BẢN TIN NỘI BỘ

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

1. Dữ liệu số - nền tảng phát triển Chính phủ số

Ngày 09/4/2020 Chính phủ đã ban hành Nghị định số 47/2020/NĐ-CP về quản lý, kết nối, chia sẻ dữ liệu số của cơ quan nhà nước. Đây là một mốc quan trọng trong quá trình xây dựng Chính phủ điện tử hướng tới Chính phủ số.

Nghị định số 47/2020/NĐ-CP là văn bản quy phạm pháp luật đầu tiên đặt trọng tâm vào vấn đề dữ liệu trong Chính phủ điện tử. Nếu như các văn bản pháp luật trước đó chủ yếu đề cập đến hệ thống thông tin và cơ sở dữ liệu (như Luật Công nghệ thông tin, Luật An toàn thông tin mạng) thì Nghị định này trọng tâm vào dữ liệu, là nội dung bên trong và là yếu tố cốt lõi trong xây dựng Chính phủ điện tử. Thêm vào đó, Nghị định này nhấn mạnh "dữ liệu số" sẽ là nền tảng để phát triển hướng tới Chính phủ số.

Nghị định quy định làm rõ các nội dung về quản lý dữ liệu trong cơ quan nhà nước để xây dựng hạ tầng dữ liệu trong Chính phủ điện tử bền vững và nhất quán. Cụ thể:

Quy định quy trình, yêu cầu để xác lập danh mục cơ sở dữ liệu quốc gia (CSDLQG), CSDL của Bộ, ngành, địa phương đã được quy định tại Luật Công nghệ thông tin. Các CSDL này sẽ tạo thành hệ thống các CSDL lõi trong cơ quan nhà nước có mối quan hệ, thống nhất với nhau. Các CSDLQG sẽ là các CSDL chứa dữ liệu chủ (master data) để các CSDL trong cơ quan nhà nước tham chiếu tạo sự nhất quán và đồng bộ trong toàn hệ thống các CSDL trong cơ quan nhà nước. CSDLQG xác định phạm vi đựa trên dữ liệu và mục đích chứ không chỉ dựa trên tên của lĩnh vực.

Dữ liệu phải được xây dựng tạo thuận lợi chia sẻ cho bên ngoài, được xác định ngay từ khi xây dựng thay vì chỉ tập trung xây dựng phục vụ nhu cầu nội bộ làm hạn chế chia sẻ dữ liệu. Các hệ thống thông tin trong cơ quan nhà nước khi được xây dựng phải được xác định các hạng mục xây dựng cấu trúc dữ liệu, chia sẻ dữ liệu cũng như khai thác dữ liệu được chia sẻ ngay từ khi triển khai; hạng mục duy trì, kết nối chia sẻ cũng phải được xác định rõ ràng.

Xác định được vai trò của dữ liệu đối với phát triển Chính phủ số, Nghị định đã đặt vấn đề Chính phủ cũng như các Bộ, ngành, địa phương phải có chiến lược về dữ liệu để định hình phương hướng và tầm nhìn khi triển khai xây dựng dữ liệu với sự dẫn dắt của Chiến lược dữ liệu quốc gia. Đây là nhiệm vụ phải thực hiện trong thời gian tới.

Dữ liệu là yếu tố trọng tâm để phát triển Chính phủ điện tử phục vụ người dân, doanh nghiệp

Trong Nguyên tắc của Nghị định đã khẳng định: Dữ liệu hình thành trong hoạt động của cơ quan nhà nước được chia sẻ phục vụ các hoạt động của cơ quan nhà nước hướng tới phục vụ người dân, doanh nghiệp. Đồng thời, Nghị định cũng đưa ra quy định để thực thi nguyên tắc thu thập dữ liệu một lần (Once-Only). Khi dữ liệu đã được cơ quan nhà nước thu thập và quản lý, chia sẻ thì cơ quan nhà nước sẽ không

được yêu cầu người dân, doanh nghiệp cung cấp lại. Nội dung này được đề cập trong cả Nguyên tắc chung của Nghị định cũng như Nguyên tắc quản lý dữ liệu. Thêm vào đó, công dân, doanh nghiệp có quyền yêu cầu cơ quan nhà nước đang quản lý dữ liệu cá nhân của mình chia sẻ cho cơ quan nhà nước khác để hạn chế phải cung cấp lại dữ liệu tạo thuận tiện cho người dân, doanh nghiệp và đơn giản hóa thủ tục hành chính.

Tiếp cận về quản lý, kết nối và chia sẻ phù hợp với định hướng hiện đại, theo xu hướng công nghệ mới

Một trong những điểm mới trong Nghị định về quản lý, kết nối, chia sẻ dữ liệu số của cơ quan nhà nước là các quy định được dựa trên các cách thức tiếp cận về dữ liệu, chia sẻ dữ liệu, sử dụng công nghệ mới trong bối cảnh hiện nay. Cụ thể:

- Sử dụng dịch vụ chia sẻ dữ liệu làm nền tảng cơ bản cho hoạt động kết nối, chia sẻ dữ liệu trong cơ quan nhà nước. Thay vì triển khai kết nối theo hướng "bắt tay trực tiếp", "xin-cho" thì Nghị định đưa vào các quy định theo hướng chia sẻ dữ liệu là phục vụ cho các cơ quan khác qua "dịch vụ chia sẻ dữ liệu" theo "đăng ký, yêu cầu". Dịch vụ chia sẻ dữ liệu được triển khai qua giao diện API của hệ thống thông tin, là cách thức thông dụng, phổ biến hiện nay. Việc xác định chia sẻ dữ liệu qua dịch vụ cũng là tiền đề để triển khai các giải pháp mới hướng tới xây dựng đám mây dữ liệu của Chính phủ số trong tương lai.

- Việc chia sẻ dữ liệu cũng qua hai hình thức là chia sẻ dữ liệu mặc định và chia sẻ dữ liệu theo yêu cầu đặc thù đáp ứng tất cả các trường hợp chia sẻ dữ liệu thực tế. Chia sẻ dữ liệu mặc định được ưu tiên triển khai và xác định: coi dữ liệu như "hàng hóa" được chuẩn hóa thay vì "tự cung tự cấp" để cung cấp rộng rãi cho các cơ quan nhà nước tạo điều kiện thuận lợi tối đa cho lưu thông dữ liệu trong Chính phủ điện tử.

- Lần đầu tiên, Nghị định đã đưa ra chính sách để thực hiện các công việc Quản trị dữ liệu. Đây là nội dung rất cần thiết khi dữ liệu ngày càng đóng vai trò và trọng tâm trong ứng dụng công nghệ thông tin để bảo đảm dữ liệu ngày càng bền vững, tin cậy và được làm giàu. Để thực hiện quản trị dữ liệu, các cơ quan nhà nước sẽ phải thực hiện các nội dung công việc như kiểm kê, đánh giá chất lượng dữ liệu hàng năm, tích hợp dữ liệu phục vụ ra quyết định, xây dựng chiến lược dữ liệu để có tầm nhìn dài hạn về phát triển dữ liệu.

Đơn giản hóa quá trình kết nối, chia sẻ dữ liệu số, tạo hành lang pháp lý minh bạch và thuận lợi cho dữ liệu lưu chuyển từ nơi có đến nơi cần

Để giải quyết vướng mắc và thúc đẩy quá trình chia sẻ dữ liệu giữa các cơ quan nhà nước, Nghị định đã quy định rõ việc cung cấp, chia sẻ và sử dụng dữ liệu trong cơ quan nhà nước. Quá trình kết nối, chia sẻ dữ liệu có một số điểm sau:

- Quá trình kết nối và chia sẻ dữ liệu là quá trình chuẩn bị sẵn sàng, đăng ký và cấp quyền khai thác các dịch vụ dữ liệu (chia sẻ dữ liệu mặc định) và được chuẩn hóa phù hợp với đa mục đích khai thác khác nhau. Chỉ khi dịch vụ dữ liệu chưa có sẵn thì các cơ quan mới cần trao đổi và chia sẻ dữ liệu theo yêu cầu đặc thù. Điều này

giúp các dịch vụ dữ liệu ngày càng tinh gọn và hiệu quả, thuận lợi cho việc quản lý, vận hành, duy trì và tiết kiệm kinh phí.

- Việc đăng ký và đáp ứng chia sẻ dữ liệu cũng như quản lý, đáp ứng các yêu cầu chia sẻ dữ liệu được thực hiện trực tuyến dựa trên các hệ thống quản lý dịch vụ chia sẻ dữ liệu, tạo điều kiện thuận lợi cũng như tăng cường tính minh bạch, có kiểm soát của quá trình chia sẻ dữ liệu. Xử lý vướng mắc cũng có quy định rõ ràng cho các cơ quan khi gặp khó khăn trong quá trình thực hiện.

- Mỗi cơ quan chỉ định một cán bộ chuyên trách về dữ liệu để cung cấp thông tin, tiếp nhận và xử lý các vấn đề về kết nối, chia sẻ dữ liệu và các vấn đề khác về dữ liệu.

- Thực hiện kết nối, chia sẻ và sử dụng cũng có quy định rõ về thời hạn sử dụng dữ liệu, tạm ngừng, chấm dứt chia sẻ dữ liệu để làm căn cứ xử lý các vấn đề phát sinh khi sử dụng, khai thác dữ liệu.

Thiết đặt nền tảng cho chính phủ mở, quy định dữ liệu mở làm cơ sở để thúc đẩy sự phát triển và sáng tạo của xã hội, cộng đồng

Chính phủ mở là một nấc phát triển của Chính phủ điện tử khi Chính phủ cung cấp dữ liệu cho cộng đồng để thực hiện chủ trương "Nhà nước kiến tạo phát triển". Lần đầu tiên, một văn bản pháp lý đưa nội dung "Dữ liệu mở của cơ quan nhà nước" đánh dấu một mốc quan trọng để thực thi chủ trương này, đồng thời cũng thể hiện sự tích cực của Việt Nam khi sẵn sàng cung cấp dữ liệu mở cho cộng đồng, người dân, doanh nghiệp. Quy định pháp lý về dữ liệu mở cũng là một nội dung khá mới không chỉ đối với Việt Nam mà còn đối với nhiều nước trên thế giới khi công bố dữ liệu mở của các nước chủ yếu được triển khai dưới dạng sáng kiến.

Nội dung quy định về dữ liệu mở được xây dựng trên cơ sở tương thích với các quy định thông dụng phổ biến trên thế giới như: dữ liệu mở phải toàn vẹn, phản ánh đầy đủ thông tin cần cung cấp, cập nhật, máy có thể đọc được, ở định dạng mở, miễn phí, tự do sử dụng...

Nghị định cũng quy định các cơ quan nhà nước phải xây dựng một kế hoạch và triển khai cung cấp dữ liệu mở theo kế hoạch đã xây dựng. Kế hoạch phải đảm bảo có yêu cầu tối thiểu và phù hợp với nhu cầu của người dân, doanh nghiệp. Cơ chế triển khai dữ liệu mở cũng tạo cơ hội cho người dân, doanh nghiệp trong xã hội, cộng đồng tham gia ý kiến phản hồi, đóng góp mở rộng dữ liệu mở.

Link tham khảo: http://antoanthongtin.vn/chinh-sach---chien-luoc/du-lieu-so---nen-tang-phat-trien-chinh-phu-so-106026

2. Nhiều ứng dụng chống virus phổ biến dễ bị lỗ hổng bảo mật

Rack911 Labs vừa tiết lộ 28 chương trình chống virus phổ biến, bao gồm Microsoft Defender, McAfee Endpoint Security và Malwarebytes, đang đối diện với lỗ hổng bảo mật.

Theo Engadget, báo cáo cho biết lỗ hổng bảo mật này cho phép kẻ tấn công xóa các tập tin cần thiết và có thể được sử dụng để nhắc nhở người dùng cài đặt phần mềm độc hại. Cuộc tấn công được biết đến với tên "symlink races", chúng sử dụng

các liên kết tượng trưng và các mối nối thư mục để liên kết các tập tin độc hại với các tập tin hợp pháp trong suốt thời gian giữa việc quét một tập tin để tìm virus và khi nó bị xóa.

Đáng chú ý, Rack911 Labs cho rằng cách tiếp cận không chỉ hoạt động trên các bộ phần mềm bảo mật mà còn trên các nền tảng hệ điều hành khác nhau.

Những kẻ xâm nhập vẫn sẽ cần phải tải xuống và chạy mã cần thiết trước khi khởi chạy một cuộc tấn công "symlink races", vì vậy đây là một công cụ để tạo điều kiện cho một vi phạm hiện có hơn là bắt đầu nó. Các nhà nghiên cứu cũng lưu ý hầu hết các nhà cung cấp phần mềm bảo mật (AVG, F-Secure, McAfee và Symantec) đã sửa lỗi, trong khi một số vẫn chưa.

Điều này khiến một số phần mềm chống virus vẫn dễ bị tổn thương, làm giảm hiệu quả trong việc chống virus của nó và làm cho phần mềm độc hại gây ra những hậu quả nhất định. Các nhà nghiên cứu khuyến khích người dùng cần thường xuyên cập nhật phần mềm bảo mật ngay cả khi chỉ đơn giản là giảm thiệt hại tiềm tàng nếu ai đó xâm phạm vào hệ thống của người dùng.

Khuyến nghị: Người dùng cần chắc chắn luôn cập nhật phiên bản mới nhất của phần mềm diệt virus để bảo đảm an toàn thông tin.

Link tham khảo: https://thanhnien.vn/cong-nghe/nhieu-ung-dung-chong-virus-pho-bien-de-bi-lo-hong-bao-mat-1216635.html

3. Apple vá hai lỗ hổng zero-day trên iOS

Các nhà nghiên cứu của ZecOps vừa công bố hai lỗ hổng zero-day ảnh hưởng đến ứng dụng Mail mặc định trên iOS. Cả hai đều có thể bị tấn công từ xa và đã bị khai thác trên thực tế trong nhiều năm.

Để khai thác, hacker chỉ cần gửi một email đến ứng dụng Mail mặc định trên các thiết bị iOS (iPhone hoặc iPad).

Theo Satnam Narang, trưởng nhóm nghiên cứu: "Khai thác những lỗ hổng này có thể cho phép kẻ tấn công làm rò rỉ, chỉnh sửa hoặc xóa các email trong ứng dụng Mail. Nghiêm trọng hơn, nếu kết hợp với một lỗi trong kernel chưa được vá khác sẽ tạo điều kiện cho kẻ tấn công giành được quyền truy cập vào thiết bị.".

Lỗ hổng đầu tiên là lỗi ghi out-of-bound (ghi ngoại vi).

- Thư viện bị ảnh hưởng:

"/System/Library/PrivateFrameworks/MIME.framework/MIME"

- Chức năng dính lỗ hổng: "[MFMutableData appendBytes:length:]"

Lỗ hổng thứ hai là một lỗi tràn bộ nhớ heap (heap overflow) có thể được kích hoạt từ xa.

Cả hai lỗi này đều do cùng một nguyên nhân: không xử lý chính xác giá trị trả về từ các cuộc gọi của hệ thống.

Để khai thác lỗ hổng không nhất thiết phải có một lượng email thật sự lớn, chỉ cần vừa đủ để có thể làm tiêu hao bộ nhớ RAM. Có nhiều cách để thực hiện điều này, như sử dụng RTF (Rich text format) hoặc các phương pháp khác.

Lỗ hổng có thể được kích hoạt trước khi toàn bộ email được tải về, vì vậy nội dung email sẽ không nhất thiết phải được lưu giữ trên thiết bị. Không loại trừ khả năng kẻ tấn công có thể xóa toàn bộ các email còn lại nếu khai thác thành công.

Trên iOS 13, kẻ tấn công sẽ không cần tương tác từ nạn nhân nếu ứng dụng Mail được mở ở chế độ chạy nền.

Tấn công trên iOS 12 sẽ cần nạn nhân click vào email. Khi đó cuộc tấn công sẽ được kích hoạt trước khi hiển thị nội dung email và người dùng không nhận ra dấu hiệu bất thường nào.

Riêng trên iOS 12, lỗ hổng sẽ được kích hoạt không cần tương tác từ người dùng nếu kẻ tấn công kiểm soát được máy chủ mail.

Cả hai lỗ hổng đều tồn tại kể từ bản iOS 6 (phát hành tháng 09/2012) khi iPhone 5 được ra mắt. Cuộc tấn công đầu tiên được phát hiện là trên iOS 11.2.2 vào tháng 01/2018.

Mục tiêu của kẻ tấn công là các cá nhân từ các tổ chức thuộc Fortune 500 của Bắc Mỹ, cùng với các chuyên gia đến từ một nhà mạng tại Nhật Bản và một số mục tiêu "VIP" khác.

Apple đã phát hành bản iOS 13.4.5 beta để giảm thiểu nguy cơ bị tấn công từ hai lỗ hổng này. Bản vá chính thức sẽ sớm cập nhật đến người dùng.

Theo các chuyên gia, trong thời gian chờ cập nhật bản vá chính thức, người dùng nên tắt ứng dụng Mail trên các thiết bị iOS.

Khuyến nghị: Người dùng không nên sử dụng ứng dụng mail mặc định trên iOS cho đến khi có bản vá lỗ hổng để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/apple-va-hai-lo-hong-zero-day-tren-ios.13520/

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	Oracle	CVE 2020 2950 CVE 2020 2915 CVE 2020 2961 …	Nhóm 228 lỗ hổng trong các sản phẩm của Oracle (Oracle Business Intelligence Enterprise Edition, Enterprise Manager Base Platform,…) cho phép đối tượng tấn công truy cập trái phép, kiểm soát hệ thống máy chủ bị nhiễm, tấn công DoS.	Đã có thông tin xác nhận và bản vá.
2	Netgear	CVE 2019 20638 CVE 2019 20767 CVE 2020 11770 …	Nhóm 155 lỗ hổng trong các thiết bị của Netgear (MR1100, D6100, D3600, R7800,…) cho phép đối tượng tấn công thu thập thông tin, tấn công command injection, tấn công XSS.	Đã có thông tin xác nhận và bản vá
3	Microsoft	CVE 2020 0969 CVE 2020 0970 CVE 2020 0967 …	Nhóm 113 lỗ hổng trong các sản phẩm của Microsoft (chakracore and edge, internet explorer 9/11, windows_products,…) cho phép đối tượng tấn công 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
4	Google	CVE 2020 6438 CVE 2020 6441 CVE 2020 6445 …	Nhóm 41 lỗ hổng trong các phần mềm của Google (version < 81.0.4044.92, Google Android 8,9,10) cho phép đối tượng tấn công chèn và thực thi mã tùy ý, leo thang đặc quyền.	Đã có thông tin xác nhận và bản vá
5	Cisco	CVE 2019 1866 CVE 2020 3126 CVE 2020 3260 …	Nhóm 19 lỗ hổng trong các thiết bị của Cisco (Cisco Webex Meetings, Webex Business Suite, IoT Field Network Director,…) cho phép đối tượng tấn công thực thi mã	Đã có thông tin xác nhận và bản vá

			từ xa, tấn công giả mạo, tấn công từ chối dịch vụ, tấn công CSRF.	
6	IBM	CVE 2019 4593 CVE 2020 4274 CVE 2020 4294 …	Nhóm 19 lỗ hổng trong phần mềm IBM (QRadar7.3.0 7.3.3,Maximo Asset Management 7.6, MQ 9.0 and 9.1,…) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã từ xa, tấn công từ chối dịch vụ, tấn công giả mạo.	Chưa có thông tin xác nhận và bản vá
7	Samsung	CVE 2015 8546 CVE 2015 5524 CVE 2015 9547 …	Nhóm 04 lỗ hổng trong các thiết bị của SamSung (Galaxy mobile,…) cho phép đối tượng tấn công thu thập thông tin, thực thi mã từ xa, tấn công giả mạo.	Chưa có thông tin xác nhận và bản vá
8	Zoom	CVE 2020 11877 CVE 2020 11876 CVE 2019 18822	Nhóm 03 lỗ hổng trong phần mềm Zoom (Zoom Call Recording 6.3.1, Zoom Client for Meetings 4.6.11) cho phép đối tượng, truy cập trái phép, leo thang đặc quyền.	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	xdqzpbcgrvkj.ru
7	xmlinstcp.ddbbvt.eu
8	xjpakmdcfuqe.in
9	xjpakmdcfuqe.ru
10	xjpakmdcfuqe.biz

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.