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

1. An toàn, an ninh mạng là điều kiện cơ bản, yếu tố sống còn cho công cuộc chuyển đổi số quốc gia

Phát biểu khai mạc Hội thảo ngày An toàn thông tin Việt Nam 2019, đồng chí Bộ trưởng Bộ Thông tin và Truyền thông (TT&TT) Nguyễn Mạnh Hùng đã nhấn mạnh: "Bảo đảm an toàn, an ninh không gian mạng đồng nghĩa với xây đắp cho tương lai, giúp đất nước thịnh vượng hơn. An toàn, an ninh mạng là điều kiện cơ bản, yếu tố sống còn cho công cuộc chuyển đổi số quốc gia, phát triển chính phủ điện tử hướng tới chính phủ số, nền kinh tế số, xã hội số."

Đồng chí nhận định rõ, Thế giới và Việt Nam đã và đang bước vào không gian mạng với cuộc cách mạng số, trong đó có nhiều thách thức và cơ hội song hành. Không gian mạng là một không gian hoàn toàn mới, cứ mỗi giây lại có khoảng 108 cuộc tấn công mạng và 32 mã độc mới được tạo ra. Trên không gian mạng, các quốc gia phải đối mặt với những thách thức giống nhau, và vì vậy, có cơ hội để trở thành một thế giới sát cánh bên nhau.

Trong khuôn khổ Ngày An toàn thông tin (ATTT) Việt Nam năm 2019 năm nay, với chủ đề "Nâng tầm an toàn, an ninh mạng quốc gia trong kỷ nguyên số", đồng chí Bộ trưởng TT&TT đã chỉ ra một một số nội dung cần thực hiện như sau:

Thứ nhất, đã đến lúc chúng ta phải thay đổi cách nghĩ.

Nếu như trước đây, chúng ta đẩy mạnh triển khai ứng dụng và phát triển CNTT trước, thì giờ đây, ứng dụng và phát triển CNTT phải song hành cùng an toàn, an ninh mạng.

Trong mọi dự án CNTT đều phải có cấu phần an toàn, an ninh mạng như một cấu phần bắt buộc. Thủ tướng Chính phủ đã chỉ đạo: tỷ lệ chi cho an toàn, an ninh mạng tối thiểu 10% tổng kinh phí chi cho CNTT. Ở Việt Nam hiện nay, tỷ lệ này đang ở mức dưới 5%.

Nếu như trước đây khi xảy ra ra sự cố, thì chúng ta cố gắng giữ kín, càng ít người biết càng tốt, thì giờ đây, theo Bộ trưởng, chúng ta phải hiểu rằng: không ai an toàn một mình trong không gian mạng. Càng chia sẻ, chúng ta càng an toàn hơn.

"Không chia sẻ thì sau chúng ta lại sẽ là một ai đấy nữa bị tấn công tương tự, và sau đó lại là một người tiếp theo, và cứ như vậy. Mức độ bảo đảm an toàn, an ninh mạng của một cơ quan, tổ chức không phải nằm ở việc cơ quan, tổ chức đó có bị tấn công hay không? Mà nằm ở cách thức cơ quan, tổ chức đó phản ứng như thế nào sau khi bị tấn công.

Chúng ta cần phải có một mạng lưới chuyên gia và đơn vị chuyên trách dưới sự điều phối của cơ quan chức năng. Thông tin phải được chia sẻ kịp thời. Khi sự cố xảy ra với một đơn vị, các đơn vị sẽ cùng coi đây là trách nhiệm của mình, sẵn sàng tham gia ứng cứu theo sự điều phối chung, vì một không gian mạng an toàn hơn cho tất cả chúng ta".

Thứ hai, đã đến lúc chúng ta phải thay đổi cách làm.

Nếu như trước đây, khi đầu tư, chúng ta thường chú trọng đầu tư cho giải pháp, thiết bị mà ít chú trọng đến con người, quy trình, thì giờ đây, con người là quan trọng nhất, sau đó đến quy trình, rồi mới đến giải pháp, thiết bị. Mỗi cơ quan, tổ chức cần bảo đảm tỷ lệ hợp lý, cân đối cả 3 yếu tố này.

Nếu như trước đây, chúng ta thường tự đầu tư, tự bảo đảm an toàn, an ninh mạng cho cơ quan, tổ chức của mình, thì giờ đây, chúng ta phải hiểu rằng, những dịch vụ tốt nhất được cung cấp bởi những doanh nghiệp (DN) chuyên nghiệp nhất.

Các cơ quan, tổ chức một mặt kiện toàn lực lượng tại chỗ, mặt khác thuê dịch vụ giám sát, bảo vệ của các DN đã được Bộ TTTT cấp phép. Định kỳ thực hiện kiểm tra, đánh giá. Bộ TTTT giao Trung tâm Giám sát an toàn không gian mạng quốc gia thuộc Cục ATTT thực hiện giám sát quốc gia trên không gian mạng để phát hiện, cảnh báo sớm nguy cơ mất an toàn, an ninh mạng.

Bộ trưởng nhấn mạnh: “An toàn, an ninh mạng luôn là điều kiện tiên quyết để phát triển chính phủ điện tử".

Thứ ba, về việc nâng cao tiềm lực an toàn, an an ninh mạng quốc gia.

Việt Nam cần phải làm chủ công nghệ để bảo đảm an toàn, an ninh mạng. Cơ quan, tổ chức nhà nước phòng, chống tấn công mạng, ưu tiên sử dụng các sản phẩm “Make in Vietnam”. Tới đây, Bộ TT&TT sẽ giao nhiệm vụ cụ thể cho các doanh nghiệp (DN) tiên phong nhằm phát triển hệ sinh thái sản phẩm an toàn, an ninh mạng Việt Nam phục vụ CPĐT, đô thị thông minh và hệ thống thông tin quan trọng quốc gia.

Hệ sinh thái là một mô hình tổng thể, toàn diện và đầy đủ các giải pháp. DN có thế mạnh về giải pháp nào sẽ được giao để tập trung phát triển sâu, chuyên nghiệp về giải pháp đó, được ưu tiên và khuyến nghị sử dụng.

Cùng với đó, một Liên minh cũng sẽ được thành lập nhằm hợp tác, hỗ trợ lẫn nhau trong phát triển sản phẩm, bảo đảm các sản phẩm có sự liên thông, kết nối. Liên minh DN này cũng cam kết sử dụng sản phẩm của nhau để cung cấp một giải pháp tổng thể cho khách hàng.

Việt Nam có lợi thế lớn khi có xấp xỉ 1 triệu nhân lực trong lĩnh vực ICT. Nguồn nhân lực an toàn, an ninh mạng vào loại tốt trên thế giới, với những chuyên gia đạt đẳng cấp quốc tế.

Cùng với khát vọng vươn lên mạnh mẽ, với sự ủng hộ của Nhà nước và liên kết chặt chẽ của Liên minh, Việt Nam hoàn toàn có thể sinh ra những DN lớn mạnh để trở thành cường quốc an toàn, an ninh mạng, nhằm bảo vệ sự thịnh vượng của Việt Nam trên không gian mạng. Và chúng ta sẽ không bỏ lỡ cơ hội ấy.

Bộ trưởng cũng cho biết: Thời gian vừa qua, cơ quan nhà nước và các DN, chuyên gia đang chung tay, chung sức bảo đảm an toàn, an ninh mạng quốc gia.

Với vai trò là cơ quan quản lý nhà nước, Bộ TT&TT luôn sẵn sàng hướng dẫn, hỗ trợ và tạo điều kiện cho các DN phát triển. Đặc biệt là DN an toàn, an ninh mạng. Cơ quan quản lý nhà nước gần đây đã áp dụng một tư duy mới, không truyền thống,

không tuần tự. Các DN an toàn, an ninh mạng cũng cần một sự đột phá trong tư duy và phương pháp tiếp cận. Chúng ta luôn phải tự tin và vào cuộc thực sự để thực hiện khát vọng của mình.

Qua 12 năm được tổ chức, Ngày ATTT Việt Nam đã trở thành một sự kiện thường niên quan trọng, là diễn đàn để các cơ quan, tổ chức, cá nhân trong và ngoài nước trao đổi, chia sẻ thông tin, kinh nghiệm, giải pháp, góp phần nâng cao nhận thức của xã hội về ATTT. Nhân dịp này, Bộ trưởng Nguyễn Mạnh Hùng kêu gọi và đề nghị:

Thứ nhất, các cơ quan, tổ chức và toàn thể cộng đồng cùng tham gia bảo đảm một không gian mạng an toàn, lành mạnh, rộng khắp. Cần rất nhiều nỗ lực để thực hiện điều này. Cơ quan quản lý nhà nước, các doanh nghiệp và chuyên gia an toàn, an ninh mạng cần là những người có sứ mệnh tiên phong mở đường, chung vai gánh vác trách nhiệm này.

Thứ hai, Hiệp hội ATTT Việt Nam cần đẩy mạnh, thay đổi tư duy và đổi mới hoạt động, giữ vai trò hạt nhân đối với các DN an toàn, an ninh mạng, trở thành cầu nối, sợi dây liên kết giữa các tổ chức, DN trong nước và nước ngoài.

Những sự kiện như Ngày ATTT Việt Nam hàng năm cần được tổ chức nhiều hơn và thiết thực hơn nữa, phát triển thành sự kiện quy mô khu vực và quốc tế.

Thứ ba, Việt Nam cần tham gia tích cực, đóng góp thiết thực hơn cho các hoạt động an toàn, an ninh mạng quốc tế. Đặc biệt đối với các hoạt động do Liên minh Viễn thông thế giới (ITU) khởi xướng. Tạo ra một không gian mạng Việt Nam an toàn, chia sẻ thông tin, tổ chức các sự kiện khu vực và quốc tế, đóng góp cho thị trường quốc tế. Các DN lớn mạnh, sản phẩm an toàn, an ninh mạng chất lượng cao là phương pháp tốt nhất để thực hiện mục tiêu này.

Link tham khảo: http://antoanthongtin.vn/an-toan-thong-tin/an-toan-an-ninh-mang-la-dieu-kien-co-ban-yeu-to-song-con-cho-cong-cuoc-chuyen-doi-so-quoc-gia-105677

2. Trang tin, cổng thông tin điện tử VN thường xuyên bị tấn công mạng

Tình hình an toàn thông tin mạng tại Việt Nam năm 2019 diễn biến rất phức tạp. Dữ liệu giám sát của Trung tâm Ứng cứu khẩn cấp không gian mạng đã ghi nhận nhiều sự kiện an toàn mạng kể từ đầu năm đến nay.

Sáng 24/12, Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC) (Cục An toàn thông tin - Bộ Thông tin và Truyền thông) đã triển khai Chương trình diễn tập khu vực phía Bắc với chủ đề "Diễn tập phòng chống tấn công vào cổng/trang thông tin điện tử".

Theo Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam, trong năm 2019, tình hình an toàn thông tin mạng diễn biến rất phức tạp. Dữ liệu của Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam cũng cho thấy, các cổng/trang thông tin điện tử luôn là nơi hứng chịu nhiều cuộc tấn công nhất của các hacker. Do đó, việc bảo vệ an toàn các cổng, trang thông tin điện tử là vô cùng quan trọng.

Cuộc diễn tập được Bộ TT&TT tổ chức nhằm nâng cao năng lực cho Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia. Thông qua các hoạt động diễn tập, cán bộ ATTT tại các đơn vị thành viên Mạng lưới sẽ được huấn luyện và nâng cao kỹ năng phát hiện - ứng cứu sự cố.

Những chuyên gia tham gia buổi diễn tập sẽ được chia thành các đội. Mỗi đội sẽ được cấp quyền quản lý một hệ thống máy chủ riêng được cài đặt mô phỏng một cổng thông tin điện tử và đang chạy thực trên cloud. Các đội có tài khoản quản trị vào hệ thống máy chủ của mình với địa chỉ được Ban tổ chức cấp cho từng đội.

Các cuộc tấn công mạng hoàn toàn như sự cố tấn công thật vào hệ thống máy chủ của từng đội theo các phương thức khác nhau. Các đội phải đăng nhập vào hệ thống máy chủ, quản trị, bảo vệ hệ thống của mình, kiểm tra, phát hiện sự cố, lấy các bằng chứng (evidences) để phân tích, điều tra, xác định xem hệ thống của mình đang bị sự cố tấn công gì.

Bên cạnh đó, nhiệm vụ của các đội tham gia còn là tìm kiếm con đường mà hacker xâm nhập vào hệ thống. Ngoài ra, họ phải tìm hiểu xem hacker đã đánh cắp, chỉnh sửa những gì, từ đó có phương án ứng phó, xử lý. Với cách làm mới này, các đội được diễn tập đúng như thực tế sự cố xảy ra trên hệ thống thực.

Chia sẻ tại buổi diễn tập, Thứ trưởng Bộ TT&TT Nguyễn Thành Hưng cho rằng, tình hình an ninh mạng tại Việt Nam sẽ ngày càng nghiêm trọng hơn trong thời gian tới, khi mà dữ liệu, tài sản số của ngày càng nhiều. Tình hình trên đòi hỏi chúng ta phải có nhận thức cao hơn trong việc phòng, chống tấn công mạng, cũng như có khả năng cao hơn trong việc sẵn sàng ứng cứu khi xảy ra các sự cố.

Theo Thứ trưởng Nguyễn Thành Hưng, nhận thức, hành động liên quan đến công tác đảm bảo an toàn thông tin của các bộ, ngành, địa phương đã ngày càng tăng lên, song do điều kiện chủ quan và khách quan nên mối quan tâm thực sự vẫn chưa đồng đều giữa các đơn vị, có nơi làm tốt nhưng cũng có nơi còn làm chưa tốt.

Thứ trưởng Nguyễn Thành Hưng cho rằng, trong công tác đảm bảo an toàn thông tin, cần phải thực hiện việc "phòng bệnh hơn chữa bệnh". Do vậy, thông qua cuộc diễn tập lần này, Bộ TT&TT mong muốn các thành viên mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia có thể trao đổi với các chuyên gia, nhà quản lý và thực hành việc diễn tập phòng chống tấn công mạng vào các cổng/ trang thông tin điện tử.

Điều này sẽ góp phần cho việc đảm bảo an toàn thông tin cho các cổng/trang thông tin điện tử của các bộ, ngành, địa phương và hỗ trợ tốt hơn cho chủ trương xây dựng Chính phủ điện tử, cung cấp các dịch vụ công trực tuyến cho người dân, doanh nghiệp.

Team 11 gồm 2 đ/c của Cục Bưu điện Trung ương cùng với thành viên từ 3 đơn vị khác đã nỗ lực và đạt kết quả đứng thứ 3 sau team đứng thứ nhất – đội Viettel và team đứng thứ 2 - đội các ngân hàng trên tổng số gần 20 đội tham dự.

Link tham khảo: https://vietnamnet.vn/vn/thong-tin-truyen-thong/trang-tin-cong-thong-tin-dien-tu-vn-thuong-xuyen-bi-tan-cong-boi-toi-pham-mang-602974.html

3. Lỗ hổng trên Twitter cho phép hacker thu thập dữ liệu, kiểm soát tài khoản

Một lỗ hổng trong ứng dụng Twitter trên Android bị hacker khai thác nhằm thu thập thông tin nhạy cảm hoặc chiếm quyền kiểm soát tài khoản. Lỗ hổng không ảnh hưởng đến phiên bản dành cho iOS.

Mới đây, Twitter đã ra thông báo về bản vá cho lỗ hổng này. Công ty cho biết, họ đã thông báo cho người dùng bị lộ thông tin qua email và ứng dụng Twitter.

Những người dùng không thể cập nhật bản vá được khuyên sử dụng phiên bản web của Twitter để bảo vệ tài khoản và ngăn chặn các tấn công tiềm ẩn.

Theo Twitter, lỗ hổng có thể bị khai thác nhằm thu thập dữ liệu như tin nhắn, các tweet và thông tin địa điểm, thậm chí là chiếm quyền kiểm soát tài khoản người dùng mục tiêu – ví dụ gửi các tweet hoặc tin nhắn trên danh nghĩa người dùng.

Trong khi các chi tiết kĩ thuật không được tiết lộ, một hãng truyền thông tên tuổi đưa tin việc, khai thác lỗ hổng là "một quá trình phức tạp liên quan đến hành động đưa mã độc vào các khu vực lưu trữ bị hạn chế của ứng dụng Twitter."

Twitter cho rằng, không có bằng chứng cụ thể nào cho thấy điểm yếu bị khai thác trong các cuộc tấn công, nhưng cũng không loại trừ hoàn toàn khả năng đó.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng Android cần cập nhật bản vá mới nhất của Twitter để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/lo-hong-tren-twitter-cho-phep-hacker-thu-thap-du-lieu-kiem-soat-tai-khoan.13101/

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	Microsoft	CVE-2019-1485 CVE-2019-1461 CVE-20191476 …	Nhóm 30 lỗ hổng trên một số sản phẩm của Microsoft (Word software, PowerPoint,…) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã lệnh từ xa, tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá.
2	Android	CVE-2019-2232 CVE-2019-2224 CVE-2019-2218 …	Nhóm 17 lỗ hổng trên hệ điều hành Android (Android-10 Android ID:A-141003796,…) 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
3	Qualcomm	CVE-2019-2310 CVE-2019-10494 CVE-2019-10520 …	Nhóm 20 lỗ hổng trên thiết bị Qualcomm (Snapdragon Auto, Snapdragon Consumer IOT...) cho phép đối tượng tấn công chèn và thực thi mã tùy ý. 02 lỗ hổng có điểm CVSS: 10.0 (đặc biệt nghiêm trọng).	Đã có thông tin xác nhận và bản vá
4	Chrome	CVE-2019-13732 CVE-2019-13750 CVE-2019-13741 …	Nhóm 40 lỗ hổng trên trình duyệt Chrome (trước version 79.0.3945.79) cho phép đối tượng tấn công chèn và thực thi mã lệnh từ xa.	Đã có thông tin xác nhận và bản vá
5	Linux	CVE-2019-19447 CVE-2019-19449 CVE-2019-19768 …	Nhóm 07 trên hệ điều hành Linux (Linux kernel) cho phép đối tượng tấn công thực thi mã lệnh từ xa, chiếm quyền điều khiển hệ thống.	Đã có thông tin xác nhận và bản vá
6	Advantech	CVE-2019-3951	01 lỗ hổng trên Advantech (Advantech WebAccess trước version 8.4.3) cho phép đối tượng tấn công chèn và thực thi mã lệnh, tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá

7	Apache	CVE-2014-0242 CVE-2014-0212 CVE-2018-11805 …	Nhóm 04 lỗ hổng trên phần mềm Apache (Apache Spam Assassin, mod-wsgi) cho phép đối tượng tấn công tấn công từ chối dịch vụ.	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	mel.cloudcontentsmak.com
2	zdlnx.tk
3	xblqlxb.cf
4	strikotunrev.top
5	d3s1.me
6	pudloxan.com
7	andandgivingfor.ru
8	oiqbgenbchsss.com
9	maildeliveryyboys.at
10	jimmy.gamboa1102@yahoo.com.com:laura22

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.