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

1. Quy định về việc gửi, nhận văn bản điện tử trên mạng thông tin diện rộng của Đảng và trên mạng Internet

Được ban hành ngày 02/01/2020, Quy định 217-QĐ/TW (sau đây gọi tắt là Quy định 217) 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 217 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.

Nguyên tắc gửi, nhận văn bản trên mạng

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.

Cơ quan phát hành văn bản điện tử không phát hành văn bản giấy đến cơ quan tiếp nhận văn bản điện tử khi đã gửi văn bản điện tử có ký số, ngoại trừ một số trường hợp sau:

Văn bản chung: gồm các văn bản liên quan công tác tổ chức bộ máy, nhân sự, công tác kiểm tra, giám sát, giải quyết khiếu nại, tố cáo; các văn bản liên quan tới việc giải quyết chế độ, chính sách, tài chính,….

Văn bản đặc thù, bao gồm:

- Văn bản của Trung ương như: Các nghị quyết, kết luận của Ban Chấp hành Trung ương; nghị quyết, chỉ thị của Bộ Chính trị, Ban Bí thư; các văn bản kết luận hội nghị Bộ Chính trị, Ban Bí thư; các văn bản kết luận, thông báo kết luận, chỉ đạo trực tiếp địa phương, thông báo ý kiến đồng chí Tổng Bí thư, Thường trực Ban Bí thư; các văn bản liên quan đến tổ chức Đại hội Đảng toàn quốc, hội nghị Trung ương, hội nghị cán bộ toàn quốc, các hội nghị Bộ Chính trị, Ban Bí thư, các cuộc làm việc, tiếp khách của đồng chí Tổng Bí thư, đồng chí Thường trực Ban Bí thư.

- Văn bản của các cơ quan đảng ở Trung ương như: Báo cáo kết quả thực hiện các nghị quyết, chỉ thị của Trung ương; các đề án, công văn, tờ trình, dự thảo nghị quyết, quyết định, quy định, quy chế, kết luận, báo cáo chuyên đề... gửi Bộ Chính trị, Ban Bí thư, Thường trực Ban Bí thư để báo cáo và xin ý kiến; văn bản chỉ đạo liên quan đến các lĩnh vực theo chức năng, nhiệm vụ của cơ quan.

- Văn bản của các cơ quan đảng ở địa phương như: Báo cáo kết quả thực hiện các nghị quyết, chỉ thị của Trung ương; các văn bản xin ý kiến Bộ Chính trị, Ban Bí

thư, Thường trực Ban Bí thư; các đề án, tờ trình, các dự thảo nghị quyết, quyết định, quy định, quy chế, đề án, tờ trình do cơ quan đảng ở địa phương ban hành.

Cơ quan tiếp nhận văn bản điện tử phải thực hiện quy trình: Kiểm tra nguồn gốc, tính hợp thức của văn bản, lấy số và đăng ký văn bản đến trên máy tính, sau đó chuyển văn bản đến người nhận để xử lý.

Chỉ sử dụng mạng Internet để gửi, nhận văn bản điện tử có nội dung thông tin không mật giữa các cơ quan đảng đối với trường hợp bên gửi hoặc bên nhận không có kết nối mạng thông tin diện rộng của Đảng hoặc mạng thông tin diện rộng của Đảng có sự cố kỹ thuật.

Yêu cầu gửi, nhận văn bản qua mạng

Quy định 217 cũng nêu rõ các yêu cầu gửi, nhận văn bản qua mạng:

Thứ nhất: Văn bản điện tử phải bảo đảm yêu cầu về thể loại, thẩm quyền ban hành, thể thức và kỹ thuật trình bày theo quy định của Ban Bí thư và hướng dẫn của Văn phòng Trung ương Đảng.

Thứ hai: Văn bản điện tử phải được bảo đảm tính xác thực về nguồn gốc, tính pháp lý, sự toàn vẹn, an toàn thông tin, dữ liệu trong quá trình gửi, nhận, xử lý và lưu trữ.

Thứ ba: Văn bản điện tử phải được gửi ngay trong ngày ký ban hành, chậm nhất là trong buổi sáng của ngày làm việc tiếp theo. Sau khi tiếp nhận, nếu văn bản điện tử đến bảo đảm giá trị pháp lý phải được xử lý kịp thời, không chờ văn bản giấy (nếu có). Trường hợp văn bản điện tử thuộc loại "khẩn" phải được đặt ở chế độ ưu tiên, ghi rõ mức độ "khẩn", gửi ngay sau khi ký số và phải được trình, chuyển giao xử lý ngay sau khi tiếp nhận.

Thứ tư: Văn bản điện tử gửi, nhận trên mạng phải được theo dõi, cập nhật tự động trạng thái gửi, nhận, xử lý trên hệ thống đối với trường hợp sử dụng phần mềm Hệ thống thông tin điều hành tác nghiệp hoặc trạng thái gửi, nhận với trường hợp sử dụng phần mềm gửi, nhận văn bản trên mạng Internet. Trường hợp gửi qua thư điện tử công vụ, văn bản điện tử phải được cập nhật, quản lý bằng phần mềm Hệ thống thông tin điều hành tác nghiệp.

Thứ năm: Bảo đảm các yêu cầu về hạ tầng kỹ thuật, công nghệ, an toàn thông tin và giải pháp kết nối, liên thông.

Phương thức gửi, nhận văn bản trên mạng

Đối với phương thức gửi, nhận văn bản trên mạng, có 3 phương thức được quy định tại Quy định 217, bao gồm: sử dụng phần mềm Hệ thống thông tin điều hành tác nghiệp được quy định dùng chung trong các cơ quan Đảng để gửi, nhận văn bản điện tử giữa các cơ quan đảng trên mạng thông tin diện rộng của Đảng; Sử dụng phần mềm gửi, nhận văn bản trên mạng Internet hoặc thư điện tử công vụ để gửi, nhận văn bản điện tử giữa các cơ quan Đảng trên mạng Internet; Thông qua Trục liên thông văn bản quốc gia để gửi, nhận văn bản giữa các cơ quan đảng với các cơ quan nhà nước.

Trong trường hợp có sự cố về kỹ thuật hoặc bên gửi hay bên nhận chưa đáp ứng các yêu cầu về hạ tầng kỹ thuật, công nghệ, an toàn thông tin, giải pháp kết nối, liên thông để gửi, nhận văn bản điện tử, các cơ quan gửi văn bản giấy theo đường truyền thống; đồng thời khẩn trương khắc phục các sự cố, triển khai các giải pháp kỹ thuật, kết nối để thực hiện việc gửi, nhận văn bản qua mạng.

Yêu cầu thông tin của văn bản điện tử

Hệ thống thông tin điều hành tác nghiệp, phần mềm gửi, nhận văn bản trên mạng Internet của các cơ quan Đảng phải thể hiện các thông tin sau của văn bản điện tử: Mã định danh của cơ quan, tổ chức (cấu trúc mã định danh cơ quan, tổ chức thực hiện theo Quy định số 15-QĐ/VPTW, ngày 30/01/2018 của Văn phòng Trung ương Đảng); Số và ký hiệu văn bản; Ngày, tháng, năm ban hành văn bản; Thể loại văn bản; Mức độ khẩn (khẩn/thượng khẩn/hoả tốc); Trích yếu nội dung văn bản; Hồ sơ, tài liệu gửi kèm; Trạng thái xử lý (đã đến, đã tiếp nhận, đã chuyển xử lý, đang xử lý, đã hoàn thành, từ chối nhận (trả lại), thu hồi, xoá...); Họ tên người ký; Bên gửi/nhận; Thời gian gửi, nhận; Thời hạn xử lý; Lịch sử gửi, nhận văn bản.

Về tổ chức thực hiện

Văn phòng Trung ương Đảng có trách nhiệm chủ trì, phối hợp với các cơ quan đảng ở Trung ương và các tỉnh uỷ, thành uỷ triển khai, tổ chức, hướng dẫn thực hiện Quy định; Giúp Thường trực Ban Bí thư theo dõi, đôn đốc, kiểm tra việc thực hiện Quy định này; hằng năm chịu trách nhiệm tổng hợp, báo cáo Ban Bí thư về tình hình, kết quả triển khai Quy định; đề xuất sửa đổi, bổ sung nếu cần thiết.

Các cơ quan Đảng chịu trách nhiệm bảo đảm kết nối, liên thông giữa các hệ thống thông tin điều hành tác nghiệp, phần mềm gửi, nhận văn bản trên mạng Internet; Giám sát, kiểm soát việc gửi, nhận văn bản điện tử để bảo đảm an toàn, an ninh thông tin, định kỳ kiểm tra việc thực hiện Quy định 217 tại các cơ quan, đơn vị trực thuộc; Thống nhất kết nối, liên thông Hệ thống thông tin điều hành tác nghiệp với các phần mềm gửi, nhận, quản lý văn bản của cơ quan đảng với các cơ quan nhà nước trong địa phương theo hướng dẫn của Văn phòng Trung ương Đảng; Tổ chức quản lý, định kỳ sao lưu dữ liệu bảo đảm an ninh, an toàn thông tin và chuyển lưu trữ theo quy định. Căn cứ Quy định 217 và tình hình thực tiễn, các cơ quan đảng ban hành quy chế cụ thể, phù hợp để áp dụng thực hiện tại nội bộ cơ quan Đảng.

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 của Ban Chấp hành Trung ương Đảng chính thức có hiệu lực từ ngày 02/01/2020.

Link tham khảo: http://antoanthongtin.vn/chinh-sach---chien-luoc/quy-dinh-ve-viec-gui-nhan-van-ban-dien-tu-tren-mang-thong-tin-dien-rong-cua-dang-va-tren-mang-intern-105982

2. Microsoft: Hacker lợi dụng Covid-19 tấn công mạng mọi quốc gia trên thế giới

Theo nghiên cứu mới từ Microsoft, hacker đã triển khai các cuộc tấn công có chủ đề Covid-19 tại 241 quốc gia và vùng lãnh thổ.

Trên blog đăng hôm 8/4, Microsoft cho biết "mọi quốc gia trên thế giới đều chứng kiến ít nhất một vụ tấn công có chủ đề Covid-19". Các đối tượng xấu thiết kế lại email lừa đảo (phishing) và mã độc khác để nhắc tới căn bệnh này. Các nước đang trải qua dịch bệnh - nơi mọi người cần thông tin y tế nhất - dễ bị tổn thương nhất.

Theo ông Rob Lefferts, Phó Chủ tịch Microsoft 365 Security, các cuộc tấn công theo sát diễn biến dịch bệnh trên toàn cầu. Những nước có số người nhiễm Covid-19 cao nhất đồng thời là các nước bị ảnh hưởng nhiều nhất từ tấn công lợi dụng Covid-19. Sự bối rối, lo lắng, nỗi sợ hãi khiến họ bấm vào những đường link và đó là điều mà hacker mong muốn.

Bộ công cụ an ninh mạng Microsoft Threat Protection phát hiện gần 60.000 email chứa các tập tin đính kèm hoặc URL độc hại liên quan tới Covid-19 được gửi đi mỗi ngày. Tuy nhiên, "tin mừng" là nó chỉ chiếm 2% trong tổng số các email lừa đảo.

Ngoài tấn công lừa đảo, đối tượng xấu còn lợi dụng Covid-19 theo các cách khác, chẳng hạn Zoombombing – tấn công vào các cuộc họp trực tuyến để làm gián đoạn hội nghị.

Khuyến nghị: Người dùng cần kiểm tra kỹ các thông tin về dịch Covid-19 và chỉ tin tưởng vào các trang thông tin chính thống để tránh bị lừa đảo cũng như đảm bảo an toàn thông tin.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/bao-mat/microsoft-hacker-loi-dung-covid-19-tan-cong-mang-moi-quoc-gia-tren-the-gioi-632139.html

3. Google Play Store gỡ ứng dụng Android VPN dính lỗ hổng nghiêm trọng

Google vừa xóa chương trình Android VPN khỏi cửa hàng Google Play sau khi được các nhà nghiên cứu thông báo về một lỗ hổng nghiêm trọng. Ứng dụng này là SuperVPN, đã được tải xuống hơn 100 triệu lần.

Mạng riêng ảo (VPN) cho phép người dùng tạo kết nối được mã hóa đến các máy chủ trực tuyến đóng vai trò là cổng vào Internet. Chúng cho phép người dùng truy cập Internet an toàn khi sử dụng các kết nối không tin cậy. Về lý thuyết, chúng ngăn chặn kẻ xấu đánh hơi được lưu lượng truy cập của người dùng trên các mạng không an toàn. SuperVPN là một trong nhiều chương trình phục vụ chức năng này cho các thiết bị Android.

Tháng 2, VPNpro - một công ty đánh giá và tư vấn các sản phẩm VPN - đã cảnh báo về một lỗ hổng trong sản phẩm này có thể gây ra cuộc tấn công man-in-the-middle (MITM), cho phép kẻ xâm nhập can thiệp vào kết nối người dùng và dịch vụ VPN.

Theo đó, chương trình gửi đi dữ liệu được mã hóa, nhưng đồng thời cũng kèm theo khoá giải mã được hardcode (mã hóa cứng). Giải mã dữ liệu tiết lộ thông tin về

máy chủ SuperVPN, chứng chỉ và thông tin xác thực. VPNpro đã có thể thay thế dữ liệu đó bằng dữ liệu của riêng mình.

Điều này có nghĩa là kẻ tấn công có thể buộc SuperVPN kết nối tới máy chủ giả mạo, cho phép họ xem tất cả dữ liệu của người dùng, bao gồm mật khẩu, văn bản riêng và tin nhắn thoại, theo VPNpro.

Sau khi phát hiện ra lỗ hổng vào tháng 10/2019, VPNpro đã thông báo cho SuperSoftTech, công ty phát triển của SuperVPN – có khả năng có trụ sở tại Bắc Kinh, nhưng không nhận được phản hồi. Vì thế, hãng đã thông báo cho Chương trình Phần thưởng bảo mật của Google Play. Đội ngũ này cũng không nhận được phản hồi từ SuperSoftTech, vì vậy họ đã gỡ chương trình này khỏi cửa hàng Google Play vào ngày 7/4/2020.

Đây không phải là lần đầu tiên SuperVPN được báo cáo tồn tại lỗ hổng an ninh. Ứng dụng cũng đã được đề cập trong một nghiên cứu năm 2016 về các rủi ro bảo mật trong VPN Android, đứng vị trí thứ ba trong bảng xếp hạng các VPN Android thường được gắn cờ là có hoạt động giống như phần mềm độc hại bởi các phần mềm diệt virus.

SuperVPN cũng không phải là VPN Android duy nhất tồn tại lỗ hổng nghiêm trọng khiến người dùng dễ bị tấn công MITM. Kiểm tra nhanh cho thấy một số phần mềm với lỗ hổng tương tự vẫn có mặt trên Play Store.

Khuyến nghị: Người quản trị và người dùng cần gỡ bỏ ứng dụng SuperVPN và đổi lại thông tin đã kết nối qua ứng dụng để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/google-play-store-go-ung-dung-android-vpn-dinh-lo-hong-nghiem-trong.13472/

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	Apache	CVE-2020-1934 CVE-2019-17564 CVE-2020-1927 ...	Nhóm 10 lỗ hổng trong một số thành phần của Apache (HTTP Server, Dubbo NetBeans,…) cho phép đối tượng tấn công tấn công XSS.	Đã có thông tin xác nhận và bản vá.
2	Wordpress	CVE-2020-7947 CVE-2020-6009 CVE-2020-6008 …	Nhóm 10 lỗ hổng trong phần mềm Wordpress (LearnDash plugin, Auth0 plugin,…) cho phép đối tượng tấn công chèn và thực thi mã từ xa, tấn công XSS, SQL Injection.	Đã có thông tin xác nhận và bản vá
3	Apple	CVE-2015-7334 CVE-2020-9769 CVE-2020-3847 …	Nhóm 49 lỗ hổng trong các sản phẩm của Apple (watchOS, macOS Catalina, Apple Safari, tvOS,…) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã từ xa.	Đã có thông tin xác nhận và bản vá
4	Lenovo	CVE-2015-5684 CVE-2015-5684 CVE-2015-7334 …	Nhóm 08 lỗ hổng trong một số thành phần và sản phẩm của Lenovo (Lenovo Solution Center,…) cho phép đối tượng bypassed, tấn công thực thi mã từ xa. 01 lỗ hổng có điểm CVSS: 10.0 (đặc biệt nghiêm trọng).	Đã có thông tin xác nhận và bản vá
5	Gitlab	CVE-2020-10956 CVE-2020-10954 CVE-2020-10952 …	Nhóm 05 lỗ hổng trong Gitlab (Gitlab EE/CE 8.11-12.9.1, Gitlab 8.1,…) cho phép đối tượng tấn công thu thập thông tin, tấn công từ chối dịch vụ, tấn công SSRF.	Đã có thông tin xác nhận và bản vá
6	Zoom	CVE-2020-11500 CVE-2020-11470 CVE-2020-11469	Nhóm 03 lỗ hổng trong Zoom (Zoom Client for Meetings <=4.6.9) cho phép đối tượng tấn công truy cập trái phép tài khoản người dùng, tấn công leo	Chưa có thông tin xác nhận và bản vá

			thang chiếm quyền cao nhất của hệ thống.	
7	Dell	CVE-2020-5344 CVE-2020-5347 CVE-2020-5348	Nhóm 03 lỗ hổng trong thiết bị của Dell (Dell EMC, Dell Latitude 7202) cho phép đối tượng tấn công chèn và thực thi mã tùy ý, tấn công từ chối dịch vụ. 01 lỗ hổng có điểm CVSS: 10.0 (đặc biệt nghiêm trọng).	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	iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
5	xdqzpbcgrvkj.ru
6	xjpakmdcfuqe.in
7	disorderstatus.ru
8	xjpakmdcfuqe.ru
9	amnsreiuojy.ru
10	track.saygggames.io

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.