BẢN TIN NỘI BỘ
CẬP NHẬT VỀ AN TOÀN THÔNG TIN VÀ CẢNH BÁO LỖ HỔNG BẢO MẬT

1. Ban Cơ yếu Chính phủ quyết tâm triển khai xây dựng, phát triển Chính phủ điện tử

Trong thời gian qua, công tác xây dựng và phát triển Chính phủ điện tử đã đạt được nhiều kết quả tích cực đáng ghi nhận, tạo được sự thống nhất giữa Ban, Bộ, ngành, địa phương, các cơ quan, đơn vị trong toàn quốc. Đây là sự vào cuộc mạnh mẽ của Chính phủ, các Bộ, ngành, địa phương và người dân. Trong đó phải kể đến vai trò quan trọng Ban Cơ yếu Chính phủ - đơn vị luôn nâng cao quyết tâm xây dựng, triển khai Chính phủ điện tử.

Trong thời gian qua, Đảng, Chính phủ luôn quan tâm, coi trọng việc phát triển ứng dụng công nghệ thông tin, xây dựng Chính phủ điện tử trong hoạt động của các cơ quan nhà nước và phục vụ người dân, doanh nghiệp. Trên cơ sở đó, các bộ, ban, ngành, địa phương đã có nhiều bước chuyển mình, đạt được các kết quả bước đầu trong công tác xây dựng Chính phủ điện tử. Theo báo cáo đánh giá về Chính phủ điện tử của Liên hợp quốc, năm 2018, Chỉ số phát triển Chính phủ điện tử (EGDI) của Việt Nam xếp hạng thứ 88/193 quốc gia (tăng 01 bậc so với năm 2016). Trong đó, chỉ số thành phần về dịch vụ công trực tuyến (OSI) tăng 15 bậc lên thứ hạng 59/193 quốc gia (so với năm 2016).

Tuy nhiên, nhiều nội dung triển khai Chính phủ điện tử chưa đạt được kết quả như mong đợi, có phần khiêm tốn. Có thể kể đến: xếp hạng về Chính phủ điện tử còn thấp, dưới mức trung bình trong khu vực ASEAN; chỉ số hạ tầng, viễn thông (TII) giảm 10 bậc (100/193) so với năm 2016; khung pháp lý đồng bộ về xây dựng Chính phủ điện tử còn chưa được hoàn thiện; việc xây dựng cơ sở dữ liệu quốc gia, hạ tầng CNTT nền tảng phục vụ phát triển Chính phủ điện tửu còn chậm; bảo mật, an toàn, an ninh thông tin thấp, chưa kết nối, chia sẻ dữ liệu giữa các hệ thống thông tin; tỷ lệ sử dụng dịch vụ công trực tuyến còn rất thấp….

Để giải quyết vấn đề này, ngày 7/3/2019, Chính phủ đã ban hành Nghị quyết số 17/NQ-CP về một số nhiệm vụ, giải pháp trọng tâm phát triển Chính phủ điện tử giai đoạn 2019 - 2020, định hướng đến năm 2025 (Nghị quyết 17/NQ-CP). Mục tiêu chính của Nghị quyết là hoàn thiện nền tảng Chính phủ điện tử nhằm nâng cao hiệu lực, hiệu quả hoạt động của bộ máy hành chính nhà nước và chất lượng phục vụ người dân, doanh nghiệp. Chính phủ yêu cầu sự vào cuộc mạnh mẽ, quyết liệt của các bộ, ban, ngành, như: Văn phòng chính phủ, Bộ Thông tin và Truyền thông, Bộ Công an, Bộ Quốc phòng, Ban Cơ yếu chính phủ….

Nắm bắt được vấn đề này, ngày 20/6/2019, Ban Cơ yếu Chính phủ đã khẩn trương ban hành Kế hoạch triển khai thực hiện Nghị quyết 17/NQ-CP, để tổ chức triển khai kịp thời, hiệu quả các nhiệm vụ của Ban Cơ yếu Chính phủ được giao tại Nghị quyết 17/NQ-CP; nâng cao hiệu lực, hiệu quả hoạt động của Ban Cơ yếu Chính phủ và chất lượng cung cấp sản phẩm, giải pháp bảo mật, xác thực, giám sát an toàn thông tin phục vụ xây dựng Chính phủ điện tử của các bộ, ngành địa phương. Kế

hoạch triển khai là sở cứ để Ban Cơ yếu Chính phủ xác định cụ thể các nhiệm vụ, thời hạn hoàn thành cũng như phân công trách nhiệm cho các cơ quan, đơn vị chuyên trách trong Ban, các Hệ Cơ yếu để đạt các mục tiêu đề ra.

Năm nhiệm vụ trọng tâm trong giai đoạn 2019 - 2020, định hướng đến 2025

Căn cứ vào các nhiệm vụ được giao tại Nghị quyết 17/NQ-CP, Ban Cơ yếu Chính phủ xác định 5 nhiệm vụ chính cần thực hiện trong giai đoạn 2019 - 2020, định hướng đến 2025.

Thứ nhất, Xây dựng, hoàn thiện thể chế tạo cơ sở pháp lý đầy đủ, toàn diện cho việc triển khai xây dựng, phát triển Chính phủ điện tử

Trong lĩnh vực lập pháp, việc hoàn thiện hệ thống quy phạm pháp luật là điều kiện tiên quyết, cơ sở để xây dựng, phát triển Chính phủ điện tử. Để thực hiện nhiệm vụ này, Ban Cơ yếu Chính phủ đã và sẽ tích cực phối hợp với Bộ TT&TT, Bộ Nội vụ và VPCP để xây dựng các Nghị định, quy định liên quan đến công tác xây dựng Chính phủ điện tử, như: Nghị định về định danh và xác thực điện tử cho các cá nhân, tổ thức, các văn bản hướng dẫn; Nghị định thay thế Nghị định số 110/2004/NĐ-CP này 8/5/2004 của Chính phủ về công tác văn thư và Đề án thực hiện nhiệm vụ lưu trữ tài liệu điện tử của các cơ quan; Nghị định về thực hiện thủ tục hành chính trên môi trường điện tử…. Song song với đó, Ban Cơ yếu Chính phủ cũng triển khai xây dựng, hoàn thiện các văn bản quy định của Ban theo quy định phục vụ xây dựng, phát tiển của Chính phủ điện tử.

Đặc biệt, trong thời gian tới, Ban Cơ yếu Chính phủ sẽ chủ trì xây dựng 02 Đề án quan trọng là: Đề án triển khai các hệ thống bảo vệ thông tin thuộc phạm vi bí mật nhà nước dùng mật mã đáp ứng yêu cầu triển khai Chính phủ điện tử và Đề án Xây dựng Trung tâm an toàn thông tin mạng cho Hệ thống Chính phủ điện tử. Khi được triển khai, kết quả của 2 đề án này sẽ giúp đảm bảo an toàn, an ninh thông tin Chính phủ điện tử, đáp ứng yêu cầu "Không để xảy ra sự cố lộ, lọt dữ liệu" mà Thủ tướng Nguyễn Xuân Phúc đặt ra tại Lễ khai trương Hệ thống thông tin phục vụ họp và xử lý công việc của Chính phủ vừa qua (24/6).

Thứ hai, Xây dựng nền tảng công nghệ phát triển Chính phủ điện tử của Ban Cơ yếu Chính phủ

Hoàn thành xây dựng, cập nhật kiến trúc Chính phủ điện tử của Ban Cơ yếu Chính phủ phù hợp với Khung kiến trúc Chính phủ điện tử Việt Nam (phiên bản 2.0) và thường xuyên cập nhật, ban hành các phiên bản tiếp theo phù hợp với các phiên bản cập nhật Khung kiến trúc Chính phủ điện tử Việt Nam; triển khai áp dụng Kiến trúc Chính phủ điện tử của Ban Cơ yếu Chính phủ đã được ban hành.

Thứ ba, Xây dựng, phát triển Chính phủ điện tử của Ban Cơ yếu Chính phủ gắn kết chặt chẽ giữa ứng dụng công nghệ thông tin với cải cách hành chính, đổi mới lề lối, phương thức làm việc.

Để triển khai đồng bộ, Ban Cơ yếu Chính phủ sẽ tiến hành xây dựng Hệ thống thông tin báo cáo đáp ứng các yêu cầu tại Nghị định 09/2019/NĐ-CP. Bên cạnh đó,

triển khai các sản phẩm, giải pháp bảo mật, xác thực, an toàn thông tin phục vụ xây dựng, phát triển Chính phủ điện tử trong Ban Cơ yếu Chính phủ.

Đối với công tác quản lý nhà nước về mật mã dân sự, trong thời gian tới, Ban Cơ yếu Chính phủ sẽ khẩn trương xây dựng và triển khai Hệ thống thông tin điện tử quản lý nhà nước về mật mã dân sự phục vụ xây dựng, phát triển Chính phủ điện tử.

Thứ tư, Triển khai các sản phẩm, giải pháp bảo mật, xác thực, giám sát an toàn thông tin phục vụ xây dựng Chính phủ điện tử của các bộ, ngành, địa phương

Trong công cuộc xây dựng và bảo vệ tổ quốc, bên cạnh nhiệm vụ xuyên suốt đảm bảo tuyệt đối bí mật, chính xác, kịp thời thông tin phục vụ sự lãnh đạo, chỉ đạo, chỉ huy của Đảng, Nhà nước, Ban Cơ yếu Chính phủ nói riêng và ngành Cơ yếu Việt Nam nói chung đã đứng trước những thách thức to lớn và các nhiệm vụ mới. Hiện nay, Ban Cơ yếu Chính phủ đã và đang tập trung triển khai các giải pháp kỹ thuật đồng bộ để đáp ứng các yêu cầu về bảo mật và an toàn thông tin. Để đáp ứng được nhiệm vụ này, Ban Cơ yếu Chính phủ đã từng bước triển khai các giải pháp kỹ thuật tổng thể theo lộ trình. Việc triển khai chữ ký số (CKS) chỉ là những bước đi đầu tiên của Ban trong vấn để đảm bảo bảo mật và an toàn cho Chính phủ điện tử. Để phục vụ xây dựng Chính phủ điện tử, Ban Cơ yếu Chính phủ xác định cần thực hiện 3 nhóm nhiệm vụ đề ra: bảo đảm bảo mật; xác thực, định danh và giám sát an toàn thông tin.

Thứ năm, Đảm bảo nguồn lực triển khai xây dựng Chính phủ điện tử

Về nguồn lực vật lực, Ban Cơ yếu Chính phủ xác định rõ cần thực hiện tốt công tác xây dựng kế hoạch trung hạn, ngắn hạn bảo đảm triển khai các nhiệm vụ, giải pháp xây dựng Chính phủ điện tử của Ban; tổ chức ký kết và thực hiện thỏa thuận phối hợp triển khai các sản phẩm, giải pháp phục vụ xây dựng, phát triển Chính phủ điện tử của các Bộ, ngành, địa phương; tăng cường công tác phối hợp, trao đổi, học tập kinh nghiệm với một số đơn vị liên quan trong và ngoài nước.

Về nguồn lực nhân lực, trong thời gian tới, Ban giao cho Học viện Kỹ thuật mật mã chủ trì xây dựng và triển khai kế hoạch đào tạo, tập huấn, huấn luyện quản lý, triển khai, sử dụng các sản phẩm, giải pháp bảo mật, xác thực, giám sát an toàn thông tin phục vụ xây dựng, phát triển chính phủ điện tử cho lực lượng cơ yếu các cấp và các đầu mối chuyên trách của các bộ, ngành, địa phương.

Một số chỉ tiêu cụ thể trong giai đoạn 2019 – 2020, định hướng đến 2025

Căn cứ vào các nhiệm vụ đề ra, Ban Cơ yếu Chính phủ quyết tâm triển khai thành công một số chỉ tiêu trọng tâm như sau:

Về gửi, nhận văn bản điện tử; báo cáo điện tử của Ban Cơ yếu Chính phủ

Phấn đấu đến hết năm 2020, Hệ thống quản lý văn bản và điều hành của Ban Cơ yếu Chính phủ được kết nối, liên thông với Trục liên thông văn bản quốc gia phục vụ gửi, nhận văn bản điện tử.

Đạt tỷ lệ 100% các cơ quan, đơn vị và cán bộ, công chức trong Ban được cấp chứng thư số và văn bản trao đổi giữa các cơ quan, đơn vị (trừ văn bản mật) dưới dạng điện tử;

Phấn đấu đến hết năm 2020, 80% hồ sơ công việc tại Ban Cơ yếu Chính phủ được xử lý trên môi trường mạng (không bao gồm hồ sơ xử lý công việc có nội dung mật), đạt tỷ lệ 100% vào năm 2025.

Rút ngắn từ 30 – 50% thời gian họp, giảm tối đa việc sử dụng tài liệu giấy thông qua Hệ thống thông tin phục vụ họp và xử lý công việc, văn phòng điện tử.

Đến cuối năm 2020, tối thiểu 30% báo cáo định kỳ (không bao gồm nội dung mật) được gửi, nhận qua Hệ thống thông tin báo cáo quốc gia, đạt 80% vào năm 2025.

Về triển khai các sản phẩm, giải pháp bảo mật, xác thực, giám sát, an toàn thông tin phục vụ xây dựng Chính phủ điện tử của các bộ, ngành, địa phương.

Năm 2020, 100% cán bộ, công chức trong cơ quan nhà nước được cấp chứng thư số phục vụ quản lý, điều hành, tác nghiệp trên môi trường mạng. Năm 2025, đạt tỷ lệ 60% cán bộ, công chức, viên chức trong cơ quan hành chính nhà nước các cấp được cấp chứng thư số phục vụ quản lý, điều hành, tác nghiệp trên môi trường mạng.

Hỗ trợ 100% các cơ quan hành chính nhà nước cấp Vụ, Cục, Sở và tương đương trở lên hoàn thành tích hợp chữ ký số chuyên dùng Chính phủ trên hệ thống quản lý văn bản và điều hành phục vụ gửi, nhận văn bản điện tử đến năm 2020.

Hoàn thành xây dựng và triển khai Đề án triển khai các hệ thống bảo vệ thông tin thuộc phạm vi bí mật nhà nước dùng mật mã đáp ứng yêu cầu triển khai Chính phủ điện tử và đề án triển khai Đề án Xây dựng Trung tâm an toàn thông tin mạng cho Hệ thống Chính phủ điện tử trong năm 2020.

Phấn đấu đạt tỷ lệ 100% cơ quan hành chính nhà nước các cấp hoàn thành tích hợp chữ ký số chuyên dùng Chính phủ trên Hệ thống quản lý văn bản và điều hành phục vụ gửi, nhận văn bản điện tử đến hết năm 2025.

100% doanh nghiệp có thể sử dụng dịch vụ công trực tuyến mức 4 về cấp giấy phép sản phẩm mật mã dân sự trong năm 2025.

Kết luận

Trong thời gian qua, được sự quan tâm của Đảng, Nhà nước, Quân ủy Trung ương và trực tiếp là đồng chí Bộ trưởng Bộ Quốc phòng, cùng với sự nỗ lực phấn đấu của cán bộ, nhân viên các Hệ Cơ yếu, các cơ quan, đơn vị thuộc Ban, Ngành Cơ yếu Việt Nam đã hoàn thành nhiều nhiệm vụ trên các mặt công tác, bảo đảm thông tin lãnh đạo, chỉ đạo, chỉ huy của Đảng, Nhà nước và lực lượng vũ trang được bí mật, chính xác, kịp thời trong mọi tình huống và các nhiệm vụ đột xuất trong thời kỳ mới. Trong thời gian tới, Ban Cơ yếu Chính phủ sẽ đề cao quyết tâm góp phần xây dựng, phát triển Chính phủ điện tử tại Việt Nam, đảm bảo an toàn thông tin, an ninh mạng, đưa Việt Nam vào nhóm 4 nước dẫn đầu ASEAN trong xếp hạng Chính phủ điện tử.

Link tham khảo: http://antoanthongtin.vn/chinh-sach---chien-luoc/ban-co-yeu-chinh-phu-quyet-tam-trien-khai-xay-dung-phat-trien-chinh-phu-dien-tu-105722

2. Camera an ninh – Nỗi lo bảo mật

Ngày nay, đi đâu chúng ta cũng thấy mọi nơi đều được lắp đặt camera an ninh, từ các trung tâm thương mại, đường phố, cơ quan, trường học, cửa hàng và đến cả

nhà riêng. Việc này phổ biến đến mức nhiều khi chúng ta quên mất rằng chính mình có thể bị giám sát ở bất kỳ đâu, kể cả là ở nhà.

Vụ việc lộ clip nhạy cảm được cho là của ca sĩ VMH mấy ngày gần đây đang làm dư luận lo lắng. Nghiêm trọng hơn, hình ảnh đưa lên cho thấy đây chính là nhà riêng của nạn nhân.

Điều kiện để truy cập và chiếm quyền điều khiển camera thì kẻ xấu cần phải kết nối được đến thiết bị camera đó, đồng thời phải qua mặt được khâu xác thực của camera. Chúng tôi đưa ra ba kịch bản mà kẻ xấu có thể sử dụng để truy cập vào hệ thống camera an ninh:

a. Lợi dụng việc chia sẻ kết nối mạng với những người xung quanh

Một điều khá phổ biến hiện nay là bạn có thể dễ dàng chia sẻ mật khẩu truy cập Wi-fi cho những người xung quanh. Khi đó, bạn sẽ tạo điều kiện những người này kết nối đến hệ thống camera trong nhà. Tiếp đó, kẻ xấu sẽ lợi dụng việc đặt mật khẩu yếu hoặc mặc định (được thiết lập khi lắp đặt camera) để truy cập vào thiết bị và thực hiện việc giám sát camera.

Thay vì là hệ thống giám sát an ninh, camera lại trở thành công cụ theo dõi chính người chủ của ngôi nhà.

b. Cho, tặng, nhượng lại thiết bị nhưng không xóa phần mềm xem CAM hoặc bị lộ tài khoản xem CAM

Khi lắp đặt camera an ninh, thường thì người dùng sẽ được cài đặt một ứng dụng và cấp tài khoản để xem hình ảnh trên điện thoại hoặc máy tính bảng. Nhưng đôi khi, người dùng cho, tặng hoặc chuyển nhượng các thiết bị này lại quên mất cần phải xóa ứng dụng, dữ liệu của mình đi, vì vậy họ đã vô tình đưa công cụ, phần mềm xem dữ liệu camera cho người khác. Và với ai có ý đồ xấu thì họ sẽ lợi dụng để trích xuất dữ liệu.

c. Camera cho phép xem từ Internet trên thiết bị tồn tại lỗ hổng bảo mật

Do hệ thống camera có kết nối Internet nên kẻ xấu có thể kết nối được đến thiết bị đó. Tên này sẽ lợi dụng lỗ hổng bảo mật (lỗi từ nhà sản xuất) để xâm nhập vào hệ thống camera từ xa và xem được các hình ảnh riêng tư, nhạy cảm mà không cần thông tin đăng nhập.

Các hành vi truy cập trái phép vào hệ thống camera của cá nhân tổ chức là vi phạm Luật an ninh mạng. Những người phát tán các hình ảnh riêng tư và nhạy cảm trên Internet sẽ chịu hình phạt từ việc phạt hành chính đến nặng hơn là truy cứu hình sự tùy theo mức độ vi phạm.

Khuyến nghị:

Phòng ATTT khuyến nghị:

- Ngay sau khi lắp đặt thiết bị mạng, camera cần đổi ngay mật khẩu truy cập, tránh để mật khẩu mặc định, mật khẩu cần phải đủ mạnh.

- Hạn chế chia sẻ kết nối Wi-fi gia đình, việc chia sẻ này là không thể kiểm soát được, vì trên thị trường hiện nay có ứng dụng chia sẻ Wi-fi trên các kho ứng dụng có thể chia sẻ cho bất kỳ ai ở trong phạm vị phát sóng Wi-fi.

- Khi không sử dụng thiết bị cá nhân, nên xóa toàn bộ dữ liệu trên thiết bị về trạng thái ban đầu (factory reset).

- Chọn các thiết bị mạng, camera từ những nhà sản xuất có thương hiệu, có nguồn gốc rõ ràng.

- Không cài đặt app từ các kho ứng dụng không chính thống để tránh bị cài đặt phần mềm theo dõi, đánh cắp thông tin.

- Cài đặt thường trực phần mềm an ninh trên thiết bị (điện thoại, máy tính, máy tính bảng) để bảo vệ trước các nguy cơ tấn công mạng.

- Thường xuyên cập nhật bản vá của các thiết bị, đồng thời không tiếp tay cho kẻ xấu phát tán những hình ảnh riêng tư, nhạy cảm.

Link tham khảo: https://whitehat.vn/threads/camera-an-ninh-%E2%80%93-noi-lo-bao-mat.13108/

3. Các mã độc tống tiền khiến hàng trăm thành phố lớn điêu đứng năm 2019

Có ít nhất 174 thành phố, với hơn 3.000 tổ chức đã bị ransomware tấn công trong năm 2019. Thiệt hại gây ra bởi các cuộc tấn công ransomware ước tính rất lớn.

Số lượng này tương đương mức tăng ít nhất 60% so với năm 2018. Yêu cầu tiền chuộc của tin tặc có thể lên đến 5.000.000 USD tùy trường hợp, tuy nhiên chi phí thực tế và thiệt hại gây ra bởi các cuộc tấn công mạng ước tính sẽ lớn hơn nhiều.

Phát hiện này nằm trong Bản tin bảo mật của Kaspersky "Kaspersky's Security Bulletin: Story of the Year 2019".

Tấn công ransomware là vấn đề nhức nhối, ảnh hưởng không nhỏ đến các doanh nghiệp trên toàn thế giới trong nhiều năm qua. Năm 2019 đã chứng kiến sự phát triển nhanh chóng của một xu hướng đã hình thành trước đó, khi các tin tặc nhắm mục tiêu tấn công mã độc vào những tổ chức lớn.

Các nhà nghiên cứu cho biết mặc dù những mục tiêu bị tấn công ít có khả năng chi trả cho một khoản tiền chuộc lớn, nhưng họ có xu hướng đồng ý với các yêu cầu mà tin tặc đưa ra - như chặn một dịch vụ nào đó của thành phố. Việc này sẽ ảnh hưởng trực tiếp đến phúc lợi của công dân, cũng như dẫn đến hậu quả không chỉ về tài chính mà cả những vấn đề xã hội nhạy cảm khác.

Theo số liệu được công khai, hiện tại số tiền chuộc ở nhiều mức khác nhau, có thể lên đến 5.300.000 USD tùy trường hợp. Các nhà nghiên cứu cho rằng những số liệu này không thể hiện chính xác chi phí cuối cùng cần chi trả cho một cuộc tấn công, vì hậu quả chúng gây ra sẽ kéo dài và nặng nề hơn nhiều.

"Xu hướng tấn công vào các thành phố đang tăng lên, tuy nhiên chúng có thể bị kìm hãm và ngăn chặn bằng việc điều chỉnh cách tiếp cận với bảo mật mạng. Quan trọng hơn hết là nên từ chối trả tiền chuộc và đưa ra quyết định này như một tuyên bố chính thức", ông Fedor Sinitsyn, Nhà nghiên cứu bảo mật tại Kaspersky cho biết.

Các phần mềm độc hại đến từ các thủ phạm khác nhau, tuy nhiên, ba họ mã độc khét tiếng nhất, theo các nhà nghiên cứu của Kaspersky là: Ryuk, Purga và Stop.

Ryuk xuất hiện hơn một năm trước, và kể từ đó, Ryuk đã hoạt động trên toàn thế giới, cả về tấn công tổ chức và cá nhân. Mô hình phát tán của Ryuk thường thông qua mã độc cửa sau, từ đó lây lan bằng các phương tiện phishing với tệp đính kèm độc hại được ngụy trang dưới dạng tài liệu tài chính.

Purga đã được biết đến từ năm 2016, nhưng chỉ gần đây, các thành phố mới được phát hiện là nạn nhân của trojan này. Purga có nhiều vector tấn công khác nhau - từ lừa đảo đến tấn công dò mật khẩu.

Stop cryptor là mã độc mới xuất hiện được 1 năm. Chúng được phát tán bằng cách ẩn bên trong trình cài đặt phần mềm. Phần mềm độc hại này đang trở nên phổ biến, đứng thứ 7 trong số 10 họ mã độc Trojan phổ biến nhất theo bảng xếp hạng Q3 2019.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng Android cần cập nhật bản vá mới nhất của Twitter để đảm bảo an toàn thông tin.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/bao-mat/cac-ma-doc-tong-tien-khet-tieng-khien-hang-tram-thanh-pho-lon-dieu-dung-nam-2019-603679.html

TECHNICAL PAGES:

1. Chi tiết về thông tin một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam trong tuần, cụ thể như sau:

STT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Advantech	CVE-2019-18257	01 lỗ hổng trên phần mềm Advantech (Advantech DiagAnywhere Server) cho phép đối tượng tấn công chèn và thực thi mã tùy ý.	Đã có thông tin xác nhận và bản vá.
2	Apple	CVE-2019-6232 CVE-2019-8802 CVE-2019-8590 …	Nhóm 245 lỗ hổng trên một số sản phẩm, ứng dụng của Apple (iCloud for Windows, macOS Catalina, Safari,…) cho phép đối tượng tấn công thu thập thông tin chèn và thực thi mã lệnh từ xa, tấn công từ chối dịch vụ. 25 lỗ hổng có điểm CVSS: 9.3 (nghiêm trọng).	Đã có thông tin xác nhận và bản vá
3	Linux	CVE-2019-19815 CVE-2019-19814 CVE-2019-19813 …	Nhóm 06 lỗ hổng trên hệ điều hành Linux (Linux kernel) cho phép đối tượng thực thi mã tùy ý.	Đã có thông tin xác nhận và bản vá
4	Apache	CVE-2019-12413 CVE-2019-12414 CVE-2019-15600 …	Nhóm 06 lỗ hổng trên phần mềm Apache (http-server, Xerces, Incubator Superset..) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã lệnh tùy ý.	Đã có thông tin xác nhận và bản vá
5	Huawei	CVE-2019-5278 CVE-2019-5248 CVE-2019-5250 …	Nhóm 11 trên thiết bị Huawei (Cloud Engine, CloudUSM-EUA, Mate 20 Pro…) cho phép đối tượng tấn công thu thập thông tin, thực thi mã lệnh từ xa, tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
6	Adobe	CVE-2019-8254 CVE-2019-8255 CVE-2019-16446 …	Nhóm 25 lỗ hổng trên phần mềm Adobe (ColdFusion, Acrobat and Reader, Photo shop CC) cho phép đối tượng	Chưa có thông tin xác nhận và bản vá

			tấn công thu thập thông tin, chèn và thực thi mã lệnh.	
7	Intel	CVE-2019-14599 CVE-2019-11088 CVE-2019-11131 …	Nhóm 40 lỗ hổng trên thiết bị Intel (Control Center-I, Intel® AMT,) cho phép đối tượng tấn công tấn công thu thập thông tin, tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
8	Qualcomm	CVE-2019-10607 CVE-2019-2274 CVE-2018-11980 …	Nhóm 28 lỗ hổng trên thiết bị Qualcomm (Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile…) cho phép đối tượng tấn công chèn và thực thi mã tùy ý.	Đã có thông tin xác nhận và bản vá

2. Danh sách IP/tên miền độc hại có nhiều kết nối từ Việt Nam

STT	**Tên miền/IP**
1	mel.cloudcontentsmak.com
2	strikotunrev.top
3	d3s1.me
4	localhost.localdomain
5	pudloxan.com

3. Các cán bộ kỹ thuật đầu mối về ATTT cần thực hiện:
   - Xử lý các lỗ hổng phát hiện tại bảng 1 (nếu có).
   - Chặn, xử lý các truy nhập tới các tên miền độc hại tại bảng 2.