BẢN TIN NỘI BỘ

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

1. Thách thức từ Covid-19: Cơ hội để phát triển và ứng dụng công nghệ số sâu rộng

Thách thức từ dịch bệnh Covid-19 vừa tạo áp lực vừa mở ra cơ hội để ngành thông tin và truyền thông (TT&TT) phát triển và ứng dụng công nghệ số sâu rộng hơn trong xã hội, để xã hội vẫn vận hành thông suốt theo phương thức mới, thích ứng nhanh với mọi thay đổi.

Đây là nhận định của Thứ trưởng Bộ TT&TT Phan Tâm tại Hội thảo trực tuyến "5G và công nghệ băng thông rộng thúc đẩy phát triển kinh tế số: Tầm nhìn và giải pháp công nghệ" diễn ra ngày 27/3 vừa qua. Hội thảo được tổ chức bởi Hội Vô tuyến Điện tử và Tập đoàn IDG, dưới sự bảo trợ của Bộ TT&TT.

Phát triển hạ tầng số, sẵn sàng đáp ứng nhu cầu bùng nổ về kết nối và xử lý dữ liệu

Phát biểu tại Hội thảo, Thứ trưởng Phan Tâm cho biết: Bộ TT&TT đang nghiên cứu, chủ trì xây dựng Đề án Chuyển đổi số quốc gia với kỳ vọng sớm đưa Việt Nam trở thành quốc gia số, ổn định và thịnh vượng, tiên phong thử nghiệm các công nghệ và mô hình mới, đổi mới căn bản, toàn diện hoạt động quản lý, điều hành của Chính phủ, hoạt động sản xuất kinh doanh của doanh nghiệp (DN), phương thức sống, làm việc của người dân, phát triển môi trường số an toàn, nhân văn, rộng khắp.

Chương trình chuyển đổi số quốc gia sẽ giúp: (1) xây dựng Chính phủ số để Chính phủ hoạt động hiệu quả, hiệu lực hơn, minh bạch hơn; (2) xây dựng nền Kinh tế số thúc đẩy đổi mới sáng tạo, tạo ra giá trị mới, giúp tăng năng suất lao động, tạo động lực tăng trưởng mới, thoát bẫy thu nhập trung bình; (3) xây dựng Xã hội số giúp người dân bình đẳng về cơ hội tiếp cận dịch vụ, đào tạo, tri thức, thu hẹp khoảng cách phát triển, giảm bất bình đẳng. Các ngành, lĩnh vực sẽ được tối ưu hoá, thông minh hóa để nâng cao chất lượng cuộc sống của người dân.

Theo Thứ trưởng Phan Tâm, nền kinh tế số, xã hội số cùng các ứng dụng số đều vận hành dựa trên một hạ tầng số. Do vậy, mục tiêu xuyên suốt trong thời gian tới của ngành TT&TT là phát triển hạ tầng số, sẵn sàng đáp ứng nhu cầu bùng nổ về kết nối và xử lý dữ liệu, có khả năng giám sát mạng lưới đến từng nút mạng và bảo đảm an toàn, an ninh mạng được tích hợp sẵn ngay từ khi thiết kế, xây dựng.

Để hiện thực hóa các mục tiêu trên, Thứ trưởng cho biết, hoạt động đầu tư, kinh doanh dịch vụ viễn thông cần có những đổi mới. Nhà khai thác cần xây dựng kế hoạch phát triển hạ tầng mạng đi trước một bước, tập trung đầu tư mở rộng mạng cáp quang, tăng tỷ lệ dịch vụ Internet cáp quang đến hộ gia đình; mở rộng vùng phủ sóng, nâng cao chất lượng dịch vụ 4G và từng bước triển khai 5G hiệu quả, đầu tư vào trung tâm dữ liệu, hạ tầng điện toán đám mây,…. những thành tố cơ bản của hạ tầng số.

Bên cạnh đó, cần tăng cường chia sẻ, sử dụng chung cơ sở hạ tầng để tiết kiệm chi phí, bảo đảm cảnh quan môi trường và sự an toàn của người dân; đẩy mạnh hợp

tác phát triển các ứng dụng, dịch vụ mang lại nhiều giá trị cho xã hội như: giao thông thông minh, thành phố thông minh,... đồng thời hỗ trợ, thúc đẩy các dịch vụ trực tuyến.

Công nghệ 5G đang được Chính phủ quan tâm và đặt trọng tâm thúc đẩy phát triển thông qua kiến tạo các chính sách thuận lợi và thông thoáng nhất cho DN. Thứ trưởng khẳng định: "Phát triển công nghệ 5G nằm trong chiến lược phát triển hạ tầng và dịch vụ thông tin băng rộng của Việt Nam".

Bên cạnh chính sách phát triển hạ tầng vật lý, các chính sách về quản lý việc cung cấp, sử dụng dịch vụ công nghệ số trên hạ tầng số đang được Bộ TT&TT nghiên cứu đề xuất sửa đổi, bổ sung thường xuyên để theo kịp nhu cầu phát triển của xã hội.

Đối với những mô hình kinh doanh mới có liên quan trong lĩnh vực ICT, chưa được luật pháp quy định rõ ràng, Thứ trưởng cho biết: Bộ TT&TT đang tích cực đề xuất cho phép triển khai thử nghiệm. Theo hướng này, Bộ TT&TT đang thúc đẩy Đề án thí điểm thanh toán không dùng tiền mặt, thông qua hợp tác nghiên cứu chính sách Mobile Money với Diễn đàn kinh tế thế giới (WEF).

Covid -19: Thúc đẩy phát triển và ứng dụng công nghệ số sâu rộng

Theo thông tin của Cục Viễn thông, tính đến hết tháng 1/2020, hạ tầng công nghệ viễn thông Việt Nam có sự phát triển vượt bậc, tổng thuê bao băng rộng cố định là 15,1 triệu thuê bao, tổng thuê bao băng rộng di động đạt gần 65 triệu thuê bao.

Theo thống kê, trong 2 tháng chịu tác động của dịch Covid-19, doanh thu từ hoạt động cung cấp dịch vụ viễn thông tăng gần 28% và dự đoán sẽ tiếp tục tăng trong những tháng kế tiếp.

Đặc biệt, giữa lúc dịch bệnh Covid-19 diễn biến phức tạp, các hoạt động kinh tế "tại gia" trên nền tảng Internet băng rộng đã có bước phát triển nhảy vọt. Theo đó, hạ tầng viễn thông càng trở nên quan trọng, được kỳ vọng là phương thức giúp xã hội thoát khỏi khó khăn do tác động tiêu cực của Covid-19.

Ông Lê Văn Tuấn, Phó Cục trưởng Cục Viễn thông, Bộ TT&TT cho biết: "Dịch bệnh Covid-19 xảy ra, hiện có rất nhiều người ở nhà làm việc, kinh doanh từ xa. Điều đó cho thấy vai trò quan trọng của hệ thống băng rộng cố định".

Còn theo Chủ tịch Hội Vô tuyến điện tử Trần Đức Lai, thực tế chứng minh, chỉ trong vòng 2-3 năm trở lại đây, sự phát triển hạ tầng băng thông rộng đã mở đường cho tất cả các ngành kinh tế khác phát triển.

Theo báo cáo "Nền kinh tế số Đông Nam Á năm 2019" do Google, Temasek và Bain thực hiện, nền kinh tế số Việt Nam năm 2019 trị giá 12 tỉ USD, cao gấp 4 lần so với giá trị của năm 2015 và dự đoán chạm mốc 43 tỉ USD vào năm 2025 với tốc độ tăng trưởng bình quân đạt xấp xỉ 33%.

Còn theo Đại học Tufts (Mỹ), Việt Nam đang đứng ở vị trí 48/60 quốc gia có tốc độ số hóa nền kinh tế trong năm 2019. Chính phủ Việt Nam xác định một trong những trụ cột của nền kinh tế số là hạ tầng viễn thông, bao gồm cả hạ tầng băng rộng di động lẫn băng rộng cố định.

Link tham khảo: http://antoanthongtin.vn/chinh-sach---chien-luoc/thach-thuc-tu-covid-19-co-hoi-de-phat-trien-va-ung-dung-cong-nghe-so-sau-rong-105974

2. SpaceX cấm nhân viên sử dụng ứng dụng Zoom vì lo ngại về quyền riêng tư

SpaceX đã cấm nhân viên sử dụng ứng dụng hội nghị truyền hình Zoom vì những lo ngại về quyền riêng tư và bảo mật quan trọng sau khi cơ quan thực thi pháp luật Mỹ cảnh báo người dùng về sự an toàn của ứng dụng nổi tiếng này.

Việc sử dụng ứng dụng Zoom và các ứng dụng thông tin liên lạc kỹ thuật số khác đã tăng vọt khi nhiều người Mỹ đã được lệnh ở nhà để làm chậm sự lây lan của Covid-19.

Lệnh cấm của SpaceX đối với ứng dụng Zoom minh chứng cho những thách thức gắn kết đối với các nhà sản xuất hàng không vũ trụ khi họ phát triển công nghệ được coi là quan trọng đối với an ninh quốc gia đồng thời cố gắng giữ an toàn cho nhân viên khỏi bệnh hô hấp lây lan nhanh.

Trong một email ngày 28/3, SpaceX đã thông báo với tất cả nhân viên của họ rằng, tất cả quyền truy cập vào ứng dụng Zoom đã bị vô hiệu hóa. Hiện tại, nhiều người trong công ty đã sử dụng ứng dụng này cho các hội nghị và hỗ trợ cuộc họp. Từ bây giờ hãy sử dụng email, văn bản hoặc điện thoại làm phương tiện liên lạc thay thế. Tuy nhiên, một đại diện của SpaceX đã không trả lời yêu cầu bình luận này.

Stephanie Schierholz, phát ngôn viên của cơ quan vũ trụ Mỹ (NASA) cho biết, NASA, một trong những khách hàng lớn nhất của SpaceX cũng cấm nhân viên của mình sử dụng ứng dụng Zoom.

Ngày 30/3, Văn phòng Boston của FBI cũng đã đưa ra cảnh báo về ứng dụng Zoom, trong đó họ khuyên người dùng không nên tổ chức các cuộc họp trên trang web công khai hoặc chia sẻ liên kết rộng rãi sau khi nhận được hai báo cáo về các cá nhân không xác định xâm nhập các buổi học, một hiện tượng chia sẽ màn hình được gọi là zoombombing.

Zoom không trả lời ngay lập tức các yêu cầu bình luận về quyết định của SpaceX, nhưng đã khuyên người dùng nên sử dụng tất cả các chức năng bảo mật trên nền tảng của nó.

Là một nhà thầu quốc phòng, SpaceX có trụ sở tại California đã được phân loại là một doanh nghiệp thiết yếu vì vậy được phép mở cửa hoạt động mặc dù đã có lệnh phong tỏa ở California và Texas.

Khuyến nghị: Người dùng không sử dụng ứng dụng Zoom khi cần trao đổi các thông tin nhạy cảm, tuân thủ các biện pháp bảo mật của ứng dụng để đảm bảo an toàn thông tin.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/bao-mat/spacex-cam-nhan-vien-su-dung-ung-dung-zoom-vi-lo-ngai-ve-quyen-rieng-tu-630346.html

3. Hàng nghìn máy tính chạy SQL Server của Microsoft dính backdoor và mã độc ẩn mình

Các nhà nghiên cứu bảo mật vừa tiết lộ một chiến dịch độc hại nhắm vào các máy tính Windows chạy SQL server của Microsoft (MS-SQL server) để cài backdoor

và các loại mã độc khác, bao gồm cả các công cụ truy cập từ xa (RAT) và đào tiền ảo.

Chiến dịch tấn công này có tên là "Vollgar", sử dụng cách thức brute-force mật khẩu để xâm nhập vào SQL server của Microsoft có thông tin đăng nhập yếu và đang mở công khai dịch vụ SQL Server ra Internet.

Các nhà nghiên cứu cho biết đã có khoảng 2.000 đến 3.000 máy chủ bị lây nhiễm mã độc hằng ngày trong vài tuần qua. Các lĩnh vực bị nhắm đến có thể là y tế, hàng không, công nghệ thông tin và viễn thông, giáo dục trên đại học tại Trung Quốc, Ấn Độ, Mỹ, Hàn Quốc và Thổ Nhĩ Kỳ.

May mắn là, các nhà nghiên cứu đã phát hành một đoạn script cho phép quản trị hệ thống phát hiện các máy chủ SQL Windows bị xâm nhập bằng hình thức tấn công này.

Các bước trong chiến dịch Vollgar: Tấn công MS-SQL sau đó cài mã độc trên hệ thống

Các cuộc tấn công Vollgar bắt đầu bằng cách brute-force mật khẩu đăng nhập vào dịch vụ MS-SQL. Nếu khai thác thành công, nó sẽ cho phép kẻ xâm nhập thực thi một số thay đổi trên cấu hình để chạy lệnh MS-SQL độc hại và tải tệp tin chứa mã độc về thiết bị.

Ngoài việc đảm bảo các file cmd.exe và ftp.exe có các quyền thực thi cần thiết, kẻ đứng sau cuộc tấn công Vollgar cũng tạo ra các tài khoản mới trong cơ sở dữ liệu của MS-SQL và hệ điều hành với đặc quyền cao.

Sau khi hoàn thành quá trình cài đặt, tiến trình sẽ tải các đoạn script (2 đoạn VBScript và một FTP script), các script này được thực thi vài lần, mỗi lần ở vị trí khác nhau trên hệ thống để tránh bị lỗi.

Một trong những payload khởi tạo là SQLAGENTIDC.exe hoặc SQLAGENTVDC.exe, bước đầu cho dừng các tiến trình trong danh sách với mục đích đảm bảo số lượng tài nguyên hệ thống tối đa cũng như loại bỏ các nguy cơ khác và sự hiện diện của chúng trên các máy tính bị lây nhiễm.

Bước tiếp theo, tiến trình này sẽ đưa vào các công cụ truy cập từ xa khác và công cụ đào tiền ảo XMRig như Monero, VDS hay Vollar.

Tấn công hạ tầng lưu trữ trên hệ thống bị xâm nhập

Kẻ tấn công nắm giữ toàn bộ hạ tầng của máy đã bị xâm nhập, bao gồm cả máy chủ C&C đặt tại Trung Quốc.

Một khi máy Windows client bị nhiễm ping được đến máy chủ C&C, thì C&C sẽ nhận được đầy đủ thông tin chi tiết về thiết bị như địa chỉ IP public, vị trí, phiên bản hệ điều hành, tên máy tính và dòng CPU của máy Client.

Có hai chương trình C&C cài trên máy chủ đặt tại Trung Quốc được phát triển bởi hai nhà cung cấp khác nhau. Có những điểm tương đồng trong khả năng kiểm soát từ xa của hai đơn vị này, cụ thể là tải file về, cài đặt các dịch vụ Windows mới, keylogging, chụp màn hình, kích hoạt camera và microphone và thậm chí khởi tạo một cuộc tấn công từ chối dịch vụ phân tán (DDoS).

Sử dụng mật khẩu mạnh để tránh bị tấn công brute-force

Để thực hiện cuộc tấn công này, điều kiện cần là máy chủ MS-SQL có mật khẩu yếu và phải mở dịch vụ MS-SQL ra Internet.

Khuyến nghị: Người quản trị cần đặt khẩu mạnh đối với các thông tin đăng nhập và tuân thủ các quy định để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/hang-nghin-may-tinh-chay-sql-server-cua-microsoft-dinh-backdoor-va-ma-doc-an-minh.13444/

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 2020 3797 CVE 2020 3793 CVE 2020 3805 ...	Nhóm 42 lỗ hổng trong phần mềm Adobe (Photoshop CC 2019, Acrobet and Reader,…) 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.
2	Gitlab	CVE 2020 10953 CVE 2020 10955 CVE 2020 10956 …	Nhóm 05 lỗ hổng trong Gitlab (Gitlab EE/CE 11.1 12.9, Gitlab 8.1,…) cho phép đối tượng tấn công thu thập thông tin, tấn công từ chối dịch vụ, tấn công SSRF.	Chưa có thông tin xác nhận và bản vá
3	Samsung	CVE 2019 20622 CVE 2019 20560 CVE 2019 20561 …	Nhóm 123 lỗ hổng trong thiết bị của Samsung (ID SVE 2019 15230,…) cho phép đối tượng tấn công thu thập thông tin, thực thi mã lệnh tùy ý. 13 lỗ hổng có điểm CVSS: 10.0 (đặc biệt nghiêm trọng)	Đã có thông tin xác nhận và bản vá
4	Firefox	CVE 2020 6805 CVE 2020 6807 CVE 2020 6808 …	Nhóm 05 lỗ hổng trong trình duyệt Firefox (Firefox<74, Firefox ESR<68.6,…) cho phép đối tượng tấn công chèn và thực thi mã tùy ý, tấn công giả mạo.	Chưa có thông tin xác nhận và bản vá
5	Chrome	CVE 2020 6428 CVE 2020 6427 CVE 2020 6424 …	Nhóm 09 lỗ hổng trong trình duyệt Chrome (version trước 80.0.3987.149) cho phép đối tượng tấn công chèn và thực thi mã tùy ý.	Đã có thông tin xác nhận và bản vá
6	Apache	CVE 2019 17559 CVE 2019 17565 CVE 2020 1944 …	Nhóm 06 lỗ hổng trong một số thành phần của Apache (Traffic Server, Apache Shiro,…) cho phép đối tượng chèn và thực thi mã tùy ý.	Đã có thông tin xác nhận và bản vá
7	Wordpress	CVE 2020 9392 CVE 2019 12498	Nhóm 05 lỗ hổng trong phần mềm Wordpress (pricing table	Đã có thông tin

		CVE 2020 10385 …	by supsystic plugin, WP Live Chat Support plugin,…) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã từ xa, tấn công XSS, SQL injection.	xác nhận và bản vá
8	D-link	CVE 2019 12767 CVE 2020 8864 CVE 2020 8863	Nhóm 03 lỗ hổng trong thiết bị của D link (DAP 1650, DIR 867, DIR 878,…) cho phép đối tượng tấn công chèn và thực thi mã lệnh từ xa.	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	ydbnsrt.me
6	xjpakmdcfuqe.in
7	xjpakmdcfuqe.biz
8	xdqzpbcgrvkj.ru
9	xdqzpbcgrvkj.ru
10	amnsreiuojy.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.