BẢN TIN NỘI BỘ

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

1. Khai trương Cổng Dịch vụ công Quốc gia

Ngày 07/12/2019, Văn phòng Chính phủ đã tổ chức Họp báo thông tin về khai trương Cổng dịch vụ công quốc gia. Đồng chí Mai Tiến Dũng, Ủy viên Trung ương Đảng, Bộ trưởng Chủ nhiệm Văn phòng Chính phủ đã tham dự và chủ trì buổi Họp báo.

Tham dự buổi Họp báo còn có đại diện Tổng cục đường bộ, Bộ Giao thông Vận tải; Cục Thương mại điện tử và Kinh tế số, Bộ Công Thương; Tập đoàn Điện lực Việt Nam; Tập đoàn Bưu chính Viễn thông Việt Nam (VNPT); Cục Kiểm soát thủ tục hành chính, Văn phòng Chính phủ (VPCP); Cơ quan Phát triển Pháp.

Đồng chí Mai Tiến Dũng cho biết, theo dự kiến, chiều 09/12, Thủ tướng Chính phủ sẽ khai trương Cổng dịch vụ công quốc gia (Cổng DVCQG). Đây là dấu ấn rất quan trọng với mục tiêu Chính phủ hướng tới người dân và doanh nghiệp.

Tại buổi Họp báo, ông Ngô Hải Phan, Cục trưởng Cục Kiểm soát thủ tục hành chính, VPCP đã báo cáo về công tác chuẩn bị và nội dung của Cổng DVCQG.

Cổng DVCQG có vai trò quan trọng trong xây dựng Chính phủ điện tử. Đây là hệ thống kết nối Chính phủ với người dân và doanh nghiệp qua phương thức điện tử. Nhận thức rõ vai trò của Cổng DVCQG, Chính phủ, Thủ tướng Chính phủ đã giao VPCP chủ trì, phối hợp với các Bộ, ngành, địa phương xây dựng Cổng DVCQG, với mong muốn tạo dựng một địa chỉ hỗ trợ, cung cấp thông tin và thủ tục hành chính dịch vụ công liên tục, chính xác, hiệu quả, thể hiện tinh thần phục vụ của Chính phủ.

VPCP đã phối hợp với các Bộ, ngành, địa phương, các doanh nghiệp công nghệ thông tin, các doanh nghiệp cung ứng dịch vụ công ích, các tổ chức quốc tế, chuyên gia trong và ngoài nước để nghiên cứu, xây dựng Cổng DVCQG trên cơ sở bám sát quy định tại Nghị định số 61/2018/NĐ-CP của Chính phủ về thực hiện cơ chế một cửa, một cửa liên thông trong giải quyết thủ tục hành chính và Quyết định số 274/QĐ-TTg của Thủ tướng Chính phủ phê duyệt Đề án Cổng DVCQG.

Sau 9 tháng tích cực triển khai, việc thiết lập Cổng DVCQG về cơ bản đã hoàn thành. Cổng DVCQG bao gồm 6 cấu phần chính:

- Cơ sở dữ liệu quốc gia về thủ tục hành chính và Bộ câu hỏi/trả lời liên quan đến thủ tục hành chính. Những thủ tục, dịch vụ công thiết yếu liên quan với vòng đời của một công dân, doanh nghiệp đều được cung cấp công khai, chính xác, kịp thời trên Cổng DVCQG.

- Nền tảng xác thực, đăng nhập một lần kết nối với các Cổng dịch vụ công cấp Bộ, cấp tỉnh và Hệ thống thông tin một cửa cấp Bộ, cấp tỉnh.

- Nền tảng thanh toán trực tuyến để phục vụ cho việc thanh toán trực tuyến của dịch vụ công.

- Hệ thống phản ánh, kiến nghị của người dân, doanh nghiệp để kịp thời phản ánh, kiến nghị đến cơ quan, nhà nước có thẩm quyền về hành vi chậm trễ, thực hiện

không đúng các quy định về thủ tục hành chính và những cơ chế, chính sách vướng mắc trong quá trình thực hiện.

- Tích hợp các dịch vụ công trực tuyến của các Bộ, ngành, địa phương trên cơ sở những dịch vụ công nào đã được tái cấu trúc quy trình thật sự đơn giản, thuận lợi thì mới được tích hợp lên Cổng DVCQG.

- Hệ thống hỗ trợ trực tuyến và Tổng đài hỗ trợ.

Cổng DVCQG cung cấp 7 chức năng chính như sau:

- Chức năng đăng nhập một lần, sử dụng một tài khoản của Cổng DVCQG để đăng nhập Cổng dịch vụ công của Bộ, ngành, địa phương.

- Tra cứu về thông tin thủ tục hành chính, dịch vụ công của tất cả các ngành, lĩnh vực, các địa phương trên toàn quốc.

- Theo dõi chi tiết toàn bộ quá trình giải quyết thủ tục hành chính, dịch vụ công.

- Hỗ trợ thực hiện thủ tục hành chính, dịch vụ công theo hướng cá nhân hóa thông tin người dùng, cung cấp các tiện ích liên quan đến việc thực hiện dịch vụ công.

- Tiếp nhận, phản ánh kiến nghị liên quan đến việc giải quyết thủ tục hành chính; các quy định về cơ chế, chính sách, thủ tục hành chính; các sáng kiến, cải cách, chuyển xử lý và theo dõi chi tiết tình trạng xử lý của các Bộ, ngành, địa phương.

- Thanh toán trực tuyến các phí, lệ phí thực hiện thủ tục hành chính dịch vụ công sử dụng tài khoản của các ngân hàng và các trung gian thanh toán.

- Đánh giá sự hài lòng của người dân, doanh nghiệp trong giải quyết thủ tục hành chính dịch vụ công, cũng như thực hiện phản ánh kiến nghị.

Các giải pháp, chức năng trên Cổng DVCQG được các chuyên gia trong nước và quốc tế đánh giá bảo đảm chất lượng, phù hợp với các tiêu chuẩn theo thông lệ quốc tế. VPCP đã phối hợp với Bộ Công an và Bộ TT&TT đánh giá mức độ an toàn, an ninh thông tin của Cổng DVCQG và đã sẵn sàng các giải pháp bảo vệ, đối phó, ứng cứu, bảo đảm an toàn, an ninh thông tin. Ngoài vai trò của Bộ Công an và Bộ TT&TT, Bộ Tư lệnh 86 và Ban Cơ yếu Chính phủ đã tích cực phối hợp trong việc đảm bảo an toàn, an ninh thông tin cho Hệ thống.

Cùng với VPCP, các Bộ, ngành, địa phương đã rất tích cực trong việc rà soát, chuẩn hóa cơ sở dữ liệu quốc gia về thủ tục hành chính; nâng cấp, tích hợp, cung cấp các dịch vụ công trực tuyến trên Cổng DVCQG; xây dựng các bộ câu hỏi/trả lời với ngôn ngữ đời sống dễ hiểu để hỗ trợ giải quyết các thủ tục hành chính cho người dân, doanh nghiệp; xây dựng triển khai cổng dịch vụ công, hệ thống thông tin một cửa điện tử cấp Bộ, cấp tỉnh kết nối với Cổng DVCQG để kết nối, tích hợp, chia sẻ tình hình kết quả giải quyết hồ sơ thủ tục hành chính thuộc thẩm quyền của Bộ, ngành, địa phương.

Sau thời gian vận hành thử nghiệm, đến nay Cổng DVCQG đã đủ điều kiện và sẵn sàng đi vào hoạt động chính thức. Với phương châm lấy người dân, doanh nghiệp làm trung tâm phục vụ và không để lại ai ở phía sau, Cổng DVCQG là đầu mối giúp công khai, minh bạch các thông tin liên quan đến thủ tục hành chính và cung cấp, hỗ trợ thực hiện dịch vụ công theo nhu cầu sử dụng, phù hợp với từng đối tượng; đảm

bảo khả năng giám sát, kiểm tra, đánh giá của cá nhân, tổ chức và trách nhiệm giải trình của cơ quan nhà nước trong thực hiện dịch vụ công.

Chỉ cần truy cập một địa chỉ duy nhất (dichvucong.gov.vn) bằng một tài khoản duy nhất, người dân, doanh nghiệp có thể đăng nhập được đến tất cả các cổng dịch vụ công cấp Bộ, cấp tỉnh thực hiện dịch vụ công trực tuyến; theo dõi tình trạng giải quyết, đánh giá chất lượng giải quyết và gửi phản ánh, kiến nghị không phụ thuộc vào thời gian, địa giới hành chính.

Đồng thời với vai trò đầu mối kết nối với các cổng dịch vụ công, cơ sở dữ liệu thực hiện dịch vụ công trực tuyến qua Cổng DVCQG sẽ giúp người dân, doanh nghiệp thuận lợi hơn nhiều do có thể tái sử dụng các thông tin đã có và tiết kiệm thời gian chuẩn bị hồ sơ, từ đó giảm đáng kể chi phí xã hội trong thực hiện thủ tục hành chính, đặc biệt là những thủ tục hành chính có liên quan đến nhiều cơ quan tổ chức.

Theo tính toán, giả định số lượng giao dịch như của năm 2018, việc chuyển từ phương thức trực tiếp sang trực tuyến tại Cổng DVCQG sẽ tiết kiệm chi phí xã hội được 4.222 tỷ đồng/năm, trong đó tính riêng chi phí tiết kiệm được do thực hiện qua Cổng DVCQG mang lại khoảng 1.736 tỷ đồng. Con số này sẽ tiếp tục tăng lên, tỷ lệ thuận với số lượng dịch vụ công trực tuyến được tích hợp trên Cổng DVCQG.

Các nền tảng dữ liệu dùng chung cũng sẽ hạn chế được đầu tư dàn trải tại các Bộ, ngành, địa phương và giúp tăng cường hiệu quả quản lý nhà nước, giám sát, đánh giá việc giải quyết thủ tục hành chính, tăng trách nhiệm giải trình và năng lực phản ứng chính sách, thúc đẩy quá trình cải cách hành chính.

Cổng DVCQG hướng tới việc số hóa hồ sơ, giấy tờ giấy, chuyển hoạt động sử dụng hồ sơ, văn bản giấy, giao dịch trực tiếp sang hoạt động sử dụng hồ sơ, văn bản điện tử, giao dịch điện tử và cung cấp dịch vụ công không phụ thuộc vào thời gian, địa giới hành chính; thúc đẩy cải cách hành chính, nhất là cải cách thủ tục hành chính thông qua việc ứng dụng công nghệ thông tin; cải thiện vị trí của Việt Nam về chỉ số dịch vụ công trực tuyến trong chỉ số phát triển Chính phủ điện tử theo xếp hạng hàng năm của Liên hợp quốc.

Đồng chí Mai Tiến Dũng khẳng định, đây là đòi hỏi thực tiễn của người dân, doanh nghiệp. Khi người dân, doanh nghiệp thực hiện thủ tục ở cơ quan chính quyền, phải gặp trực tiếp và làm thủ tục nhiều lần tại nhiều cơ quan, đặc biệt là thủ tục hồ sơ kèm theo nhiều hồ sơ phụ. Như vậy, chi phí thời gian và công sức, chưa nói đến vấn đề tiêu cực đã tạo cho người dân và doanh nghiệp những khó khăn nhất định.

Ngoài ra, một số khó khăn khác có thể kể đến như, việc thực hiện dịch vụ công diễn ra trong điều kiện chưa hoàn thiện đồng bộ các vấn đề về thể chế, về cơ sở dữ liệu khiến việc triển khai. Người dân, doanh nghiệp vẫn còn mang tư tưởng truyền thống là đến làm thủ tục trực tiếp có thể an toàn và tin tưởng hơn. Cũng như những vấn đề về ứng dụng công nghệ của người dân, vấn đề thiết bị, trình độ kiến thức,... Đây chính là những rào cản trong việc triển khai Cổng DVCQG.

Cổng DVCQG chính là sự quyết tâm đặc biệt, sát sao của Thủ tướng Chính phủ. Trong công cuộc cách mạng công nghiệp 4.0, Thủ tướng chỉ đạo phải tập trung vào

vấn đề ứng dụng công nghệ thông tin. Quan trọng hơn, ngoài việc phục vụ người dân và doanh nghiệp, cần nhận thấy rằng đây là vấn đề trong việc phải xây dựng môi trường kinh doanh lành mạnh tại Việt Nam để thể hiện chính phủ kiến tạo, hướng tới người dân và doanh nghiệp, từ đó xây dựng những dịch vụ phục vụ mang lại lợi ích cho người dân, thể hiện trách nhiệm của các cơ quan nhà nước đối với người dân.

Đồng chí Mai Tiến Dũng cho biết thêm, sau khi khai trương Cổng DVCQG vào ngày 09/12 theo dự kiến, VPCP cùng các Bộ, ngành, cơ quan, đặc biệt là tập đoàn VNPT sẽ có kế hoạch trải nghiệm với người dân để thấy rằng việc thực hiện những thủ tục hành chính trực tuyến sẽ đi vào thực tế đối với người dân.

Link tham khảo: http://antoanthongtin.vn/Detail.aspx?NewsID=f53a5c2c-c03a-4808-9a36-b0110c236296&CatID=6a79a9d0-0aed-4380-83ff-f60ad2498410

2. Cảnh giác bộ gõ Unikey giả mạo chiếm đoạt quyền điều khiển máy tính

Hãng bảo mật CMC Cyber Security vừa phát hiện mẫu mã độc sử dụng kỹ thuật mới để tấn công người dùng bằng cách lợi dụng phần mềm Unikey, bộ gõ tiếng Việt phổ biến nhất dành cho người dùng Việt Nam.

Theo CMC, khi Unikey chạy, phần mềm sẽ tải lên chương trình của Windows và tin tặc đã lợi dụng điều này để chèn một tập tin kbdus.dll độc hại vào thư mục UnikeyNT.exe. Tập tin độc hại này sẽ được ưu tiên tải lên thay vì chương trình của Windows, có nghĩa khi Unikey được bật, mã độc cũng sẽ được thực thi khiến người dùng không thể phát hiện.

Một chuyên gia bảo mật hoạt động độc lập cho biết do Unikey là bộ gõ rất phổ biến trong nước, nên khi người dùng cài đặt cần lưu ý nguồn tải và thường chương trình này không có bất kỳ tập tin .dll nào theo kèm. Vì thế, sau khi cài đặt mà phát hiện có thêm tập tin này cần phải cảnh giác và xóa bộ gõ vừa cài.

Mã độc sẽ thu thập các thông tin máy tính nạn nhân, mã hóa và gửi những dữ liệu này đến máy chủ của tin tặc. Theo nhận định của CMC, chiến dịch tấn công có chủ đích APT mới này được đầu tư nghiên cứu kỹ và cực kỳ nguy hiểm.

Để bảo vệ máy tính khỏi cuộc tấn công APT này, các chuyên gia CMC khuyến cáo người dùng nên kiểm tra kỹ thư mục cài đặt Unikey, loại bỏ file kbdus.dll cùng thư mục; cài phần mềm chống mã độc để bảo vệ máy tính của mình; cùng với chỉ tải và sử dụng Unikey chính chủ từ trang web Unikey.org.

Theo các chuyên gia CMC, các cơ quan, tổ chức cần nâng cao an toàn thông tin cho hệ thống của mình, đưa ra các phương án rà soát, phòng chống và sẵn sàng ứng phó khi xảy ra các mối nguy hại.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần vào đúng trang chủ download Unikey để đảm bảo an toàn thông tin.

Link tham khảo: https://thanhnien.vn/cong-nghe/canh-giac-bo-go-unikey-gia-mao-chiem-doat-quyen-dieu-khien-may-tinh-1156174.html

3. Lỗi mới trên Linux cho phép chiếm quyền kết nối VPN được mã hóa

Một nhóm các nhà nghiên cứu vừa tiết lộ một lỗ hổng nghiêm trọng ảnh hưởng đến hầu hết các hệ điều hành Linux và giống Unix, bao gồm FreeBSD, OpenBSD, macOS, iOS và Android, có thể cho phép 'kẻ tấn công liền kề' từ xa theo dõi và giả mạo các kết nối VPN được mã hóa.

Lỗ hổng (CVE-2019-14899) nằm trong networking slack (chồng giao thức) của nhiều hệ điều hành và có thể bị khai thác để tấn công cả giao thức IPv4 và IPv6.

Theo các nhà nghiên cứu, do lỗ hổng không phụ thuộc vào công nghệ VPN được sử dụng, cuộc tấn công hoạt động trên các giao thức mạng riêng ảo được triển khai rộng rãi như OpenVPN, WireGuard, IKEv2/IPSec…

Lỗ hổng này có thể bị khai thác bởi một kẻ tấn công mạng – đang kiểm soát điểm truy cập hoặc đã kết nối đến mạng của nạn nhân - chỉ bằng cách gửi các gói mạng không được yêu cầu đến thiết bị mục tiêu và bắt các phản hồi, ngay cả khi chúng được mã hóa.

Theo giải thích của các nhà nghiên cứu, mặc dù tác động khác nhau đến từng hệ điều hành bị ảnh hưởng, lỗ hổng cho phép kẻ tấn công:

- xác định địa chỉ IP ảo của nạn nhân được chỉ định bởi máy chủ VPN
- xác định xem có kết nối đến một trang web cụ thể hay không
- xác định chính xác số seq và ack bằng cách đếm các gói được mã hóa và/hoặc kiểm tra kích thước của chúng
- đưa dữ liệu vào luồng TCP và chiếm được các kết nối.

"Điểm truy cập sau đó có thể xác định IP ảo của nạn nhân bằng cách gửi các gói SYN-ACK đến thiết bị nạn nhân trên toàn bộ không gian IP ảo", nhóm nghiên cứu cho biết.

"Khi một SYN-ACK được gửi đến đúng IP ảo trên thiết bị nạn nhân, thiết bị sẽ phản hồi bằng RST; khi SYN-ACK được gửi đến IP ảo không chính xác, kẻ tấn công không nhận được gì".

Theo các nhà nghiên cứu, cuộc tấn công không hoạt động đối với các thiết bị macOS/iOS như mô tả.

Thay vào đó, kẻ tấn công cần "sử dụng cổng mở trên máy Apple để xác định địa chỉ IP ảo". Trong thử nghiệm của họ, các nhà nghiên cứu sử dụng "cổng 5223, được sử dụng cho iCloud, iMessage, FaceTime, Game Center, Photo Stream và các thông báo đẩy…".

Các nhà nghiên cứu đã thử nghiệm và khai thác thành công lỗ hổng trên các hệ điều hành và hệ thống sau đây, nhưng họ tin rằng danh sách này có thể mở rộng hơn nữa:

- Ubuntu 19.10 (systemd)
- Fedora (systemd)
- Debian 10.2 (systemd)
- Arch 2019.05 (systemd)
- Manjaro 18.1.1 (systemd)

- Devuan (sysV init)
- MX Linux 19 (Mepis + antiX)
- Vô hiệu Linux (runit)
- Slackware 14,2 (rc.d)
- Deepin (RC.d)
- FreeBSD (RC.d)
- OpenBSD (RC.d)

Các nhà nghiên cứu cho biết: "Hầu hết các bản phân phối Linux mà chúng tôi đã thử nghiệm đều dễ bị tấn công, đặc biệt là các bản phân phối Linux sử dụng phiên bản systemd sau ngày 28 tháng 11 năm ngoái mà đã tắt tính năng lọc theo đường dẫn ngược (reverse path filtering)".

"Tuy nhiên, gần đây chúng tôi đã phát hiện ra rằng cuộc tấn công cũng hoạt động chống lại IPv6, do đó, việc lọc theo đường dẫn ngược lại không phải là một giải pháp hợp lý."

Để giảm thiểu rủi ro, các nhà nghiên cứu đề nghị bật tính năng lọc đường dẫn ngược, thực hiện lọc bogon và mã hóa kích thước và thời gian gói để ngăn kẻ tấn công thực hiện bất kỳ can thiệp.

Các nhà nghiên cứu sẽ tiết lộ chi tiết kỹ thuật về lỗ hổng sau khi các nhà cung cấp bị ảnh hưởng, bao gồm Systemd, Google, Apple, OpenVPN, WireGuard và các bản phân phối Linux khác nhau phát hành giải pháp và bản vá thỏa đáng.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người quản trị và người dùng cần cập nhật ngay các bản vá mới nhất của các ứng dụng VPN để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/loi-moi-tren-linux-cho-phep-chiem-quyen-ket-noi-vpn-duoc-ma-hoa.13032/

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-2011-3600 CVE-2011-2177 …	Nhóm 02 lỗ hổng trên phần mềm Apache (Ofbiz, Openoffice) cho phép đối tượng tấn công chèn và thực thi mã lệnh tùy ý.	Chưa có thông tin xác nhận và bản vá.
2	Chrome	CVE-2019-5866 CVE-2019-13704 CVE-2019-13719	Nhóm 99 lỗ hổng trên trình duyệt web Chrome cho phép đối tượng tấn công khai thác trang HTML để tấn công mục tiêu.	Đã có thông tin xác nhận và bản vá
3	Cisco	CVE-2019-15990 CVE-2019-15995 CVE-2019-15996	Nhóm 24 lỗ hổng trên một số sản phẩm của Cisco (Business RV Series Routers, DNA Spaces…) cho phép đối tượng tấn công chèn và thực thi mã tùy ý.	Chưa có thông tin xác nhận và bản vá
4	D-link	CVE-2013-6811	01 lỗ hổng trên thiết bị D-link (DSL-6740U gateway) cho phép đối tượng tấn công chèn và thực thi mã lệnh từ xa.	Chưa có thông tin xác nhận và bản vá
5	HP	CVE-2019-18909 CVE-2019-16285 CVE-2019-16286	Nhóm 05 lỗ hổng trên thiết bị HP (ThinPro…) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã tùy ý.	Chưa có thông tin xác nhận và bản vá
6	Kaspersky	CVE-2019-15688 CVE-2019-15685 CVE-2019-15687 …	Nhóm 04 lỗ hổng trên sản phẩm của Kaspersky (Total Security, Small Office Security, Internet Security,…) cho phép đối tượng tấn công thu thập thông tin, vô hiệu hóa từ xa tính năng bảo mật của mục tiêu.	Chưa có thông tin xác nhận và bản vá
7	Linux	CVE-2019-14815 CVE-2019-19227 CVE-2019-19318	Nhóm 10 lỗ hổng trên hệ điều hành Linux (Kernel) cho phép đối tượng tấn công chèn thực thi mã tùy ý, tấn công từ chối	Chưa có thông tin xác nhận và

			dịch vụ.	bản vá
8	Wordpress	CVE-2015-9537 CVE-2019-19306 CVE-2015-9538 …	Nhóm 04 lỗ hổng trên một số thành phần của Wordpress (the NextGEN Galery plugin, Zoho CRM Lead Magnet, NextGEN Galery,...) cho phép đối tượng tấn công tấn công khai thác XSS.	Chưa có thông tin xác nhận và bản vá
	Gitlab	CVE-2019-18448 CVE-2019-18447 CVE-2019-18452 …	Nhóm 19 lỗ hổng trong Gitlab (Gitlab Community and Enterprise Edition) cho phép đối tượng tấn công tấn công từ chối dịch vụ.	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	soplifan.ru
5	xjpakmdcfuqe.com
6	u2yxyrlph.ru
7	xdqzpbcgrvkj.ru
8	morphed.ru
9	gxokop.info
10	www.cityofangelsmagazine.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.