài ra, cần sử dụng quyền quản trị trên hệ thống mạng để thực hiện việc quét kiểm tra an ninh của hệ thống máy tính hoặc mạng máy tính dùng HĐH Windows.

3. Sử dụng Microsoft Baseline Security Analyzer

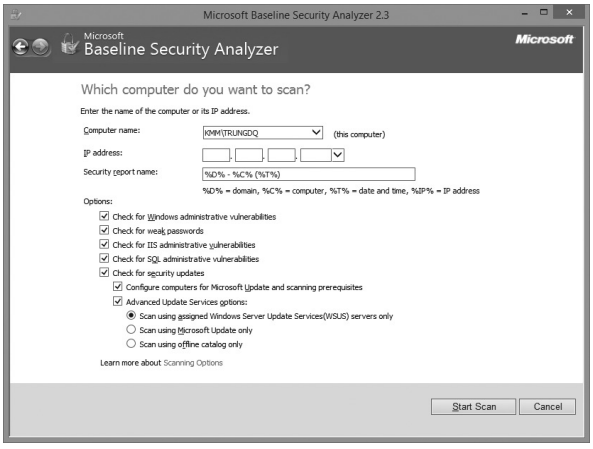
Thực hiện quét kiểm tra an ninh hệ thống

- Kích hoạt chương trình Microsoft Baseline Sercurity Analyzer, giao diện của MBSA rất đơn giản và thân thiện. Ở màn hình giao diện chính của chương trình công cụ MBSA cung cấp 3 tính năng cho người dùng: quét 1 máy tính (scan a

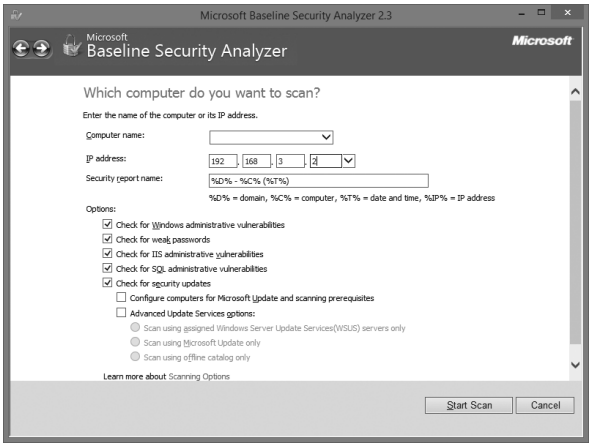
computer), quét nhiều máy tính (scan multiple computers) và xem báo cáo kết quả quét bảo mật (view existing security scan reports).



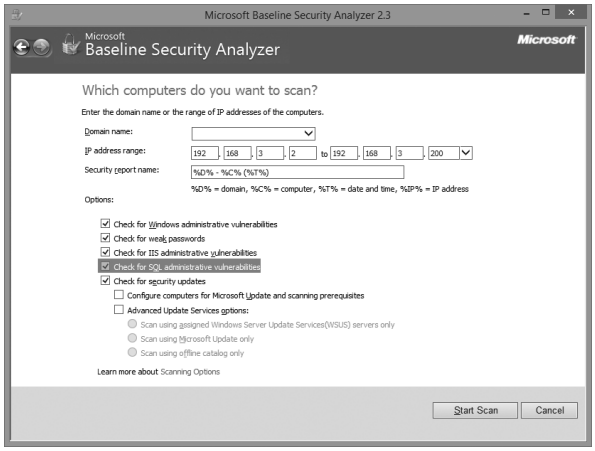
- Thực hiện quét máy tính cục bộ bằng việc chọn chức năng *Scan a computer,* nhập địa chỉ IP của máy cần quét vào mục *IP Address* rồi chọn các mục cần quét trong phần các tùy chọn quét và nhấn nút *Start Scan* để bắt đầu quét



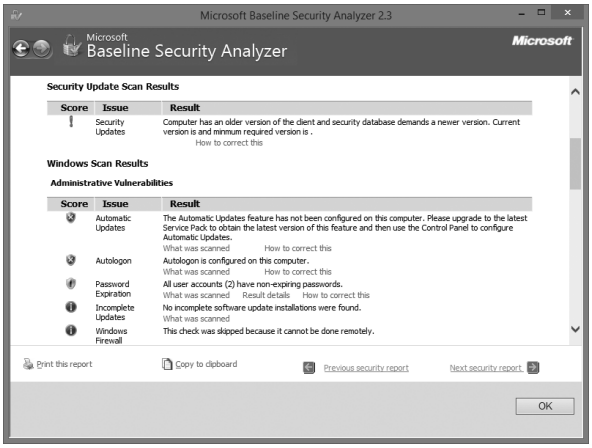
- Thực hiện quét một máy tính ở xa bằng cách chọn chức năng *Scan a computer* rồi chọn các mục cần quét trong phần các tùy chọn quét và nhấn nút *Start Scan* để bắt đầu quét



- Thực hiện quét một nhóm các máy tính trong mạng bằng việc chọn chức năng *Scan multiple computers,* nhập tên miền vào mục *Domain name* hoặc nhập dải địa chỉ IP của các máy cần quét vào mục *IP Address range* rồi chọn các mục cần quét trong phần các tùy chọn quét và nhấn nút *Start scan* để bắt đầu quét



- Quá trình quét và phân tích sẽ tùy thuộc vào các tùy chọn quét được chọn và số lượng máy cần quét. Khi hoàn tất MBSA sẽ cung cấp một bảng đầy đủ các lỗi phát hiện được trong từng mục đồng thời cung cấp đường dẫn đến các cách thực hiện sửa lỗi.



- MBSA phân chia các mức độ rủi ro an toàn khác nhau:

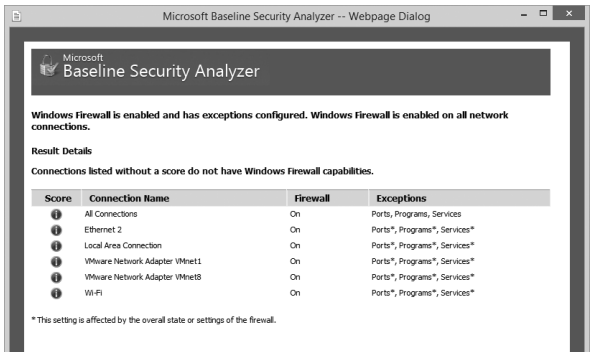
Biểu tượng	*Ý nghĩa*
	Mục nguy hiểm cần sửa ngay lập tức
	Cảnh báo nguy hiểm

Mục được quét là an toàn

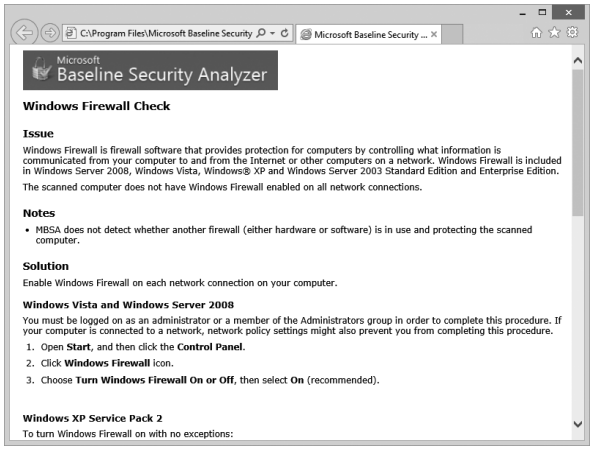
Cần cập nhật mới

Cảnh báo: Chương trình không thể cập nhật CSDL quét an toàn

- Nhấn vào mục *Result details* để xem chi tiết kết quả quét



- Nhấn vào mục *How to correct this* để chuyển đến tài liệu hướng dẫn cách sửa lỗi



Ngoài chế độ làm việc với giao diện đồ họa, MBSA còn có chế độ làm việc dòng lệnh: chạy chương trình mbsacli.exe trong thư mục C:\Program Files\Microsoft Baseline Security Analyzer 2. Chế độ dòng lệnh có nhiều tùy chọn linh hoạt hơn chế độ đồ họa (như cho phép đưa vào tham số "username" và "password"), chạy mbsacli.exe /? để xem các tùy chọn.

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 mất an toàn thông tin cần nhanh chóng thông tin về Tổ Ứng cứu sự cố mạng máy tính của Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa 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

BẢO ĐẢM AN TOÀN THÔNG TIN KHI SỬ DỤNG MẠNG KHÔNG DÂY

Mạng không dây - Wireless LAN (WLAN) là mô hình mạng được sử dụng cho một khu vực có

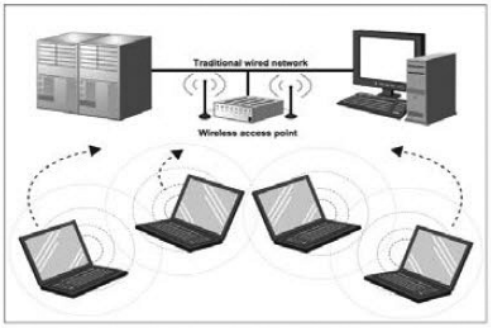
phạm vi nhỏ như một tòa nhà, khuôn viên của một công ty, trường học. WLAN sử dụng băng tần phục vụ công nghiệp, khoa học y tế: 2.4GHz và 5GHz, không chịu sự quản lý của chính phủ cũng như không cần cấp giấy phép sử dụng, vì vậy tồn tại nhiều vấn đề liên quan tới an toàn thông tin của người dùng trong mạng WLAN. Ngoài ra do sử dụng môi trường truyền dẫn vô tuyến nên WLAN rất dễ bị rò rỉ thông tin do tác động của môi trường bên ngoài, đặc biệt là sự tấn công của các tin tặc. Do đó, đi đôi với phát triển WLAN phải phát triển các khả năng bảo mật WLAN an toàn, để cung cấp thông tin hiệu quả, tin cậy cho người sử dụng.

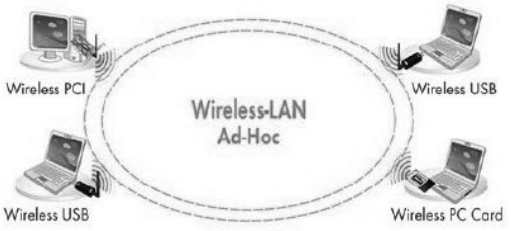
Một số vấn đề bảo đảm an toàn thông tin cho mạng không dây WLAN bao gồm các nội dung:

- Cấu trúc mạng không dây WLAN.
- Các hình thức tấn công mạng không dây phổ biến.
- Một số khuyến nghị nhằm đảm bảo an toàn thông tin mạng không dây trong thực tế.

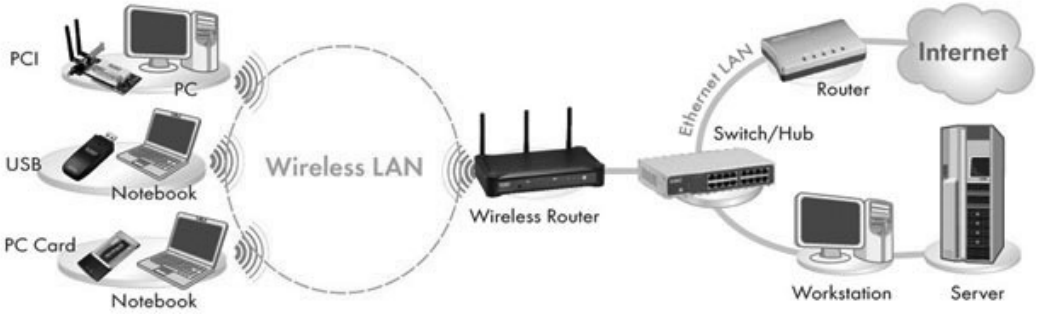
1. Cấu trúc mạng không dây WLAN

Một mạng không dây thông thường gồm có 2 phần: các thiết bị truy nhập không dây (Wireless Client), các điểm truy nhập (Access Points - AP).





- Chế độ cơ sở (Intrastructure mode): Các máy trong mạng sử dụng một hoặc nhiều thiết bị định tuyến hay thiết bị thu phát để thực hiện các hoạt động trao đổi dữ liệu với nhau.



2. Các hình thức tấn công mạng không dây phổ biến

2.1. Tấn công không thông qua xác thực (deauthentication attack)

Trong mạng không dây khi một thiết bị mới gia nhập vào mạng nó sẽ phải đi qua quá trình xác thực, sau quá trình xác nhận, thiết bị này sẽ thực hiện các quá trình có liên quan khác để có thể trao đổi dữ liệu và quảng bá trong toàn mạng. Trong suốt quá trình xác thực chỉ có một vài bản tin dữ liệu, quản lý và điều khiển là được chấp nhận. Một trong các bản tin đó mang lại cho thiết bị khả năng đòi hỏi không qua xác thực từ các nút khác. Bản tin đó được sử dụng khi một thiết bị muốn chuyển giữa hai mạng không dây khác nhau. Khi một thiết bị nhận được bản tin "không qua xác thực" này nó sẽ tự động rời khỏi mạng và quay trở lại trạng thái gốc ban đầu của nó.

Trong tấn công không qua chứng thực, tin tặc sẽ sử dụng một thiết bị giả mạo để tìm ra địa chỉ của điểm truy nhập (AP) đang điều khiển mạng (địa chỉ của AP có thể dễ dàng được tìm thấy nếu tin tặc "lắng nghe" lưu lượng giữa AP và các thiết bị khác). Khi tin tặc có được địa chỉ của AP, chúng sẽ

gửi quảng bá các bản tin "không chứng thực" ra toàn mạng khiến cho các thiết bị trong mạng ngay lập tức dừng trao đổi thông tin với mạng. Sau đó tất cả các thiết bị đó sẽ cố kết nối lại, xác thực lại và liên kết lại với AP tuy nhiên do việc truyền các bản tin "không qua xác thực" được lặp lại liên tục khiến cho mạng rơi vào tình trạng bị dừng hoạt động.

2.2. Tấn công bằng cách gửi lại bản tin (Reply Attack)

Tin tặc thực hiện các cuộc tấn công Replay Attack bằng cách đứng chắn giữa việc truyền thông tin hợp lệ, tin tặc không thay đổi bản tin mà chỉ gửi lại nó trong thời điểm thích hợp theo sự lựa chọn của tin tặc do các bản tin trong mạng không dây không có thứ tự một cách rõ ràng.

2.3. Giả mạo điểm truy cập

Đây là kiểu tấn công mà tin tặc đứng ở giữa và trộm lưu lượng truyền giữa 2 thiết bị. Kiểu tấn công này tồn tại là do trong mạng không dây không yêu cầu xác thực 2 hướng giữa AP và thiết bị truy nhập. AP phát quảng bá ra toàn mạng, do vậy tin tặc có thể dễ dàng nghe trộm và lấy được tất cả các thông tin mà chúng cần.

Rất khó khăn để tạo một cuộc tấn công theo kiểu "đứng giữa" trong mạng có dây bởi vì kiểu tấn công này yêu cầu truy cập thực sự đến đường truyền. Trong mạng không dây thì lại rất dễ bị tấn công kiểu này. Tin tặc tạo ra một AP thu hút nhiều thiết bị truy nhập hơn AP thật. AP giả này có thể được thiết lập bằng cách sao chép tất cả các cấu hình của AP thật đó là: SSID, địa chỉ MAC...

Bước tiếp theo là làm cho nạn nhân thực hiện kết nối tới AP giả. Cách thứ nhất là đợi cho người dùng tự kết nối. Cách thứ hai là gây ra một cuộc tấn công từ chối dịch vụ trong AP thật do vậy người dùng sẽ phải kết nối lại với AP giả. Trong mạng không dây sự lựa chọn AP được thực hiện bởi cường độ của tín hiệu nhận. Do đó tin tặc sẽ thực hiện các biện pháp kỹ thuật để làm cho AP giả có cường độ tín hiệu mạnh hơn, ví dụ như: đặt AP giả gần người dùng hơn là AP thật; sử dụng kỹ thuật anten định hướng. Sau khi nạn nhân kết nối tới AP giả, nạn nhân vẫn hoạt động như bình thường do vậy nếu nạn nhân kết nối đến một AP thật khác thì dữ liệu của nạn nhân đều đi qua AP giả. Tin tặc sẽ sử dụng các tiện ích để ghi lại mật khẩu của nạn nhân khi trao đổi thông tin và sẽ có được tất cả những thông tin để đăng nhập vào mạng chính thống.

2.4. Tấn công dựa trên thuật toán đa truy cập cảm nhận sóng mang (CSMA)

Trong mạng không dây sử dụng thuật toán đa truy cập cảm nhận sóng mang (CSMA) để tránh xung đột. CSMA là một thành phần của lớp MAC.

Tin tặc khai thác CSMA bằng cách làm cho các thiết bị trong mạng đều tin tưởng rằng có một thiết bị đang truyền tin tại thời điểm hiện tại và sẽ không tiến hành truyền tin vào mạng để tránh xung đột. Có các cách sau để đạt được điều này: tạo ra một thiết bị giả mạo để truyền tin một cách liên tục; sử dụng bộ tạo tín hiệu vô tuyến; làm cho card mạng chuyển thành chế độ kiểm tra để nó truyền đi liên tiếp một mẫu kiểm tra.

2.5. Giả mạo địa chỉ MAC

Trong mạng không dây, lọc địa chỉ MAC là một cách để ngăn người dùng bất hợp pháp gia nhập vào mạng. Tuy nhiên tin tặc lại có thể dễ dàng giả mạo địa chỉ MAC vì giá trị được đưa ra trong firmware của phần cứng có thể thay đổi được.

Mà trong mạng không dây thì địa chỉ MAC được quảng bá ra toàn mạng, do đó tin tặc chỉ cần chặn lại một vài gói tin để lấy địa chỉ MAC. Và bằng việc giả mạo địa chỉ MAC tin tặc sẽ được nhận dạng như một người dùng hợp pháp trong mạng.

2.6. Tấn công từ chối dịch vụ

Đây là hình thức tấn công làm cho các mạng không dây không thể phục vụ được người dùng, từ chối dịch vụ với những người dùng hợp pháp.

Khi sóng radio truyền trong môi trường, nó rất dễ bị ảnh hưởng bởi các yếu tố khách quan cũng như chủ quan. Tin tặc có thể lợi dụng điều này để tấn công từ chối dịch vụ bằng cách tạo ra các sóng có cùng tần số với tần số truyền tín hiệu để gây nhiễu cho đường truyền.

3. Một số khuyến nghị bảo đảm an toàn thông tin mạng không dây trong thực tế

3.1. Đối với người dùng tại gia và cơ các cơ quan, văn phòng nhỏ

Đối với người sử dụng trong phạm vi nhà ở và văn phòng nhỏ chi phí triển khai các biện pháp bảo đảm an toàn thông tin là một vấn đề không được để ý đầu tư. Các biện pháp sau có thể giảm thiểu rủi ro mất an toàn thông tin:

- Cập nhật phần mềm, firmware các thiết bị truy nhập và các điểm truy nhập với phiên bản

mới nhất do nhà sản xuất cung cấp.

- Kích hoạt các phương thức mã hóa WEP/WPA/WPA2 theo thứ tư ưu tiên sử dụng WPA2, WPA nếu thiết bị hỗ trợ.

- Thay đổi tên mạng không dây (SSID) mặc định do nhà sản xuất cài đặt sẵn, chú ý không sử dụng các tên gọi có gợi ý như tên đường phố hay địa chỉ, công ty hay nhà riêng hay họ tên của các thành viên trong gia đình, cơ quan, văn phòng.

- Không kích hoạt chức năng quảng bá SSID (chú ý: phải đảm bảo người dùng hợp pháp đã có thông tin SSID trên thiết bị của họ).

- Lọc địa chỉ MAC: Một vài điểm truy cập có khả năng chấp nhận các kết nối chỉ đối với các địa chỉ MAC đáng tin cậy là các địa chỉ duy nhất trên mạng (không trùng khớp nhau). Thực hiện điều này là rất khó khăn trong một môi trường với hơn 20 người sử dụng do việc thiết lập điểm truy cập bằng tay rất mất thời gian. Tuy nhiên, nó có thể được thiết lập một cách đơn giản trong môi trường nhà ở và môi trường văn phòng nhỏ.

3.2. Đối với người dùng tại các cơ quan, tổ chức, văn phòng vừa và nhỏ

Các cơ quan, tổ chức, văn phòng vừa và nhỏ có thể là một phần của một tổ chức lớn hơn. Đảm bảo an toàn thông tin là vấn đề quan trọng và phải cân bằng với hiệu xuất sử dụng khi số lượng người dùng tăng.

- Cập nhật phần mềm, firmware các thiết bị truy nhập và các điểm truy nhập với phiên bản mới nhất do nhà sản xuất cung cấp.

- Kích hoạt các phương thức mã hóa WEP/ WPA/ WPA2 theo thứ tư ưu tiên sử dụng WPA2, WPA nếu thiết bị hỗ trợ.

- Sử dụng mạng riêng ảo (VPN): Trong trường hợp có thể được sử dụng các điểm truy nhập kích hoạt IPSec hoặc các tường lửa mà chúng có thể thiết lập các đường ống VPN từ người dùng đầu cuối tới điểm truy nhập. Phần mềm VPN cho phép quá trình nhận thực và mã hóa hiệu quả hơn trong mạng công cộng bao gồm các thành phần vô tuyến và hữu tuyến.

- Thay đổi mật khẩu mặc định của nhà sản xuất, sử dụng các mật khẩu an toàn cho các điểm truy nhập.

- Đảm bảo các mật khẩu được mã hóa trước khi truyền qua mạng. Khi gửi mật khẩu tới người sử dụng, sử dụng một chương trình mã hóa để đảm bảo rằng các mật khẩu không bao giờ được gửi đi một cách rõ ràng mà những người sử dụng khác có thể hiểu được.

- Luôn lưu ý kiểm tra cấu hình điểm truy nhập để đảm bảo thiết bị này không bị "reset" về các thiết lập mặc định do một nguyên nhân khách quan hay chủ quan nào đó (các thiết lập mặc định của điểm truy nhập không có khả năng bảo đảm an toàn thông tin khi có một ai đó nhấn vào nút "reset". Điều này làm cho điểm truy nhập dễ bị tấn công bởi các tin tặc).

3.3. Đối với người sử dụng của các cơ quan, tổ chức, tập đoàn lớn.

Đối với người sử dụng của các cơ quan, tổ chức, tập đoàn lớn, yêu cầu an toàn thông tin cao. Ngoài các khuyến nghị ở trên các cơ quan, tổ chức có thể xem xét các yếu tố sau:

- Giám sát các điểm truy nhập: sử dụng các công cụ hỗ trợ vận hành để giám sát mạng một cách liên tục và kiểm tra các điểm truy nhập không tuân thủ các nguyên tắc về cấu hình. Một vài điểm truy nhập không có các thiết lập an toàn thông tin theo quy định tương ứng có thể là một điểm truy nhập bí mật thiết lập bởi tin tặc.

- Xác thực: Tích hợp các mạng WLAN vào trong cơ chế nhận thực bằng cách sử dụng các máy chủ nhận thực RADIUS hoặc LDAP. Các mật khẩu và tên người sử dụng có thể được mã hóa hoặc các chứng chỉ số có thể được sử dụng để nâng cao khả năng nhận thực.

- Điều khiển sóng vô tuyến: Tối thiểu hóa quá trình truyền sóng vô tuyến trong các khu vực không có người sử dụng như các khu vực đỗ xe hay các khu vực lân cận văn phòng. Thử nghiệm các anten để tránh các vùng phủ bên ngoài các biên giới điều khiển về mặt vật lý trong điều kiện thuận lợi. Nếu có thể, không đặt các điểm truy nhập tại biên của khu vực nhà ở hay văn phòng.

- Phân vùng các thiết bị: Đưa các điểm truy nhập vào một vùng mạng trung lập giữa mạng nội bộ và mạng internet (DMZ). Thiết lập cấu hình cho tường lửa để cho phép truy nhập đối với người sử dụng hợp lệ dựa trên các địa chỉ MAC, làm cho các tin tặc khó khăn hơn khi tấn công vào mạng.

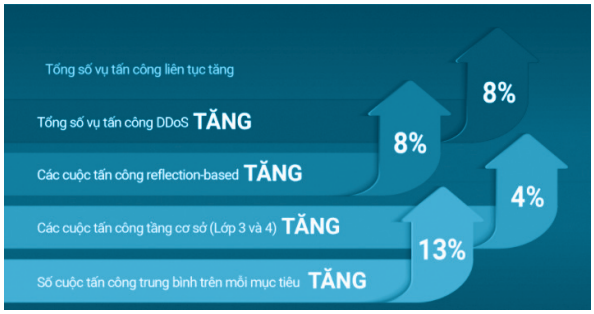
(Nguồn Cục An toàn thông tin - Bộ Thông tin và Truyền thông)

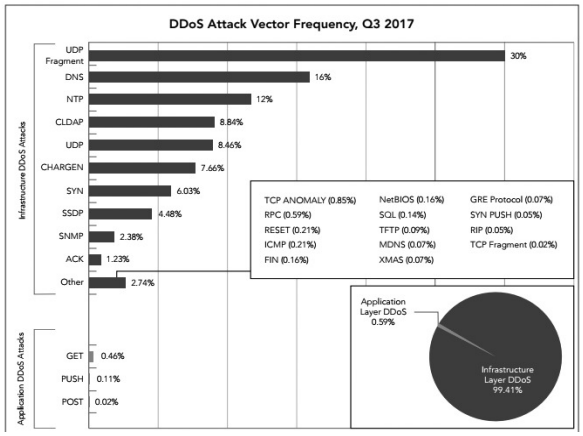
THỐNG KÊ TÌNH HÌNH AN TOÀN THÔNG TIN
TỔ ỨNG CỨU SỰ CỐ

I - Tình hình An toàn thông tin Quý III năm 2017 trong nước và quốc tế

1. Tình hình tấn công DDoS

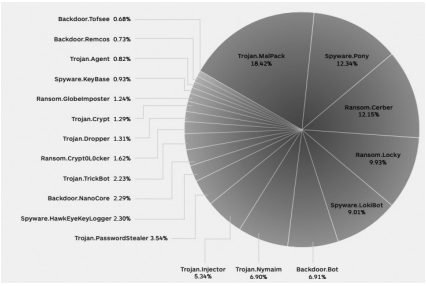
Theo báo cáo của An ninh mạng trong Quý 3 của Akamai các cuộc tấn công DDoS tiếp tục tăng so với Quý 2, cụ thể như sau:





Thống kê các kiểu tấn công DDoS thông qua các giao thức trong quý III

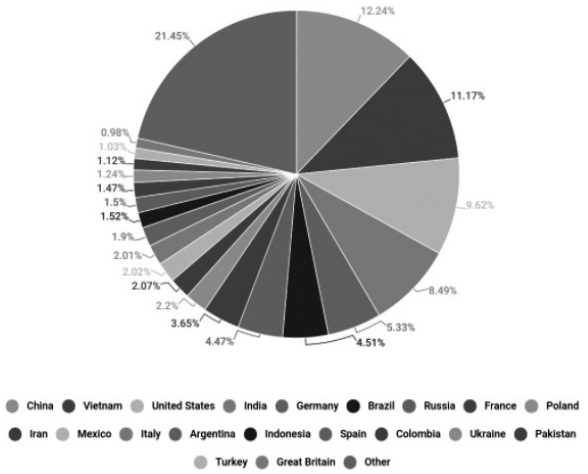
2. Tình hình mã độc lây lan thông qua hệ thống thư điện tử trong quý III



Nguồn: malwarebytes

3. Tình hình Spam và tấn công Phishing trong Quý III

Báo cáo của Kaspersky Lab về tình hình thư rác và lừa đảo trực tuyến trong quý III cho biết, Việt Nam tiếp tục nằm trong nhóm các quốc gia có nguồn phát tán thư rác đứng đầu với vị trí thứ 2 (11,17%), đứng đầu là Trung Quốc (12,24%) và thứ 3 là Mỹ (9,62%).



Báo cáo của Kaspersky Lab về tình hình tấn công Phishing trên phạm vi toàn cầu. Dẫn đầu là Brazil với 19.95%, thứ 2 là Australia với 16.51%...

Thống kê tình hình tấn công Phishing trên phạm vi toàn cầu

Nguồn: Kaspersky

4. Phương thức tấn công mới BlueBorne đe dọa an ninh hàng tỷ thiết bị

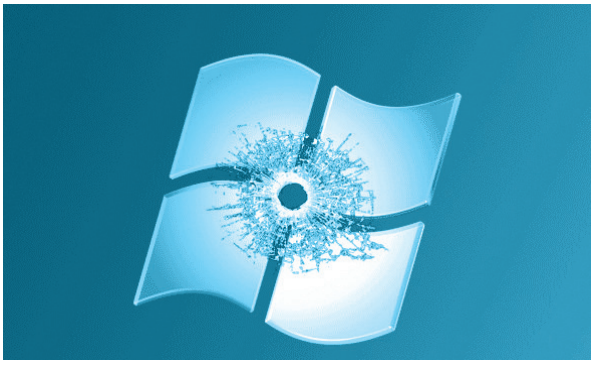
Phương pháp tấn công mới BlueBorne được phát hiện, khai thác kết nối Bluetooth của thiết bị và lan rộng qua không khí (airborne), đe dọa an

ninh khoảng 8,2 tỷ thiết bị gồm smartphone, máy tính và thiết bị IoT. Sử dụng phương pháp này, hacker có thể chiếm quyền kiểm soát thiết bị, truy cập mạng và dữ liệu doanh nghiệp, phát tán mã độc tới các thiết bị lân cận, tạo các botnet lớn...

Người dùng được khuyến cáo cập nhật các phiên bản hệ điều hành mới nhất. Đối với các thiết bị chưa được hỗ trợ bản vá, các chuyên gia khuyến cáo người dùng tắt Bluetooth và hạn chế sử dụng để đảm bảo an toàn.

5. Microsoft vá lỗ hổng nghiêm trọng trong Word/RTF/.Net

Trong bản cập nhật định kỳ tháng 9, Microsoft vá lỗ hổng nghiêm trọng trong Word/RTF/.Net . Người dùng cần cập nhật bản vá lỗ hổng Zero-day (CVE-2017-11826), cho phép hacker kiểm soát máy tính của người dùng. Theo đó, người dùng khi mở một tập tin độc hại đính kèm trong mail và chọn Enable Editing là đã cho phép hacker thực thi mã độc để kiểm soát hoàn toàn thiết bị.



Nhằm tránh bị ảnh hưởng bởi lỗ hổng, người dùng không click vào Enable Editing, cập nhật bản vá mới nhất từ nhà cung cấp.

6. Công cụ CCleaner phát tán malware tới hàng triệu PC

Trung tuần tháng 9, phần mềm dọn dẹp CCleaner 5.33 bị phát hiện chứa mã độc, đe dọa an ninh 2,27 triệu máy tính trên toàn thế giới. Mã độc ẩn giấu trong ứng dụng thu thập dữ liệu người dùng gồm tên thiết bị, phần mềm cài đặt, chương trình đang chạy, địa chỉ IP, MAC... và gửi về máy chủ C&C của hacker.

Người dùng CCleaner 5.33 được khuyến cáo gỡ bỏ phần mềm sớm nhất có thể, trong trường hợp cần sử dụng, hãy chọn một phiên bản khác của ứng dụng.

7. Tin tặc tấn công người dùng qua tiện ích mở rộng trên Google Chrome

Tiện ích mở rộng trên Chrome Web Developer được sử dụng bởi hơn một triệu người dùng đã bị tin tặc chiếm đoạt. Tin tặc sử dụng các phương thức lừa đảo nhằm truy cập vào tài khoản dành cho lập trình viên của Google, thay đổi thông tin và cập nhật tiện ích thực hiện các hành vi độc hại. Mã độc có thể đọc toàn bộ nội dung trang web nhằm can thiệp lưu lượng, do thám phím bấm,...

Người dùng tiện tích Web Developer được khuyến cáo cập nhật ngay phiên bản 0.5 và xem xét thay đổi mật khẩu tài khoản trực tuyến của mình.

8. Hơn 1000 phần mềm gián điệp được phát hiện trên Google Store

Tin tặc nặc danh đã thực hiện đưa hơn 1000 ứng dụng độc hại lên các chợ ứng dụng bên thứ ba và chợ ứng dụng chính thức Google Play Store. Các ứng dụng này có thể theo dõi hầu hết hành vi của người dùng và ghi lén cuộc gọi.

Mã độc gián điệp có tên SonicSpy có khả năng phát tán mạnh mẽ thông qua các chợ ứng dụng và giả mạo dưới dạng các phần mềm nhắn tin. Ở

thời điểm hiện tại, mã độc Sonic có thể thực hiện các hành vi như nghe lén cuộc gọi, âm thanh từ microphone, chiếm kiểm soát máy ảnh và ảnh chụp màn hình, thực hiện cuộc gọi và gửi tin nhắn ra ngoài. Bên cạnh đó, phần mềm gián điệp này còn có thể đánh cắp thông tin từ lịch sử cuộc gọi, danh bạ và thông tin điểm truy cập Wi-Fi mà thiết bị kết nối.

Cách đơn giản nhất để bảo vệ chính mình đó là thận trọng với các ứng dụng lừa đảo, có dấu hiệu mạo danh các thương hiệu khác, ngay cả khi tải chúng về từ Google Play Store. Không tải ứng dụng từ nguồn bên thứ ba, cài đặt phần mềm diệt virus và luôn cập nhật ứng dụng trong thiết bị.

9. Phát hiện 2 lỗ hổng Zero-Day trong Foxit PDF Reader

Các nhà nghiên cứu mới phát hiện 2 lỗ hổng bảo mật nghiêm trọng trong Foxit Reader, phần mềm chuyên dụng đọc tệp tin PDF, cho phép tin tặc thực thi mã tùy ý trên máy tính nạn nhân.

Lỗ hổng thứ nhất (CVE-2017-10951) là lỗ hổng cho phép đưa (tiêm) câu lệnh vào phần mềm, được phát hiện bởi nhà nghiên cứu Ariele Caltabiano tại công ty Trend Micro. Lỗ hổng thứ hai (CVE-2017-10952) là lỗ hổng được phát hiện bởi chuyên gia Steven Seeley tại Offensive Security.

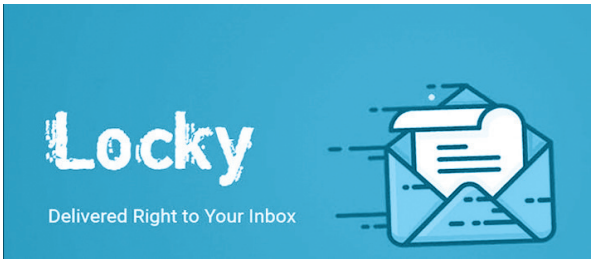
Tin tặc có thể khai thác những lỗ hổng này bằng cách gửi một tệp tin PDF giả mạo cho nạn nhân. Foxit từ chối vá cả 2 lỗ hổng do tính năng đọc an toàn "Safe reading mode" được bật mặc định trong Foxit Reader. Hơn 800 ứng dụng trên Google Play chứa mã độc quảng cáo Xavier

9. VNCERT phát hiện chiến dịch mã độc APT tấn công vào Việt Nam thông qua tài liệu Word

Trung tâm ứng cứu khẩn cấp máy tính Việt Nam - VNCERT phát hiện ra dấu hiệu của chiến dịch tấn công nhằm vào các hệ thống thông tin quan trọng tại Việt Nam thông qua việc phát tán và điều khiển mã độc có chủ đích (APT). Trung tâm yêu cầu Lãnh đạo đơn vị chỉ đạo các đơn vị thuộc phạm vi quản lý thực hiện khẩn cấp các công việc theo Công văn số 298/VNCERT-ĐPƯC.

10. Mã độc Locky phát tán thông qua email tới 23 triệu người dùng

Tin tặc gửi tới hơn 23 triệu email chứa mã độc trong ngày 28 tháng 8 tại Mỹ. Đây được coi là một trong những chiến dịch phát tán mã độc lớn nhất trong nửa cuối năm 2017.



Theo các nhà nghiên cứu, email mà tin tặc gửi đi rất da dạng bao gồm các cụm từ gây chú ý như "please print","documents," "images," "photos," "pictures," và "scans" nhằm thuyết phục nạn nhân mở email. Email chứa tệp tin đính kèm dưới dạng file nén ZIP bên trong chứa tệp tin Visual Basic Script (VBS). Ngay sau khi nạn nhân nhấn vào tệp tin VBS, chương trình sẽ tự động tải phiên bản mã độc Locky mới nhất có tên Lukitus, mã hóa toàn bộ tệp tin trên máy tính và thêm đuôi [.]lukitus vào cuối tên tệp tin.

Sau quá trình mã hóa kết thúc, mã độc hiển thị thông tin tiền chuộc trên màn hình, hướng dẫn nạn nhân tải và cài đặt trình duyệt Tor và truy cập địa chỉ của tin tặc để thanh toán.

Biến thể Locky Lukitus yêu cầu 0.5 Bitcoin (~$2,300) từ tin tặc để có thể khôi phục lại dữ liệu. Hiện tại chưa có cách nào hóa giải mã độc này.

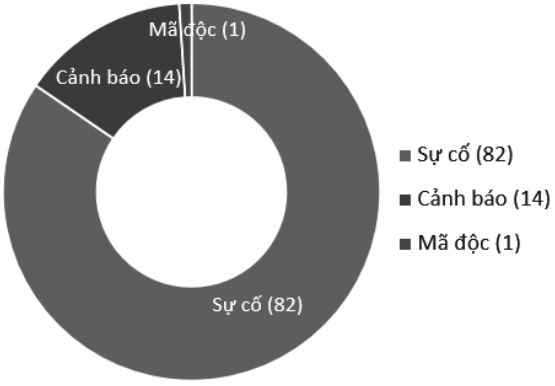
II - Tình hình An toàn thông tin trên địa bàn tỉnh trong quý III/2017

1. Thống kê các website trên địa bàn tỉnh bị tấn công

Ngày	Domain
18/9/2017	yensaothanhhoa.com/vantindat/images/Iran-Cyber.html
07/9/2017	baohiemthanhhoa.com/gss.html
07/9/2017	tuyendungthanhhoa.vn/gss.html
07/9/2017	inanthanhhoa.com/gss.html
07/9/2017	xaydungthanhhoa.com/gss.html
07/9/2017	viettelthanhhoa.vn/gss.html
07/9/2017	iphonethanhhoa.com/gss.html
07/9/2017	quangcaotaithanhhoa.com/gss.html
07/9/2017	noithatotothanhhoa.com/gss.html
05/9/2017	dietmoithanhhoa.com
25/8/2017	mazdathanhhoa.vn/Relaz.html
07/8/2017	laptopcuthanhhoa.com

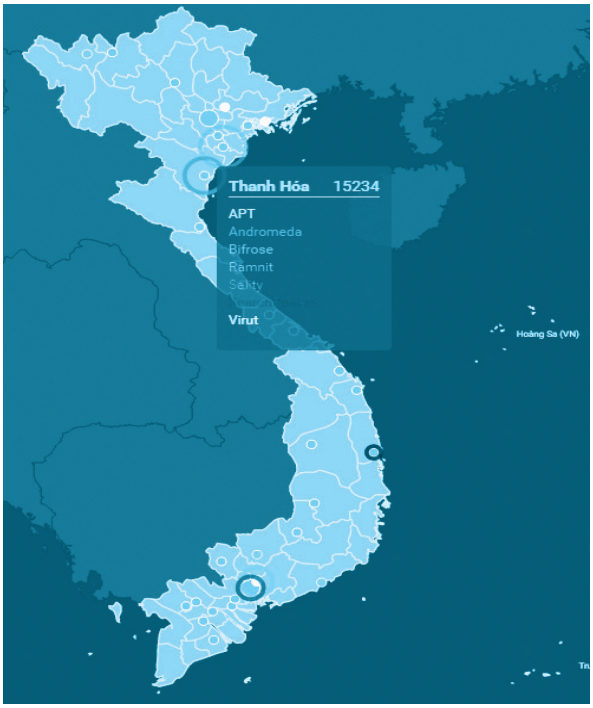
2. Tổng hợp tình hình ứng cứu sự cố trên địa bàn tỉnh

Trong quý III, 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 82 lượt hỗ trợ, cảnh báo cho 14 đơn vị liên quan đến mã độc, Website và an toàn thông tin cho phần mềm dùng chung của tỉnh.



Theo số liệu giám sát an toàn thông tin của nhà mạng Viettel, trên địa bàn tỉnh ghi nhận hơn 15.000 các lượt tấn công bao gồm các tấn công có chủ đích APT, các mã độc kết nối và tham gia vào mạng máy tính ma Botnet như Andromeda, Bifrose, Kazy, Ramnit, Sality... Trong số các địa phương, Thanh Hóa nằm trong số 10 tỉnh có tỉ lệ lây nhiễm mã độc cao nhất cả nước.

Theo ghi nhận của Trung tâm An ninh mạng và An toàn dữ liệu, trong thời gian từ 01/8-30/9



ghi nhận có 213 cuộc tấn công vào khai thác lỗ hổng ứng dụng Web và 09 cuộc tấn công chiếm đoạt quyền quản trị vào các dịch vụ đang hoạt động tại Trung tâm.

3. Công văn an toàn thông tin

- Ngày 07/9/2017 Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) ban hành công văn số 298/VNCERT-ĐPƯC về việc giám sát, ngăn chặn khẩn cấp hệ thống máy chủ điều khiển mã độc tấn công có chủ đích APT
- Ngày 08/9/2017 Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa ban hành công văn số 172/TTCNTT&TT-QTHT về việc giám sát, ngăn chặn khẩn cấp mã độc tấn công có chủ đích tại các cơ quan, đơn vị trên địa bàn tỉnh
- Ngày 06/9/2017 Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa ban hành công văn số 167/TTCNTT&TT-QTHT đến 172/TTC-NTT&TT-QTHT về việc khắc phục các điểm yếu về an toàn thông tin khi sử dụng phần mềm Quản lý văn bản và Hồ sơ công việc cho 06 cơ quan trên địa bàn tỉnh.
- Ngày 10/8/2017 UBND tỉnh ban hành công văn số 9449/UBND-CNTT về việc giao triển khai thực hiện các quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia.

TIN HOẠT ĐỘNG

Hội thi ứng dụng công nghệ thông tin trong khối cơ quan nhà nước tỉnh Thanh Hóa năm 2017

Sáng ngày 27/9/2017, Sở Thông tin và Truyền thông phối hợp với Văn phòng UBND tỉnh, Sở Nội vụ, Sở Khoa học - Công nghệ, Hội Tin học tỉnh và Đoàn TNCS Hồ Chí Minh tỉnh Thanh Hóa tổ chức Hội thi ứng dụng công nghệ thông tin trong khối cơ quan nhà nước tỉnh Thanh Hóa năm 2017.

Với chủ đề "Đẩy mạnh ứng dụng CNTT trong việc xây dựng nền hành chính hiện đại", hội thi năm 2017 có 35 đội tham gia với 70 thí sinh đại diện các sở, ban, ngành, UBND các huyện, thị xã, thành phố trên địa bàn tỉnh. Nội dung thi năm nay đặt ra những yêu cầu mới, khả năng về kiến thức của các thí sinh phải bảo đảm đáp ứng chuẩn kỹ năng sử dụng CNTT, hướng tới xây dựng chính quyền điện tử, giúp công khai, minh bạch các hoạt động của cơ quan nhà nước ngày càng tốt hơn; thành thạo sử dụng thư điện tử và Internet; tập trung kỹ năng ứng dụng CNTT phục vụ công tác chuyên môn, nghiệp vụ ở cơ quan, đơn vị; chủ trương, chính sách của Đảng, Nhà nước về CNTT; các văn bản quy phạm pháp luật về CNTT...

Tại hội thi, 35 đội đã tham gia dự thi vòng sơ khảo để lựa chọn 12 đội xuất sắc nhất tham dự vòng chung kết. Các đội thi lọt vào vòng chung kết được tham gia phần thi thực hành và phần thi thuyết trình theo các chủ đề do Ban Tổ chức đề ra. Bên cạnh đó, các đội có thể đăng ký tham dự thi sản phẩm, giải pháp, ý tưởng sáng tạo về CNTT phục vụ mục tiêu xây dựng chính phủ điện tử, phục vụ cải cách hành chính.

Hội thi ứng dụng CNTT trong khối cơ quan Nhà nước tỉnh Thanh Hóa năm 2017 là hoạt động thường niên, nhằm khích lệ phong trào nghiên cứu, ứng dụng và phát triển CNTT hỗ trợ công tác chuyên môn, nghiệp vụ phục vụ công tác quản lý hành chính nhà nước trong đội ngũ cán bộ, công chức tiếp tục được đẩy mạnh, góp phần quan trọng phát triển kinh tế - xã hội của tỉnh.

Chiều cùng ngày, Ban tổ chức đã tổ chức tổng kết và trao giải thưởng cho các đội tham dự hội thi; Tham dự có đồng chí Trần Duy Bình, Giám đốc Sở Thông tin và Truyền thông, Đồng chí Nguyễn Bá Tải - Phó Giám đốc Sở Nội vụ, Đồng chí Nguyễn Ngọc Túy, Phó Giám đốc Sở Khoa học và Công nghệ, Đồng chí Nguyễn Xuân Sang - Phó Chủ tịch Liên hiệp hội KHKT tỉnh và các lãnh đạo một số sở, ban, ngành của tỉnh. Ban tổ chức đã trao 01 giải nhất, 01 giải nhì và 02 giải ba cho phần thi sản phẩm sáng tạo; 01 giải nhì và 01 giải ba cho phần thi giải pháp, ý tưởng sáng tạo; giải tập thể thuộc khối sở, ban, ngành cấp tỉnh có 01 giải nhất, 01 giải nhì, 01 giải ba và 02 giải khuyến khích; giải tập thể thuộc khối UBND cấp huyện có 01 giải nhất, 01 giải nhì, 02 giải ba và 03 giải khuyến khích và 10 giải cá nhân có thành tích xuất sắc nhất cho các thí sinh tham dự thi Hội thi.

NGÔ PHƯƠNG

Trung tâm CNTT&TT tham dự diễn tập ứng cứu sự cố an ninh mạng ACID 2017

Sáng ngày 11/9 tại Hà Nội, Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) đã điều phối chương trình diễn tập quốc tế về ứng cứu sự cố an ninh mạng trên quy mô toàn khu vực Đông Nam Á (ACID 2017) tại Việt Nam. Chương trình có sự tham gia của 15 đội ứng cứu khẩn cấp đến từ các quốc gia thuộc Đông Nam Á và các quốc gia Úc, Trung Quốc, Ấn Độ, Nhật Bản và Hàn Quốc.

Phát biểu khai mạc sự kiện, Thứ trưởng Bộ TT&TT Nguyễn Thành Hưng cho biết, việc tổ chức hoạt động diễn tập quốc tế thường xuyên nhằm mục đích củng cố và duy trì kênh liên lạc thông suốt giữa các nước, sẵn sàng phối hợp ứng cứu sự cố an toàn mạng trong các trường hợp khẩn cấp; và cũng chính là cơ hội để các cán bộ kỹ thuật được rèn luyện kỹ năng trong tình huống thực tế, giúp nâng cao kiến thức, tích lũy kinh nghiệm cho công tác chuyên môn trong ứng cứu sự cố an toàn mạng.

ACID 2017 sẽ tiếp tục tập trung vào xu hướng bảo mật không gian mạng mới nhất dành cho các đơn vị thành viên mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia khi thực hiện các nhiệm vụ xử lý sự cố mạng. Chương trình diễn tập an toàn không gian mạng với chủ đề "Phòng chống hiểm họa của việc thiếu xác thực và kiểm soát truy cập yếu kém" sẽ kích hoạt một số các kịch bản để tạo điều kiện cho các CERT tham gia thực tế vào công tác xử lý, điều tra, phân tích, khắc phục và báo cáo sự cố. Đây cũng là cơ hội để các đội tham dự diễn tập được thực hành kỹ năng xây dựng và triển khai kế hoạch ứng phó sự cố đảm bảo an toàn thông tin mạng.

ACID 2017 có sự tham gia của các đội đại diện cho 10 quốc gia khu vực ASEAN và 5 nước đối thoại là Australia, Trung Quốc, Ấn Độ, Nhật Bản và Hàn Quốc để tạo cơ hội cho các CERT (Đội phản ứng nhanh an ninh mạng máy tính) tương tác, rèn luyện thực hành và tinh

chỉnh cả về quy trình, thủ tục và kỹ năng xử lý, giải quyết các sự cố an toàn thông tin mạng.

Tham gia ACID 2017 năm nay, Trung tâm CNTT&TT cử 03 thành viên trong Tổ Ứng cứu sự cố của Trung tâm tham gia cùng với các đội diễn tập. Cụ thể, đội Core Team bao gồm những chuyên gia của VNCERT (Trung tâm ứng cứu khẩn cấp máy tính Việt Nam), Bkav, Viettel, VNPT, CMC Infosec, VNPT Technology... sẽ là đội chính, thực hiện các hoạt động diễn tập. Đội Core Team có trách nhiệm hướng dẫn cho bất cứ thành viên nào tham gia chương trình hôm nay nếu cần sự hỗ trợ để giải quyết tình huống sự cố và các vấn đề leo thang đặc quyền được đưa ra.

Nhiệm vụ của các đội diễn tập yêu cầu tích cực thực hành, điều tra chứng cứ số liên quan đến sự cố; phân tích, xác định hành vi của đối tượng tấn công; đề xuất các biện pháp cảnh báo, khắc phục, giảm thiểu tác động, khôi phục hoạt động của hệ thống và các biện pháp phòng ngừa, ngăn chặn sự lây nhiễm, lan rộng của sự cố cần được thực hiện đối với tất cả các tổ chức có liên quan.

HOÀNG ANH TUẤN

Trung tâm Công nghệ thông tin và truyền thông Thanh Hóa tham dự Diễn đàn Vietnam ICT Summit 2017

Sáng ngày 06 tháng 9 năm 2017, Hiệp hội Phần mềm và Dịch vụ CNTT Việt Nam (VINASA) đã chính thức tổ chức Diễn đàn Cấp cao CNTT-TT Việt Nam (Vietnam ICT Summit) 2017 lần thứ 7 tại Hà Nội. Đáng chú ý tại sự kiện năm nay có sự góp mặt của Phó Thủ tướng Vũ Đức Đam, cùng hơn 500 lãnh đạo cấp cao.

Đây là diễn đàn chính sách, công nghệ thường niên với sự tham dự của các lãnh đạo cấp cao của Chính phủ, các bộ, ngành, các tập đoàn kinh tế, các đơn vị ứng dụng CNTT, nhằm chia sẻ tầm nhìn, xu thế phát triển, đặc biệt là cùng trao đổi các giải pháp lớn đưa CNTT làm nền tảng tạo phương thức phát triển mới, hiện đại hóa đất nước.

Tại diễn đàn, đại diện của VINASA đã trình bày báo sơ bộ của tổ chức sau khi thực hiện khảo sát trên 300 đơn vị liên quan tới cuộc CMCN 4.0. Qua đó thấy được những thế mạnh của Việt Nam, điển hình là nguồn nhân lực, khi có tới 77,7% đơn vị đánh giá đây là điểm mấu chốt cần khai thác để chiếm lấy ưu thế.

Bên cạnh đó, còn các yếu tố như "nhận thức và quyết tâm hành động của Chính phủ (chiếm 70,4%)", "Hạ tầng công nghệ thông tin và viễn thông (chiếm 59,1%)". Cũng theo khảo sát, để hiện thực hóa những lợi thế này, thì Việt Nam cần triển khai các giải pháp quan trọng như đào tạo nguồn nhân lực, đưa ra giải pháp thúc đẩy chuyển đổi số trong toàn bộ nền kinh tế, thúc đẩy khởi nghiệp và các ý tưởng sáng tạo.

Tại sự kiện, Phó Thủ tướng Vũ Đức Đam kêu gọi các đơn vị đoàn thể, doanh nghiệp, tổ chức cơ quan chính phủ cùng nhau vì lợi ích của chính đơn vị mình, nhưng lớn hơn là vì lợi ích chung. "Chúng ta hãy làm những việc mà vốn không mới, nhưng với một quyết tâm mới, nhằm mang lại một tâm thế mới cho tất cả chúng ta", Phó Thủ tướng phát biểu.

Trong nội dung Diễn đàn Vietnam ICT Summit 2017 còn thảo luận sâu vào 4 chuyên đề chính, gồm: "Nhận thức về Việt Nam 4.0" bàn về việc xây dựng chiến lược số để Việt Nam tiếp cận CMCN 4.0 và điều kiện thiết yếu để hiện thực hóa chiến lược; "Thế mạnh kinh tế số Việt Nam - Công nghiệp số, Nông nghiệp thông minh, Du lịch thông minh"; "Thành phố thông minh -Smart City"; và "Nhân lực số, đổi mới sáng tạo và khởi nghiệp" của các diễn giả là các chuyên gia đầu ngành kinh tế công nghệ như Ts. Mai Liêm Trực, Pgs. Ts. Trần Đình Thiên, Ts. Võ Trí Thành, PGS. Ts. Trần Văn Nhung, PGs. Ts. Trương Gia Bình... ; và lãnh đạo các tập đoàn công nghệ lớn như: Viettel, FPT, Microsoft, MISA, VNPT, CISCO, VNG, Shoppee...

LÊ VĂN TUẤN

Trung tâm CNTT&TT Thanh Hóa tổ chức thi cấp Chứng chỉ ứng dụng Công nghệ thông tin đợt 3 năm 2017

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

Sáng ngày 06 tháng 8 năm 2017, Trung tâm Công nghệ thông tin và truyền thông Thanh Hóa tổ chức kỳ thi sát hạch cấp Chứng chỉ công nghệ thông tin chuẩn cơ bản, đợt 3 năm 2017; Hội đồng thi được Sở Giáo dục và đào tạo thành lập gồm 14 người, bao gồm đầy đủ các Ban theo quy định về việc tổ chức thi và cấp chứng chỉ ứng dụng công nghệ thông tin tại Thông tư liên tịch số 17/2016/TTLT-BGDĐT-BTTT ngày 21 tháng 6 năm 2016 giữa Bộ Giáo dục và Đào tạo và Bộ Thông tin và Truyền thông.

Kỳ thi Đợt 3 năm 2017, có 32 thí sinh đăng ký dự thi và chỉ có 24/32 thí sinh đã vượt qua 2 phần thi của mình là phần thi trắc nghiệm lý thuyết trực tuyến trên phần

mềm và phần thi thực hành kỹ năng trên máy tính; toàn bộ hồ sơ về kỳ thi đã được gửi Sở Giáo dục và đào tạo tỉnh để tiến hành cấp chứng chỉ, phôi chứng chỉ được Bộ Giáo dục và Đào tạo cấp theo số lượng thí sinh thi đậu, được Sở GDĐT Thanh Hóa phê duyệt.

Theo kế hoạch, Trung tâm liên tục thu hồ sơ đăng ký bồi dưỡng, ôn thi và được tổ chức thi 01 lần vào hằng tháng trong năm.

Mọi thông tin về đăng ký bồi dưỡng, ôn thi và đăng ký thi xin liên hệ về: ***Phòng Đào tạo và Dịch vụ - Trung tâm CNTT&TT Thanh Hóa***, số 73 Hàng Than, phường Lam Sơn, thành phố Thanh Hóa.

Số điện thoại: 02373. 718.698 Hoặc thông qua website: http://ict.thanhhoa.gov.vn

NGUYỄN TÌNH

VĂN BẢN MỚI

Ngày 12 tháng 9 năm 2017, Bộ Thông tin và Truyền thông ban hành Thông tư số 20/2017/TT-BTTTT Quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc.

Thông tư này thay thế cho Thông tư 27/2011/TT-BTTTT ngày 04/10/2011 của Bộ Thông tin và Truyền thông quy định về điều phối các hoạt động ứng cứu sự cố mạng Internet Việt Nam.

Thông tư quy định rõ về phân cấp tổ chức thực hiện ứng cứu sự cố bảo đảm an toàn thông tin mạng trên toàn quốc. Theo đó, Bộ Thông tin và Truyền thông là cơ quan thường trực về ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia (gọi tắt là Cơ quan thường trực quốc gia) và Ban điều phối ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia (Ban điều phối ứng cứu quốc gia); Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam VNCERT là cơ quan điều phối quốc gia về ứng cứu sự cố (Cơ quan điều phối quốc gia)...

Nguyên tắc điều phối, ứng cứu sự cố là chủ động, kịp thời, nhanh chóng, chính xác, đồng bộ và hiệu quả; phối hợp chặt chẽ, chính xác, đồng bộ và hiệu quả giữa các cơ quan tổ chức, doanh nghiệp trong nước và nước ngoài. Ứng cứu sự cố trước hết phải được thực hiện, xử lý bằng lực lượng tại chỗ và trách nhiệm chính của chủ quản hệ thống thông tin.

Ban điều hành mạng lưới tổ chức triển khai các nhiệm vụ của mạng lưới ứng cứu sự cố, gồm các hoạt động chính là nghiên cứu, thu thập, tiếp nhận, phân tích, xác minh, đánh giá, cảnh báo về sự cố, rủi ro an toàn thông tin mạng và phần mềm độc hại.

Bên cạnh đó, Thông tư cũng quy định rõ về quy trình ứng cứu sự cố an toàn thông tin mạng gồm các bước: Tiếp nhận, phân tích, ứng cứu ban đầu và thông báo sự cố; triển khai ứng cứu, ngăn chặn và xử lý sự cố; xử lý sự cố, gỡ bỏ và khôi phục; tổng kết, đánh giá.

Thông tư có hiệu lực thi hành kể từ ngày 01/11/2017./.

Ngày 12 tháng 9 năm 2017, Bộ Thông tin và Truyền thông ban hành Thông tư số 19/2017/TT-BTTTT công tác bảo vệ bí mật nhà nước trong ngành thông tin và truyền thông

Theo Thông tư, bí mật nhà nước trong ngành Thông tin và Truyền thông gồm: Tin, tài liệu về vụ việc, tài liệu, vật, địa điểm, thời gian, lời nói, hồ sơ và các nội dung liên quan khác được quy định tại danh mục bí mật nhà nước độ Tối mật và danh mục bí mật nhà nước độ Mật của ngành Thông tin và Truyền thông; tin, tài liệu thuộc danh mục bí mật nhà nước của Bộ, ngành, địa phương, cơ quan khác mà các cơ quan, đơn vị, tổ chức trong ngành Thông tin và Truyền thông đang quản lý, sử dụng, lưu giữ trong quá trình phối hợp công tác.

Thông tư cũng nêu rõ những hành vi bị nghiêm cấm: Thu thập, lưu giữ, chuyển giao, làm lộ, làm mất, chiếm đoạt, mua bán, tiêu hủy trái phép tài liệu, vật mang bí mật nhà nước trong ngành Thông tin và Truyền thông; trao đổi, cung cấp tin, tài liệu, vật mang bí mật nhà nước cho các cơ quan, tổ chức, đơn vị, cá nhân; in, sao, chụp tài liệu có nội dung bí mật nhà nước khi chưa được cấp có thẩm quyền phê duyệt.

Bên cạnh đó, cấm soạn thảo, lưu trữ, trao đổi, sao chụp tin, tài liệu mật trên máy tính, thiết bị có kết nối Internet hoặc có kết nối với các thiết bị khác có kết nối Internet; sử dụng các thiết bị có tính năng ghi âm, ghi hình, thu phát tín hiệu và thực hiện việc ghi âm, ghi hình trong các cuộc họp có nội dung bí mật nhà nước khi chưa được người chủ trì cuộc họp cho phép.

Thông tư quy định, cá nhân được giao nhiệm vụ tiếp xúc dưới mọi hình thức với bí mật nhà nước trong lĩnh vực Thông tin và Truyền thông phải thực hiện nghiêm túc, đầy đủ các quy định tại Thông tư này và các quy định khác có liên quan của pháp luật về công tác bảo vệ bí mật nhà nước, và phải cam kết bảo vệ bí mật nhà nước bằng văn bản. Văn bản cam kết bảo vệ bí mật nhà nước được lưu hồ sơ nhân sự của cơ quan, đơn vị chủ quản.

Cá nhân được giao nhiệm vụ tiếp nhận, xử lý, lưu trữ, quản lý tài liệu mật, quản lý các dấu mật và đóng dấu độ mật, dấu thu hồi vào văn bản theo sự chỉ đạo của người có thẩm quyền phải cam kết bảo vệ bí mật nhà nước trong lĩnh vực Thông tin và Truyền thông bằng cách lập danh sách ghi rõ họ tên, chức vụ, đơn vị công tác và ký tên vào danh sách. Cá nhân được tiếp xúc (nghe phổ biến, nghiên cứu, sử dụng) với tin tức, tài liệu độ "Tuyệt mật", "Tối mật" phải cam kết bảo vệ bí mật nhà nước trong lĩnh vực Thông tin và Truyền thông bằng cách lập danh sách ghi rõ họ tên, chức vụ, đơn vị công tác, những nội dung bí mật được tiếp xúc và ký tên vào danh sách. Thủ trưởng cơ quan, đơn vị hoặc cá nhân được ủy quyền chịu trách nhiệm lập danh sách này, cùng ký tên và nộp lưu hồ sơ nhân sự của cơ quan, đơn vị chủ quản.

Thông tư này có hiệu lực thi hành kể từ ngày 01/11/ 2017.

NGUYỄN PHƯƠNG