BẢN TIN NỘI BỘ

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

1. Bộ TT&TT phê duyệt kế hoạch tổ chức thực hiện các nhiệm vụ phát triển Chính phủ điện tử đến năm 2020

Theo kế hoạch, thời gian tới, song song với việc triển khai các nhiệm vụ phát triển Chính phủ điện tử đến năm 2020 của Bộ Thông tin và Truyền thông (TT&TT), Bộ sẽ tập trung theo dõi, đôn đốc, hỗ trợ các Bộ, ngành, địa phương hoàn thành các mục tiêu, chỉ tiêu nêu tại Nghị quyết 17 của Chính phủ. Đồng thời, Bộ TT&TT cũng sẽ đánh giá tổng thể việc triển khai thực hiện các nhiệm vụ trong Nghị quyết 17 của Chính phủ, định kỳ hàng quý báo cáo Chính phủ về tình hình thực hiện Nghị quyết này, bao gồm những tồn tại, khó khăn vướng mắc để đề xuất phương án tháo gỡ, giải quyết.

Tại kế hoạch, Bộ TT&TT đã nhấn mạnh mục tiêu và các chỉ tiêu chính trong phát triển Chính phủ điện tử tại Việt Nam đến hết năm 2020 đã được Chính phủ đề ra tại Nghị quyết 17, cụ thể: Đưa thông tin và dịch vụ của Chính phủ tới mọi người, mọi lúc, mọi nơi; 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; Phát triển Chính phủ điện tử dựa trên dữ liệu và dữ liệu mở hướng tới Chính phủ số, nền kinh tế số và xã hội số; Bảo đảm an toàn thông tin và an ninh mạng; Nâng xếp hạng Chính phủ điện tử theo đánh giá của Liên Hợp quốc tăng từ 10 đến 15 bậc năm 2020, đưa Việt Nam vào nhóm 4 nước dẫn đầu ASEAN trong xếp hạng Chính phủ điện tử theo đánh giá của Liên Hợp quốc đến năm 2025.

Bộ TT&TT đã đề ra 22 chỉ tiêu chính cần thực hiện đến hết năm 2020, trong đó có một số chỉ tiêu mang tính chất định lượng như: ít nhất 20% số lượng người dân và doanh nghiệp tham gia hệ thống thông tin Chính phủ điện tử phải được xác thực định danh điện tử thông suốt và hợp nhất trên tất cả các hệ thống thông tin của các cấp chính quyền từ trung ương đến địa phương; Tỷ lệ hồ sơ giải quyết trực tuyến trên tổng số hồ sơ giải quyết thủ tục hành chính của từng Bộ, ngành, địa phương phải đạt 20% trở lên; Tích hợp 30% các dịch vụ công trực tuyến mức độ 3, 4 của các Bộ, ngành, địa phương với Cổng Dịch vụ công quốc gia; 100% hồ sơ giải quyết thủ tục hành chính được thực hiện thông qua Hệ thống thông tin một cửa điện tử cấp Bộ, cấp Tỉnh; 50% Cổng Dịch vụ công cấp Bộ, cấp Tỉnh cung cấp giao diện cho các thiết bị di động; 100% dịch vụ công được hỗ trợ giải đáp thắc mắc cho người dân, doanh nghiệp; 100% các phần mềm quản lý văn bản và điều hành của các Bộ, ngành, địa phương được kết nối, liên thông qua trục văn bản quốc gia phục vụ gửi, nhận văn bản điện tử.…

Đáng chú ý, trong Kế hoạch triển khai thực hiện các nhiệm vụ phát triển Chính phủ điện tử đến hết năm 2020 của Bộ TT&TT, Bộ cũng đã giao cụ thể cơ quan chủ trì, cơ quan phối hợp và đặt rõ thời gian cần hoàn thành những nội dung công việc của từng nhiệm vụ như:

Về nhiệm vụ 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, cụ thể là việc nghiên cứu, đề xuất sửa đổi Quy chế phối hợp trong hoạt động bảo đảm an toàn, an ninh thông tin trên mạng phù hợp với tình hình thực tiễn, Cục An toàn thông tin được giao chủ trì sẽ cùng phối hợp với Bộ Công an, Bộ Quốc phòng và Ban Cơ yếu Chính phủ. Thời hạn đến tháng 12/2019 sẽ trình Thủ tướng Chính phủ xem xét phê duyệt Quy chế mới sửa đổi.

Ban Cơ yếu Chính phủ được giao chủ trì xây dựng Chính phủ điện tử bảo đảm gắn kết chặt chẽ với bảo đảm an ninh, an toàn thông tin, an ninh quốc gia, bảo vệ thông tin cá nhân. Cụ thể, hết Quý II/2020, Ban Cơ yếu Chính phủ phải triển khai dịch vụ chứng thực chữ ký số, xác thực điện tử cho các hệ thống thông tin và các thiết bị di động để thuận tiện cho việc sử dụng của cán bộ, công chức, viên chức, các cơ quan nhà nước. Hết quý IV/2020, Ban Cơ yếu Chính phủ cần tập trung phát triển, mở rộng hạ tầng kỹ thuật chứng thực điện tử chuyên dùng Chính phủ đáp ứng yêu cầu cung cấp, quản lý và sử dụng chữ ký số phục vụ xây dựng Chính phủ điện tử.

Trong kế hoạch theo dõi, đôn đốc, thúc đẩy triển khai các nhiệm vụ xây dựng Chính phủ điện tử, Ban Cơ yếu Chính phủ cũng được giao chủ trì nhiệm vụ xây dựng 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, thời gian hoàn thành trong quý IV/2019.

Trong kế hoạch này, Bộ TT&TT cũng xác định rõ những giải pháp chủ yếu để thực hiện được các mục tiêu, nhiệm vụ đã đề ra, như xác định Tỉnh điểm, Bộ điểm để tổ chức triển khai điểm về Chính phủ điện tử, chính quyền điện tử. Trên cơ sở đó nhân rộng mô hình thành công cho các Bộ, địa phương trên toàn quốc.

Link tham khảo: http://www.antoanthongtin.vn/Detail.aspx?CatID=c89750d1-fc5f-482b-b5b0-babc105c84de&NewsID=df22083f-1b13-4322-8538-609557f66463

2. Facebook lại để lộ dữ liệu người dùng

Gần 100 nhà phát triển ứng dụng được Facebook tạo điều kiện tiếp cận dữ liệu người dùng không hạn chế. Lỗi này hoàn toàn của Facebook.

Theo đó, tên và ảnh profile của người dùng Facebook đã bị một nhóm các nhà phát triển tiếp cận từ tháng 4/2018.

Sự cố xảy ra do thay đổi của Facebook sau bê bối Cambridge Analytica từ tháng 3 năm ngoái. Thay đổi này vô tình tạo điều kiện cho nhà phát triển ứng dụng tiếp cận thông tin người dùng.

Facebook đã yêu cầu các nhà phát triển ứng dụng liên quan xóa bỏ toàn bộ thông tin mà họ đã truy cập từ hệ thống.

Facebook không nói rõ nhóm phát triển ứng dụng nào chịu trách nhiệm trong việc này. Ngoài ra, không có thông tin về việc dữ liệu người dùng nào đã bị làm dụng.

Trong một động thái liên quan, Facebook đã chặn hàng nghìn ứng dụng mà không nêu lý do tại sao. CEO Zuckerberg còn cho biết công ty cân nhắc cấm cả quảng cáo chính trị trên mạng xã hội này.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần lưu ý không lưu những thông tin nhạy cảm trên ứng dụng để đảm bảo an toàn thông tin khi sử dụng mạng xã hội.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/bao-mat/facebook-lai-de-lo-du-lieu-nguoi-dung-586163.html

3. Apple Mail trên macOS lưu trữ nội dung email mã hóa trong plaintext

Ứng dụng Apple Mail trên macOS lưu trữ các email được mã hóa ở dạng plaintext bên trong cơ sở dữ liệu có tên snippets.db.

Lỗi được phát hiện vào đầu năm nay bởi một chuyên gia của Apple có tên Bob Gendler.

Tới nay, lỗi này vẫn không được khắc phục, mặc dù Gendler đã nói với công ty về vấn đề này hồi tháng 7.

Lỗi xảy ra do tính năng cho phép Siri cung cấp thông tin về các số liên lạc theo yêu cầu của người dùng.

Theo Gendler, Siri sử dụng một quy trình gọi là "suggest" để quét các ứng dụng khác nhau để lấy thông tin liên hệ. Bất cứ thứ gì tìm thấy, Siri sẽ lưu trữ bên trong tệp snippets.db để sử dụng khi cần đưa ra gợi ý về số liên lạc.

Gendler phát hiện ra rằng nếu người dùng đã cấu hình Apple Mail để gửi và nhận email được mã hóa, Siri sẽ thu thập phiên bản dạng plaintext của các email, lưu trữ chúng trong cơ sở dữ liệu này.

"Đây là một vấn đề lớn đối với các chính phủ, tập đoàn và những người thường xuyên sử dụng email được mã hóa và luôn cho rằng thông tin của mình sẽ được bảo vệ", Gendler nói trong một bài đăng trên blog được công bố trong tuần này.

"Thông tin mật hoặc tuyệt mật, những bí mật kinh doanh… sẽ bị lộ lọt bằng cách này, trong cơ sở dữ liệu này"

Gendler nói rằng lỗi xuất hiện trên tất cả các phiên bản macOS từ Sierra đến Catalina mới nhất.

Chuyên gia nói rằng việc vô hiệu hóa Siri sẽ không có tác dụng gì cả, vì quy trình "gợi ý" sẽ tiếp tục lấy các email để có thể sẵn sàng vào lần tiếp theo Siri được kích hoạt.

Cách duy nhất để ngăn Siri tiếp cận các email được mã hóa là yêu cầu nó không đọc nội dung từ Apple Mail.

Có 3 cách để vô hiệu hóa các quá trình này:

1) Vào System Preferences → Siri → Siri Suggestions & Privacy, sau đó bỏ chọn Apple Mail.

2) Chạy từ Mac Terminal lệnh sau (như một người dùng bình thường, không cần quyền truy cập quản trị viên):

defaults write com.apple.suggestions SiriCanLearnFromAppBlacklist -array com.apple.mail

3) Triển khai cấu hình System-Level (cho tất cả người dùng) để tắt Siri khỏi việc lấy dữ liệu từ Apple Mail.

Gendler cho biết tùy chọn thứ ba là vĩnh viễn, vì một bản cập nhật hệ điều hành trong tương lai sẽ không vô tình kích hoạt lại việc lấy nội dung email của Siri.

Bước cuối cùng, là xóa tệp snippets.db. Việc để Siri ngừng quét nội dung Apple Mail không có nghĩa tệp này tự động xóa, vì vậy người dùng sẽ cần phải tự làm điều đó. Tệp được đặt trong "/Users/(username)/Library/Suggestions/".

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng macOS cần cập nhật ngay khi có bản vá để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/apple-mail-tren-macos-luu-tru-noi-dung-email-ma-hoa-trong-plaintext.12924/

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	Adobe	CVE-2019-8088 CVE-2019-8084 CVE-2019-8081	Nhóm 09 lỗ hổng trên phần mềm Adobe (Experience Manager versions 6.5, 6.4, 6.3, …) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã lệnh từ xa.	Đã có thông tin xác nhận và bản vá.
2	Apache	CVE-2019-0205 CVE-2014-2945 CVE-2019-0210	Nhóm 05 lỗ hổng trên phần mềm Apache (Thrift, Airflow, Struts…) cho phép đối tượng tấn công chèn và thực thi mã lệnh từ xa.	Đã có thông tin xác nhận và bản vá
3	Cisco	CVE-2011-2538	01 lỗ hổng trên sản phẩm của Cisco (Cisco Video Communications Server) cho phép đối tượng tấn công có quyền điều khiển và thực thi mã lệnh từ xa Lổ hổng có điểm CVSS cao 9.0	Đã có thông tin xác nhận và bản vá
4	D-link	CVE-2019-10079 CVE-2019-12415	Nhóm 03 lỗ hổng trên thiết bị D-link (DIR-865, DIR-865l …)cho phép đối tượng tấn công thu thập thông tin	Đã có thông tin xác nhận và bản vá
5	Tp-link	CVE-2013-4848	01 lỗ hổng trên thiết bị Tp-link (TL-WDR4300) cho phép đối tượng tấn công khai thác thông tin người dùng để tấn công giả mạo trên trình duyệt web của mục tiêu. Lổ hổng có điểm CVSS cao 9.3	Đã có thông tin xác nhận và bản vá
6	Google	CVE-2019-5043 CVE-2016-5202	Nhóm 02 lỗ hổng trên Google (Google Chrome, Nest CAM IQ Indoor)cho phép đối tượng tấn công tấn công từ chối dịch vụ	Đã có thông tin xác nhận và bản vá
7	Linksys	CVE-2013-4658	01 Lổ hổng trên router của Linksys (EA6500) cho phép đối tượng tấn công chiếm	Đã có thông tin

			quyền điều khiển hệ thống thiết bị. Lổ hổng có điểm CVSS đặc biệt nghiêm trọng 10.0	xác nhận và bản vá
8	Rconfig	CVE-2019-16663 CVE-2019-16662	Nhóm 02 lỗ hổng trong Rconfig (version 3.9.2) cho phép đối tượng tấn công chèn và thực thi mã lệnh từ xa. Lổ hổng có điểm CVSS đặc biệt nghiêm trọng 10.0, 9.0	Đã có thông tin xác nhận và bản vá
9	Advantech	CVE-2019-18229 CVE-2019-18227 CVE-2019-13551 CVE-2019-13547	Nhóm 04 lổ hổng trên một số thành phần, sản phẩm của Advantech (WISE-PaaS/RMM) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã lệnh 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	o6jwuwuds.ru
5	soplifan.ru
6	xjpakmdcfuqe.com
7	xdqzpbcgrvkj.ru
8	l677e13te.ru
9	somicrososoft.ru
10	morphed.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.