BẢN TIN NỘI BỘ

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

1. Định danh, xác thực trên cổng dịch vụ công quốc gia: hướng tới nền tảng định danh điện tử quốc gia

Một trong những tính năng, hợp phần quan trọng nhất của Cổng DVCQG là giải pháp định danh, xác thực với công dân, tổ chức. Theo đó, Cổng DVCQG cho phép tổ chức, cá nhân đăng ký tài khoản; cung cấp chức năng đăng nhập một lần và các cơ chế xác thực người dùng để thực hiện các thủ tục hành chính tại Cổng Dịch vụ công cấp Bộ, cấp Tỉnh.

Hệ thống định danh, xác thực trên Cổng DVCQG gồm ba hợp phần chính: Hệ thống định danh điện tử (IDP – Cổng DVCQG); nền tảng trao đổi danh tính điện tử; giải pháp xác thực đăng nhập, đăng xuất một lần. Giải pháp này sẽ được áp dụng cho các hệ thống do Văn phòng Chính phủ triển khai và hoàn toàn có thể mở rộng để áp dụng với hệ thống thông tin của các cơ quan nhà nước và khu vực tư nhân như một nền tảng cho việc định danh số trong thời gian tới. Bài viết này sẽ cung cấp chi tiết các kết quả triển khai, mô hình kỹ thuật và đưa ra một số đề xuất, kiến nghị.

GIỚI THIỆU

Một số khái niệm về định danh, xác thực điện tử

Danh tính quốc gia (National IDentity) được Chính phủ cấp phát duy nhất cho từng đối tượng, nó cho phép nhận dạng, xác thực và phân biệt với người khác để thực hiện các quyền, nghĩa vụ liên quan. Thẻ căn cước, Chứng minh nhân dân chính là một loại thẻ định danh quốc gia. Dự thảo Nghị định về định danh, xác thực điện tử đưa ra một số khái niệm như sau:

- Danh tính điện tử hay danh tính số (e-Identity) là tập hợp các thông tin điện tử phục vụ việc xác định duy nhất một cá nhân, tổ chức.

- Định danh điện tử (e-Identification) là quá trình xác định danh tính điện tử của cá nhân, tổ chức.

- Xác thực điện tử (e-Authentication) là việc xác minh danh tính điện tử của người sử dụng; là điều kiện bắt buộc để cho phép thực hiện giao dịch điện tử.

Việc định danh, xác thực điện tử gồm nhiều hình thức như: Tài khoản/mật khẩu; thiết bị lưu mã (token); điện thoại di động và thẻ SIM. Định danh, xác thực điện tử cung cấp vai trò đặc biệt quan trọng trong Hệ sinh thái số để đảm bảo truy cập an toàn và dễ dàng tới các dịch vụ công trực tuyến.

Theo đó, Tổ chức cung cấp định danh xác thực và cung cấp định danh điện tử cho cá nhân, tổ chức tới đăng ký. Định danh này được tin tưởng, sử dụng ở các Cơ quan cung cấp dịch vụ công.

Mức độ bảo đảm của danh tính điện tử (IAL - Identity Assurance Level) và xác thực điện tử (AAL - Authenticator Assurance Level) được phân loại theo 03 mức độ: Thấp (Low), trung bình (Substantial), cao (High) - tương ứng với việc phân loại của châu Âu được mô tả chi tiết trong Bảng 1.

Bảng 1. Mức độ bảo đảm theo quy định của Châu Âu

Mức độ bảo đảm	Mức độ bảo đảm của danh tính điện tử (chứng minh danh tính khi đăng ký)	Mức độ xác thực
Thấp	Cung cấp danh tính từ cơ quan chức năng (từ xa hoặc trực tiếp)	Một yếu tố (mật khẩu hoặc mã PIN)
Trung bình	- Cung cấp danh tính (từ xa hoặc trực tiếp); - Xác thực danh tính bởi cơ quan đăng ký.	Nhiều yếu tố (điện thoại di động kết hợp với mã PIN)
Cao	- Cung cấp giấy tờ danh tính trực tiếp tại cơ quan đăng ký; - Xác thực danh tính sử dụng các nguồn chính thống và các tài liệu của cơ quan quản lý.	- Nhiều yếu tố; - Phải truy nhập tới dữ liệu/khóa cá nhân trên các thiết bị vật lý; - Có giải pháp mã hóa bảo vệ thông tin định danh cá nhân.

Có 02 mô hình cung cấp định danh chính ở quy mô quốc gia:

Mô hình liên hiệp định danh: Cho phép nhà cung cấp dịch vụ định danh, xác thực cung cấp và kết nối, tích hợp qua Nền tảng trao đổi danh tính (Identity Exchange Platform - IDX). Các nhà cung cấp dịch vụ định danh có thể là khu vực tư nhân như tài khoản ngân hàng (Thụy Điển, Na Uy, Singapore, Nigeria), tài khoản do doanh nghiệp cung cấp (Anh, Pháp); hoặc khu vực công như: Thẻ căn cước điện tử, định danh di động (Đức, Hà Lan, Pakistan, Estonia, Kenya, Bỉ, Oman).

Mô hình hệ thống định danh, xác thực tập trung: Do nhà nước xây dựng thống nhất cho các cơ quan triển khai (tại Nga, Singapore).

Thực trạng định danh, xác thực tại Việt Nam

Số liệu khảo sát năm 2019 cho thấy, hầu hết các bộ, ngành, địa phương đều xây dựng các giải pháp định danh, xác thực điện tử phục vụ việc cung cấp dịch vụ công trực tuyến của mình. Việc định danh phần lớn ở mức độ thấp, không yêu cầu người sử dụng phải đăng ký trực tiếp hoặc được đối chiếu với các CSDL như CSDL dân cư, thuế, bảo hiểm, xã hội…

Về chức năng xác thực: Trang/Cổng Dịch vụ công các Bộ, ngành, địa phương sử dụng biện pháp xác thực mức độ thấp nhất trong các biện pháp xác thực điện tử (tài khoản, mật khẩu), không đảm bảo giá trị pháp lý, tính an toàn, bảo mật với hồ sơ dịch vụ công.

Cổng dịch vụ công quốc gia

Với quan điểm công khai, minh bạch, lấy người dân, doanh nghiệp làm trung tâm phục vụ, Cổng DVCQG kết nối, cung cấp thông tin về thủ tục hành chính và dịch vụ công trực tuyến; hỗ trợ thực hiện, giám sát, đánh giá việc giải quyết thủ tục hành chính, dịch vụ công trực tuyến và tiếp nhận, xử lý phản ánh, kiến nghị của cá nhân, tổ chức trên toàn quốc. Theo đó, cá nhân, tổ chức dễ dàng truy cập Cổng DVCQG theo nhu cầu người dùng từ máy tính, máy tính bảng hoặc điện thoại di động được kết nối internet để hưởng nhiều lợi ích như:

- Đăng ký và được cấp một tài khoản của Cổng DVCQG; từ đó đăng nhập một lần tới Cổng Dịch vụ công của Bộ, ngành, địa phương; không phải cập nhật các trường thông tin, tài liệu đã được lưu trữ trong tài khoản Cổng DVCQG;

- Tra cứu thông tin, dịch vụ công các ngành, lĩnh vực, các địa phương; Gửi phản ánh kiến nghị liên quan đến việc giải quyết thủ tục hành chính, dịch vụ công;

- Đề nghị hỗ trợ thực hiện thủ tục hành chính, dịch vụ công qua tổng đài hoặc trực tuyến;

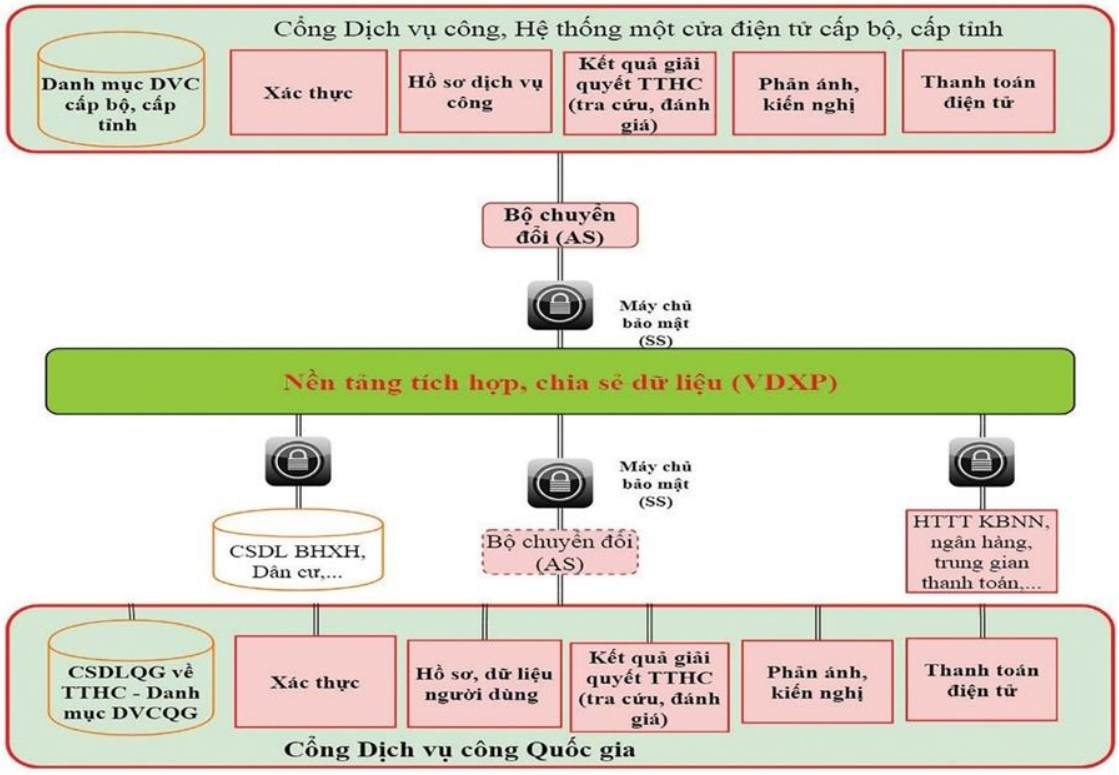
- Theo dõi toàn bộ quá trình giải quyết thủ tục hành chính và xử lý phản ánh kiến nghị;

- Thực hiện thủ tục hành chính tại nhiều tỉnh, thành phố;

- Sử dụng tài khoản của các ngân hàng, trung gian thanh toán để thanh toán trực tuyến phí, lệ phí thực hiện thủ tục hành chính; dịch vụ công;

- Đánh giá sự hài lòng trong giải quyết thủ tục hành chính.

Sau hai tháng khai trương (09/12/2019), Cổng DVCQG đã kết nối, tích hợp với 09/22 bộ, ngành, 63/63 địa phương và 7 tập đoàn, tổng công ty, ngân hàng để cung cấp các dịch vụ công trực tuyến cho người dân, doanh nghiệp như: Đổi giấy phép lái xe; Cấp giấy phép lái xe quốc tế; Cấp chứng nhận xuất xứ hàng hóa; Nộp thuế điện tử với doanh nghiệp… Có hơn 13,4 triệu lượt truy cập; hơn 854 nghìn hồ sơ đồng bộ trạng thái. Đã tiếp nhận, xử lý hơn 4.150 phản ánh, kiến nghị của người dân, doanh nghiệp; hỗ trợ gần 3.900 cuộc gọi qua Tổng đài hỗ trợ. Trong đó, dịch vụ xác thực, đăng nhập một lần đã được triển khai tại 07 bộ, cơ quan và 63/63 tỉnh, thành phố; đã có 44.200 tài khoản đăng ký.



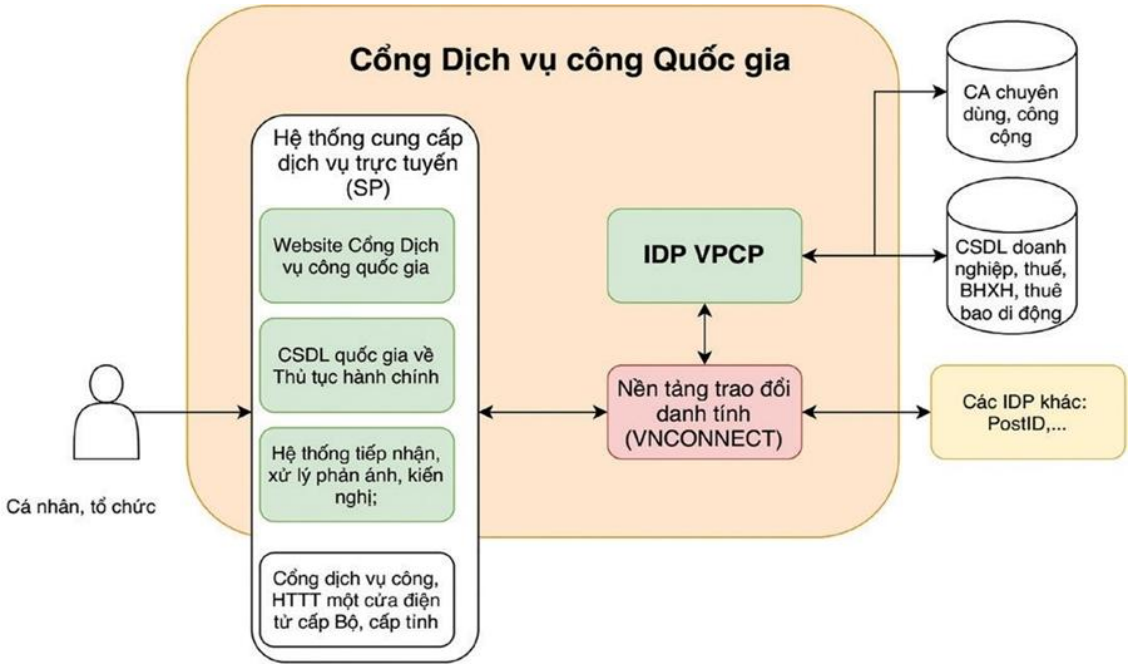
Hình 1. Mô hình kết nối Cổng DVCQG với Cổng Dịch vụ công, Hệ thống thông tin một cửa điện tử cấp Bộ, cấp Tỉnh

VỀ GIẢI PHÁP ĐỊNH DANH, XÁC THỰC TRÊN CỔNG DVCQG

Mô hình kỹ thuật, giải pháp định danh, xác thực điện tử

Cổng DVCQG kết nối với Cổng Dịch vụ công, Hệ thống thông tin một cửa điện tử cấp bộ, tỉnh qua Nền tảng tích hợp, chia sẻ dữ liệu của Văn phòng Chính phủ (phát triển từ Trục liên thông văn bản quốc gia) trong Mạng truyền số liệu chuyên dùng của các cơ quan Đảng, nhà nước (Hình 1). Trong mô hình này, các đơn vị tích hợp, chia sẻ dữ liệu với Cổng DVCQG cần cài đặt một máy chủ bảo mật để cho phép việc xác thực các hệ thống tích hợp, chia sẻ dữ liệu qua Nền tảng này. Thông tin, dữ liệu gửi, nhận qua Nền tảng này đều được ký số, mã hóa bằng chứng thư số của Ban Cơ yếu Chính phủ để bảo đảm an toàn, an ninh thông tin.

Giải pháp định danh, xác thực cá nhân, tổ chức trên Cổng DVCQG thực hiện theo mô hình liên hiệp định danh gồm các thành phần chính như sau (Hình 2):



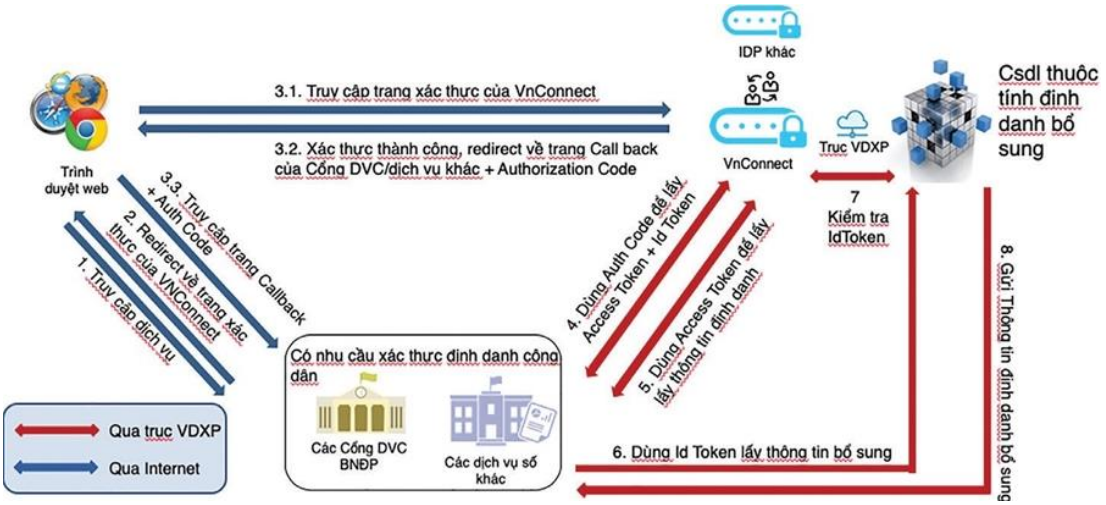
Hình 2. Giải pháp định danh, xác thực trên Cổng DVCQG

- Các hệ thống thông tin cung cấp dịch vụ trực tuyến (Service Provider - SP) là các Hệ thống trong Cổng DVCQG gồm: Website Cổng DVCQG, Hệ thống CSDL quốc gia về thủ tục hành chính, Hệ thống tiếp nhận, xử lý phản ánh, kiến nghị của người dân, doanh nghiệp.

- Nền tảng trao đổi danh tính (VNConnect).

- Hệ thống cung cấp dịch vụ định danh cho cá nhân, tổ chức (IDP VPCP) do Văn phòng Chính phủ xây dựng, vận hành. Hệ thống này kết nối tới CSDL bảo hiểm xã hội, thuê bao di động, chứng thư số chuyên dùng của Ban Cơ yếu Chính phủ, chứng thư số công cộng để phục vụ việc xác minh danh tính số của đối tượng.

Việc tích hợp đăng nhập một lần của Cổng dịch vụ công, Hệ thống thông tin một cửa điện tử cấp Bộ, tỉnh và các hệ thống thông tin khác được thực hiện theo tiêu chuẩn mở OpenID Connect gồm các bước chính (Hình 3): Hệ thống cung cấp dịch vụ (SP) gửi yêu cầu xác thực của người dùng tới nhà cung cấp dịch vụ định danh (IDP); Người dùng xác thực trên ứng dụng; IDP gửi mã xác thực cho SP; SP gửi yêu cầu mã truy nhập (Access Token) tới IDP và IDP cung cấp mã truy nhập cho SP.



Hình 3. Mô hình tích hợp đăng nhập một lần

Về mức độ bảo đảm của định danh, xác thực trên Cổng DVCQG

Đối với cá nhân

- Về mức độ bảo đảm của danh tính điện tử: Việc đăng ký danh tính trên Hệ thống cung cấp dịch vụ định danh của Văn phòng Chính phủ với cá nhân hiện nay tương ứng với mức độ trung bình (IAL2) và mức độ cao (IAL3) theo phân loại của Châu Âu và dự thảo Nghị định về định danh và xác thực điện tử.

Mức độ trung bình gồm các hình thức: Qua Thuê bao di động, hoặc Bảo hiểm xã hội. Theo đó, cá nhân đăng ký tài khoản sẽ khai báo các thông tin cơ bản như tên đăng nhập (số căn cước công dân hoặc chứng minh nhân dân), họ tên, ngày sinh, số điện thoại hoặc số bảo hiểm xã hội, dữ liệu này sẽ được kiểm tra với cơ sở dữ liệu (CSDL) của Bảo hiểm xã hội Việt Nam hoặc CSDL của các nhà mạng viễn thông.

Mức độ cao gồm các hình thức: Đăng ký qua thiết bị chứng thư số (USB Token) hoặc thẻ SIM tích hợp chứng thư số. Theo quy định tại Nghị định số 130/2018/NĐ-CP ngày 27/09/2018 của Chính phủ, việc đăng ký chứng thư số cá nhân phải đăng ký trực tiếp với cơ quan cung cấp dịch vụ chứng thư số, do vậy đáp ứng yêu cầu bảo đảm danh tính mức độ cao.

- Về mức độ xác thực danh tính điện tử: Tương ứng với mức độ bảo đảm danh tính điện tử, có 02 mức độ xác thực danh tính người dùng là mức độ trung bình và mức độ cao.

Hình thức xác thực trung bình: Gồm hai yếu tố là tài khoản (số căn cước công dân hoặc chứng minh nhân dân) và mật khẩu (điều bạn biết); mật khẩu một lần OTP được gửi qua tin nhắn tới điện thoại (thứ bạn có). Hình thức xác thực bằng sinh trắc học sẽ được nghiên cứu, triển khai trong thời gian tới.

Hình thức xác thực mức độ cao: Gồm hai yếu tố có sử dụng giải pháp mã hóa qua chứng thư số gồm: Thiết bị USB Token, SIM tích hợp chứng thư số và mật khẩu để xác thực chữ ký số trên thiết bị.

Đối với doanh nghiệp

Theo số liệu của Bộ Thông tin và Truyền thông, hiện nay tất cả các doanh nghiệp đều sở hữu chứng thư số, chủ yếu được sử dụng cho các dịch vụ: Thuế, hải quan và bảo hiểm xã hội. Cổng DVCQG sử dụng giải pháp định danh, xác thực ở cấp độ cao

qua các chứng thư số này. Thêm vào đó, thông tin doanh nghiệp được kiểm tra, xác thực với thông tin doanh nghiệp trên CSDL quốc gia về đăng ký doanh nghiệp.

Kết quả và những công việc ưu tiên triển khai trong thời gian tới

Tính đến ngày 11/02/2020, giải pháp định danh, xác thực điện tử trên Cổng DVCQG đã có trên 47.000 danh tính điện tử được đăng ký (trên 46.800 của cá nhân (Bảng 2) và 240 của doanh nghiệp). Với việc cung cấp dịch vụ đăng nhập một lần (SSO), cá nhân, tổ chức sử dụng danh tính điện tử và xác thực trên Cổng DVCQG có thể thực hiện dịch vụ công trực tuyến tại Cổng dịch vụ công của tất cả các bộ, ngành, địa phương trên toàn quốc. Hoàn thành tích hợp SSO với 07/22 Bộ, cơ quan thuộc Chính phủ và 63/63 tỉnh, thành phố.

Bảng 2. Định danh điện tử cá nhân thực hiện trên Cổng DVCQG (từ ngày 09/12/2019 tới ngày 11/02/2020)

<table>
<tr><th>Định danh, xác thực của cá nhân</th><th>Bảo hiểm xã hội</th><th colspan="2">Thuê bao di động</th><th>USB Token</th><th>SIM PKI</th></tr>
<tr><td rowspan="6">Số lượng</td><td colspan="3">Mức độ trung bình</td><td colspan="2">Mức độ cao</td></tr>
<tr><td rowspan="5">8.850</td><td colspan="2">37.784</td><td rowspan="5">39</td><td rowspan="5">198</td></tr>
<tr><td>Viettel</td><td>18.303</td></tr>
<tr><td>VNPT</td><td>14.033</td></tr>
<tr><td>Mobifone</td><td>5.381</td></tr>
<tr><td>Vietnamobile</td><td>67</td></tr>
</table>

Hệ thống đã kết nối, tích hợp với các hệ thống thông tin, CSDL phục vụ việc định danh và xác thực như: CSDL quốc gia về đăng ký doanh nghiệp của Bộ Kế hoạch và đầu tư; CSDL thuê bao di động của 04 nhà mạng lớn (Viettel, VNPT, Mobifone, Vietnamobile); CSDL bảo hiểm xã hội; Kết nối thử nghiệm với Hệ thống Định danh điện tử của Tổng công ty Bưu điện Việt Nam.

Trong thời gian tới, Văn phòng Chính phủ sẽ ưu tiên triển khai một số nhiệm vụ, để hoàn thiện Hệ thống định danh, xác thực gồm: Phối hợp với Ban Cơ yếu Chính phủ để hoàn thiện giải pháp định danh, xác thực bằng chứng thư số đối với cơ quan nhà nước, cán bộ, công chức; Tích hợp với hệ thống định danh của Tổng công ty Bưu điện Việt Nam (PostID) và các hệ thống định danh khác đáp ứng tiêu chuẩn kỹ thuật; Hoàn thành việc tích hợp với Cổng dịch vụ công, Hệ thống một cửa điện tử của các bộ, ngành, địa phương; Tích hợp với hệ thống thông tin khác của Văn phòng Chính phủ như: Hệ thống thông tin báo cáo Chính phủ, Hệ thống tham vấn chính sách, Hệ thống e-Cabinet…; Tích hợp với hệ thống nộp thuế điện tử của các ngân hàng; Triển khai giải pháp định danh, xác thực qua chứng thư số "mềm" (soft - token) và sinh trắc học.

KẾT LUẬN

Cổng DVCQG là một hợp phần quan trọng giải quyết mối quan hệ giữa Chính quyền với người dân (G2C) trong Chính phủ điện tử.

Cổng DVCQG gồm nhiều hợp phần quan trọng như CSDL quốc gia về thủ tục hành chính, nền tảng thanh toán… Đặc biệt là Hệ thống định danh, xác thực điện tử - được xây dựng theo mô hình mở, hiện đại, tương đương với giải pháp tại các quốc gia phát triển. Hệ thống đáp ứng mức độ xác thực, an toàn cao và linh hoạt với cá nhân, tổ chức.

Với mô hình này không cần thiết phải thiết lập một hệ thống định danh điện tử tập trung quốc gia, Chính phủ có thể tận dụng hệ thống định danh của các bộ, cơ quan sở hữu những CSDL quan trọng như dân cư, bảo hiểm xã hội, đăng ký kinh doanh, chứng thư số… và hệ thống định danh của các doanh nghiệp trên cơ sở phát triển Nền tảng trao đổi định danh của Cổng DVCQG.

Hệ thống định danh, xác thực này được sử dụng chung cho Văn phòng Chính phủ, các bộ, ngành, địa phương, hạn chế đầu tư các hệ thống/ tích hợp xác thực trong các hệ thống thông tin, bảo đảm một Kiến trúc Chính phủ điện tử nhất quán từ Trung ương đến địa phương. Người dân, doanh nghiệp chỉ cần một danh tính điện tử là có thể thực hiện các giao dịch điện tử với cơ quan nhà nước và có thể mở rộng ra khu vực tư trong tương lai. Với hệ thống này, Chính phủ không chỉ cung cấp một nền tảng cho khu vực công mà có thể kiến tạo Nền tảng định danh số phục vụ việc phát triển chính phủ số, xã hội số trong thời gian tới.

Link tham khảo: http://antoanthongtin.vn/ca-cqnn/dinh-danh-xac-thuc-tren-cong-dich-vu-cong-quoc-gia-huong-toi-nen-tang-dinh-danh-dien-tu-quoc-gia-106123

2. iOS 13.5.1 phát hành, khắc phục lỗ hổng jailbreak

Apple đã vá một lỗ hổng bảo mật cho phép tin tặc xây dựng công cụ bẻ khóa (jailbreak) để truy cập sâu vào phần mềm iPhone.

Theo TechCrunch, Apple thừa nhận họ đã sửa lỗ hổng zero-day giúp nhóm Un0ver cung cấp công cụ bẻ khóa vào tuần trước, bao gồm cả iOS 13.5. Mặc dù các chi tiết về lỗ hổng này vẫn chưa được công khai, Apple thường khá nhanh trong việc tìm ra lỗ hổng và khắc phục sự cố nhằm tránh cho tin tặc lợi dụng.

Đại diện nhóm Un0ver cũng thừa nhận trên trang Twitter của mình rằng bản cập nhật iOS 13.5.1 sẽ đóng lỗ hổng mà họ khai thác khiến việc jailbreak thiết bị trở nên vô dụng. Như đã biết, jailbreak là hình thức phổ biến để người dùng thoát khỏi sự hạn chế của Apple trong việc ngăn họ truy cập sâu vào hệ điều hành của iPhone.

Apple đã làm điều này để cải thiện bảo mật thiết bị và giảm khả năng cho phép tin tặc có thể tấn công bằng phần mềm. Tuy nhiên, những nhà phát triển phần mềm jailbreak nói rằng việc vượt qua các hạn chế sẽ cho phép họ tùy biến iPhone nhiều hơn giống như cách mà người dùng Android đã quen thuộc.

Các chuyên gia bảo mật thường khuyên người dùng không nên jailbreak thiết bị vì có thể khiến chủ sở hữu thiết bị chịu nhiều cuộc tấn công hơn, đồng thời khuyên người dùng cài đặt thiết bị và phần mềm của họ ngay khi có bản cập nhật.

Apple cho biết iOS 13.5.1 cũng đi kèm với nhãn Memoji mới và các sửa lỗi cùng cải tiến khác.

Để cài đặt iOS 13.5.1 trên iPhone, iPad hoặc iPod Touch, người dùng hãy vào Settings > General > Software Update, sau đó nhấp vào Download and Install ở cuối trang. Người dùng cũng có thể cài đặt bản cập nhật thông qua iTunes bằng cách kết nối thiết bị iOS với máy tính. Bản cập nhật này có dung lượng khoảng 77 MB.

Khuyến nghị: Người dùng không tự jailbreak và luôn cập nhật bản vá mới của thiết bị để bảo đảm an toàn thông tin.

Link tham khảo: https://thanhnien.vn/cong-nghe/ios-1351-phat-hanh-khac-phuc-lo-hong-jailbreak-1232422.html

3. Cisco vá hàng chục lỗ hổng trong các bộ định tuyến doanh nghiệp

Cisco vừa phát hành gói bản vá cho hàng loạt lỗ hổng trong phần mềm hệ điều hành đa nhiệm IOS của hãng. Trong đó, hàng chục lỗ hổng an ninh ảnh hưởng đến các bộ định tuyến và chuyển mạch cho doanh nghiệp.

Một trong những lỗ hổng nghiêm trọng nhất, CVE-2020-3205, cho phép kẻ tấn công không xác thực có quyền truy cập mạng có thể thực thi các lệnh shell tùy ý trên máy chủ ảo của những thiết bị bị ảnh hưởng.

Để khai thác lỗ hổng, kẻ tấn công gửi các gói tin đặc biệt đến thiết bị mục tiêu. Khai thác thành công có thể khiến hệ thống hoàn toàn bị chiếm quyền điều khiển.

Một lỗ hổng khác, CVE-2020-3198, cũng được đánh giá ở mức nghiêm trọng, có thể cho phép kẻ tấn công từ xa không xác thực thực thi mã tùy ý trên hệ thống hoặc khiến hệ thống bị crash sau đó tải lại bằng cách gửi đến những gói tin độc hại.

Cả hai lỗ hổng nghiêm trọng này đều ảnh hưởng đến các bộ định tuyến dịch vụ tích hợp công nghiệp (ISR) Cisco 809, 829 và các bộ định tuyến kết nối sê-ri 1000 (CGR).

Nhiều lỗ hổng nghiêm trọng cao ảnh hưởng đến các thiết bị mạng cho doanh nghiệp có thể bị khai thác để leo thang đặc quyền bằng các thông tin được mã hóa cứng, gây ra tình trạng DoS khi gửi lưu lượng CIP (Giao thức công nghiệp chung) đặc biệt, thực thi các lệnh shell tùy ý và khởi động các hình ảnh phần mềm độc hại. Tuy nhiên, việc khai thác những lỗ hổng này yêu cầu quyền xác thực, truy cập nội bộ hoặc một tính năng mặc định tắt được kích hoạt.

Một số lỗ hổng nghiêm trọng cao ảnh hưởng đến các sản phẩm cho doanh nghiệp có liên quan đến môi trường ứng dụng IOx, cho phép kẻ tấn công viết hoặc sửa đổi các tệp tùy ý, khởi chạy các cuộc tấn công DoS hoặc thực thi mã tùy ý với các đặc quyền leo thang.

Những lỗ hổng nghiêm trọng trung bình ảnh hưởng đến các sản phẩm cho doanh nghiệp của Cisco, có thể bị khai thác bởi những kẻ tấn công xác thực để tấn công XSS và ghi đè dữ liệu các tệp tùy ý.

Danh sách các sản phẩm Cisco bị ảnh hưởng bao gồm các ISR sê-ri 800, 809 và 829, CGR sê-ri 1000, Industrial Compute Gateway IC3000, chuyển mạch Industrial Ethernet (IE) sê-ri 4000, chuyển mạch sê-ri Catalyst IE3400 và bộ định tuyến IR510 WPAN. Hầu hết các lỗ hổng chỉ ảnh hưởng đến các thiết bị ISR cho doanh nghiệp 809 và 829 và CGR 1000.

Cisco đã thông báo cho khách hàng về việc nền tảng lưu trữ ứng dụng IOx cho phần mềm hệ điều hành IOS XE bị ảnh hưởng bởi một trong số những lỗ hổng nghiêm trọng, có thể bị khai thác bởi kẻ tấn công từ xa, không xác thực để thực thi các lệnh IOx API.

Cisco cũng cho biết chưa có lỗ hổng nào bị khai thác trong thực tế.

Khuyến nghị: Người quản trị và người dùng cần kiểm tra và cập nhật bản vá mới nhất của sản phẩm Cisco để bảo đảm an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/cisco-va-hang-chuc-lo-hong-trong-cac-bo-dinh-tuyen-doanh-nghiep.13706/

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	IBM	CVE 2020 4490 CVE 2020 4226 CVE 2020 4352 …	Nhóm 20 lỗ hổng trong các sản phẩm của IBM (Business Automation Workflow, MobileFirst Platform Foundation, …) cho phép đối tượng tấn công thu thập thông tin, leo thang đặc quyền.	Đã có thông tin xác nhận và bản vá.
2	Mozilla	CVE-2020-12390 CVE-2020-12396 CVE-2020-12389 …	Nhóm 13 lỗ hổng trong phần mềm Mozilla (Firefox ESR < 68.8, Thunderbird < 68.8.0, Firefox <76,…) cho phép đối tượng tấn công chèn và thực thi mã tùy ý, tấn công giả mạo. 01 lỗ hổng có CVSS:10,0 (đặc biệt nghiêm trọng)	Đã có thông tin xác nhận và bản vá
3	Wordpress	CVE-2020-13693 CVE-2020-13642 CVE-2020-13643 …	Nhóm07 lỗ hổng trong phần mềm Wordpress (SiteOrigin Page Builder plugin < 2.10.16, Accordion plugin<2.2.9, bbPress plugin < 2.6.5) cho phép đối tượng tấn công chèn và thực thi mã từ xa, leo thang quyền.	Đã có thông tin xác nhận và bản vá
4	Huawei	CVE-2020-1798 CVE-2020-1870 CVE-2020-1832 …	Nhóm 07 lỗ hổng trong các sản phẩm của Huawei(E6878-370, CloudEngine12800, P30 smartphones,…) cho phép đối tượng tấn công truy cập trái phép, thu thập thông tin, chèn và thực thi mã từ xa, tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
5	Cisco	CVE-2020-3280 CVE-2020-3272 CVE-2020-3314 …	Nhóm 06 lỗ hổng trong các sản phẩm của Cisco (DHCP server, Unified CCX, MP,…) cho phép đối tượng tấn công chèn và thực thi mã từ xa, tấn công SQL, tấn công từ chối	Đã có thông tin xác nhận và bản vá

			dịch vụ.	
6	Linux	CVE-2020-13434 CVE-2020-10711 CVE-2020-10751	Nhóm 03 lỗ hổng trong hệ điều hành Linux (Linux kernel <5.7) cho phép đối tượng tấn công khai thác lỗi xử lí con trỏ NULL để gây ra tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
7	Lenovo	CVE-2020-8330 CVE-2020-8329	Nhóm 02 lỗ hổng trong thành phần của thiết bị của Lenovo (Printer LJ4010DN<1.01) 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	xjpakmdcfuqe.ru
5	xjpakmdcfuqe.in
6	xjpakmdcfuqe.biz
7	xjpakmdcfuqe.com
8	amnsreiuojy.ru
9	xmlinstcp.ddbbvt.eu
10	gu2tcqt0v.ru

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.