BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CƠ QUAN THƯỜNG TRỰC CỦA UỶ BAN QUỐC GIA VỀ CHUYỂN ĐỔI SỐ

BÁO CÁO CHUYÊN ĐỀ

Tuần 12/2022

Tài liệu tham khảo phục vụ Uỷ ban Quốc gia về Chuyển đổi số

Số: **03**/BC-UBQGCĐS Ngày 25 tháng 3 năm 2022 **LƯU HÀNH NỘI BỘ**

Bộ Thông tin và Truyền thông, cơ quan thường trực của Uỷ ban Quốc gia về Chuyển đổi số gửi báo cáo chuyên đề tham khảo phục vụ công tác lãnh đạo, chỉ đạo, điều phối của Ủy ban Quốc gia và Ban Chỉ đạo chuyển đổi số của các bộ, ngành, địa phương như sau:

BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Tháng 6 năm 2021, theo báo cáo xếp hạng an toàn, an ninh mạng toàn cầu (GCI) năm 2020 được Liên minh Viễn thông quốc tế, Việt Nam đã tiến bộ 25 bậc, từ vị trí thứ 50 vươn lên vị trí thứ 25 trong số 194 quốc gia, vùng lãnh thổ được xếp hạng, thứ 7 trong khu vực Châu Á – Thái Bình Dương và thứ 4 khu vực Đông Nam Á.

Đạt được kết quả nêu trên là nhờ nỗ lực lớn của Việt Nam trong một chặng đường dài, thể hiện rõ qua quyết tâm chính trị lớn của Đảng, Chính phủ đối với vấn đề bảo đảm an toàn, an ninh mạng; nỗ lực của các bộ, ngành, địa phương triển khai bảo đảm an toàn thông tin. Thể hiện rõ vai trò của các cơ quan, đơn vị để Việt Nam có một hành lang pháp lý về an toàn, cơ bản đầy đủ.

Các bộ, cơ quan ngang bộ, UBND các tỉnh đã nỗ lực để đưa tỷ lệ bảo đảm an toàn thông tin theo mô hình bốn lớp từ 0% năm 2019 lên 100% vào cuối năm 2020. Ngoài ra, Bộ Thông tin và Truyền thông có các chương trình, đề án bài bản, dài hạn, phát triển nguồn lực an toàn thông tin mạng và xây dựng Hệ sinh thái sản phẩm an toàn thông tin mạng "Make in VietNam".

Việc cải thiện thứ hạng trong bảng xếp hạng toàn cầu về chỉ số an toàn, an ninh mạng không hề đơn giản và việc bảo đảm an toàn thông tin mạng dài hạn là thách thức của Việt Nam. Thời gian tới, để cải thiện thứ hạng trong bảng xếp hạng toàn cầu về chỉ số an toàn, an ninh mạng và là nền tảng vững chắc phục vụ chuyển đổi số cần sự nỗ lực, quyết tâm hơn nữa của các bộ, cơ quan ngang bộ, UBND cấp tỉnh. Bộ Thông tin và Truyền thông sẽ tiếp tục hỗ trợ xây dựng hệ sinh thái sản phẩm an toàn thông tin "Make in Viet Nam" và phát triển đội ngũ chuyên gia xuất sắc, nâng cao năng lực an toàn, an ninh mạng Việt Nam.

1. Tình hình đảm bảo an toàn thông tin mạng

1.1. Số liệu tấn công mạng

Trong tháng 02/2022, đã ghi nhận, cảnh báo và hướng dẫn xử lý 1.260 cuộc tấn công mạng gây ra sự cố vào các hệ thống thông tin tại Việt Nam (181 cuộc lừa đảo - phishing, 118 cuộc tấn công thay đổi giao diện - Deface, 961 cuộc tấn công cài, cắm mã độc - Malware), giảm 8,89% so với tháng 01/2022. Số lượng địa chỉ IP Việt Nam nằm trong các mạng botnet là: 879.342 địa chỉ, giảm 9,52% so với tháng 01/2022.

Đến tháng 02/2022, Bộ Thông tin và Truyền thông (Cục An toàn thông tin) đã gắn tín nhiệm mạng cho 1.544 website.

1.2. Bảo đảm an toàn hệ thống thông tin theo cấp độ

a) Bộ, ngành

Theo thống kê báo cáo của các bộ, ngành, đến tháng 12/2021, tổng số hệ thống thông tin (HTTT) của bộ, ngành là 674, trong đó HTTT được phê duyệt Hồ sơ đề xuất cấp độ (HSĐXCĐ) là: 322, chiếm 48%, cụ thể:

TT	Cấp độ	Tháng 12/2021			Kế hoạch 2022	
		Số HT	Số HT đã phê duyệt	Tỷ lệ phê duyệt	Số HT	Tỷ lệ
1	Cấp độ 1	138	52	38%	86	100%
2	Cấp độ 2	241	107	45%	134	100%
3	Cấp độ 3	255	152	60%	103	100%
4	Cấp độ 4	37	9	25%	28	100%
5	Cấp độ 5	03	02	67%	01	100%

b) Địa phương

Đến tháng 12/2021, tổng số HTTT của địa phương là: 2.179, trong đó HTTT được phê duyệt HSĐXCĐ là: 523, chiếm 24%, cụ thể:

TT	Cấp độ	Tháng 12/2021			Kế hoạch 2022	
		Số HT	Số HT đã phê duyệt	Tỷ lệ phê duyệt	Số HT	Tỷ lệ
1	Cấp độ 1	398	37	9%	361	100%
2	Cấp độ 2	1.390	340	25%	1.050	100%
3	Cấp độ 3	386	139	37%	247	100%
4	Cấp độ 4	9	7	78%	2	100%
5	Cấp độ 5	0	0		0	

c) Cả nước

Tổng số HTTT của cả nước là: 2.853, trong đó HTTT được phê duyệt là: 845, chiếm 30%, như sau:

TT	Cấp độ	Tháng 12/2021			Kế hoạch 2022	
		Số HT	Số HT đã phê duyệt	Tỷ lệ phê duyệt	Số HT	Tỷ lệ
1	Cấp độ 1	536	89	17%	447	100%
2	Cấp độ 2	1.631	447	27%	1.184	100%
3	Cấp độ 3	641	291	45%	350	100%
4	Cấp độ 4	46	16	35%	30	100%
5	Cấp độ 5	03	02	67%	01	100%

1.3. Phát triển thị trường an toàn thông tin mạng

Tình hình sản xuất kinh doanh và phát triển lĩnh vực ATTT mạng vẫn tương đối ổn định: Doanh thu tháng 02/2022, tăng 41,1% so với tháng 01/2022, tăng 22,3% so với cùng kỳ tháng 02/2021.

Tổng số doanh nghiệp được cấp phép đến nay là: 92 doanh nghiệp (tăng 01 so với tháng 01/2022; tăng 05 so với 12/2020). Trong đó:

- 74 doanh nghiệp được cấp phép nhập khẩu sản phẩm;
- 16 doanh nghiệp được cấp phép sản xuất sản phẩm;
- 58 doanh nghiệp được cấp phép cung cấp dịch vụ;
- 61 doanh nghiệp có trụ sở tại thành phố Hà Nội;
- 29 doanh nghiệp có trụ sở tại thành phố Hồ Chí Minh;
- 01 doanh nghiệp có trụ sở tại thành phố Hải Phòng.

Tỷ lệ nhóm sản phẩm, dịch vụ ATTT mạng của Việt Nam so với 22 nhóm sản phẩm hệ sinh thái ATTT mạng đạt 95,5%. Tỷ lệ sản xuất/nhập khẩu tháng 02/2022 đạt 55%.

1.4. Mạng lưới ứng cứu sự cố

Đến tháng 02/2022, mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia có 220 thành viên, bao gồm: 58 thành viên thuộc bộ, ngành; 63 thành viên thuộc địa phương và 99 thành viên thuộc các doanh nghiệp và các tổ chức khác.

Mạng lưới được phân thành 11 cụm, hằng năm các cụm đều xây dựng và triển khai kế hoạch hoạt động theo Cụm, tổ chức các hoạt động hỗ trợ, diễn tập ứng cứu sự cố và bảo đảm an toàn thông tin mạng.

1.5. Xếp hạng mức độ sẵn sàng Bảo đảm ATTT mạng 2021

a) Đánh giá đơn vị cấp Bộ

KHỐI CƠ QUAN XẾP LOẠI A
Ngân hàng Nhà nước Việt Nam
Bộ Giao thông vận tải

KHỐI CƠ QUAN XẾP LOẠI C
Ban Quản lý Lăng Chủ tịch Hồ Chí Minh
Bộ Lao động - Thương binh và Xã hội
Bộ Nông nghiệp và Phát triển nông thôn
Đài Tiếng nói Việt Nam
Viện Hàn lâm Khoa học Xã hội Việt Nam

KHỐI CƠ QUAN XẾP LOẠI B	
Bảo hiểm xã hội Việt Nam	Bộ Tư pháp
Bộ Công Thương	Bộ Văn hóa, Thể thao và Du lịch
Bộ Giáo dục và Đào tạo	Bộ Xây dựng
Bộ Kế hoạch và Đầu tư	Bộ Y tế
Bộ Khoa học và Công nghệ	Đài truyền hình Việt Nam
Bộ Ngoại giao	Thanh Tra Chính phủ
Bộ Nội vụ	Thông tấn xã Việt Nam
Bộ Tài chính	Ủy ban Dân tộc
Bộ Tài nguyên và Môi trường	Văn phòng Chính phủ
	Viện Hàn lâm Khoa học và Công nghệ Việt Nam

b) Đánh giá đơn vị cấp tỉnh

KHỐI CƠ QUAN XẾP LOẠI A	
Cần Thơ	Thái Nguyên
Đà Nẵng	Thừa Thiên Huế
Quảng Ngãi	Vĩnh Phúc
Quảng Ninh	

KHỐI CƠ QUAN XẾP LOẠI C	
Bắc Kạn	Hà Nội
Bạc Liêu	Hậu Giang
Cà Mau	Lai Châu
Cao Bằng	Ninh Bình
Đắk Nông	Quảng Trị
	Sơn La

KHỐI CƠ QUAN XẾP LOẠI B					
An Giang	Bình Thuận	Hà Tĩnh	Kon Tum	Phú Thọ	Tiền Giang
Bà Rịa - Vũng Tàu	Đắk Lăk	Hải Dương	Lâm Đồng	Phú Yên	Trà Vinh
Bắc Giang	Điện Biên	Hải Phòng	Lạng Sơn	Quảng Bình	Tuyên Quang
Bắc Ninh	Đồng Nai	Hồ Chí Minh	Lào Cai	Quảng Nam	Vĩnh Long
Bến Tre	Đồng Tháp	Hòa Bình	Long An	Sóc Trăng	Yên Bái
Bình Định	Gia Lai	Hưng Yên	Nam Định	Tây Ninh	
Bình Dương	Hà Giang	Khánh Hòa	Nghệ An	Thái Bình	
Bình Phước	Hà Nam	Kiên Giang	Ninh Thuận	Thanh Hóa	

2. Kinh nghiệm quốc tế

2.1. Bảo đảm an toàn các hệ thống thông tin cơ quan nhà nước, lĩnh vực quan trọng nhìn từ cuộc xung đột giữa Nga - Ucraina.

Trong cuộc xung đột giữa Nga - Ucraina, không gian mạng trở thành mặt trận khốc liệt, nhiều hệ thống thông tin của các cơ quan chính phủ, ngân hàng, tổ chức tài chính và lĩnh vực quan trọng đã bị tấn công từ chối dịch vụ (DDoS -

Distributed Denial-of-Service) và nhiễm mã độc nguy hiểm xóa dữ liệu có tên WhisperGate, qua đó gây ngưng trệ và gián đoạn cung cấp dịch vụ, điển hình là:

Ngày 13/01/2022, Ucraina thông báo đã xảy ra một cuộc tấn công mạng quy mô lớn nhằm vào các trang web của chính phủ nước này khiến một số trang không truy cập được, trong đó có các trang web của Bộ Ngoại giao, Nội các, Bộ Chính sách ruộng đất, Bộ Giáo dục, Hội đồng an ninh và quốc phòng. Tiếp đó, ngày 15/02/2022, trang web của Bộ Quốc phòng, các lực lượng vũ trang, ngân hàng Privatbank và Oschadbank tiếp tục bị tấn công.

Sau đó, ngày 25/02/2022, Mykhailo Fedorov, Bộ trưởng Chuyển đổi số Ucraina, thông báo thành lập đội quân tình nguyện tấn công mạng của nước này. Các lực lượng tình nguyện tấn công mạng phía Ucraina đã sử dụng cuộc gọi, emails, tin nhắn qua các tổng đài ảo để gửi hình ảnh, video binh lính Nga tử trận trực tiếp tới người dân tại Mát-xcơ-va. Các website của chính phủ Nga liên tục bị đánh sập trong thời gian ngắn, chủ yếu bởi tấn công DDoS.

2.2. Chương trình tìm kiếm lỗ hổng cho các hệ thống quan trọng của cơ quan nhà nước

Tại Singapore, từ năm 2018 đã tổ chức chương trình tìm kiếm lỗ hổng bảo mật (bug bounty) cho các hệ thống thông tin, trang web, dịch vụ số quan trọng của các cơ quan chính phủ, trong đó kêu gọi các chuyên gia bảo mật trên thế giới tham gia chương trình này. Tại chương trình, Bug Bounty lần thứ tư, phát động vào tháng 8 năm 2021, đơn vị tổ chức thông báo giải thưởng cho mỗi báo cáo lỗ hổng tìm được sẽ dao động từ 250 USD đến 5.000 USD và chương trình sẽ có giải thưởng lớn nhất lên đến 150.000 USD (khoảng gần 3,5 tỷ đồng) cho báo cáo "đặc biệt", tìm được lỗ hổng đặc biệt nghiêm trọng.

Tại Mỹ, các cơ quan về đảm bảo an toàn thông tin của chính phủ Mỹ đã tổ chức nhiều chương trình tìm kiếm lỗ hổng, sáng kiến an toàn thông tin để kêu gọi cộng đồng chuyên gia ATTT tìm kiếm, cung cấp thông tin lỗ hổng đối với các hệ thống của cơ quan chính phủ thuộc chương trình. Điển hình như Bộ An ninh nội địa (DHS - Department of Homeland Security) đã công bố chương trình "Hack DHS - Hack Bộ An ninh nội địa", hay Bộ Quốc phòng Mỹ (Department of Defense) từ năm 2019 công bố chương trình "Hack the Pentagon" (Hack Lầu Năm Góc), các chuyên gia ATTT khi tham gia các chương trình này được trả thưởng tương ứng với giá trị, mức độ nghiêm trọng của lỗ hổng tìm được.

Thông qua các chương trình Bug Bounty, các cơ quan đảm bảo ATTT mạng, an ninh mạng của chính phủ các nước sẽ huy động được tri thức của cộng đồng chuyên gia, nhanh chóng giúp khắc phục và phòng ngừa các nguy cơ mất an toàn đối với các hệ thống của cơ quan chính phủ.

3. Một số tồn tại, hạn chế

Thời gian qua, các bộ, ngành, địa phương và các cơ quan liên quan đã nỗ lực triển khai các nhiệm vụ về bảo đảm an toàn thông tin mạng, chưa để xảy ra các sự cố nghiêm trọng. Tuy nhiên, kết quả vừa qua chưa xứng tầm với yêu cầu về đảm bảo an toàn thông tin mạng phục vụ hoạt động chuyển đổi số theo quan điểm chỉ đạo của Thủ tướng Chính phủ tại Quyết định số 749/QĐ-TTg ngày 03/6/2020 là "*Bảo đảm an toàn, an ninh mạng là then chốt để chuyển đổi số thành công và bền vững, đồng thời là phần xuyên suốt, không thể tách rời của chuyển đổi số*", điển hình:

- Còn nhiều bộ, ngành, địa phương chưa triển khai, tuân thủ quy định pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ (tỷ lệ phê duyệt bằng 0%), gồm: *Bộ Lao động - Thương binh và Xã hội; Bộ Nông nghiệp và Phát triển nông thôn; Bộ Nội vụ; Bộ Xây dựng; Văn phòng Chính phủ; Thanh tra Chính phủ; Ủy ban Dân tộc; Viện Hàn lâm Khoa học và xã hội Việt Nam; Ban quản lý Lăng Chủ tịch Hồ Chí Minh An Giang; Bắc Giang; Bà Rịa – Vũng Tàu; Bạc Liêu; Bến Tre; Bình Dương; Bình Phước; Cà Mau; Đắk Nông; Điện Biên; Đồng Nai; Đồng Tháp; Hà Giang; Hà Nội; Hà Tĩnh; Hải Dương; Hậu Giang; Hồ Chí Minh; Kiên Giang; Lai Châu; Ninh Bình; Phú Yên; Quảng Bình; Quảng Nam; Tây Ninh*.

- Chưa quan tâm, ưu tiên nguồn lực cho đội ngũ nhân lực an toàn thông tin mạng. Đến tháng 02/2022, chỉ có 03/22 đơn vị chuyên trách công nghệ thông tin (CNTT), an toàn thông tin (ATTT) thuộc bộ, cơ quan ngang bộ có phòng chuyên trách về ATTT, chiếm 13,6%; 100% Sở (62 Sở Thông tin và Truyền thông, 01 Sở Văn hóa, Thông tin, Thể thao và Du lịch) thuộc UBND các tỉnh và thành phố trực thuộc Trung ương **không có phòng chuyên trách ATTT** thuộc Sở. Chỉ có 07/63 Sở có phòng chuyên trách về ATTT thuộc Trung tâm trực thuộc Sở.

- Tỷ lệ chi cho ATTT trên tổng chi cho CNTT còn thấp. Theo khảo sát số liệu chi năm 2021, có 10/26 bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ[1] và 25/63 tỉnh, thành phố trực thuộc Trung ương[2] có tỷ lệ chi cho ATTT so với chi cho CNTT thấp hơn mức yêu cầu tối thiểu là 10%.

- Chưa quan tâm, ưu tiên nguồn lực cho hoạt động kiểm tra, đánh giá ATTT định kỳ cho các hệ thống thông tin thuộc phạm vi quản lý theo quy định tại Nghị định số 85/2016/NĐ-CP, không thực hiện kiểm tra, đánh giá an toàn thông tin mã nguồn (code review).

Những tồn tại, hạn chế nêu trên không được kịp thời khắc phục sẽ đặt ra nhiều thách thức lớn cho việc đảm bảo an toàn thông tin mạng, góp phần thực hiện công cuộc chuyển đổi số thành công.

---

[1] 10 cơ quan gồm: Các Bộ: Tư pháp, Tài chính, Giáo dục và Đào tạo, Y tế, Lao động - Thương binh và Xã hội, Ủy ban Dân tộc, Đài truyền hình Việt Nam, Đài Tiếng nói Việt Nam, Viện Hàn lâm Khoa học Xã hội Việt Nam, Ban Quản lý Lăng Chủ tịch Hồ Chí Minh.

[2] 26 tỉnh:Quảng Trị, Cà Mau, Lai Châu, Hà Nam, Bạc Liêu, Phú Thọ, Cần Thơ, Bắc Giang, Hà Giang, Kiên Giang, Bình Phước, Hậu Giang, Đắk Nông, Lạng Sơn, Bình Dương, Bắc Ninh, Nghệ An, Sơn La, Cao Bằng, Gia Lai, Bắc Kạn, Thanh Hóa, Hải Phòng, Thái Bình, Sóc Trăng, Ninh Bình.

4. Kiến nghị, đề xuất

Trong thời gian tới, nhằm hiện thực quan điểm chỉ đạo về bảo đảm an toàn, an ninh mạng là then chốt để chuyển đổi số thành công và bền vững, đồng thời là phần xuyên suốt, không thể tách rời của chuyển đổi số. Bộ Thông tin và Truyền thông đề nghị các bộ, ngành, địa phương:

(1) Tổ chức phổ biến, quán triệt tới toàn bộ các tổ chức, cá nhân liên quan về hai nguyên tắc bảo đảm an toàn, an ninh mạng, cụ thể là hệ thống thông tin chưa kết luận bảo đảm an toàn, an ninh mạng chưa đưa vào sử dụng; hệ thống thử nghiệm, có dữ liệu thật thì phải tuân thủ đầy đủ quy định như hệ thống chính thức. Thời hạn hoàn thành: Tháng 5/2022.

(2) Tổ chức triển khai đầy đủ bốn giải pháp bảo đảm ATTT mạng, cụ thể là phần mềm nội bộ do đơn vị chuyên nghiệp phát triển, tuân thủ phát triển theo quy trình DevSecOps; hệ thống thông tin triển khai đầy đủ phương án bảo đảm ATTT mạng theo cấp độ; hệ thống thông tin được kiểm tra, đánh giá ATTT mạng trước khi đưa vào sử dụng, khi nâng cấp, thay đổi, định kỳ theo quy định; hệ thống thông tin được quản lý, vận hành theo mô hình 4 lớp theo Chỉ thị số 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ. Thời hạn hoàn thành: Tháng 10/2022.

(3) Tổ chức xác định, phân loại và phê duyệt HSĐXCĐ của 100% các hệ thống thông tin thuộc phạm vi quản lý. Thời hạn hoàn thành: Tháng 9/2022.

(4) Tăng cường tổ chức diễn tập thực chiến về ATTT theo hướng dẫn của Bộ Thông tin và Truyền thông. Tối thiểu tổ chức 01 diễn tập thực chiến trong năm 2022. Thời hạn hoàn thành: Tháng 11/2022.

(5) 100% các hệ thống thông tin kết nối, chia sẻ với cơ sở dữ liệu quốc gia về dân cư hoàn thành phê duyệt HSĐXCĐ và triển khai đầy đủ phương án bảo đảm an toàn thông tin. Thời hạn hoàn thành: Tháng 06/2022.

(6) Chủ quản các hệ thống thông tin quan trọng, hệ thống thông tin cấp độ 4, 5 tăng cường hoạt động kiểm tra, đánh giá tìm kiếm lỗ hổng bảo mật theo quy định và phải tham gia chương trình tìm kiếm lỗ hổng bảo mật (Bug Bounty) do Bộ Thông tin và Truyền thông chủ trì, phát động.

(7) 100% bộ, ngành, địa phương có phòng chuyên trách về ATTT thuộc đơn vị chuyên trách về CNTT, ATTT hoặc phòng chuyên trách về ATTT trong Trung tâm sự nghiệp trực thuộc và phân bổ tối thiểu 05 nhân sự chuyên trách về an toàn thông tin mạng. Thời hạn hoàn thành: Tháng 11/2022.

(8) 100% hệ thống thông tin cấp độ 3 trở lên của các bộ, ngành và địa phương được triển khai giám sát an toàn thông tin mạng tập trung, có cam kết chất lượng dịch vụ và trả kinh phí (nếu thuê ngoài). Thời hạn hoàn thành: Tháng 6/2022.

Bộ Thông tin và Truyền thông kính báo cáo./.

BỘ THÔNG TIN VÀ TRUYỀN THÔNG