BẢN TIN NỘI BỘ

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

1. Tình hình triển khai Chính phủ điện tử hướng tới Chính phủ số tại Việt Nam

Không nằm ngoài xu hướng tất yếu trên thế giới, Việt Nam bắt tay xây dựng, phát triển Chính phủ điện (CPĐT) từ năm 2000 và đã đạt được một số kết quả nhất định. Theo báo cáo của Liên hợp quốc năm 2018, Chỉ số phát triển CPĐT của Việt Nam đứng thứ 88/193 quốc gia, vùng lãnh thổ và đứng thứ 6 trong khu vực Đông Nam Á (ASEAN). Dưới đây là một số thành quả bước đầu mà nước ta đã đạt được trong công cuộc xây dựng và phát triển CPĐT thời gian qua.

Kiện toàn Ủy ban quốc gia về Chính phủ điện tử và Tổ công tác giúp việc

Ngày 16/9/2019, Thủ tướng Chính phủ đã ký Quyết định số 1201/QĐ-TTg giao Bộ TT&TT là cơ quan đầu mối, giúp Ủy ban quốc gia về CPĐT điều phối công tác xây dựng, phát triển CPĐT; bảo đảm các điều kiện cần thiết cho hoạt động của Ủy ban và Tổ công tác. Theo đó, Bộ trưởng Bộ TT&TT có trách nhiệm phê duyệt danh sách, thành viên Tổ công tác và làm nhiệm vụ thường trực Tổ công tác.

Ngày 03/12/2019, Thủ tướng Chính phủ đã ký Quyết định số 1737/QĐ-TTg phê duyệt Danh sách thành viên Ủy ban Quốc gia về CPĐT và lãnh đạo Tổ công tác giúp việc Ủy ban về CPĐT. Trong đó, Chủ tịch Ủy ban là Thủ tướng Chính phủ; Phó Chủ tịch thường trực là Phó Thủ tướng Vũ Đức Đam; Bộ trưởng Bộ TT&TT là Phó Chủ tịch sẽ chịu trách nhiệm trước Chính phủ, Thủ tướng Chính phủ về xây dựng CPĐT; Đồng chí Trung tướng Đặng Vũ Sơn, Trưởng ban Ban Cơ yếu Chính phủ là Thành viên UBQG về CPĐT....

Về nhân sự Tổ công tác, Tổ trưởng là Bộ trưởng Bộ TT&TT; Các Tổ phó bao gồm: Thứ trưởng Bộ TT&TT: Nguyễn Thành Hưng và Phạm Anh Tuấn, Phó Chủ tịch UB Quản lý vốn nhà nước tại doanh nghiệp Hồ Sỹ Hùng.

Ngay sau đó, ngày 25/12/2019, Bộ trưởng Bộ TT&TT đã ký Quyết định số 2250/QĐ-BTTTT phê duyệt Danh sách thành viên và lãnh đạo các nhóm của Tổ công tác giúp việc UBQG về CPĐT, bao gồm 40 thành viên chia thành 04 nhóm: Nhóm thường trực; Nhóm An toàn, an ninh mạng; Nhóm Chính sách và thể chế; Nhóm Dữ liệu. Trong đó có 03 đồng chí thuộc Ban Cơ yếu Chính phủ là: Cục trưởng Nguyễn Hữu Hùng, Phó Cục trưởng Lê Quang Tùng (Cục Chứng thực số và Bảo mật thông tin) và Phó Cục trưởng Đặng Duy Mẫn (Cục Cơ yếu Đảng - Chính quyền). Cục Tin học hóa, Bộ TT&TT chịu trách nhiệm bảo đảm các điều kiện hoạt động của Tổ công tác.

Khai trương Cổng dịch vụ công quốc gia

Ngày 09/12/2019, Văn phòng Chính phủ đã tổ chức Lễ khai trương Cổng dịch vụ công quốc gia tại địa chỉ www.dichvucong.gov.vn với sự tham dự của Thủ tướng Nguyễn Xuân Phúc và trực tuyến tới 63 điểm cầu trên toàn quốc. Cổng dịch vụ công quốc gia là địa chỉ cho phép người dân và doanh nghiệp sử dụng một tài khoản duy nhất để truy cập dịch vụ công trực tuyến, theo dõi tình hình, đánh giá chất lượng giải

quyết và gửi phản ánh kiến nghị, không phụ thuộc vào thời gian và địa giới hành chính (Bước đầu là 8 dịch vụ trực tuyến) của tất cả các cổng dịch vụ công cấp Bộ/tỉnh.

Phê duyệt Khung kiến trúc Chính phủ điện tử 2.0

Thực hiện nhiệm vụ Thủ tướng Chính phủ giao, ngày 21/4/2015, Bộ TT&TT đã xây dựng, công bố Khung Kiến trúc Chính phủ điện tử Việt Nam phiên bản 1.0; tổ chức hướng dẫn các Bộ, ngành, địa phương xây dựng kiến trúc chi tiết của Bộ, ngành, địa phương nhằm áp dụng trong quá trình xây dựng CPĐT, CQĐT hướng tới tích hợp, kết nối các hệ thống thông tin, cơ sở dữ liệu, tránh đầu tư trùng lặp. Sau hơn 3 năm thực hiện, đến nay đa số các Bộ, ngành, địa phương đã xây dựng được kiến trúc (CPĐT đối với cấp bộ và chính quyền điện tử đối với cấp tỉnh), thực hiện duy trì, phát triển kiến trúc.

Tuy nhiên, trong cuộc Cách mạng công nghiệp 4.0, các quốc gia trên thế giới đang ứng dụng công nghệ mới để xây dựng, phát triển CPĐT. Vì vậy, Khung Kiến trúc Chính phủ điện tử Việt Nam cần được cập nhật phù hợp với xu thế này. Trong bối cảnh đó, tại Nghị quyết số 17/NQ-CP ngày 07/3/2019 của Chính phủ về một số nhiệm vụ, giải pháp trọng tâm phát triển Chính phủ điện tử giai đoạn 2019 - 2020, định hướng đến 2025, Bộ TT&TT đã được giao nhiệm vụ hoàn thành cập nhật Khung Kiến trúc Chính phủ điện tử Việt Nam, phiên bản 2.0.

Ngày 31/12/2019, Bộ trưởng Bộ TT&TT đã ký quyết định số 2323/QĐ-BTTT phê duyệt Khung kiến trúc Chính phủ điện tử Việt Nam 2.0. Những điểm mới chủ yếu của phiên bản 2.0 so với phiên bản 1.0 là: Khung Kiến trúc CPĐT phiên bản 2.0 được xây dựng phù hợp với thông lệ quốc tế và xu hướng phát triển CPĐT hướng tới chính phủ số; bổ sung các nguyên tắc xây dựng Kiến trúc CPĐT; bổ sung định hướng phát triển CPĐT của quốc gia; bổ sung khái niệm về Khung Kiến trúc CPĐT Việt Nam, Kiến trúc CPĐT cấp Bộ, Kiến trúc CQĐT cấp tỉnh; bổ sung các mô hình tham chiếu.

Bên cạnh đó, Khung Kiến trúc CPĐT Việt Nam phiên bản 2.0 còn thể hiện rõ mô hình kết nối CPĐT Việt Nam, mô tả tóm tắt các thành phần (bao gồm một số hệ thống lớn của quốc gia); cập nhật một số nội dung về các xu thế phát triển công nghệ như điện toán đám mây, dữ liệu lớn, trí tuệ nhân tạo…; thống nhất sử dụng Mạng truyền số liệu chuyên dùng của Đảng và Nhà nước làm hạ tầng truyền dẫn trong CPĐT Việt Nam; bổ sung nội dung an toàn thông tin mạng; bổ sung phương pháp tiếp cận Kiến trúc CPĐT và khung tham chiếu tương hợp.

Khai trương Hệ thống thông tin báo cáo Chính phủ

Ngày 22/01/2020, Bộ trưởng, Chủ nhiệm VPCP đã ký quyết định số 62/QĐ-VPCP phê duyệt Đề án xây dựng Hệ thống thông tin báo cáo Chính phủ và Trung tâm thông tin phục vụ sự chỉ đạo, điều hành của Chính phủ, Thủ tướng Chính phủ.

Ngày 07/02/2020, Văn phòng Chính phủ đã tổ chức Hội nghị trực tuyến toàn quốc triển khai Hệ thống thông tin báo cáo Chính phủ, quán triệt Nghị định 09/2019/NĐ-CP của Chính phủ quy định về chế độ báo cáo của cơ quan hành chính nhà nước.

Trước đó, ngày 12/7/2018, Thủ tướng Chính phủ đã ban hành Quyết định số 28/2018/QĐ-TTg về việc gửi, nhận văn bản điện tử giữa các cơ quan trong hệ thống hành chính nhà nước. Đây là căn cứ pháp lý quan trọng để các cơ quan nhà nước tăng cường sử dụng văn bản điện tử, tiến tới giảm thiểu tối đa công tác văn bản hóa, hướng tới xây dựng CPĐT và nền kinh tế số. Quyết định số 28/2018/QĐ-TTg được ban hành nhằm quy định việc gửi, nhận văn bản điện tử thông qua kết nối, liên thông các hệ thống quản lý văn bản và điều hành giữa các cơ quan trong hệ thống hành chính nhà nước. Quyết định này áp dụng đối với các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các cấp và các cơ quan, đơn vị trực thuộc và không áp dụng đối với việc gửi, nhận văn bản điện tử có nội dung thuộc bí mật nhà nước theo quy định của pháp luật.

Đồng thời, Hệ thống thông tin báo cáo Chính phủ cũng được giới thiệu tới các Bộ, ngành, địa phương và đề nghị các Bộ, ngành, địa phương tích cực chuẩn hóa chế độ báo cáo, xây dựng Hệ thống báo cáo quốc gia và tích hợp với Hệ thống thông tin báo cáo Chính phủ. Hệ thống chính thức khai trương ngày 13/3/2020.

Ban hành Danh mục văn bản điện tử không gửi kèm văn bản giấy

Ngày 04/02/2020, Văn phòng Chính phủ đã có văn bản số 775/VPCP-KSTT về Danh mục văn bản điện tử không gửi kèm văn bản giấy, đề nghị các Bộ, ngành, địa phương gửi văn bản điện tử không kèm văn bản giấy giữa các cơ quan hành chính nhà nước đối với 26 loại văn bản gồm: 04 loại văn bản quy phạm pháp luật và 22 loại văn bản hành chính. Thời gian bắt đầu thực hiện từ ngày 15/02/2020.

Tổ chức hội nghị trực tuyến lần thứ 3 về Chính phủ điện tử

Ngày 12/02/2020, Thủ tướng Chính phủ đã chủ trì Hội nghị UBQG về CPĐT và các Ban chỉ đạo CPĐT, Chính quyền điện tử các Bộ, ngành, địa phương. Hội nghị đã đánh giá kết quả thực hiện triển khai CPĐT năm 2019, xác định các hạn chế, tồn tại cần giải quyết và định hướng các nhiệm vụ trọng tâm về triển khai CPĐT năm 2020, trong đó tập trung vào các nhiệm vụ chính: Hoàn thiện thể chế; Hoàn thiện các yếu tố nền tảng; Xây dựng mạng truyền số liệu chuyên dùng thành nền tảng số; Xây dựng trung tâm giám sát quốc gia về CPĐT; Thương mại hóa 5G, ưu tiên nền tảng di động.

Thủ tướng Chính phủ đã đồng ý UBQG về CPĐT sẽ đồng thời chỉ đạo các nội dung triển khai tới Chính phủ số, Thành phố thông minh, Chuyển đổi số và Kinh tế số. Bộ TT&TT là cơ quan điều phối thống nhất về CPĐT.

Link tham khảo: http://antoanthongtin.vn/ca-cqnn/tinh-hinh-trien-khai-chinh-phu-dien-tu-huong-toi-chinh-phu-so-tai-viet-nam-105901

2. Giả danh chỉ thị Thủ tướng về Covid-19 để phát tán mã độc

Để thu hút sự chú ý, tin tặc đã phát tán mã độc qua thư điện tử có đính kèm tập tin word với tiêu đề “Chi Thi cua Thu tuong nguyen xuan phuc”.

heo Cổng thông tin điện tử Bộ Công an, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (Bộ Công an) mới đây đã phát hiện một chiến dịch tấn công mạng, phát tán mã độc qua thư điện tử (Email).

Đáng chú ý, tin tặc sử dụng các thông tin liên quan đến dịch bệnh Covid-19 để thu hút sự chú ý từ người dùng. Tin tặc thậm chí còn phát tán cả mã độc qua thư điện tử có đính kèm tập tin word với tiêu đề "Chi Thi cua Thu tuong nguyen xuan phuc.lnk" nhằm giả dạng thông báo của Thủ tướng Chính phủ về dịch Covid-19.

Tập tin có dạng shortcut với phần mở rộng là ".lnk" được ngụy trang dưới biểu tượng tập tin văn bản nhằm đánh lừa người dùng. Nếu người dùng tải tập tin đính kèm về và mở trên máy tính, mã độc sẽ được kích hoạt.

Mã độc này chỉ hoạt động trên hệ điều hành Windows. Khi được cài đặt vào máy tính, mã độc này sẽ kết nối đến máy chủ điều khiển để tải các đoạn mã độc khác và nhận lệnh điều khiển của tin tặc, đồng thời, mở tập tin văn bản để đánh lừa người dùng.

Lúc này, tin tặc có thể thực hiện nhiều lệnh thực thi khác nhau như đánh cắp dữ liệu, thông tin máy tính, sử dụng để tiếp tục phát tán sang máy tính khác...

Theo nhận định của Bộ Công an, trong bối cảnh bùng phát của dịch bệnh Covid-19, một số nhóm tin tặc đã lợi dụng tình hình này để phát động, tiến hành chiến dịch tấn công mạng có chủ đích vào các cơ quan, tổ chức trên thế giới, trong đó có Việt Nam.

Do vậy, để phòng, chống không bị tin tặc tấn công, người sử dụng Internet cần nâng cao cảnh giác, không truy cập vào những đường link lạ, không tải và mở về các tập tin không rõ nguồn gốc.

Bên cạnh đó, người dùng cần cài đặt các phần mềm diệt virus có bản quyền và thường xuyên cập nhật cơ sở dữ liệu, bản vá bảo mật cho hệ điều hành và các phần mềm ứng dụng. Trong trường hợp đã mở tệp tin đính kèm, cần ngắt kết nối Internet và liên hệ với bộ phận quản trị để khắc phục, xử lý.

Khuyến nghị: Người dùng cần tuân thủ các quy định đã ban hành và không ấn vào các đường link lạ, các tập tin không rõ nguồn gốc để đảm bảo an toàn thông tin.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/bao-mat/gia-danh-chi-thi-thu-tuong-ve-covid-19-de-phat-tan-ma-doc-625451.html

3. Cisco cảnh báo các lỗ hổng nghiêm trọng trong phần mềm SD-WAN

Các lỗ hổng nghiêm trọng tồn tại trong các sản phẩm của Cisco sử dụng phần mềm SD-WAN phiên bản trước 19.2.2.

Cisco vừa khắc phục ba lỗ hổng nghiêm trọng cao trong giải pháp mạng được điều khiển bởi phần mềm (SD-WAN) dành cho người dùng doanh nghiệp. Nếu bị khai thác, các lỗ hổng có thể cho phép kẻ tấn công thực thi lệnh với quyền root trên các hệ thống bị ảnh hưởng. Để khai thác lỗ hổng, kẻ tấn công trước tiên cần phải được xác thực trong mạng nội bộ.

Ba lỗ hổng tồn tại trong các sản phẩm phần cứng và phần mềm khác nhau của Cisco mà có sử dụng phần mềm SD-WAN phiên bản trước 19.2.2. Phần cứng bao gồm các giải pháp SD-WAN: Bộ điều khiển vBond và vSmart (thực hiện kết nối mạng), hệ thống Quản lý mạng vManage (nền tảng quản lý tập trung) và phần mềm

vBond Orchestrator (thực hiện xác thực tất cả các yếu tố trong mạng). vEdge và nền tảng định tuyến đám mây vEdge tương ứng cũng bị ảnh hưởng.

Cisco cho biết chưa phát hiện bất kỳ cuộc tấn công lợi dụng các lỗ hổng.

Lỗi nghiêm trọng nhất là lỗi xác thực đầu vào không đầy đủ (CVE-2020-3266) trong Giao diện dòng lệnh (CLI) của SD-WAN. CLI là giao diện dựa trên văn bản, được sử dụng để vận hành phần mềm và cho phép người dùng nhập các lệnh đơn vào giao diện. Mặc dù lỗ hổng chỉ có thể bị khai thác bởi những kẻ tấn công đã được xác thực trong mạng nội bộ, nhưng nếu bị khai thác, nó sẽ cho phép kẻ tấn công thực thi các lệnh với quyền root.

Lỗ hổng này có điểm CVSS 7.8.

Lỗ hổng thứ hai (CVE-2020-3264) là lỗ hổng tràn bộ đệm cũng xuất phát từ việc xác nhận đầu vào không đầy đủ trong phần mềm. Lỗ hổng này có thể cho phép kẻ tấn công cục bộ, đã được xác thực có được quyền truy cập vào thông tin mà họ không được phép truy cập và thực hiện các thay đổi đối với hệ thống mà họ không được phép thực hiện.

Kẻ tấn công có thể khai thác lỗ hổng bằng cách gửi lưu lượng truy cập tự tạo đến một thiết bị bị ảnh hưởng. Lỗ hổng có điểm CVSS 7.1.

Lỗ hổng cuối cùng (CVE-2020-3265) là một lỗ hổng leo thang đặc quyền trong phần mềm SD-WAN có thể cho phép kẻ tấn công cục bộ, đã được xác thực nâng cao đặc quyền, cuối cùng giành được đặc quyền root của hệ điều hành. Lỗ hổng này có điểm CVSS là 7.0.

Khuyến nghị: Người quản trị cần cập nhật các bản vá mới nhất của các sản phẩm nêu trên để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/cisco-canh-bao-cac-lo-hong-nghiem-trong-trong-phan-mem-sd-wan.13380/

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	Apache	CVE 2020 1947 CVE 2020 1953	Nhóm 02 lỗ hổng trên phần mềm Apache (Apache Commons Configuration) cho phép đối tượng tấn công chèn và thực thi mã từ xa.	Đã có thông tin xác nhận và bản vá.
2	Dell	CVE 2020 5342 CVE 2020 5328 CVE 2020 5327 …	Nhóm 08 lỗ hổng trên thiết bị của Dell (Dell Digital Delivery, Dell EMC Isilon OneFS…) cho phép đối tượng tấn công chèn và thực thi mã từ xa.	Đã có thông tin xác nhận và bản vá
3	D-link	CVE 2016 11021 CVE 2020 10215 CVE 2020 10214 …	Nhóm 05 lỗ hổng trên thiết bị D link (D link DCS 930L, DIR 825…) cho phép đối tượng tấn công tấn chèn và thực thi mã từ xa.	Đã có thông tin xác nhận và bản vá
4	Android	CVE 2020 0011 CVE 2020 0037 CVE 2020 0038 …	Nhóm 42 lỗ hổng hệ điều hành Android(rw_i93_sm_update_ndef,…) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã từ xa, tấn công SQL injection.	Đã có thông tin xác nhận và bản vá
5	Wordpress	CVE 2020 10257 CVE 2020 8435 CVE 2018 14502 …	Nhóm 08 lỗ hổng trên phần mềm Wordpress (ThemeREX Addons plugin,…) cho phép đối tượng tấn công chèn và thực thi mã tùy ý, tấn công SQL injection, tấn công CSRF.	Đã có thông tin xác nhận và bản vá
6	Citrix	CVE 2020 10112 CVE 2020 10111 CVE 2020 10110 CVE 2019 11345	Nhóm 04 lỗ hổng trên sản phẩm của Citrix (Citrix Gateway,…) cho phép đối tượng tấn công tấn công thu thập thông tin, tấn công XSS, tấn công Cache Poisoning.	Đã có thông tin xác nhận và bản vá
7	Gitlab	CVE 2019 12443 CVE 2019 12428 CVE 2019 13010	Nhóm 45 lỗ hổng trên sản phẩm của Gitlab (Gitlab Community Enterprise Edition…) cho phép đối tượng	Đã có thông tin xác nhận và bản vá

			tấn công thu thập thông tin, tấn công XSS, tấn công Command Injection	
8	Jenkins	CVE 2020 2159 CVE 2020 2143 CVE 2020 2140 …	Nhóm 25 lỗ hổng trong phần mềm Jenkins (Jenkins CryptoMove Plugin,…) cho phép đối tượng tấn công tấn công XSS, tấn công man in the middle, chèn và thực thi mã tùy ý, tấn công XML External Entity Processing.	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	disorderstatus.ru
2	differentia.ru
3	atomictrivia.ru
4	iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
5	ydbnsrt.me
6	tttta.sssaaaas.io
7	track.saygggggames.io
8	xdqzpbcgrvkj.ru
9	xjpakmdcfuqe.in
10	xjpakmdcfuqe.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.