BẢN TIN NỘI BỘ

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

1. Ban Cơ yếu Chính phủ chịu trách nhiệm trong việc gửi, nhận văn bản điện tử của Đảng

Ngày 02/01/2020, Ban Chấp hành Trung ương Đảng đã ban hành Quy định 217-QĐ/TW về việc gửi, nhận văn bản điện tử trên mạng thông tin diện rộng của Đảng và trên mạng Internet.

Trong đó, về việc tổ chức thực hiện, Ban Cơ yếu Chính phủ chịu trách nhiệm trong việc bảo đảm đầy đủ, kịp thời các chứng thư số theo yêu cầu ký số, bảo mật để gửi, nhận văn bản điện tử trên mạng; bảo đảm các sản phẩm mật mã tích hợp vào các phần mềm, đáp ứng yêu cầu sử dụng; hướng dẫn, hỗ trợ tích hợp giải pháp ký số, bảo mật vào các phần mềm ứng dụng phục vụ cho việc gửi, nhận văn bản trên mạng và gửi qua thư điện tử.

Quy định 217-QĐ/TW quy định việc gửi, nhận văn bản điện tử trên mạng thông tin diện rộng của Đảng và trên mạng Internet của các cơ quan Đảng thông qua các phần mềm Hệ thống thông tin điều hành tác nghiệp; gửi, nhận văn bản và thư điện tử công vụ.

Quy định này áp dụng đối với các cơ quan Đảng (bao gồm cả các đơn vị trực thuộc) từ Trung ương đến địa phương; các cơ quan, tổ chức có liên quan đến hoạt động gửi, nhận văn bản với các cơ quan Đảng nếu hạ tầng kỹ thuật, công nghệ đáp ứng được yêu cầu.

Văn bản điện tử đã ký số theo quy định của pháp luật được gửi, nhận trên mạng tại Quy định 217-QĐ/TW có giá trị pháp lý tương đương văn bản giấy. Văn bản điện tử không ký số được gửi, nhận trên mạng chỉ có giá trị tham khảo, không có giá trị pháp lý.

Quy định về gửi, nhận văn bản trên mạng cần chú ý, tất cả các văn bản có nội dung thông tin "không mật" thuộc thẩm quyền ban hành và giải quyết của các cơ quan Đảng được gửi, nhận trên mạng; văn bản có độ "mật" phải được mã hóa bằng sản phẩm mật mã của ngành Cơ yếu (cụ thể là của Ban Cơ yếu Chính phủ); văn bản có độ "tối mật" và "tuyệt mật" phải do bộ phận nghiệp vụ cơ yếu thực hiện gửi, nhận qua đường cơ yếu. Việc soạn thảo, lưu trữ, khai thác văn bản điện tử có nội dung thông tin mật có quy định riêng, đảm bảo tuân thủ theo Luật Bảo vệ bí mật nhà nước.

Văn bản điện tử sẽ được gửi, nhận thông qua phần mềm hệ thống thông tin điều hành tác nghiệp; phần mềm gửi, nhận văn bản trên mạng Internet; thư điện tử công vụ hoặc trục liên thông văn bản quốc gia.

Quy định 217-QĐ/TW của Ban Chấp hành Trung ương Đảng có hiệu lực từ ngày 02/01/2020.

Link tham khảo: http://antoanthongtin.vn/chinh-sach---chien-luoc/ban-co-yeu-chinh-phu-chiu-trach-nhiem-trong-viec-gui-nhan-van-ban-dien-tu-cua-dang-105808

2. Bộ TT&TT: Chủ động ngăn chặn thông tin sai sự thật trên mạng xã hội về dịch do virus Corona

Theo mic.gov.vn, ngày 31/1/2020, Bộ TT&TT đã có công văn 267 gửi các cơ quan báo chí, Sở TT&TT các tỉnh, thành phố trực thuộc Trung ương về việc tuyên truyền phòng, chống dịch viêm đường hô hấp cấp do virus Corona gây ra.

Công văn cho hay, dịch bệnh do virus Corona gây ra đang diễn biến rất phức tạp, rất nghiêm trọng. Ngày 31/1/2020, Tổ chức Y tế thế giới (WHO) đã ban bố tình trạng khẩn cấp toàn cầu (PHEIC) về dịch viêm đường hô hấp cấp do chủng mới của virus Corona gây ra.

Thực hiện chỉ đạo của Ban Bí thư, Thủ tướng Chính phủ về phòng, chống dịch bệnh, Bộ TT&TT yêu cầu các cơ quan báo chí và Sở TT&TT các tỉnh, thành phố trực thuộc Trung ương tập trung tổ chức công tác thông tin, tuyên truyền phòng, chống dịch bệnh.

Cụ thể, Bộ TT&TT yêu cầu các cơ quan báo chí bám sát sự chỉ đạo của Ban Bí thư tại công văn 79 ngày 29/1/2020; chỉ đạo của Thủ tướng Chính phủ tại Chỉ thị 05 ngày 28/1/2020; thông tin do Ban Chỉ đạo Quốc gia, Bộ Y tế về việc phòng, chống dịch bệnh viêm đường hô hấp cấp do chủng mới của virus Corona gây ra; phản ánh nỗ lực và quyết tâm của các ngành, các cấp và địa phương trong phòng, chống dịch bệnh.

Cùng với đó, các cơ quan báo chí cần tăng thời lượng, số lượng tin, bài khuyến cáo, hướng dẫn người dân nhận thức đầy đủ nguy cơ và cách thức phòng ngừa dịch bệnh, nâng cao ý thức người dân tuân thủ các khuyến cáo, biện pháp của cơ quan chức năng nhằm hạn chế sự lây lan của dịch bệnh. Không lơ là, chủ quan nhưng không được gây hoang mang, lo lắng trong xã hội; không để ảnh hưởng đến quan hệ đối ngoại với các nước.

Đồng thời, báo chí cũng cần cập nhật thường xuyên, liên tục, chính xác, đầy đủ trên tất cả loại hình báo chí về diễn biến tình hình dịch bệnh và các biện pháp phòng chống, ngăn chặn lây lan dịch bệnh từ nguồn chính thức của Ban Chỉ đạo Quốc gia phòng, chống dịch bệnh viêm đường hô hấp do chủng mới của virus Conora gây ra, của Bộ Y tế và các cơ quan có thẩm quyền.

"Không sử dụng "tít" và nội dung bài nghi vấn, suy đoán, gán ghép, liên hệ thiếu căn cứ, không đúng bản chất sự việc, thận trọng và phải kiểm chứng thông tin từ các cơ quan chức năng khi khai thác thông tin từ báo chí nước ngoài", công văn của Bộ TT&TT lưu ý.

Với hệ thống thông tin cơ sở, Bộ TT&TT đề nghị tập trung thời lượng, tần suất tuyên truyền, phổ biến trên hệ thống cơ sở truyền thanh - truyền hình cấp huyện, đài truyền thanh cấp xã những thông tin khuyến cáo người dân và cộng đồng để phòng ngừa, hạn chế dịch bệnh theo tài liệu của Ban Chỉ đạo Quốc gia, Bộ Y tế về phòng, chống dịch bệnh viêm đường hô hấp cấp do chủng mới của virus Conora gây ra.

Theo đó, tập trung thông tin khuyến cáo người dân cần hạn chế các hoạt động có nguy cơ gây bệnh và dấu hiệu nhận biết khi nhiễm bệnh để chủ động đi khám, thông báo ngay cho cơ sở y tế khi có các triệu chứng kể trên.

Các Sở TT&TT được yêu cầu phải tăng cường việc kiểm tra, giám sát việc thực hiện nhiệm vụ tuyên truyền về công tác phòng, chống dịch bệnh của các cơ quan báo chí và hệ thống thông tin cơ sở của địa phương; theo dõi thông tin liên tục trên mạng xã hội để phối hợp với các cơ quan có thẩm quyền chủ động đấu tranh ngăn chặn những thông tin sai sự thật gây hoang mang trong dư luận xã hội về tình hình dịch bệnh và xử lý nghiêm các vi phạm về thông tin phòng, chống dịch bệnh.

Liên quan đến công tác tuyên truyền phòng, chống dịch viêm đường hô hấp cấp do virus Corona gây ra, trong Chỉ thị 06 mới ban hành, Thủ tướng Chính phủ tiếp tục yêu cầu Bộ TT&TT chỉ đạo tăng cường thông tin, tuyên truyền về dịch bệnh, các biện pháp phòng, chống dịch bệnh. Đề nghị các cơ quan truyền thông đăng tải các bản tin về tình hình dịch bệnh chính xác, kịp thời và các biện pháp để người dân chủ động phòng, chống dịch, không hoang mang, lo lắng và phối hợp với các cơ quan chức năng phòng chống dịch hiệu quả.

Trên thực tế, những ngày vừa qua, trên mạng xã hội Facebook đã xuất hiện nhiều thông tin giả mạo, thông tin không có kiểm chứng về dịch bệnh viêm đường hô hấp cấp do chủng mới của virus Corona gây ra. Những thông tin này phần nào đã khiến người dân bị hoang mang, lo lắng.

Tại một số địa phương, cơ quan công an đã phối hợp với lực lượng chức năng xử phạt hành chính một số đối tượng tung tin sai sự thật về dịch bệnh trên mạng xã hội. Đơn cử như, theo Chinhphu.vn, ngày 28/1, sau khi xác minh thông tin lan truyền trên mạng xã hội về việc 2 du khách Trung Quốc nghi bị nhiễm virus Corona nhập viện tại Bệnh viện Lê Lợi, thành phố Vũng Tàu, Công an tỉnh Bà Rịa-Vũng Tàu đã xử phạt hành chính đối tượng Trần Văn Tùng (sinh năm 1998, trú tại phường Thắng Nhất, thành phố Vũng Tàu) với số tiền 30 triệu đồng vì đã có hành vi đăng thông tin sai sự thật.

Tiếp đó, theo Sở TT&TT tỉnh Thừa Thiên Huế, ngày 30/1/2020, Phòng An ninh chính trị nội bộ - Công an tỉnh Thừa Thiên Huế đã phối hợp với Sở TT&TT mời chủ tài khoản Facebook Nhàn Lê đến làm việc về việc tung tin sai sự thật trên mạng xã hội liên quan đến dịch do virus Corona gây ra. Cơ quan Công an đã lập biên bản vi phạm hành chính và đề xuất mức xử phạt vi phạm hành chính với chủ tài khoản Facebook Nhàn Lê bằng hình thức phạt tiền, số tiền 12,5 triệu đồng theo quy định điểm a, khoản 3, Điều 64 Nghị định 174 năm 2013 của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, CNTT và tần số vô tuyến điện.

Khuyến nghị: Toàn thể công chức, viên chức, người lao động trong đơn vị tuân thủ việc không tuyên truyền những thông tin sai sự thật về dịch bệnh theo các văn bản Bộ TTTT đã ban hành.

Link tham khảo: https://genk.vn/bo-tttt-chu-dong-ngan-chan-thong-tin-sai-su-that-tren-mang-xa-hoi-ve-dich-do-virus-corona-20200201112347382.chn

3. Cảm biến di động cũng có thể trở thành công cụ tấn công lừa đảo

Sự phức tạp, tinh vi của các hình thức tấn công mạng luôn song hành với tình hình phát triển của thế giới internet. Mới đây, một nhóm chuyên gia bảo mật quốc tế đã phát hiện ra rằng, hacker đang dùng kỹ thuật mới và độc đáo để khởi động cuộc tấn công lừa đảo theo phương thức ít ai ngờ tới, đó là lạm dụng hệ thống cảm biến được tích hợp trong điện thoại thông minh làm công cụ hỗ trợ.

Theo báo cáo của các chuyên gia bảo mật đến từ tổ chức an ninh mạng PhishLabs, những cuộc tấn công dạng này sẽ lạm dụng một tính năng có sẵn trong một số trình duyệt web phổ biến, cho phép xác định và thu thập thông tin về phương hướng và chuyển động của thiết bị. Nói cách khác, hình thức tấn công lừa đảo dạng này sẽ lạm dụng 2 loại cảm biến được tích hợp trên tất mọi chiếc điện thoại di động, máy tính bảng: Con quay hồi chuyển và gia tốc kế.

"Bằng cách kiểm tra sự hiện diện và trạng thái của các loại cảm biến điều khiển này, một trang web có thể xác định thông tin của thiết bị di động và đưa ra những phản hồi tương ứng", báo cáo của PhishLabs cho biết.

Một cuộc tấn công dựa trên cảm biến di động điển hình sẽ bắt đầu bằng một tin nhắn văn bản giả mạo, thường là từ một tổ chức tài chính hoặc những thương hiệu uy tín. Kẻ tấn công sẽ đính kèm trong tin nhắn lừa đảo này một URL độc hại, và lừa nạn nhân nhấp vào liên kết này bằng những kỹ thuật xã hội điển hình.

Thông thường, sau khi bấm vào liên kết độc hại, nạn nhân sẽ được chuyển hướng đến một website trống. Theo phản xạ, nạn nhân sẽ đóng tab chứa website trống và tiếp tục nhấp lại vào liên kết. Ở lần truy cập thứ 2 này, kết quả nhận được sẽ là phản hồi 404 từ máy chủ. Điều này cho thấy những kẻ tấn công đang tận dụng nhiều lớp biện pháp đối phó để không bị phát hiện.

Vậy các cảm biến di động đóng vai trò như thế nào? Các tác nhân độc hại sẽ sử dụng các cuộc gọi đến con quay hồi chuyển và gia tốc kế để xác định loại thiết bị mà nạn nhân đang sử dụng, thu thập một số thông tin liên quan, sau đó sử dụng dữ liệu thu được để triển khai phương án tấn công tối ưu nhất.

Khuyến nghị: Người dùng cần kiểm tra kỹ thông tin các đường link lạ được gửi đến trước khi ấn vào để đảm bảo an toàn thông tin.

Link tham khảo: https://quantrimang.com/cam-bien-di-dong-cung-co-the-tro-thanh-cong-cu-tan-cong-lua-dao-169218

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	Cisco	CVE 2019 15979 CVE 2019 15984 CVE 2019 15975 …	Nhóm 13 lỗ hổng trên một số thành phần, sản phẩm của Cisco (Cisco Data Center Network Manager,...) cho phép đối tượng tấn công chèn và thực thi mã từ xa. 10 lỗ hổng có điểm CVSS đặc biệt nghiêm trọng (9.0, 10.0)	Đã có thông tin xác nhận và bản vá.
2	Android	CVE 2019 9468 CVE 2020 0002 CVE 2019 9469 …	Nhóm 15 lỗ hổng trên hệ điều hành Android (Android kernel Android ID: A 144168326, Android 9,…) cho phép đối tượng tấn công tấn công chèn và thực thi mã tùy ý. 01 lỗ hổng có điểm CVSS nghiêm trọng 9,3	Đã có thông tin xác nhận và bản vá
3	Wordpress	CVE 2019 20361 CVE 2019 20360 CVE 2020 6166 …	Nhóm 14 lỗ hổng trên một số thành phần của phần mềm Wordpress (Minimal Coming Soon & maintenance, WordPress plugin,…) cho phép đối tượng tấn công chèn và thực thi mã tùy ý.	Đã có thông tin xác nhận và bản vá
4	Gitlab	CVE 2019 19088 CVE 2019 19628 CVE 2019 19260 …	Nhóm 21 lỗ hổng trên một số thành phần của Gitlab (Gitlab Enterprise Edition, Community and Enterprise Edition,...) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã tùy ý.	Đã có thông tin xác nhận và bản vá
5	Chrome	CVE 2019 13765 CVE 2019 5844 CVE 2019 13766 …	Nhóm 07 lỗ hổng trên hệ điều hành Chrome (trước version 73.0.3683.75) cho phép đối tượng tấn công chèn và thực thi mã tùy ý.	Đã có thông tin xác nhận và bản vá
6	Samsung	CVE 2012 3810 CVE 2012 3808	Nhóm 04 lỗ hổng trên sản phẩm của Samsung (Samsung	Đã có thông tin

		CVE 2012 3806	Kies) cho phép đối tượng tấn công thực thi mã tùy ý, tấn công từ chối dịch vụ.	xác nhận và bản vá
7	Linux	CVE 2019 19332	01 lỗ hổng trên hệ điều hành Linux (Linux kernel) cho phép đối tượng tấn công có thể tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
8	Apache	CVE 2019 20343 CVE 2020 1925	Nhóm 02 lỗ hổng trên phần mềm Apache (Apache Olingo, MojoHaus Exec Maven) cho phép đối tượng tấn công thực thi mã tùy ý.	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	xjpakmdcfuqe.biz
5	xjpakmdcfuqe.com
6	and30.blabladomdom.com
7	xjpakmdcfuqe.in
8	amnsreiuojy.ru
9	ovrz52z140.ru
10	hzmksreiuojy.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.