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

1. Đẩy mạnh cung cấp dịch vụ công trực tuyến mức độ 4 trong năm 2020

Thực hiện chỉ tiêu đến năm 2020, cung cấp 30% dịch vụ công trực tuyến mức độ 4 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, đến tháng 3/2020, Bộ Thông tin và Truyền thông (TT&TT) đã cung cấp 61 dịch vụ công trực tuyến mức độ 4, đạt tỉ lệ 30% theo yêu cầu của Chính phủ.

Ngày 19/3/2020, Bộ TT&TT đã ban hành Công văn số 929/BTTTT-THH về việc đẩy mạnh cung cấp dịch vụ công trực tuyến mức độ 4, trong đó đề nghị các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương triển khai các biện pháp quyết liệt để cung cấp dịch vụ công trực tuyến.

Nhằm tiếp tục đẩy mạnh việc cung cấp dịch vụ công trực tuyến mức độ 4, ngày 16/4/2020, Bộ đã ban hành Quyết định số 684/QĐ-BTTTT phê duyệt kế hoạch triển khai dịch vụ công trực tuyến mức độ 4 năm 2020 của Bộ.

Với mục tiêu cung cấp đầy đủ 100% các dịch vụ công trực tuyến thuộc thẩm quyền giải quyết của Bộ ở mức độ 4; phấn đấu tỷ lệ thủ tục hành chính có phát sinh hồ sơ trực tuyến trên tổng số thủ tục hành chính trực tuyến mức 3, 4 và tỷ lệ hồ sơ thủ tục hành chính được xử lý trực tuyến hàng năm tăng gấp đôi trong giai đoạn 2020 - 2021; đạt tỷ lệ dịch vụ công trực tuyến được kết nối với cổng dịch vụ công quốc gia theo lộ trình của Chính phủ giao. Theo đó, trong năm 2020, 149 dịch vụ công trực tuyến mức độ 4 sẽ được cung cấp, nâng cấp.

Các mục tiêu cụ thể trong năm 2020 là: Hoàn thiện cổng Dịch vụ công của Bộ theo hướng tập trung, thống nhất để cung cấp dịch vụ công trực tuyến thuộc thẩm quyền giải quyết của Bộ; đáp ứng quy định về tiêu chí chức năng, tính năng kỹ thuật tại Thông tư số 22/2019/TT-BTTTT ngày 31/12/2019 của Bộ trưởng Bộ TT&TT. Tích hợp 06 dịch vụ công trực tuyến với cổng dịch vụ công quốc gia; áp dụng cơ chế đăng nhập một lần SSO đồng bộ trạng thái hồ sơ thủ tục hành chính và kết nối hệ thống hỗ trợ thanh toán trực tuyến toàn quốc. Tỷ lệ dịch vụ công có phát sinh hồ sơ trực tuyến trên tổng số dịch vụ công trực tuyến đạt từ 50% trở lên. Tỷ lệ hồ sơ thủ tục hành chính được xử lý trực tuyến đạt từ 40% trở lên. Cho phép người dân, doanh nghiệp thanh toán phí, lệ phí (nếu có) trực tuyến, không dùng tiền mặt, bằng nhiều phương tiện khác nhau khi sử dụng dịch vụ công của Bộ.

Đẩy mạnh phương thức tiếp nhận hồ sơ, trả kết quả giải quyết thủ tục hành chính qua dịch vụ bưu chính công ích. Tận dụng hệ thống công nghệ thông tin sẵn có, chủ động bố trí, huy động nguồn lực tại chỗ để sẵn sàng tiếp nhận hồ sơ trực tuyến của tất cả các thủ tục hành chính. Hoàn thành việc nâng cấp các dịch vụ công mức 2 và 3 lên mức độ 4. Từng bước nâng cấp hệ thống thông tin để xử lý hồ sơ hoàn toàn trên môi trường mạng. Hỗ trợ, hướng dẫn, phổ cập kỹ năng để người dân, doanh nghiệp

nộp hồ sơ trực tuyến nhằm nâng cao số lượng hồ sơ xử lý trực tuyến của mỗi dịch vụ công.

Để thực hiện các mục tiêu trên, Bộ TT&TT đã đưa ra các nội dung triển khai:

- Thống nhất các biểu mẫu, thành phần hồ sơ trong quy trình điện tử giải quyết hồ sơ thủ tục hành chính.

- Xây dựng, ban hành quy trình nội bộ, quy trình điện tử trong xử lý hồ sơ thủ tục hành chính; chuẩn hóa mã tiếp nhận hồ sơ thủ tục hành chính theo Nghị định số 61/NĐ-CP ngày 23/4/2018 của Chính phủ.

- Xây dựng và nâng cấp cổng dịch vụ công của Bộ đáp ứng quy định về tiêu chí chức năng, tính năng kỹ thuật tại Thông tư số 22/2019/TT-BTTTT ngày 31/12/2019 của Bộ trưởng Bộ TT&TT.

- Kết nối Hệ thống dịch vụ công của các đơn vị với cổng Dịch vụ công của Bộ thông qua hệ thống chia sẻ, tích hợp dùng chung (LGSP), đáp ứng chức năng đăng nhập một lần SSO và tích hợp đồng bộ trạng thái xử lý của tất cả hồ sơ thủ tục hành chính.

- Hướng dẫn các đơn vị trong Bộ thực hiện việc tuyên truyền, quảng bá để thu hút các tổ chức, cá nhân ủng hộ và tham gia các dịch vụ công trực tuyến.

- Xây dựng quy chế tiếp nhận, giải quyết hồ sơ thủ tục hành chính trực tuyến của Bộ.

- Kết nối, tích hợp cổng dịch vụ công của Bộ với Cổng dịch vụ công quốc gia đáp ứng theo Quy chuẩn kỹ thuật quốc gia về cấu trúc, định dạng dữ liệu gói tin phục vụ kết nối Cổng Dịch vụ công quốc gia với cổng Dịch vụ công, hệ thống thông tin một cửa điện tử cấp bộ, cấp tỉnh và các cơ sở dữ liệu quốc gia, chuyên ngành tại Thông tư số 18/2019/TT-BTTTT ngày 25/12/2019 của Bộ TT&TT.

- Thiết lập kho lưu trữ hồ sơ điện tử tập trung và thực hiện số hóa hồ sơ, kết quả giải quyết thủ tục hành chính phục vụ kết nối, chia sẻ dữ liệu trong giải quyết thủ tục hành chính trên môi trường điện tử.

- Hoàn thành việc nâng cấp các dịch vụ công mức độ 2 và mức độ 3 lên mức độ 4 trên hệ thống của Bộ và của đơn vị.

Định kỳ sáu tháng, các đơn vị liên quan báo cáo Lãnh đạo Bộ tiến độ thực hiện Kế hoạch triển khai dịch vụ công trực tuyến mức độ 4 năm 2020 của Bộ.

Link tham khảo: http://antoanthongtin.vn/ca-cqnn/day-manh-cung-cap-dich-vu-cong-truc-tuyen-muc-do-4-trong-nam-2020-106076

2. CEO FIIN: "DN tín dụng đen Trung Quốc chiếm hơn 60% giao dịch cho vay qua app tại Việt Nam"

Cho đến thời điểm này, chưa có một con số thống kê chính xác các doanh nghiệp của Trung Quốc núp bóng người Việt cho vay online với mức lãi suất "cắt cổ" tại thị trường Việt Nam. Theo ông Nguyễn Hòa Bình, Chủ tịch Nexttech cho biết, hiện nay có khoảng 60 – 70 doanh nghiệp của Trung Quốc vào thị trường Việt Nam lập doanh nghiệp và thuê người Việt đứng tên để cho vay tiền online.

Tuy nhiên, ông Trần Việt Vĩnh, CEO của FIIN – một công ty hoạt động theo mô hình cho vay ngang hàng (P2P) cho rằng, có khoảng 20 doanh nghiệp Trung Quốc núp bóng kiểu này nhưng đang triển khai hơn 60 app cho vay online ở thị trường Việt Nam.

Ông Trần Việt Vĩnh cho biết, các doanh nghiệp Trung Quốc thường đăng ký núp bóng thành các công ty hoạt động kinh doanh tại Việt Nam và cho vay theo mô hình hoạt động của công ty tài chính, nhưng lại không có giấy phép kinh doanh dịch vụ tài chính tại Việt Nam. Mỗi doanh nghiệp Trung Quốc này thường tạo ra nhiều app với tên gọi khác nhau để tiếp cận tới người vay trên môi trường mạng Internet. Qua các app cho vay online này, các doanh nghiệp Trung Quốc cung cấp dịch vụ "tín dụng đen, cho vay nặng lãi" với lãi suất thậm chí có thể lên tới 700%/năm. Sau đó, họ sử dụng các hình thức thu đòi nợ kiểu "khủng bố tinh thần", bôi nhọ người vay hoặc làm phiền người có liên quan trong danh bạ của người vay.

CEO của FIIN đưa ra một con số thống kê khá giật mình rằng các doanh nghiệp tín dụng đen này của Trung Quốc lại đang chiếm tới hơn 60% số lượng giao dịch cho vay online qua app tại Việt Nam. Nếu khách hàng bị dính bẫy tín dụng đen đội lốt ứng dụng cho vay trực tuyến do các doanh nghiệp Trung Quốc điều hành sẽ phải trả lãi phí "cắt cổ", lên tới 700%/năm. "Nếu không trả lãi, khách hàng sẽ bị bọn chúng đe doạ, và bôi nhọ danh dự, nhân phẩm trên mạng xã hội. Không chỉ có vậy, những người thân quen của người vay cũng bị quấy rối, làm phiền", ông Trần Việt Vĩnh nói.

CEO của FIIN cho rằng, nếu không có biện pháp ngăn chặn kịp thời các doanh nghiệp tín dụng đen này của Trung Quốc đang hoành hành tại Việt Nam sẽ ảnh hưởng đến các công ty Fintech tại Việt Nam đang hoạt động theo mô hình P2P. Đồng thời làm cho người dân có hiểu nhầm cứ app cho vay online là tín dụng đen, là cho vay nặng lãi nên sẽ không sử dụng dịch vụ nữa. Như vậy, khách hàng sẽ có tâm lý e ngại, lo sợ khi tiếp cận dịch vụ tài chính số.

Bên cạnh đó, các công ty của Trung Quốc đang núp bóng doanh nghiệp Việt sẽ gây nhiễu loạn thông tin. Hậu quả là các cơ quan quản lý nhà nước sẽ gặp khó khăn trong việc xây dựng hành lang pháp lý cho các doanh nghiệp đổi mới sáng tạo thật sự trong lĩnh vực Fintech, kìm hãm sự phát triển của các mô hình dịch vụ tài chính mới trên mạng Internet như P2P.

Cũng theo ông Vĩnh, theo số liệu của Ngân hàng thế giới, tỷ lệ người dân Việt Nam khó tiếp cận hoặc chưa tiếp cận được các dịch vụ tài chính trực tuyến chính thức còn cao, tới gần 70%. Theo xu hướng phát triển của thế giới và khu vực, các giải pháp đổi mới sáng tạo dựa trên nền tảng công nghệ để cung ứng dịch vụ tài chính số trên môi trường online sẽ nở rộ trong thời gian tới. "Vì vậy, cơ quan quản lý nhà nước cần sớm ban hành khung pháp lý thí điểm (sandbox) cho các mô hình dịch vụ mới như P2P Lending. Các khung pháp lý thí điểm này sẽ tạo cơ hội công bằng cho các doanh nghiệp nội địa được tiếp cận và tham gia cung ứng dịch vụ tài chính trực tuyến. Đồng thời, cần công khai danh sách các công ty hoạt động đúng mô hình và đang trong chương trình thí điểm", ông Trần Việt Vĩnh nói.

Các công ty Fintech của Việt Nam cũng cho rằng, một trong những yếu tố rất quan trọng đó chính là vai trò của truyền thông thông tin để người dân có thể tự phân biệt được các dấu hiệu nhận biết các công ty Trung Quốc núp bóng app cho vay online. Qua đó, người dân có thể dễ dàng phân biệt những hoạt động tín dụng đen, cho vay nặng lãi với các công ty công nghệ tài chính của Việt Nam đang hoạt động theo đúng quy định của pháp luật.

Khuyến nghị: Hiện nay có rất nhiều app giao dịch cho vay tài chính được quảng cáo và giới thiệu, người dùng cần tìm hiểu kỹ thông tin để tránh bị lừa đảo và bảo đảm an toàn thông tin.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/ceo-fiin-dn-tin-dung-den-trung-quoc-chiem-hon-60-giao-dich-cho-vay-qua-app-tai-viet-nam-639136.html

3. Cisco vá lỗ hổng an ninh nghiêm trọng trong sản phẩm ASA và FTD

Cisco vừa phát hành bản cập nhật an ninh xử lý hơn 30 lỗ hổng trong nhiều sản phẩm, gồm 12 lỗ hổng ở mức độ cao ảnh hưởng đến Adaptive Security Appliance (ASA) và Firepower Threat Defense (FTD).

Adaptive Security Appliance (ASA) và Firepower Threat Defense (FTD) là các giải pháp an ninh đầu cuối kết hợp tường lửa, chống virus, phòng chống xâm nhập và mạng ảo VPN do Cisco sản xuất.

Lỗi nghiêm trọng nhất được phát hiện là CVE-2020-3187 (điểm CVSS 9.1) có thể bị khai thác để tấn công directory traversal, đọc hoặc xóa file trên hệ thống tồn tại lỗ hổng.

Theo Cisco, lỗi xảy ra do không xác thực chính xác đầu vào của các URL HTTP, cho phép kẻ tấn công gửi các truy vấn HTTP chứa các chuỗi ký tự để tấn công directory traversal. Vì vậy, các file bị xóa sẽ được khôi phục khi thiết bị tải lại.

Cisco giải thích: "Hacker chỉ có thể xem và xóa file trong hệ thống file của dịch vụ web. Hệ thống file này được bật khi thiết bị được cấu hình tính năng WebVPN hoặc AnyConnect. Lỗi này không giành được quyền truy cập đến các file hệ thống ASA hay FTD hay các file hệ điều hành bên dưới".

Các bản cập nhật được phát hành để xử lý lỗ hổng này gồm có:

ASA Software 9.6.4.40

ASA Software 9.8.4.15

ASA Software 9.9.2.66

ASA Software 9.10.1.37

ASA Software 9.12.3.2

ASA Software 9.13.1.7

FTD Software 6.4.0.8 và 6.5.0.4 (các bản phát hành 6.2.3.16 và 6.3.0.6 sắp công bố đều đã được cập nhật các bản vá này).

Cisco cũng xử lý lỗ hổng tấn công từ chối dịch vụ trong:

Tiêu chuẩn bảo mật SSL (Secure Sockets Layer)/ TLS (Transport Layer Security) (CVE-2020-3283)

Chức năng VPN System Logging - ghi log trong hệ thống VPN (CVE-2020-3189)

Tính năng mở tunnel GRE của FTD (CVE-2020-3179)

DNS qua gói Ipv6 (CVE-2020-3191)

Tính năng kiểm tra Giao thức điều khiển cổng đa phương tiện (MGCP - Media Gateway Control Protocol) (CVE-2020-3254)

Điều khiển hander trong SSL/TLS (CVE-2020-3196) và triển khai OSPF (CVE-2020-3298) của ASA và FTD.

Các lỗ hổng ở mức nguy cơ cao được vá gồm lỗi trong tính năng xác thực Kerberos của ASA (CVE-2020-3125), lộ thông tin trong giao diện dịch vụ web của ASA và FTD (CVE-2020-3259) và rò rỉ bộ nhớ trong quá trình thực hiện OSPF trong ASA và FTD (CVE-2020-3195).

Cisco đã phát hành bản cập nhật phần mềm để vá các lỗ hổng này nhưng không phải tất cả các sản phẩm bị ảnh hưởng đều có bản vá hoàn chỉnh. Hãng cho biết hiện chưa tìm thấy dấu hiệu khai thác các lỗ hổng trên thực tế hay mã khai thác bị công khai.

Ngoài các lỗ hổng này, Cisco cũng đưa ra khuyến cáo cho 23 lỗ hổng ở mức độ trung bình trong phần mềm FTD On-Box, Umbrella, Giám sát trình điều khiển quản lý tích hợp (IMC), UCS Director, UCS Director Express cho Big Data, FTD, Ứng dụng quản lý bảo mật nội dung (SMA), Hosted Collaboration Mediation Fulfillment (HCM-F), ASA, Firepower Management Center (FMC) và Firepower User Agent.

Chi tiết về các lỗ hổng có thể xem tại
https://tools.cisco.com/security/center/publicationListing.x

Khuyến nghị: Người quản trị và người dùng cần cập nhật 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-va-lo-hong-an-ninh-nghiem-trong-trong-san-pham-asa-va-ftd.13588/

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	Netgear	CVE 2017 18855 CVE 2017 18698 CVE 2018 21213 ...	Nhóm 133 lỗ hổng trong thiết bị của Netgear (WNR854T, D7800, R6100,…) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã tùy ý, tấn công giả mạo XSS.	Đã có thông tin xác nhận và bản vá.
2	Huawei	CVE 2020 9068 CVE 2020 1805 CVE 2020 1804 …	Nhóm 12 lỗ hổng trong các thiết bị của Huawei (smartphones, PCManager,…) cho phép đối tượng tấn công thu thập thông tin, tấn công từ chối dịch vụ, leo thang đặc quyền.	Đã có thông tin xác nhận và bản vá
3	Mozilla	CVE 2020 6823 CVE 2020 6826 CVE 2020 6825 …	Nhóm 10 lỗ hổng trong phần mềm của Mozilla (Firefox version < 75, Firefox ESR < 68.7, Thunderbird < 68.7.0) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã tùy ý, tấn công phishing URI.	Đã có thông tin xác nhận và bản vá
4	Wordpress	CVE 2020 12070 CVE 2020 11025 CVE 2020 12462 …	Nhóm 09 lỗ hổng trong phần mềm Wordpress (Advanced Woo Search Plugin, Ninja Forms Plugin, LearnPress Plugin,…) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã tùy ý, tấn công XSS, CSRF, SQL injection.	Đã có thông tin xác nhận và bản vá
5	Apache	CVE 2020 9481 CVE 2020 9488 CVE 2019 12425 …	Nhóm 07 lỗ hổng trong một số thành phần của Apache (Apache ATS, Log4j, OFBiz, NiFi Registry, …) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã từ xa, tấn công CSRF.	Đã có thông tin xác nhận và bản vá

6	IBM	CVE 2019 4750 CVE 2019 4751 CVE 2019 4729 …	Nhóm 07 lỗ hổng trong các sản phẩm của IBM (Cloud App Management, Cognos Analytics,…) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã tùy ý, tấn công giả mạo, tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
7	Google	CVE 2019 20791 CVE 2020 7645	Nhóm 02 lỗ hổng trong một số thành phần của Google (OpenThread,…) cho phép đối tượng tấn công chèn và thực thi mã từ xa.	Chưa 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.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.