BẢO HIỂM XÃ HỘI VIỆT NAM

BÁO CÁO TÓM TẮT ĐỀ TÀI

XÂY DỰNG HỆ THỐNG QUY TRÌNH ỨNG CỨU KHẨN CẤP SỰ CỐ AN TOÀN THÔNG TIN MẠNG NGÀNH BẢO HIỂM XÃ HỘI VIỆT NAM

Chủ nhiệm đề tài: Lê Vũ Toàn

Đề tài:

Xây dựng hệ thống quy trình ứng cứu khẩn cấp sự cố an toàn thông tin mạng ngành Bảo hiểm xã hội Việt Nam

Mục lục

Danh mục từ viết tắt **6**

Danh mục các bảng **7**

Danh mục hình ảnh **8**

CHƯƠNG 1: PHẦN MỞ ĐẦU **9**

I. Sự cần thiết 9

II. Mục tiêu nghiên cứu 10

2.1. Mục tiêu chung: Xây dựng hệ thống quy trình ứng cứu khẩn cấp sự cố an toàn thông tin ngành BHXH Việt Nam. 10

2.2. Mục tiêu cụ thể: 10

III. Đối tượng và phạm vi nghiên cứu 11

3.1. Đối tượng nghiên cứu 11

3.2. Phạm vi nghiên cứu 12

IV. Cách tiếp cận 12

4.1. Cách tiếp cận 12

V. Phương pháp nghiên cứu 13

5.1. Phương pháp thống kê, phân tích, tổng hợp. 13

5.2. Phương pháp hội thảo lấy ý kiến chuyên gia 13

VI. Những đóng góp mới và những vấn đề mà đề án chưa thực hiện được 13

6.1. Những đóng góp mới của đề án 13

6.2. Những vấn đề mà đề án chưa thực hiện được: 13

VII. Kết cấu đề án 13

CHƯƠNG 2: QUY ĐỊNH VỀ ỨNG CỨU SỰ CỐ AN TOÀN THÔNG TIN, BÀI HỌC KINH NGHIỆM VÀ TRÁCH NHIỆM THỰC HIỆN CỦA NGÀNH BHXH VIỆT NAM **15**

I. Một số vấn đề chung về an toàn thông tin 15

II. Một số khái niệm về ATTT 16

2.1. Khái niệm về ATTT 16

2.2. Khái niệm về sự cố ATTT 16

2.3. Khái niệm về lỗ hổng bảo mật 17

III. Quy định pháp luật về ƯCSC ATTT 17

3.1. Quy định chung về ƯCSC ATTT nghiêm trọng 17

3.2. Quy định chung về ƯCSC ATTT thông thường 17

3.3. Yêu cầu trong việc thực hiện các quy định pháp luật về ứng cứu khẩn cấp sự cố an toàn thông tin 18

3.4. Một số lưu ý trong công tác ứng cứu sự cố an toàn thông tin mạng 19

CHƯƠNG 3: THỰC TRẠNG HỆ THỐNG THÔNG TIN, NHÂN LỰC CỦA NGÀNH BHXH VIỆT NAM VÀ MỨC ĐỘ SẴN SÀNG TRONG ỨNG CỨU KHẨN CẤP SỰ CỐ AN TOÀN THÔNG TIN **20**
I. Thực trạng hệ thống thông tin ngành BHXH Việt Nam 20
1.1. Hiện trạng bảo đảm an toàn thông tin của BHXH Việt Nam 20
1.3.1. Mô hình bảo đảm an toàn thông tin tổng thể 21
1.3.2. Trung tâm điều hành an toàn, an ninh mạng (SOC) 21
1.3.3. Triển khai đảm bảo an toàn, an ninh mạng theo mô hình 4 lớp 23
1.3.4. Công tác xác định cấp độ đảm bảo an toàn hệ thống thông tin 24
1.3.5. Các giải pháp kỹ thuật 27
1.2. Kết quả thực thi bảo đảm an toàn thông tin 29
1.4.1. Kiểm tra, đánh giá an toàn thông tin 29
1.4.2. Tình hình lây nhiễm và xử lý, bóc gỡ mã độc và tấn công mạng, ứng cứu, khắc phục sự cố 33
1.4.3. Đào tạo, tập huấn, diễn tập về an toàn thông tin mạng 35
II. Hiện trang nhân lực CNTT/ATTT của Ngành BHXH 35
2.1. Tình hình chung 35
2.2. Ban Chỉ đạo Chuyển đổi số và đảm bảo ATTT mạng ngành BHXH Việt Nam 36
2.3. Trung tâm Công nghệ thông tin 37
2.4. Đội ứng cứu sự cố, bảo đảm an toàn thông tin mạng 37
III. Đánh giá hiện trạng và mức độ sẵn sàng an toàn thông tin của BHXH Việt Nam 38
3.1. Đánh giá hiện trạng mô hình bảo đảm an toàn thông tin 38
3.2. Đánh giá hiện trạng thực thi bảo đảm an toàn thông tin cho hệ thống thông tin 39
3.3. Sự cần thiết xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng 40
CHƯƠNG 4. XÂY DỰNG QUY TRÌNH ỨNG CỨU KHẨN CẤP SỰ CỐ AN TOÀN THÔNG TIN NGÀNH BHXH VIỆT NAM **42**
I. Quy trình ứng cứu sự cố an toàn thông tin nghiêm trọng tại Trung tâm dữ liệu Ngành BHXH Việt Nam 42
1.1. Quy trình tổng thể ứng cứu sự cố nghiêm trọng tại Trung tâm dữ liệu 42
1.1.1. Phát hiện hoặc tiếp nhận sự cố 43
1.1.2. Xác minh, phân tích, đánh giá và phân loại sự cố 44
1.1.3. Lựa chọn phương án và triệu tập các thành viên của bộ phận tác nghiệp ứng cứu khẩn cấp 44
1.1.4. Triển khai phương án ứng cứu ban đầu 44
1.1.5. Triển khai phương án ứng cứu khẩn cấp 44
1.1.6. Đánh giá kết quả triển khai phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia 45
1.1.7. Kết thúc 45
1.2. Quy trình ứng cứu sự cố nghiêm trọng hệ thống mạng 45
1.2.1. Phát hiện hoặc tiếp nhận sự cố 45

1.2.2. Xác minh, phân tích, đánh giá và phân loại sự cố 45
1.2.3. Lựa chọn phương án và triệu tập các thành viên của bộ phận tác nghiệp ứng cứu khẩn cấp 45
1.2.4. Triển khai phương án ứng cứu ban đầu 45
1.2.5. Triển khai phương án ứng cứu khẩn cấp 45
1.2.6. Đánh giá kết quả triển khai phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng 46
1.2.7. Kết thúc 46
1.3. Quy trình ứng cứu sự cố nghiêm trọng hệ thống máy chủ, lưu trữ 46
1.3.1. Phát hiện hoặc tiếp nhận sự cố 46
1.3.2. Xác minh, phân tích, đánh giá và phân loại sự cố 46
1.3.3. Lựa chọn phương án và triệu tập các thành viên của bộ phận tác nghiệp ứng cứu khẩn cấp 46
1.3.4. Triển khai phương án ứng cứu ban đầu 46
1.3.5. Triển khai phương án ứng cứu khẩn cấp 47
1.3.6. Đánh giá kết quả triển khai phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng 47
1.3.7. Kết thúc 47
1.4. Quy trình ứng cứu sự cố an toàn thông tin nghiêm trọng 47
1.4.1. Quy trình xử lý sự cố nghiêm trọng tấn công mã độc (Malware) 47
1.4.2. Quy trình xử lý sự cố nghiêm trọng thay đổi giao diện (Deface) 49
1.4.3. Quy trình xử lý sự cố nghiêm trọng tấn công chối dịch vụ (DoS/DDoS) 50
II. Quy trình ứng cứu sự cố an toàn thông tin thông thường tại Trung tâm dữ liệu Ngành BHXH Việt Nam 52
2.1. Quy trình tổng thể ứng cứu sự cố thông thường tại Trung tâm dữ liệu 52
2.2. Quy trình ứng cứu sự cố hệ thống mạng 54
2.3. Quy trình ứng cứu sự cố hệ thống máy chủ, lưu trữ 55
2.4. Quy trình ứng cứu sự cố an toàn thông tin 56
2.4.1. Quy trình ứng cứu sự cố tấn công lừa đảo (Phishing) 56
2.4.2. Quy trình ứng cứu sự cố tấn công khai thác lỗ hổng bảo mật (Vulnerability Exploitation) 57
III. Quy trình ứng cứu sự cố an toàn thông tin thông thường các đơn vị trong hệ thống BHXH Việt Nam 57
3.1. Quy trình tổng thể ứng cứu sự cố thông thường tại các đơn vị trong hệ thống BHXH Việt Nam 57
3.2. Quy trình ứng cứu sự cố hệ thống mạng 60
3.3. Quy trình ứng cứu sự cố hệ thống máy chủ, lưu trữ 60
3.4. Quy trình ứng cứu sự cố an toàn thông tin 61
3.4.1. Quy trình ứng cứu sự cố mã độc (Malware) 61

3.4.2. Quy trình cứu sự cố tấn công lừa đảo (Phishing) 62
CHƯƠNG 5. KẾT LUẬN VÀ CÁC KIẾN NGHỊ, ĐỀ XUẤT **64**
I. Hướng phát triển tiếp theo của đề án 64
1.1. Bổ sung các quy trình ứng cứu sự cố 64
1.2. Đánh giá rủi ro các hệ thống thông tin 64
II. Một số kiến nghị, đề xuất 65
2.1. Với Bảo hiểm xã hội Việt Nam 65
2.2. Với BHXH các tỉnh, thành phố 66
2.3. Với các cơ quan quản lý Nhà nước về ATTT 66
2.4. Với các cung cấp dịch vụ mạng, dịch vụ ATTT 66
III. Kết luận 66
DANH MỤC TÀI LIỆU THAM KHẢO **68**

Danh mục từ viết tắt

TT	Danh mục	Chữ viết tắt, rút gọn
1	An toàn thông tin	ATTT
2	Ứng cứu khẩn cấp	ƯCKC
3	Ứng cứu sự cố	ƯCSC
4	Bảo hiểm xã hội	BHXH
5	Bảo hiểm y tế	BHYT
6	Bảo hiểm thất nghiệp	BHTN
7	Công nghệ thông tin	CNTT
8	Cơ sở dữ liệu	CSDL
9	Denial of Service	DoS
10	Distributed Denial of Service	DDoS
11	Thường trực Ban Chỉ đạo Chuyển đổi số và đảm bảo ATTT mạng ngành BHXH Việt Nam	TTBCĐ BHXH VN

Danh mục các bảng

Bảng 1. Danh sách hệ thống thông tin đã được phê duyệt 26
Bảng 2. Danh sách đề xuất cấp độ các hệ thống thông tin 27
Bảng 3. Các giải pháp kỹ thuật bảo đảm ATTT tại Trung tâm dữ liệu 29
Bảng 4. Các giải pháp kỹ thuật bảo đảm ATTT tại BHXH cấp Tỉnh/TP 29
Bảng 5. Kế hoạch kiểm tra, đánh giá an toàn thông tin mạng trong giai đoạn 2022-2025 33
Bảng 6. Tình hình lây nhiễm và tấn công mạng năm 2020 tại Trung tâm dữ liệu 34
Bảng 7. Tình hình lây nhiễm và tấn công mạng từ 2021 đến hết tháng 5/2022 tại Trung tâm dữ liệu 35

Danh mục hình ảnh

Hình 1. Mô hình tổng thể bảo đảm an toàn thông tin 21
Hình 2. Các thành phần của trung tâm điều hành an ninh mạng 22
Hình 3. Mô hình giải pháp bảo đảm an toàn thông tin 28
Hình 4. Quy trình tổng thể hệ thống phương án ứng cứu sự cố an toàn thông tin mạng 42
Hình 5. Quy trình tổng thể ứng cứu sự cố nghiêm trọng tại Trung tâm dữ liệu 43
Hình 6. Quy trình tổng thể ứng cứu sự cố thông thường tại Trung tâm dữ liệu 52
Hình 7. Quy trình tổng thể ứng cứu sự cố thông thường tại các đơn vị trong hệ thống BHXH Việt Nam 58

CHƯƠNG 1: PHẦN MỞ ĐẦU

i. Sự cần thiết

Thế giới hội nhập và toàn cầu hóa hiện nay đang được phát triển trên nền tảng cốt lõi là các kết nối mạng Internet và chia sẻ dữ liệu điện tử. Mọi hoạt động kinh tế, chính trị, ngoại giao, văn hóa tinh thần, quân sự ngày nay có những bước đột phá lớn, đạt được hiệu quả vượt bậc trong quá trình thực hiện, nhờ các thao tác xử lý tự động trên hệ thống kết nối mạng máy tính với tốc độ tính theo đơn vị một phần nhiều triệu giây.

Theo đánh giá của nhiều tổ chức ATTT uy tín trên thế giới, hiện nay toàn cầu đang đối diện với hàng loạt nguy cơ mới xuất hiện và phổ biến nhanh chóng. Số lượng lỗ hổng bảo mật, mã độc, mạng máy tính ma (botnet) được phát hiện ngày càng nhiều, tạo điều kiện cho tội phạm mạng tiến hành những chiến dịch tấn công kiểu mới, cực kỳ tinh vi và nguy hiểm so với trước đây. Thay vì thực hiện những cuộc tấn công nhanh, nhiều loại mã độc có khả năng ngủ đông, dò xét, chiếm quyền trong thời gian dài, rình thời điểm sơ hở nhất của đối tượng để tiến hành các cuộc tổng tấn công. Hãng bảo mật Symantec đánh giá thiệt hại do mất ATTT trên toàn cầu ước tính hơn 1.000 tỷ USD mỗi năm.

Tin tặc không chỉ gây thiệt hại về kinh tế, mà còn gây ra những xung đột chính trị, ngoại giao. Chúng hoạt động rất tinh vi, thực hiện những chiến dịch quy mô lớn, và có thể phần đông trong số đó được hỗ trợ từ các Chính phủ. Các cuộc tấn công mạng xảy ra liên tiếp, tần suất tấn công phá hoại ngày càng lớn; tấn công có chủ đích ngày càng nhiều; phương thức tấn công, phá hoại ngày càng tinh vi, từ nhiều nguồn, trong nước, nước ngoài; các loại mã độc, phần mềm độc hại, mạng máy tính ma, lỗ hổng bảo mật v.v... ngày càng phức tạp.

Với định hướng của Quốc hội và sự chỉ đạo quyết liệt của Chính phủ, trong giai đoạn 2016-2020, ngành BHXH Việt Nam đã và đang đầu tư xây dựng, hoàn thiện hệ thống CNTT của Ngành theo định hướng Chính phủ điện tử, tích hợp, tập trung cấp quốc gia, hiện đại đạt tiêu chuẩn quốc tế, hướng tới khách hàng với quy trình nghiệp vụ tự động hóa mức độ cao được vận hành bởi nguồn nhân lực công nghệ thông tin chuyên nghiệp, chất lượng cao đáp ứng yêu cầu đảm bảo an sinh xã hội quốc gia, phục vụ người dân và doanh nghiệp ngày càng tốt hơn, toàn diện trong các lĩnh vực BHXH và BHYT.

Hệ thống CNTT của ngành BHXH Việt Nam được triển khai từ Trung ương tới tất cả BHXH cấp tỉnh, cấp huyện và các cơ sở y tế; triển khai thực hiện giao dịch điện tử trên tất cả các lĩnh vực: thu, cấp sổ BHXH; thẻ BHYT, giải quyết các chế độ BHXH, BHYT, BH thất nghiệp, giám định và thanh toán chi phí KCB BHYT... Đến nay, BHXH Việt Nam đã hoàn thành việc cung cấp dịch vụ công mức độ 4 cho tất cả các thủ tục hành chính của ngành, tổ chức, cá nhân có thể thông qua 13 nhà I-VAN hoặc thực hiện trực tiếp trên Cổng DVC của BHXH Việt Nam, Cổng DVC Quốc gia.

Hiện tại, toàn Ngành BHXH Việt Nam đang có gần 30 hệ thống ứng dụng; quản lý CSDL của gần 98 triệu người dân, tương ứng với gần 28 triệu hộ gia đình trên toàn quốc; với hơn 20 nghìn tài khoản công chức, viên chức và người lao động trong Ngành thường xuyên truy cập, khai thác và sử dụng để thực hiện các nghiệp vụ của Ngành; kết nối liên thông với trên 12.000 cơ sở khám chữa bệnh và hơn 500 nghìn tổ chức, doanh nghiệp sử dụng dịch vụ công trên toàn quốc và các bộ, ngành. Năm 2021, Hệ thống giao dịch BHXH điện tử Giao dịch điện tử tiếp nhận và xử lý hơn 87 triệu hồ sơ (chưa kể hơn 170 triệu hồ sơ đề nghị thanh toán chi phí KCB BHYT). Như vậy, nếu tính bình quân mỗi cán bộ BHXH sẽ phải giải quyết hơn 4 nghìn hồ sơ mỗi năm.

Năm 2020, BHXH Việt Nam đã đưa ứng dụng trên thiết bị di động VssID - Bảo hiểm xã hội số chính thức đi vào hoạt động, cung cấp các dịch vụ, tiện ích cho người tham gia, thụ hưởng chế độ, chính sách BHXH, BHYT, sau hơn 1 năm công bố ứng dụng, đến 31/12/2021 đã có hơn 23,8 triệu tài khoản giao dịch điện tử cá nhân (dùng để đăng nhập, sử dụng ứng dụng VssID) được đăng ký và phê duyệt.

Cùng với đó, thực hiện Nghị định số 43/2021/NĐ-CP ngày 31/3/2021 của Chính phủ quy định Cơ sở dữ liệu quốc gia về bảo hiểm, đây là 1 trong 6 CSDL quốc gia quan trọng, được Chính phủ ưu tiên triển khai, BHXH Việt Nam được giao là đơn vị chủ quản của CSLD quốc gia về bảo hiểm. Xác định rõ vai trò và trách nhiệm, BHXH Việt Nam đã và đang tích cực phối hợp với các bộ, ngành liên quan hoàn thiện quy chuẩn kỹ thuật, tập trung, hoàn thiện cơ sở dữ liệu chuyên ngành, danh mục dữ liệu mở để sẵn sàng kết nối, chia sẻ theo chỉ đạo của Chính phủ.

Do đó, việc đảm bảo an toàn thông tin cho toàn bộ hệ thống thông tin của Ngành là một thách thức rất lớn trước những nguy cơ tấn công mạng với kỹ thuật ngày càng tiên tiến của tội phạm công nghệ cao như hiện nay.

ii. Mục tiêu nghiên cứu

2.1. Mục tiêu chung*: *Xây dựng hệ thống quy trình ứng cứu khẩn cấp sự cố an toàn thông tin ngành BHXH Việt Nam.

2.2. Mục tiêu cụ thể:

- Nghiên cứu lý thuyết, quy định pháp luật, tham khảo kinh nghiệm về ứng cứu khẩn cấp sự cố an toàn thông tin; phân loại, phân nhóm các sự cố an toàn thông tin từ đó định hướng xây dựng quy trình ứng cứu cho từng nhóm các sự cố, đồng thời làm rõ trách nhiệm của BHXH Việt Nam và các đơn vị trực thuộc trong thực hiện ứng cứu khẩn cấp sự cố an toàn thông tin.

- Phân tích hiện trạng hệ thống thông tin và hiện trạng thực hiện các quy định ứng cứu khẩn cấp các sự cố đồng thời hệ thống hóa lại các sự cố an toàn thông tin của Ngành BHXH trong thời gian từ 2020 đến tháng 06/2021, trong đó chú trọng Trung tâm dữ liệu, Trung tâm dữ liệu dự phòng và hệ thống thông tin của 03 tỉnh

Long An, Sơn La và Khánh Hòa. Từ đó tổng hợp và phân loại các sự cố và cách thức khắc phục để làm căn cứ phân loại các sự cố và quy trình ứng cứu phù hợp. Từ quá trình phân tích hiện trạng, xác định và phân loại các sự cố vào 03 nhóm gồm: Sự cố hệ thống mạng; Sự cố hệ thống máy chủ, lưu trữ; Sự cố an toàn thông tin.

- Phân tích định hướng phát triển hệ thống công nghệ thông tin ngành BHXH Việt Nam; các yêu cầu và mức độ sẵn sàng trong việc thực hiện các quy định pháp luật về ứng cứu khẩn cấp sự cố an toàn thông tin của ngành BHXH Việt Nam.

- Xây dựng hệ thống gồm 09 quy trình ứng cứu khẩn cấp sự cố an toàn thông tin cho toàn bộ các hệ thống thông tin tập trung của Ngành cũng như các đơn vị thuộc BHXH Việt Nam và BHXH các Tỉnh/Thành phố dựa trên việc xác định cấp độ hệ thống thông tin và phân loại, đánh giá mức độ rủi ro, ảnh hưởng của các sự cố; phân định rõ trách nhiệm, thời gian thực hiện, kỹ thuật thực hiện và sự phối hợp của tập thể, cá nhân trong việc thực hiện các bước của quy trình. Những quy trình cần nghiên cứu, xây dựng:

- Quy trình ứng cứu sự cố hệ thống mạng tại các đơn vị trong hệ thống BHXH Việt Nam.
- Quy trình ứng cứu sự cố hệ thống máy chủ, lưu trữ tại các đơn vị trong hệ thống BHXH Việt Nam.
- Quy trình ứng cứu sự cố hệ thống an toàn thông tin tại các đơn vị trong hệ thống BHXH Việt Nam.
- Quy trình ứng cứu sự cố hệ thống mạng thông thường tại Trung tâm dữ liệu Ngành BHXH Việt Nam.
- Quy trình ứng cứu sự cố hệ thống máy chủ, lưu trữ thông thường tại Trung tâm dữ liệu Ngành BHXH Việt Nam.
- Quy trình ứng cứu sự cố an toàn thông tin tại Trung tâm dữ liệu Ngành BHXH Việt Nam.
- Quy trình ứng cứu sự cố hệ thống mạng nghiêm trọng tại Trung tâm dữ liệu Ngành BHXH Việt Nam.
- Quy trình ứng cứu sự cố hệ thống máy chủ, lưu trữ nghiêm trọng tại Trung tâm dữ liệu Ngành BHXH Việt Nam.
- Quy trình ứng cứu sự cố an toàn thông tin nghiêm trọng tại Trung tâm dữ liệu Ngành BHXH Việt Nam.

iii. Đối tượng và phạm vi nghiên cứu

3.1. Đối tượng nghiên cứu

- Quy định pháp luật, các tài liệu về ứng cứu sự cố an toàn thông tin.

- Hiện trạng hệ thống thông tin và hiện trạng ứng cứu sự cố an toàn thông tin tại BHXH Việt Nam.

- Quy trình ứng cứu sự cố an toàn thông tin.

3.2. Phạm vi nghiên cứu

- Về không gian: Trong toàn hệ thống BHXH Việt Nam.

- Về thời gian: Nghiên cứu thực trạng giai đoạn từ năm 2020 đến nay.

- Về nội dung: Phân tích cơ sở lý luận và thực tiễn về sự cố an toàn thông tin Ngành BHXH Việt Nam, đưa ra các nhóm sự cố và định hướng các yêu cầu và quy trình ứng cứu. Đối chiếu thực trạng ứng dụng, khả năng sẵn sàng ứng cứu sự cố an toàn thông tin Ngành BHXH Việt Nam với yêu cầu và định hướng quy trình để đưa ra các giải pháp về quy trình. Xây dựng quy trình và biện pháp bảo đảm ứng cứu khẩn cấp sự cố an toàn thông tin Ngành BHXH Việt Nam.

iv. Cách tiếp cận

4.1. Cách tiếp cận

- Tiếp cận từ cơ sở lý luận: Từ quan điểm của Đảng, Nhà nước, từ các quy định pháp luật về chuyển đổi số, xây dựng Chính phủ điện tử, Chính phủ số; Quy định về xây dựng và vận hành các CSDL quốc gia; Kiến trúc Chính phủ điện tử.

- Tiếp cận cơ sở pháp lý các văn bản:

- Luật An toàn thông tin mạng số 86/2015/QH13

- Luật Công nghệ thông tin số 67/2011/QH11

- Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ

- Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia

- Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn thi hành một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

- Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc.

- Tiếp cận từ cơ sở thực tiễn:

- Từ kết quả đánh giá, phân tích hiện trạng hạ tầng mạng, máy chủ, lưu trữ, an toàn thông tin tại Trung tâm dữ liệu và BHXH 03 tỉnh Long An, Sơn La, Khánh Hòa.

- Từ kinh nghiệm của một số Bộ, Ngành, các quốc gia, vùng lãnh thổ trên thế giới để nghiên cứu đúc rút kinh nghiệm áp dụng vào Bảo hiểm xã hội Việt Nam.

v. Phương pháp nghiên cứu

Để đạt được mục tiêu nghiên cứu nên trên, đề tài sử dụng phương pháp nghiên cứu:

5.1. Phương pháp thống kê, phân tích, tổng hợp.

- Phân tích, tổng hợp lý thuyết, các quy định của pháp luật và thực trạng thực hiện xây dựng quy trình ứng cứu khẩn cấp sự cố an toàn thông tin.

- Phân tích, đối chiếu, so sánh với khả năng sẵn sàng ứng cứu sự cố an toàn thông tin Ngành BHXH Việt Nam để đề xuất các giải pháp và xây dựng quy trình ứng cứu phù hợp.

5.2. Phương pháp hội thảo lấy ý kiến chuyên gia

- Tổ chức các cuộc họp, hội thảo xin ý kiến những người đã, đang và sẽ trực tiếp vận hành, sử dụng tại các đơn vị trong phạm vi nghiên cứu.

vi. Những đóng góp mới và những vấn đề mà đề án chưa thực hiện được

6.1. Những đóng góp mới của đề án

- Đánh giá thực trạng, làm rõ kết quả đạt được và những hạn chế, vướng mắc trong việc thực hiện quy định pháp luật về ứng cứu khẩn cấp sự cố an toàn thông tin của ngành BHXH Việt Nam.

- Cung cấp cơ sở khoa học, giải pháp, quy trình cụ thể cho việc xây dựng và hoạt động của hệ thống, mạng lưới ứng cứu khẩn cấp sự cố an toàn thông tin ngành BHXH Việt Nam

6.2. Những vấn đề mà đề án chưa thực hiện được:

- Xây dựng quy trình ứng cứu sự cố đối với các sự cố do sự cố do lỗi của người quản trị, vận hành hệ thống.

- Xây dựng quy trình ứng cứu sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn v.v....

vii. Kết cấu đề án

Đề án được chia thành 5 chương , cụ thể như sau:

Chương 1. Phần mở đầu.

Chương 2. Quy định về ứng cứu sự cố an toàn thông tin, bàI học kinh nghiệm và trách nhiệm thực hiện của Ngành BHXH Việt Nam.

Chương 3. Thực trạng hệ thống thông tin, nhân lực của ngành BHXH Việt Nam và mức độ sẵn sàng trong ứng cứu khẩn cấp sự cố an toàn thông tin.

Chương 4. Xây dựng hệ thống, mạng lưới và quy trình ứng cứu khẩn cấp sự cố an toàn thông tin Ngành BHXH Việt Nam.

Chương 5. Kết luận và các kiến nghị, đề xuất.

CHƯƠNG 2: QUY ĐỊNH VỀ ỨNG CỨU SỰ CỐ AN TOÀN THÔNG TIN, BÀI HỌC KINH NGHIỆM VÀ TRÁCH NHIỆM THỰC HIỆN CỦA NGÀNH BHXH VIỆT NAM

Một số vấn đề chung về an toàn thông tin

Đảm bảo an toàn thông tin cho chuyển đổi số đã được triển khai tại nhiều nước trên thế giới. Việt Nam đang trong giai đoạn chuyển đổi số, đổi mới căn bản, toàn diện hoạt động quản lý, điều hành của Chính phủ, hoạt động sản xuất kinh doanh của doanh nghiệp, phương thức sống, làm việc của người dân, phát triển môi trường số an toàn rộng khắp thì các hoạt động đảm bảo an toàn số sẽ luôn gắn liền mật thiết với quá trình này.

Trong giai đoạn vừa qua, các cuộc tấn công mạng ngày càng tinh vi, khó dự báo và mang tính toàn cầu, dẫn đến tình hình đảm bảo an toàn thông tin trên không gian mạng ở Việt Nam tiềm ẩn nhiều rủi ro, thách thức. Các cuộc tấn công mạng có thể đe dọa tới mọi hoạt động của mọi tổ chức, nếu công tác ứng phó không được thực hiện nghiêm túc sẽ gây ra hậu quả khó lường đối việc phát triển và ổn định kinh tế, chính trị, xã hội.

Ngày 16/3/2017, Thủ tướng Chính phủ đã ký Quyết định số 05/2017/QĐ-TTg về việc Ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia. Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia chính thức được công nhận và phát triển, đến nay đã có 222 thành viên là các cơ quan, tổ chức trong nước. Cũng theo đó, hoạt động ƯCSC ATTTM được hướng dẫn và quy định cách thức vận hành, các tổ chức xây dựng kế hoạch ứng phó sự cố ATTT và quy trình ứng cứu đối với các sự cố ATTT thông thường, sự cố ATTT nghiêm trọng.

Ngày 25/10/2017, Thủ tướng Chính phủ tiếp tục ký ban hành Quyết định số 1622/QĐ-TTg về việc Phê duyệt Đề án đẩy mạnh hoạt động mạng lưới ứng cứu sự cố, tăng cường năng lực cho các cán bộ, bộ phận chuyên trách ứng cứu sự cố ATTTM trên toàn quốc đến 2020, định hướng đến 2025. Các nhiệm vụ chủ yếu của quyết định này gồm: (1) Nâng cao năng lực hoạt động Cơ quan điều phối quốc gia; (2) Tăng cường và nâng cao hiệu quả hoạt động của mạng lưới ứng cứu sự cố; (3) Tăng cường hoạt động thu thập, phân tích, xác minh và cảnh báo, điều phối, ứng cứu sự cố ATTTM của Cơ quan điều phối quốc gia, các đơn vị, tổ chức thành viên của mạng lưới ứng cứu sự cố; (4) Tổ chức các chương trình diễn tập ứng cứu sự cố, phòng ngừa tấn công mạng; (5) Phát triển lực lượng và nâng cao năng lực cho đội ngũ nhân lực ứng cứu sự cố, bảo đảm ATTTM; (6) Tăng cường năng lực và tổ chức hoạt động cho các đơn vị, bộ phận chuyên trách ứng cứu sự cố trên toàn quốc; (7) Xây dựng, áp dụng các tiêu chuẩn quốc tế nhằm chuẩn hoá quy trình, dự phòng rủi ro, bảo vệ ATTTM.

Ngày 12/9/2017, Bộ Thông tin và Truyền thông đã ban hành Thông tư số 20/2017/TT-BTTTT Quy định về việc điều phối, ứng cứu sự cố ATTTM trên toàn quốc. Thông tư này làm rõ các quy định trong Quyết định 05/2017/QĐ-TTg như

phân cấp tổ chức thực hiện ứng cứu sự cố bảo đảm ATTT trên toàn quốc, nguyên tắc điều phối ƯCSC, hoạt động điều phối ƯCSC, quy trình ứng cứu sự cố ATTT thông thường, tổ chức và vận hành Mạng lưới ứng cứu sự cố, biện pháp bảo đảm thực hiện ƯCSC ATTT.

ƯCSC ATTT được xem như tuyến phòng thủ cuối cùng sau khi các biện pháp đảm bảo an toàn thông tin thất bại, việc ứng cứu sự cố nếu được thực hiện tốt sẽ giúp giảm thiểu tối đa thiệt hại khi sự cố xảy ra. Tuy nhiên, hiện nay nhận thức và hành động về ƯCSC ATTT vẫn chưa được tốt, năng lực Đội Ứng cứu sự cố vẫn còn yếu kém và nặng tính hình thức; nguy cơ sự cố xuất phát từ nhà cung cấp sản phẩm, dịch vụ bên ngoài, chuỗi cung ứng công nghệ thông tin và truyền thông luôn hiện hữu nhưng chưa có biện pháp kiểm soát; ý thức người dùng chưa tốt và đang là mắt xích yếu nhất trong đảm bảo ATTT, gây ra nhiều rủi ro đối với các hệ thống thông tin, dữ liệu của tổ chức và thông tin cá nhân.

II. Một số khái niệm về ATTT

2.1. Khái niệm về ATTT

Hệ thống thông tin là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng.

ATTT là các hoạt động bảo vệ tài sản thông tin và là một lĩnh vực rộng lớn. Nó bao gồm cả những sản phẩm và những quy trình nhằm ngăn chặn sự truy cập, phá hoại, sửa đổi, sử dụng, tiết lộ,…một cách trái phép nhằm đảm bảo cho các hệ thống thông tin thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính xác và tin cậy. ATTT là việc bảo vệ chống truy nhập (access), sử dụng (use), tiết lộ (disclose), sửa đổi (modify), hoặc phá hủy (destroy) thông tin một cách trái phép (unauthorised).

ATTT mạng là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

- Tính bí mật "Confidentiality": là đảm bảo thông tin chỉ được truy xuất bởi những đối tượng được cấp quyền.

- Tính toàn vẹn "Integrity": là đảm bảo thông tin không bị sửa đổi, hủy bỏ khi không được phép. Nếu thông tin bị thay đổi thì bên nhận phải phát hiện ra.

- Tính sẵn sàng "Availability": cho phép thông tin được sử dụng một cách kịp thời và đáng tin cậy.

2.2. Khái niệm về sự cố ATTT

Sự cố ATTT là việc thông tin, hệ thống thông tin bị tấn công hoặc gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng (sau đây gọi tắt là sự cố).

ƯCSC ATTT là hoạt động nhằm xử lý, khắc phục sự cố gây mất ATTT gồm: theo dõi, thu thập, phân tích, phát hiện, cảnh báo, điều tra, xác minh sự cố, ngăn chặn sự cố, khôi phục dữ liệu và khôi phục hoạt động bình thường của hệ thống thông tin.

Sự cố ATTT nghiêm trọng (sự cố nghiêm trọng) là sự cố hệ thống thông tin cấp độ 4, cấp độ 5 hoặc thuộc Danh mục hệ thống thông tin quan trọng quốc gia, Chủ quản hệ thống thông tin không đủ khả năng tự kiểm soát, xử lý được sự cố.

Sự cố ATTT thông thường là những sự cố không phải Sự cố ATTT nghiêm trọng.

Đầu mối ƯCSC là bộ phận hoặc cá nhân được thành viên mạng lưới ƯCSC ATTT quốc gia cử để thay mặt cho thành viên liên lạc và trao đổi thông tin với Cơ quan điều phối quốc gia về ƯCSC hoặc các thành viên khác trong hoạt động điều phối, ƯCSC.

2.3. Khái niệm về lỗ hổng bảo mật

Lỗ hổng bảo mật là điểm yếu trong hệ thống thông tin, quy trình bảo mật hệ thống, kiểm soát nội bộ hoặc quá trình thực hiện có thể bị khai thác, kích hoạt bởi nguồn tấn công.

III. Quy định pháp luật về ƯCSC ATTT

3.1. Quy định chung về ƯCSC ATTT nghiêm trọng

Quy định chung về ƯCSC ATTT nghiêm trọng được quy định tại Quyết định số 05/2017/QĐ-TTg ngày 16/03/2017 về việc quy định điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc. Quyết định đã xác định phân cấp tổ chức thực hiện ƯCSC ATTT trên toàn quốc và phương án ứng cứu các sự cố.

Quy định phương án ứng cứu sự cố bảo đảm an toàn thông tin mạng được quy định từ Điều 9 đến Điều 14 Quyết định số 05/2017/QĐ-TTg. Theo đó, phương án thực hiện ứng cứu sự cố đảm bảo an toàn thông tin bao gồm những nội dung:

- Phân nhóm sự cố an toàn thông tin

- Hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia

- Báo cáo sự cố an toàn thông tin mạng

- Tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng

- Quy trình ứng cứu sự cố an toàn thông tin mạng nghiêm trọng

3.2. Quy định chung về ƯCSC ATTT thông thường

Quy định chung về ứng cứu sự cố an toàn thông tin thông thường được quy định tại Thông tư số 20/2017/TT-BTTTT ngày 12/09/2017 quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc.

Các cơ quan, tổ chức tham gia hoạt động điều phối, ứng cứu sự cố thông thường gồm:

a. Bộ Thông tin và Truyền thông - Cơ quan thường trực về ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia (gọi tắt là Cơ quan thường trực quốc gia) và Ban điều phối ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia (gọi tắt là Ban điều phối ứng cứu quốc gia); Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam VNCERT/CC - Cơ quan điều phối quốc gia về ứng cứu sự cố (gọi tắt là Cơ quan điều phối quốc gia).

b. Ban Chỉ đạo ứng cứu khẩn cấp sự cố an toàn thông tin mạng của Bảo hiểm xã hội Việt Nam (gọi tắt là Ban Chỉ đạo ứng cứu sự cố).

c. Đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng (sau đây gọi tắt là Đơn vị chuyên trách về ứng cứu sự cố); Đội ứng cứu sự cố hoặc bộ phận ứng cứu sự cố tại Bộ, cơ quan ngang bộ, cơ quan thuộc BHXH Việt Nam (sau đây gọi tắt là Đội/bộ phận ứng cứu sự cố).

d. Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia (gọi tắt là Mạng lưới ứng cứu sự cố); và Ban Điều hành mạng lưới.

e. Chủ quản hệ thống thông tin – Bảo hiểm xã hội Việt Nam; Đơn vị vận hành hệ thống thông tin – Trung tâm Công nghệ thông tin; Ban Chỉ đạo ứng cứu sự cố BHXH Việt Nam.

3.3. Yêu cầu trong việc thực hiện các quy định pháp luật về ứng cứu khẩn cấp sự cố an toàn thông tin

Thực hiện Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia và Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc, BHXH Việt Nam đã xây dựng Kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng trong Ngành BHXH (Kế hoạch số 3280/KH-BHXH ngày 29/8/2018) và thành lập Đội ứng cứu sự cố, bảo đảm an toàn thông tin mạng Ngành BHXH Việt Nam (Quyết định số 345/QĐ-BHXH ngày 09/4/2021). Tuy nhiên, hoạt động ứng cứu khẩn cấp này chưa được quy trình hóa nên việc thực hiện không tránh khỏi những chồng chéo, không rõ chủ thể, thời điểm, thời gian thực hiện làm ảnh hưởng không ít đến hiệu quả của hoạt động. Để hoạt động ứng phó khẩn cấp sự cố an toàn thông tin trong đó có hoạt động của Đội ứng cứu sự cố, bảo đảm an toàn thông tin mạng Ngành BHXH Việt Nam được kịp thời, chuyên nghiệp, phân định rõ cả về thẩm quyền, trách nhiệm cũng như các thao tác kỹ thuật của từng đơn vị, cá nhân tham gia thì phải đặt trong một hệ thống các quy trình nhằm tối ưu hiệu quả, phân bổ hợp lý nguồn lực và thời gian, hạn chế sự chồng chéo, xung đột trong quá trình thực hiện. Đây là điều kiện quan trọng để nâng cao hiệu quả hoạt động ứng cứu khẩn cấp sự cố an toàn thông tin Ngành BHXH Việt Nam.

Thực hiện Nghị định số 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ quy định về đảm bảo an toàn hệ thống thông tin theo cấp độ và Thông tư số 03/2017/TT-BTTTT ngày 24/04/2017 về việc quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP, BHXH Việt Nam đã có Quyết định số 1954/QĐ-BHXH ngày 08/11/2019 về việc phê duyệt cấp độ an toàn hệ thống thông tin. Theo đó, BHXH Việt Nam đã xác định cấp độ 3 với 07 hệ thống thông tin. Đây là điều kiện để xác định được độ quan trọng cũng như mức độ ảnh hưởng đến các hệ thống khác cũng như đến toàn bộ hệ thống thông tin.

Ngày 31/3/2021, Chính phủ ban hành Nghị định số 43/2021/NĐ-CP quy định Cơ sở dữ liệu quốc gia về Bảo hiểm. Cơ sở dữ liệu này được Chính phủ xây dựng thống nhất trên toàn quốc, dùng chung cho các cơ quan, tổ chức, cá nhân nhằm cung cấp chính xác, kịp thời thông tin về bảo hiểm phục vụ công tác quản lý nhà nước, đáp ứng yêu cầu phát triển kinh tế - xã hội và yêu cầu chính đáng của cơ quan, tổ chức, cá nhân. Đặc biệt, trong 09 nhóm thông tin trong Cơ sở dữ liệu quốc gia về Bảo hiểm đã có 05 nhóm thông tin được trích, chọn và đồng bộ hóa dữ liệu từ các cơ sở dữ liệu chuyên ngành của BHXH Việt Nam quản lý. Ngoài ra, đối với 04 nhóm thông tin còn lại nếu chưa thể thu thập thì được đồng bộ hóa dữ liệu từ nguồn dữ liệu chuyên ngành của BHXH Việt Nam quản lý và các nguồn dữ liệu có liên quan. Nghị định này ban hành đã tiếp tục khẳng định sự tín nhiệm của Chính phủ đối với Ngành cũng như hệ thống công nghệ thông tin của Ngành BHXH Việt Nam, đồng thời cũng giao một nhiệm vụ hết sức quan trọng trong việc tạo lập nền tảng phát triển Chính phủ điện tử.

3.4. Một số lưu ý trong công tác ứng cứu sự cố an toàn thông tin mạng

Khi xảy ra sự cố mất an toàn thông tin nếu không được xử lý hoặc xử lý không đúng cách có thể để lại những hậu quả to lớn không chỉ là rò rỉ dữ liệu, thiệt hại tài chính… mà còn ảnh hưởng tới uy tín, hình ảnh của tổ chức. Do đó, cần có những lưu ý sau đây trong công tác ứng cứu sự cố an toàn thông tin mạng:

- Coi ứng cứu sự cố là tuyến phòng thủ cuối cùng của an toàn thông tin để có biện pháp đầu tư, cải thiện năng lực ứng phó nhằm giảm thiểu tối đa thiệt hại mà các cơ quan, tổ chức, doanh nghiệp phải hứng chịu khi sự cố xảy ra.

- Hoạt động ứng cứu sự cố an toàn thông tin mạng phải tiếp cận theo hướng chủ động: Chủ động xây dựng các phương án phát hiện, xử lý đối với các tình huống tấn công mạng; chủ động thực hiện săn tìm các mối đe dọa trong hạ tầng công nghệ thông tin; chủ động rà quét để phát hiện và khắc phục kịp thời lỗ hổng bảo mật;

- Hoạt động báo cáo, chia sẻ thông tin về sự cố cần được cập nhật kịp thời, thường xuyên cho cơ quan điều phối quốc gia về ứng cứu sự cố an toàn thông tin mạng, nâng cao năng lực phối hợp giữa các thành viên trong mạng lưới và cơ quan điều phối quốc gia trong công tác ứng cứu sự cố.

- Xây dựng, triển khai, cập nhật kịp thời các phương án, kịch bản ứng cứu sự cố và diễn tập thường xuyên.

- Thường xuyên thực hiện truy tìm các mối đe dọa an toàn thông tin mạng tồn tại bên trong hệ thống và dò quét lỗ hổng bảo mật, kiểm thử xâm nhập.

- Thường xuyên diễn tập thực chiến để đánh giá khả năng phòng ngừa xâm nhập, phát hiện kịp thời các điểm yếu về quy trình, công nghệ, con người trong các hệ thống thông tin.

- Chủ động theo dõi, phát hiện sớm các nguy cơ tấn công, thông tin về các lỗ hổng, điểm yếu đã được cảnh báo đối với hệ thống đang được sử dụng và thực hiện khắc phục kịp thời.

- Triển khai thường xuyên các chương trình tập huấn cho người dùng để nhận diện các nguy cơ mất an toàn thông tin và cách phòng chống.

- Triển khai các chiến dịch đánh giá nhận thức và khả năng phòng ngừa mất an toàn thông tin cho người dùng cuối.

- Rà soát, quản lý chặt chẽ để đảm bảo người dùng không sử dụng phầm mềm vi phạm bản quyền; xử lý nghiêm các trường hợp vi phạm bản quyền phần mềm, vi phạm các quy định về đảm bảo an toàn thông tin.

- Hướng dẫn người dùng phản ánh các sự cố mất an toàn thông tin.

CHƯƠNG 3: THỰC TRẠNG HỆ THỐNG THÔNG TIN, NHÂN LỰC CỦA NGÀNH BHXH VIỆT NAM VÀ MỨC ĐỘ SẴN SÀNG TRONG ỨNG CỨU KHẨN CẤP SỰ CỐ AN TOÀN THÔNG TIN

1. Thực trạng hệ thống thông tin ngành BHXH Việt Nam

1.1. Hiện trạng bảo đảm an toàn thông tin của BHXH Việt Nam

Trong những năm qua, BHXH đã chú trọng đầu tư các giải pháp và trang thiết bị cho công tác đảm bảo an toàn, an ninh thông tin một cách bài bản và có chọn lựa phù hợp. Từ việc lựa chọn đầu tư trang thiết bị có nguồn gốc xuất xứ tại các nước, khu vực có trình độ khoa học công nghệ và cơ chế đảm bảo an toàn thông tin cao như EU, G7 đến việc lựa chọn ứng dụng các giải pháp an toàn thông tin của thuộc top 3 trong bảng đánh giá, xếp hạng các giải pháp ATTT được các tổ chức độc lập có uy tín đánh giá; Hoàn thiện, ban hành quy chế, chính sách đảm bảo ATTT; Áp dụng hệ thống quản lý ATTT mạng theo tiêu chuẩn, quy chuẩn kỹ thuật đối với hoạt động của hệ thống thông tin; Phân công lãnh đạo phụ trách và thành lập hoặc chỉ định bộ phận đầu mối chịu trách nhiệm về ATTT mạng; triển khai các biện pháp nâng cao nhận thức về ATTT cho lãnh đạo và cán bộ, công chức, viên chức và người lao động trong các cơ quan, đơn vị; Thường xuyên cập nhật các chính sách an ninh bảo mật, các bản vá lỗ hổng bảo mật; kiểm soát chặt chẽ vấn đề an ninh bảo mật thông qua Trung tâm điều hành hệ thống CNTT ngành BHXH; Tổ chức triển khai diễn tập ứng cứu khẩn cấp sự cố an toàn thông tin trong toàn Ngành.

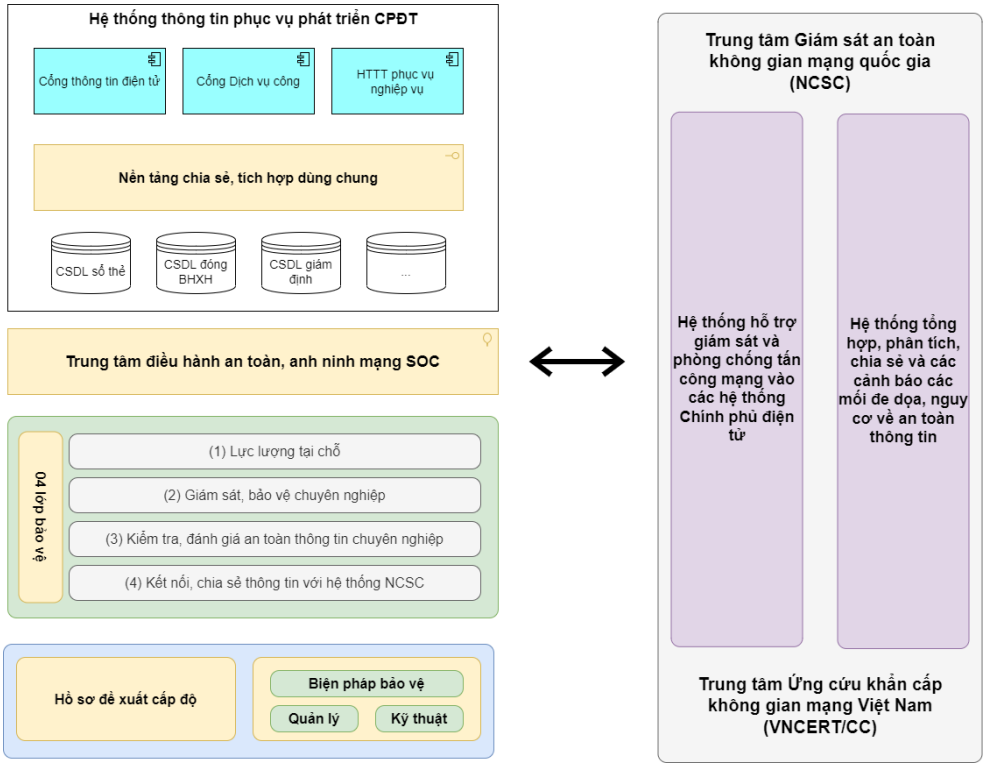
1.1.1. Mô hình bảo đảm an toàn thông tin tổng thể

Mô hình bảo đảm an toàn thông tin tổng thể của Bảo hiểm xã hội Việt Nam bao gồm các thành phần:

- (1) Trung tâm điều hành an toàn, an ninh mạng.

- (2) Mô hình tổ chức "04 lớp" bảo đảm an toàn thông tin mạng.

- (3) Hồ sơ đề xuất cấp độ



Hình 1. Mô hình tổng thể bảo đảm an toàn thông tin

1.1.2. Trung tâm điều hành an toàn, an ninh mạng (SOC)

BHXH Việt Nam trong thời gian qua đã từng bước xây dựng và hoàn thiện Trung tâm SOC (Security Operation Center) là nơi tập trung sử dụng con người, quy trình và công nghệ để liên tục giám sát và cải thiện tình hình ATTT của Ngành trong khi ngăn chặn, phát hiện, phân tích và ứng phó với các sự cố ATTT mạng.

Các chức năng chính của hệ thống SOC:

- Giám sát trạng thái an ninh của toàn bộ hệ thống công nghệ thông tin theo thời gian thực trên một giao diện quản lí tập trung duy nhất.

- Giám sát, phát hiện và cảnh báo bất thường tại từng nút mạng hoặc trên từng thiết bị.

- Cảnh báo sớm các điểm yếu, nguy cơ an ninh có thể xảy ra.

- Hỗ trợ ứng cứu và xử lí các sự cố an ninh mạng.

- Tự động tối đa các qui trình nghiệp vụ, tối ưu nhân lực vận hành hệ thống.

- Hỗ trợ báo cáo theo ngày, theo tuần, theo tháng, theo quí, theo năm.

Trung tâm SOC phải đảm bảo cả 03 yếu tố: Con người, Quy trình, Công nghệ.

Hình 2. Các thành phần của trung tâm điều hành an ninh mạng

Hiện BHXH Việt Nam đã có những trang thiết bị, giải pháp bảo đảm an toàn thông tin tuy nhiên chưa có giám sát chuyên sâu, quy trình cũng như đội ngũ chuyên gia an toàn thông tin có trình độ cao cho những hoạt động điều tra, phân tích, xử lý những sự cố nghiêm trọng.

Những công tác quản trị hiện đang thực hiện tại Trung tâm SOC:

a. Công tác quản trị, vận hành hệ thống an toàn thông tin

Ngoài việc quản trị, vận hành các trang thiết bị chuyên dụng về an ninh bảo mật đã được BHXH Việt Nam trang bị thì cần giám sát, phân tích và xử lý các vấn đề liên quan đến an ninh bảo mật với nhiều mức nhiều lớp khác nhau từ lớp mạng lớp ứng dụng lớp CSDL cho đến lớp đầu cuối, cụ thể:

- Kiểm tra định kỳ tình trạng hoạt động của thiết bị an toàn thông tin thông qua việc kiểm tra và đánh giá tình trạng sử dụng tài nguyên của thiết bị.

- Nâng cấp phần mềm, cài đặt bản vá cho các thiết bị khi có phiên bản mới.

- Tối ưu thông số kỹ thuật, các chính sách an ninh bảo mật trên các thiết bị.

- Định kỳ sao lưu cấu hình, chính sách hiện tại của các thiết bị an ninh bảo mật

- Rà soát hệ thống và thực hiện việc xử lý khi phát hiện các sự cố mất an toàn thông tin xảy ra đối với hệ thống:

- Thực hiện việc xử lý và ghi lại hướng dẫn xử lý lỗi.

- Ngăn chặn kết nối từ các địa chỉ nằm trong danh sách đen của các hãng an ninh bảo mật trên thế giới và của các đơn vị chuyên trách về an ninh bảo mật của Việt Nam kết nối tới hệ thống.

- Sử dụng công cụ thu thập và phân tích log; công cụ rà quét lỗ hổng bảo mật để rà soát, đánh giá an ninh bảo mật đối với các trang thiết bị CNTT của BHXH Việt Nam từ đó kịp thời phát hiện và ngăn chặn các cuộc tấn công vào hệ thống.

- Sử dụng các công cụ phân tích điểm yếu ứng dụng, rò quét lỗ hổng bảo mật mã nguồn phần mềm để rà soát, đánh giá an ninh bảo mật các hệ thống phần mềm ứng dụng của BHXH Việt Nam từ đó đưa ra các báo cáo, khuyến nghị và phối hợp với đơn vị quản lý, phát triển phần mềm khắc phục điểm yếu an toàn thông tin của ứng dụng.

- Lập báo cáo tình trạng hệ thống theo ca làm việc và báo cáo tổng hợp định kỳ hàng tháng.

- Đánh giá hệ thống định kỳ và lập báo cáo đánh giá, đề xuất phương án thay đổi, nâng cấp hệ thống 6 tháng/ 1 lần.

b. Áp dụng hệ thống quản lý an toàn thông tin mạng theo tiêu chuẩn, quy chuẩn kỹ thuật đối với hoạt động của hệ thống thông tin

Nhận thức được việc phòng chống những rủi ro về ATTT do bị tấn công phá hoại có chủ đích phải đi kèm phương án phòng chống những rủi ro có thể gặp phải bởi: Quy trình quản lý, vận hành không đảm bảo; Việc quản lý quyền truy cập chưa được kiểm tra và xem xét định kỳ; Nhận thức của cán bộ trong việc sử dụng và trao đổi thông tin chưa đầy đủ…. Do đó, ngoài các biện pháp kỹ thuật, Trung tâm CNTT đã áp dụng các chính sách, quy định, quy trình vận hành các hệ thống thông tin theo tiêu chuẩn quốc tế ISO 27001:2013 để giảm thiểu rủi ro tối đa cho các hệ thống CNTT của Ngành từ ngày 06/1/2020.

1.1.3. Triển khai đảm bảo an toàn, an ninh mạng theo mô hình 4 lớp

Căn cứ Chỉ thị số 14/CT-TTg của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam, BHXH Việt Nam hoàn thành việc triển khai bảo đảm ATTT cho hệ thống thông tin ngành BHXH theo mô hình "4 lớp", cụ thể như sau:

a. "Lớp 1" Lực lượng tại chỗ

BHXH Việt Nam đã ban hành Kế hoạch số 3280/KH-BHXH ngày 29/8/2018 về việc Ứng phó sự cố bảo đảm ATTT mạng trong ngành BHXH Việt Nam quy định nguyên tắc, phương châm ứng phó sự cố bằng lực lượng tại chỗ do Đơn vị vận hành hệ thống thông tin là đầu mối gồm Trung tâm CNTT, Văn phòng BHXH Việt Nam, các đơn vị sự nghiệp trực thuộc BHXH Việt Nam, BHXH các tỉnh, thành phố trực thuộc Trung ương. Quy định Đơn vị chuyên trách về ứng cứu sự

cố ATTT mạng ngành BHXH là Trung tâm CNTT thuộc BHXH Việt Nam thực hiện các công tác tham mưu, kiểm tra, đôn đốc thực hiện các quy định của pháp luật về bảo đảm an toàn, an ninh mạng trong ngành BHXH và tham gia thành viên Mạng lưới ứng cứu sự cố ATTT mạng quốc gia.

BHXH Việt Nam đã thành lập Đội ứng cứu sự cố ATTT, đây là lực lượng chuyên trách ATTT, được đào tạo bài bản và có năng lực xử lý và ứng cứu sự cố cho toàn bộ các hệ thống thông tin của Ngành.

- Công chức chuyên trách ATTT: Phó Giám đốc Trung tâm CNTT, Đội trưởng đội ứng cứu sự cố.

- Viên chức bán chuyên trách về an toàn thông tin: cán bộ Phòng CNTT tại các đơn vị trong hệ thống BHXH Việt Nam.

- Đội ngũ nhân viên vận hành hệ thống ATTT: 65 người làm việc tại Trung tâm điều hành hệ thống thông tin ngành BHXH Việt Nam.

- Công chức kiêm nhiệm về an toàn thông tin: 24 thành viên trong Ban Chỉ đạo chuyển đổi số và đảm bảo ATTT ngành BHXH Việt Nam (Lãnh đạo Ngành, Thủ trưởng các đơn vị trực thuộc BHXH Việt Nam).

b. "Lớp 2" Thuê đơn vị giám sát, bảo vệ ATTT mạng

BHXH Việt Nam đã tổ chức thuê dịch vụ CNTT để giám sát, ứng cứu sự cố, bảo vệ ATTT mạng cho các hệ thống thông tin ngành BHXH. c. "Lớp 3" Thuê đơn vị độc lập kiểm tra, đánh giá định kỳ

BHXH Việt Nam đã tổ chức thuê dịch vụ CNTT để đánh giá ATTT cho các hệ thống thông tin ngành BHXH, đặc biệt là các hệ thống cung cấp dịch vụ công trực tuyến cho doanh nghiệp và người dân.

c. "Lớp 4" Kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia

BHXH Việt Nam đã thực hiện cung cấp, chia sẻ thông tin về phòng, chống mã độc bao gồm:

- Cung cấp đầy đủ các dải địa chỉ IP Public, tên miền của các hệ thống thông tin trong ngành BHXH cung cấp các dịch vụ ra bên ngoài cũng như có giao tiếp với mạng internet với Trung tâm Giám sát ATTT mạng quốc gia (NCSC) theo địa chỉ ais@mic.gov.vn

- Phối hợp với Cục An toàn Thông tin – Bộ Thông tin và Truyền thông hoàn thành triển khai Công văn số 2973/BTTTT-CATTT ngày 04/9/2019 về việc hướng dẫn triển khai hoạt động giám sát an toàn thông tin trong cơ quan, tổ chức nhà nước.

1.1.4. Công tác xác định cấp độ đảm bảo an toàn hệ thống thông tin

Tại Quyết định số 1954/QĐ-BHXH ngày 08/11/2019 của Tổng Giám đốc Bảo hiểm xã hội Việt Nam phê duyệt cấp độ an toàn hệ thống thông tin cấp độ 3

cho 7 hệ thống thông tin của ngành BHXH Việt Nam kèm theo phương án bảo đảm an toàn thông tin với tiêu chuẩn quốc gia TCVN 11930:2017 tương ứng, phù hợp cấp độ 3.

Tại Quyết định số 1137/QĐ-BHXH ngày 08/11/2019 của Giám đốc Trung tâm Công nghệ thông tin phê duyệt cấp độ an toàn hệ thống thông tin cấp độ 2 cho 10 hệ thống thông tin kèm theo phương án bảo đảm an toàn thông tin với tiêu chuẩn quốc gia TCVN 11930:2017 tương ứng, phù hợp cấp độ 2.

Việc tổ chức triển khai phương án bảo đảm an toàn thông tin cho các hệ thống nếu trên đã được phê duyệt theo tiêu chuẩn quốc gia TCVN 11930:2017 đã được thuyết mình tại hồ sơ cấp độ kèm theo Quyết định số 1954/QĐ-BHXH, Quyết định số 1137/QĐ-BHXH. Trong giai đoạn cuối năm 2021, đầu năm 2022, Trung tâm CNTT tiếp tục thực hiện rà soát, xây dựng hồ sơ và phê duyệt cấp độ đối với các hệ thống đã đưa vào sử dụng nhưng chưa được phê duyệt cấp độ trong đó ưu tiên một số hệ thống từ cấp độ 3 lên cấp độ 4 trình Bộ Thông tin và Truyền thông thẩm định bộ hồ sơ đề xuất cấp độ.

STT	Tên hệ thống thông tin	Cấp độ đề xuất	Văn bản phê duyệt
1	Hệ thống quản lý văn bản điều hành	2	Quyết định số 1337/QĐ-CNTT ngày 08/11/2019
2	Hệ thống Quản lý truy cập (IAM)	2	Quyết định số 1337/QĐ-CNTT ngày 08/11/2019
3	Hệ thống quản lý chính sách xã hội	2	Quyết định số 1337/QĐ-CNTT ngày 08/11/2019
4	Hệ thống quản lý nhân sự	2	Quyết định số 1337/QĐ-CNTT ngày 08/11/2019
5	Hệ thống giám sát	2	Quyết định số 1337/QĐ-CNTT ngày 08/11/2019
6	Hệ thống Thanh tra kiểm tra	2	Quyết định số 1337/QĐ-CNTT ngày 08/11/2019
7	Hệ thống Tổng đài và chăm sóc khách hàng	2	Quyết định số 1337/QĐ-CNTT ngày 08/11/2019
8	Hệ thống trao đổi và tích hợp thống nhất ngành BHXH	2	Quyết định số 1337/QĐ-CNTT ngày 08/11/2019
9	Hệ thống tổng hợp và phân tích dữ liệu tập trung ngành BHXH (DWH)	2	Quyết định số 1337/QĐ-CNTT ngày 08/11/2019

10	Hệ thống Đào tạo trực truyến	2	Quyết định số 1337/QĐ-CNTT ngày 08/11/2019
11	Hệ thống giám định BHYT	3	Quyết định số 1954/QĐ-BHXH ngày 8/11/2019
12	Hệ thống Cấp mã số BHXH và quản lý BHYT hộ gia đình	3	Quyết định số 1954/QĐ-BHXH ngày 8/11/2019
13	Hệ thống giao dịch BHYT điện tử	3	Quyết định số 1954/QĐ-BHXH ngày 8/11/2019
	Hệ thống quản lý thu sổ thẻ BHYT	3	Quyết định số 1954/QĐ-BHXH ngày 8/11/2019
14	Hệ thống Cổng thông tin điện tử	3	Quyết định số 1954/QĐ-BHXH ngày 8/11/2019
15	Hệ thống Thư điện tử Ngành	3	Quyết định số 1954/QĐ-BHXH ngày 8/11/2019
16	Hệ thống Trung tâm dữ liệu Ngành	3	Quyết định số 1954/QĐ-BHXH ngày 8/11/2019

Bảng 1. Danh sách hệ thống thông tin đã được phê duyệt

Qua thời gian vận hành và phát triển, BHXH Việt Nam đang tiến hành đề xuất lại cấp độ đối với toàn bộ hệ thống thông tin. Danh sách cấp độ đề xuất của các hệ thống thông tin tại Trung tâm dữ liệu BHXH Việt Nam:

STT	Tên hệ thống	Cấp độ đề xuất
1	Cổng thông tin điện tử ngành BHXH (bao gồm cổng tiếng Việt, cổng tiếng Anh, cổng thành phần của BHXH tỉnh, thành phố)	3
2	Cổng Dịch vụ công và phần mềm một cửa điện tử ngành BHXH (Hệ thống Giao dịch BHXH điện tử và phần mềm tiếp nhận và quản lý hồ sơ)	4
3	Hệ thống ứng dụng dịch vụ thông tin trên nền tảng thiết bị di động (VssID)	4
4	Hệ thống thông tin Giám định BHYT (Cổng tiếp nhận dữ liệu, phần mềm giám định BHYT, phần mềm giám sát hệ thống)	4
5	Hệ thống Quản lý đấu thầu thuốc	3
6	Hệ thống Chăm sóc khách hàng (tổng đài)	3

7	Hệ thống tương tác đa phương tiện giữa người dân và doanh nghiệp với cơ quan BHXH (SMS)	4
8	Hệ thống Thu nộp, chi trả BHXH điện tử (bao gồm Quản lý tài khoản đầu tư tự động)	4
9	Hệ thống Cấp mã số BHXH và Quản lý BHYT Hộ gia đình	4
10	Hệ thống Quản lý Thu và Sổ - Thẻ	4
11	Hệ thống Xét duyệt chính sách	3
12	Hệ thống Kế toán tập trung	3
13	Hệ thống Quản lý đầu tư quỹ	3
14	Hệ thống Thẩm định quyết toán	3
15	Hệ thống Quản lý nhân sự	3
16	Hệ thống Quản lý hoạt động thanh tra, kiểm tra	3
17	Hệ thống Thi đua khen thưởng	3
18	Hệ thống Tổng hợp và phân tích dữ liệu tập trung ngành BHXH	3
19	Hệ thống Lưu trữ hồ sơ điện tử ngành BHXH	3
20	Hệ thống Đào tạo trực tuyến	3
21	Hệ thống Quản lý văn bản và điều hành	3
22	Hệ thống Thư điện tử	3
23	Hệ thống Quản lý định danh và truy cập (IAM)	3
24	Hệ thống cơ sở hạ tầng (bao gồm Trung tâm dữ liệu Ngành và Trung tâm dữ liệu dự phòng)	4

Bảng 2. Danh sách đề xuất cấp độ các hệ thống thông tin

1.1.5. Các giải pháp kỹ thuật

Biện pháp kỹ thuật bảo đảm an toàn thông tin:

Hình 3. Mô hình giải pháp bảo đảm an toàn thông tin

a. Giải pháp tại Trung tâm dữ liệu:

TT	Giải pháp
A	**Giải pháp về Network:**
1	Tường lửa lớp lõi
2	Tường lửa lớp biên
3	Tường lửa chuyên dụng chống tấn công CSDL
4	Hệ thống cảnh báo truy nhập trái phép (IDS/IPS)
5	Hệ thống chống tấn công DDOS
6	Hệ thống phòng chống tấn công có chủ đích APT Network
7	Hệ thống chống thất thoát dữ liệu qua mạng (Network DLP)
8	Hệ thống phân tích truy vết tấn công mạng (Network Forensic)
B	**Giải pháp về ứng dụng Web/Email:**
9	Tường lửa cho ứng dụng Web
10	Hệ thống Proxy Web và cách ly WEB (isolate)
11	Hệ thống tường lửa cho Email
12	Hệ thống phòng chống tấn công có chủ đích Email
13	Hệ thống phân tích mã nguồn và rà quét lỗ hổng trên WEB
C	**Giải pháp quản lý, giám sát an toàn thông tin máy chủ/máy trạm:**
14	Hệ thống AD trong toàn Ngành quản lý phân quyền user
15	Hệ thống quản lý giám sát tài khoản đặc quyền Cyber-ark
16	Hệ thống quản lý truy cập và xác thực tập trung
17	Hệ thống Antivirus cho máy chủ ảo hóa và máy trạm
18	Phần mềm quản lý giám sát dò quét lỗ hổng bảo mật: Rapid7
19	Phần mềm quản lý, cập nhật bản vá cho các thiết bị (Patch management)
20	Phần mềm phát hiện và phản ứng với các cuộc tấn công chưa được biết đến EDR
21	Hệ thống quản lý truy cập WAN (NAC)
22	Hệ thống chống thất thoát dữ liệu người dùng (DLP)
23	Hệ thống VPN có mã hóa, bảo vệ IPsec

24	Hệ thống bảo mật thông qua xác thực số (HSM; chữ ký số)
25	Mã hóa cơ sở dữ liệu (Data masking)
D	**Giải pháp thu thập phân tích Log/Event:**
26	Hệ thống thu thập và phân tích log (SIEM)
27	Hệ thống quản lý phản hồi các sự cố (SOAR)
28	Hệ thống quản trị, giám sát tập trung các thiết bị tường lửa (Palo Alto)

Bảng 3. Các giải pháp kỹ thuật bảo đảm ATTT tại Trung tâm dữ liệu

b. Giải pháp kỹ thuật tại BHXH Tỉnh/TP và BHXH Quận/Huyện:

TT	Giải pháp
A	**Giải pháp về Network:**
1	Tường lửa phân vùng WAN
2	Tường lửa phân vùng Internet
B	**Giải pháp về ứng dụng Web/Email:**
3	Hệ thống Proxy Web và cách ly WEB (isolate)
C	**Giải pháp quản lý, giám sát an toàn thông tin máy chủ/máy trạm:**
4	Hệ thống AD trong toàn Ngành quản lý phân quyền user
5	Hệ thống Antivirus cho máy chủ và máy trạm
6	Phần mềm quản lý, cập nhật bản vá cho các thiết bị (Patch management)
7	Phần mềm phát hiện và phản ứng với các cuộc tấn công chưa được biết đến EDR
8	Hệ thống quản lý truy cập WAN (NAC)
9	Hệ thống VPN có mã hóa, bảo vệ IPsec
10	Hệ thống bảo mật thông qua xác thực số (HSM; chữ ký số)
D	**Giải pháp thu thập phân tích Log/Event:**
11	Hệ thống thu thập và phân tích log (SIEM)

Bảng 4. Các giải pháp kỹ thuật bảo đảm ATTT tại BHXH cấp Tỉnh/TP

1.2. Kết quả thực thi bảo đảm an toàn thông tin

1.2.1. Kiểm tra, đánh giá an toàn thông tin

Về đánh giá an toàn thông tin mã nguồn các hệ thống thông tin, BHXH Việt Nam đang tự thực hiện kiểm tra, đánh giá an toàn thông tin bằng cách sử dụng công cụ rò quét lỗ hổng bảo mật mã nguồn phần mềm (HPE Fortify Static Code Analyzer - SCA).

Về đánh giá phát hiện mã độc, điểm yếu, lỗ hổng, kiểm thử xâm nhập hệ thống thông tin, trong năm 2020 - 2021, Trung tâm CNTT đã phối hợp với Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT) thực hiện kế hoạch định kỳ đánh giá mức độ sẵn sàng cho 04 hệ thống CNTT quan trọng của Ngành bao gồm:

- Cổng thông tin điện tử bảo hiểm xã hội (https://baohiemxahoi.gov.vn/ và https://vss.gov.vn/)

- Cổng giao dịch điện tử bảo hiểm xã hội (địa chỉ https://dichvucong.baohiemxahoi.gov.vn/ và https://tnhs.baohiemxahoi.gov.vn/)

- Cổng/Trang thông tin điện tử tiếp nhận thông tin bảo hiểm (gdbhyt.baohiemxahoi.gov.vn),

- Cổng/Trang thông tin điện tử giám định BHYT (giamdinh.baohiemxahoi.gov.vn).

Thông qua các kết quả kiểm tra, BHXH Việt Nam đã phối hợp với các đơn vị liên quan kịp thời nâng cấp bản vá và khắc phục các lỗ hổng bảo mật đảm bảo an toàn cho các hệ thống phần mềm của Ngành. Kết quả kiểm tra, đánh giá năm 2021 có 07 lỗ hổng, điểm yếu được phát hiện, trong đó có 01 lỗ hổng mức độ nghiêm trọng, 03 lỗ hổng mức độ cao, 02 lỗ hổng mức độ trung bình và 01 lỗ hổng mức độ thấp. Toàn bộ lỗ hổng, điểm yếu (07) đã được xử lý, khắc phục ngay sau khi được phát hiện. Hiện tại, không còn tồn tại các lỗ hổng, điểm yếu nêu trên (đã có thực hiện kiểm tra, đánh giá lại sau khi tiến hành xử lý, khắc phục các lỗ hổng, điểm yếu).

Ngoài ra, BHXH Việt Nam thực hiện thuê dịch vụ giám sát gián tiếp đối với các tên miền (domain) và các địa chỉ IP với các nội dung:

- Theo dõi, thu thập, phân tích các dữ kiện, thông tin an toàn mạng từ nguồn giám sát mạng Internet của nhà cung cấp dịch vụ và từ nhiều nguồn khác mà nhà cung cấp dịch vụ thu thập được để phát hiện sớm các nguy cơ, sự cố, lỗ hổng bảo mật, và các mã độc, tấn công mạng liên quan đến hệ thống công nghệ thông tin của Bảo hiểm xã hội.

- Xây dựng báo cáo định kỳ về hoạt động theo dõi, cảnh báo nguy cơ, mã độc trong hệ thống công nghệ thông tin của Bảo hiểm xã hội, đồng thời nghiên cứu, đề xuất phương án xử lý và hỗ dõi trợ tư vấn, hướng dẫn khách hàng cách thức xử lý các điểm yếu, nguy cơ, lỗ hổng và các mã độc phát hiện được trong hệ thống của khách hàng.

- Tổng hợp báo cáo định kỳ về tình hình an ninh mạng, mã độc tại Việt Nam để từ đó có các phương án chủ động đảm bảo an toàn thông tin cho các hệ thống thông tin của Bảo hiểm xã hội.

Thông qua các báo cáo, cảnh báo BHXH Việt Nam đã thực hiện ngăn chặn sớm các cuộc tấn công từ các mạng Botnet tới hệ thống của BHXH Việt Nam. Nhanh chóng có biện pháp cập nhật, cách ly các mã độc mới xuất hiện trước khi có ảnh hưởng tới hệ thống của BHXH Việt Nam.

An toàn thông tin là một lĩnh vực thay đổi và mở rộng nhanh chóng. Sản phẩm CNTT ngày càng phát triển với nhiều mẫu mã, chủng loại, phiên bản. Song song với việc phát triển và sử dụng các sản phẩm CNTT này là nguy cơ mất an toàn thông tin từ các điểm yếu lỗ hổng. Theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 với các hệ thống thông tin từ cấp 3 trở lên phải được thực hiện đánh giá rà soát định kỳ hàng năm.

Trên cơ sở đó, có thể nói việc hệ thống website cần được đánh giá an toàn thông tin thường xuyên, định kỳ là việc không thể thiếu, vì vậy Trung tâm CNTT đang lên kế hoạch kiểm tra, đánh giá mức độ sẵn sàng cho 27 hệ thống thông tin đang hoạt động, vận hành của ngành BHXH Việt Nam được triển khai trong giai đoạn 2022 – 2025 một cách toàn diện từ Ứng dụng lẫn Hạ tầng của các hệ thống một cách bài bản. Cụ thể:

STT	Tên hệ thống	Hình thức đánh giá
1	Cổng thông tin điện tử ngành BHXH (bao gồm: cổng tiếng Việt, cổng tiếng Anh, cổng thành phần của BHXH tỉnh, thành phố)	Whitebox
2	Hệ thống Giao dịch BHXH điện tử (Cổng dịch vụ công BHXH Việt Nam, Phần mềm Tiếp nhận và quản lý hồ sơ)	Whitebox
3	Ứng dụng dịch vụ thông tin trên nền tảng thiết bị di động (VssID)	Whitebox
4	Cổng tiếp nhận dữ liệu thanh toán chi phí KCB BHYT (Hệ thống Giám định BHYT)	Whitebox
5	Phần mềm giám định BHYT (Hệ thống Giám định BHYT)	Whitebox
6	Phần mềm giám sát hệ thống giám định BHYT (Hệ thống Giám định BHYT)	Whitebox

7	Hệ thống Quản lý đấu thầu thuốc (Phần mềm Quản lý đấu thầu thuốc, Phần mềm Quản lý thuốc)	Whitebox
8	Hệ thống Chăm sóc khách hàng (Phần mềm Tổng đài tiếp nhận cuộc gọi, Phần mềm Quản lý thông tin khách hàng, Phần mềm Quản lý câu hỏi thường gặp)	Whitebox
9	Hệ thống tương tác đa phương tiện giữa người dân và doanh nghiệp với cơ quan BHXH (SMS)	Whitebox
10	Hệ thống Thu nộp, chi trả BHXH điện tử (bao gồm dịch vụ Quản lý tài khoản đầu tư tự động)	Whitebox
11	Hệ thống cấp số định danh và quản lý BHYT Hộ Gia Đình	Whitebox
12	Phần mềm Quản lý thu và sổ thẻ	Whitebox
13	Phần mềm Quản lý xét duyệt chính sách	Whitebox
14	Hệ thống Kế toán tập trung (Bao gồm phần mềm Thẩm định quyết toán)	Whitebox
15	Phần mềm Quản lý đầu tư quỹ	Whitebox
16	Hệ thống Quản lý nhân sự ngành BHXH	Whitebox
17	Hệ thống Quản lý hoạt động thanh tra, kiểm tra	Whitebox
18	Hệ thống Thi đua khen thưởng	Whitebox
19	Hệ thống tổng hợp và phân tích dữ liệu tập trung ngành BHXH (DWH)	Whitebox
20	Hệ thống Lưu trữ hồ sơ điện tử ngành BHXH	Whitebox
21	Hệ thống Đào tạo nghiệp vụ ngành BHXH (Phần mềm bồi dưỡng trực tuyến)	Whitebox
22	Hệ thống Quản lý văn bản và điều hành	Whitebox
23	Hệ thống Thư điện tử ngành BHXH	Whitebox

24	Hệ thống Quản lý định danh và chia sẻ dữ liệu (Phần mềm Quản lý truy cập, Phần mềm Quản lý định danh, Phần mềm lưu trữ dữ liệu người dùng và danh mục dùng chung)	Whitebox
25	Hệ thống trao đổi và tích hợp thông tin thống nhất Ngành BHXH (SOA)	Whitebox
26	Hệ thống Chữ ký số chuyên dùng Ngành BHXH (PKI)	Whitebox
27	Hệ thống Quản lý thiết bị	Whitebox
28	Hệ thống Cơ sở hạ tầng (bao gồm: Trung tâm dữ liệu Ngành và Trung tâm dữ liệu dự phòng)	Blackbox

Bảng 5. Kế hoạch kiểm tra, đánh giá an toàn thông tin mạng trong giai đoạn 2022-2025

1.2.2. Tình hình lây nhiễm và xử lý, bóc gỡ mã độc và tấn công mạng, ứng cứu, khắc phục sự cố

Tình trạng lẫy nhiễm, xử lý, bóc gỡ mã độc tại các máy chủ, máy trạm:

- 100% máy tính trang bị cho CCVC toàn ngành đang hoạt động đều cài đặt các phần mềm diệt và phòng chống virus và cài đặt phần mềm phòng, chống mã độc (với số liệu được ghi nhận là 23.806 máy).

- BHXH Việt Nam đã thực hiện triển khai giải pháp phòng, chống mã độc F-Secure cài đặt bảo vệ cho 100% máy trạm, thiết bị đầu cuối liên quan và Trend Micro cài đặt bảo vệ cho 100% máy chủ từ trước tháng 5/2018. Giải pháp phòng, chống mã độc được BHXH Việt Nam trang bị có chức năng cho phép quản trị tập trung; có dịch vụ, giải pháp hỗ trợ kỹ thuật 24/7, có khả năng phản ứng kịp thời trong việc phát hiện, phân tích và gỡ bỏ phần mềm độc hại; có cơ chế tự động cập nhật phiên bản hoặc dấu hiệu nhận dạng mã độc mới theo Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng, chống phần mềm độc hại. Việc kết nối, chia sẻ thông tin về mã độc với với hệ thống kỹ thuật của Trung tâm Giám sát ATTT mạng quốc gia theo Công văn số 2290/BTTTT-CATTT ngày 17/7/2018 về việc hướng dẫn kết nối, chia sẻ thông tin về mã độc giữa các hệ thống kỹ thuật đang được BHXH Việt Nam phối hợp triển khai.

Tình hình lây nhiễm và tấn công mạng năm 2020 được ghi nhận tại Trung tâm dữ liệu Ngành:

STT	Nội dung	Năm 2020
1	Số cuộc dò quét điểm yếu hệ thống	932.518
2	Số lượng mã độc tấn công hệ thống tầng network	29.529
3	Số lượt hành động tấn công vào hệ thống Trung tâm dự phòng	59.477
4	Số link giả mạo đính kèm vào thư điện tử	1.845
5	Số lượng thư điện tử có virus trên tầng ứng dụng	9.485
6	Số lượng thư điện tử bị nghi ngờ là thư rác	118.194
7	Số lượng virus trong môi trường máy chủ ảo hóa	139
8	Phát hiện và ngăn chặn kết nối đến CnC server	123
9	Địa chỉ IP/máy tính tồn tại điểm yếu	211

Bảng 6. Tình hình lây nhiễm và tấn công mạng năm 2020 tại Trung tâm dữ liệu

Tình hình lây nhiễm và tấn công mạng từ 2021 đến hết tháng 5/2022 được ghi nhận tại Trung tâm dữ liệu Ngành:

STT	Nội dung	Năm 2021	Năm 2022 (tháng 1-5)
1	Số cuộc dò quét điểm yếu hệ thống lớp biên	1.097.136	973.249
2	Số cuộc dò quét điểm yếu hệ thống lớp lõi	402.583	54.768
3	Số lượng mã độc tấn công hệ thống lớp biên	225.194	168.455
4	Số lượng mã độc tấn công hệ thống lớp lõi	4.573	242
5	Số lượng mã độc tấn công có chủ đích vào hệ thống	54.217	32.356
6	Số lượt hành động tấn công vào hệ thống Cơ sở dữ liệu	67.935	8.678
7	Số link giả mạo đính kèm vào thư điện tử	1.833	2.318
8	Số lượng thư điện tử có virus trên tầng ứng dụng	531	759
9	Số lượng thư điện tử bị nghi ngờ là thư rác	640.437	169.390

Bảng 7. Tình hình lây nhiễm và tấn công mạng từ 2021 đến hết tháng 5/2022 tại Trung tâm dữ liệu

Toàn bộ những tấn công mạng và lây nhiễm mã độc trên đều được các hệ thống giám sát, vận hành an toàn thông tin của BHXH Việt Nam phát hiện và ngăn chặn, không gây ra thiệt hại đối với các hệ thống thông tin.

1.2.3. Đào tạo, tập huấn, diễn tập về an toàn thông tin mạng

Hàng năm, BHXH tổ chức các khóa học quản lý, vận hành các hệ thống CNTT cho cán bộ chuyên trách về CNTT của cơ quan BHXH các cấp.

Đến năm 2020 BHXH Việt Nam đã phối hợp với Cục An toàn thông tin và các đơn vị liên quan tổ chức các khóa đào tạo, cấp chứng chỉ, chứng nhận về an toàn thông tin cho cán bộ chuyên trách về CNTT tại BHXH Việt Nam và BHXH cấp tỉnh tập huấn và thực hiện diễn tập về an toàn thông tin mạng nhằm nâng cao trình độ cho đội ngũ cán bộ làm công tác đảm bảo an toàn thông tin, sẵn sàng ứng phó khi có sự cố xảy ra với 09 khóa học và 20 lớp. Cụ thể là: Khóa bồi dưỡng an toàn thông tin cho cán bộ lãnh đạo, áp dụng bồi dưỡng trực tuyến qua hệ thống cầu truyền hình (Khóa A1); Khóa bồi dưỡng an toàn thông tin cho cán bộ quản lý (Khóa B1); Khóa học dành cho người dùng cuối - Chương trình khung bồi dưỡng an toàn thông tin cho người dùng mức độ cơ bản, áp dụng bồi dưỡng trực tuyến qua hệ thống cầu truyền hình (Khóa C1); Khóa bồi dưỡng an toàn thông tin cho cán bộ kỹ thuật (Khóa D1); Khóa bồi dưỡng tổng quan dành cho cán bộ chuyên trách về an toàn thông tin (Khóa E1); Khóa bồi dưỡng kiện toàn an toàn thông tin cho hệ điều hành (Windows, Linux/Unix) (Khóa E2); Khóa bồi dưỡng kiện toàn an toàn thông tin cho các thiết bị mạng (Khóa E3); Khóa bồi dưỡng vận hành bảo đảm an toàn thông tin cho hạ tầng mạng (Khóa E4); Khóa bồi dưỡng ứng phó và xử lý tấn công mạng (Khóa E5).

Trong năm 2020 và 2022, BHXH Việt Nam đã thực hiện 02 đợt diễn tập, mỗi đợt gồm 03 cụm Miền Bắc, Miền Trung – Tây Nguyên và Miền Nam. Đặc biệt, trong năm 2022, diễn tập năm nay có thêm nội dung "diễn tập thực chiến", bám sát yêu cầu tại Chỉ thị số 60/CT-BTTTT ngày 16/9/2021 của Bộ Thông tin và Truyền thông, nội dung này được thực hiện trên hệ thống thật, không có kịch bản trước nhưng được quy định về mục tiêu, đối tượng tham gia, công cụ sử dụng, mức độ khai thác và thời gian diễn ra nhằm giảm thiểu rủi ro.

Trong năm 2020, BHXH Việt Nam tổ chức thành công 01 đợt diễn tập chuyển đổi hoạt động của toàn bộ các hệ thống thông tin trọng yếu của Ngành từ Trung tâm dữ liệu Ngành sang Trung tâm dự phòng và phục hồi thảm họa trong 03 ngày (từ 21-23/8/2020).

2. Hiện trạng nhân lực CNTT/ATTT của Ngành BHXH

2.1. Tình hình chung

Toàn Ngành có khoảng 20.000 CBCCVC làm nghiệp vụ và sử dụng máy tính cho công việc. Phần lớn cán bộ đều được đào tạo tin học ở mức cơ bản, có thể nhanh chóng tiếp cận với các phần mềm ứng dụng CNTT.

Ngày 31/3/2021, Thủ tướng Chính phủ ký ban hành Nghị định số 43/2021/NĐ-CP quy định Cơ sở dữ liệu quốc gia về bảo hiểm, đây là cơ sở dữ liệu cực kỳ quan trọng. Để đáp ứng được yêu cầu đặt ra ngày càng lớn, Hệ thống công nghệ thông tin (CNTT) của ngành Bảo hiểm xã hội đã được triển khai kịp thời đáp ứng được yêu cầu quản lý nghiệp vụ BHXH, BHYT.

Song song với bước phát triển đó, lực lượng cán bộ thực hiện công tác đảm bảo an toàn thông tin cần được tăng cường để đủ để đáp ứng được hết các yêu cầu đảm bảo an toàn thông tin cho Ngành.

Các cán bộ chuyên trách về CNTT: 459 người tại các đơn vị trong hệ thống BHXH Việt Nam đều có trình độ từ Đại học trở lên tuy nhiên còn ít về số lượng so với quy mô các hệ thống ứng dụng CNTT hiện có của BHXH, do vậy BHXH Việt Nam cũng gặp nhiều khó khăn trong công tác quản lý và vận hành hệ thống ứng dụng cũng như đảm bảo an toàn thông tin trong toàn Ngành.

BHXH Việt Nam cũng đã thuê dịch vụ quản trị, vận hành HTTT và ATTTT với đội ngũ nhân viên là 65 người làm việc tại Trung tâm điều hành hệ thống thông tin ngành BHXH Việt Nam.

2.2. Ban Chỉ đạo Chuyển đổi số và đảm bảo ATTT mạng ngành BHXH Việt Nam

BHXH Việt Nam đã thành lập Ban Chỉ đạo ứng dụng CNTT do Tổng Giám đốc làm Trưởng ban, giao 01 Phó Tổng Giám đốc làm Phó Trưởng ban thường trực phụ trách chỉ đạo và điều hành về hoạt động ứng dụng Công nghệ thông tin và đảm bảo an toàn thông tin toàn Ngành.

Trung tâm CNTT là đơn vị đầu mối chịu trách nhiệm về an toàn thông tin mạng, trực tiếp thực hiện công tác đảm bảo an toàn thông tin mạng toàn Ngành.

Tại BHXH các tỉnh, thành phố, Giám đốc hoặc Phó giám đốc phụ trách CNTT là người chịu trách nhiệm trực tiếp chỉ đạo công tác đảm bảo về an toàn thông tin mạng; phòng CNTT chịu trách nhiệm đảm bảo công tác an toàn thông tin tại đơn vị, báo cáo Trung tâm CNTT khi có sự cố nằm ngoài phạm vi kiểm soát để hỗ trợ giải quyết.

BHXH Việt Nam có 01 Phó Tổng Giám đốc phụ trách chỉ đạo và điều hành về hoạt động ứng dụng CNTT toàn Ngành. Phó Tổng Giám đốc phụ trách CNTT đóng vai trò:

- Chỉ đạo xây dựng thể chế, chính sách đến chiến lược phát triển hệ thống CNTT, nguồn nhân lực CNTT.

- Chỉ đạo, điều phối hoàn thiện mô hình tổng thể về kiến trúc Chính phủ của Ngành, thực hiện kết nối liên thông tới các Bộ, Ngành để hoàn thiện mô hình kiến trúc chính phủ điện tử Việt Nam.

- Chỉ đạo, tổ chức thực hiện các chương trình ứng dụng CNTT, tránh chồng chéo, trùng lắp. Nâng cao vai trò, năng lực của cơ quan chuyên trách CNTT của Ngành.

- Đôn đốc, điều phối triển khai các hệ thống CNTT quan trọng của Ngành, đảm bảo tính liên thông đồng bộ giữa các hệ thống CNTT theo mô hình kiến trúc tổng thể hệ thống CNTT của Ngành.

Trong Kế hoạch số 3280/KH-BHXH ngày 29/08/2018 của Bảo hiểm xã hội Việt Nam đã quy định Ban Chỉ đạo chuyển đổi số là Ban Chỉ đạo ứng cứu khẩn cấp sự cố ATTT mạng.

2.3. Trung tâm Công nghệ thông tin

Trung tâm CNTT là đơn vị chuyên trách về ứng cứu sự cố ATTT mạng của BHXH Việt Nam. Trung tâm CNTT chịu trách nhiệm quản lý, tổ chức và triển khai các chương trình, các hoạt động bảo đảm an toàn thông tin trong toàn Ngành.

Xây dựng, trình Tổng Giám đốc ban hành các văn bản hướng dẫn, quy định về quản lý kỹ thuật, chất lượng hệ thống hạ tầng thông tin và an toàn thông tin mạng; ứng cứu sự cố an toàn thông tin mạng; phát triển nguồn nhân lực quản trị mạng, đảm bảo an toàn thông tin thuộc phạm vi quản lý của Bảo hiểm xã hội Việt Nam.

Thực hiện các hoạt động bảo đảm an toàn thông tin mạng và phương án ứng cứu sự cố an toàn thông tin mạng theo quy định; tổ chức diễn tập an toàn thông tin; đầu mối điều phối ứng cứu sự cố an toàn thông tin mạng trong toàn Ngành; theo dõi, quản lý, đánh giá việc thực hiện chế độ quản trị mạng, đảm bảo an toàn thông tin trong hệ thống Bảo hiểm xã hội Việt Nam

2.4. Đội ứng cứu sự cố, bảo đảm an toàn thông tin mạng

Căn cứ Quyết định số 3280/QĐ-BHXH ngày 29/08/2018 của Bảo hiểm xã hội Việt Nam về việc ứng phó sự cố bảo đảm an toàn thông tin mạng trong ngành Bảo hiểm xã hội. Ngày 09/04/2021, Bảo hiểm xã hội Việt Nam ban hành Quyết định số 345/QĐ-BHXH về việc thành lập Đội ứng cứu sự cố, bảo đảm an toàn thông tin mạng ngành Bảo hiểm xã hội với 36 thành viên.

Đội ứng cứu của BHXH Việt Nam được xây dựng theo mô hình chuyên trách với hơn 70% là cán bộ chuyên trách. Cơ cấu đội ứng cứu bao gồm các vị trí:

- Lãnh đạo: Đội trưởng, đội phó.

- Các thành viên chuyên trách An toàn thông tin gồm các vị trí:

- Ứng cứu sự cố ATTT.
- Phân tích/giám sát ATTT.

- An toàn cơ sở hạ tầng.
- Tiếp nhận và phân loại sự cố ATTT

- Các thành viên hỗ trợ:

- Quản trị cơ sở dữ liệu.
- Quản trị hệ thống/mạng.

3. Đánh giá hiện trạng và mức độ sẵn sàng an toàn thông tin của BHXH Việt Nam

3.1. Đánh giá hiện trạng mô hình bảo đảm an toàn thông tin

Căn cứ Công văn số 235/CATTT-ATHTTT ngày 08/04/2020 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc hướng dẫn mô hình đảm bảo an toàn thông tin cấp Bộ, Tỉnh, thành phần bảo đảm an toàn thông tin cần có 6 thành phần: (1) Hệ thống thông tin phục vụ phát triển CPĐT, CQĐT và ĐTTM cấp bộ, tỉnh; (2) Trung tâm điều hành an toàn, an ninh mạng; (3) Mô hình tổ chức "04 lớp" bảo đảm an toàn thông tin; (4) Mô hình tham chiếu về biện pháp quản lý an toàn thông tin; (5) Mô hình tham chiếu về giải pháp, công nghệ; (6) Mô hình tham chiếu Trung tâm điều hành an toàn, an ninh mạng.

- Trung tâm điều hành an toàn, an ninh mạng: Có 3 thành phần là Con người, Quy trình, Công nghệ. Yếu tố Công nghệ cần được đánh giá đầu tiên, tiếp đến là yếu tố Con người, cuối cùng là Quy trình. Các thành phần, giải pháp cơ bản và nâng cao của SOC như Threat Intelligence, Vul Scan, SOAR đều đã được BHXH triển khai để đảm bảo giám sát, phát hiện, cảnh báo những bất thường trong toàn bộ hệ thống thông tin và tự động hóa các quy trình, tối ưu nhân lực vận hành hệ thống. Tuy nhiên, Trung tâm điều hành an toàn, an ninh mạng vẫn cần được bổ sung những chuyên gia để đảm bảo công tác phân tích, truy vết các cuộc tấn công nguy hiểm cũng như tăng khả năng làm chủ công nghệ.

- Đối với mô hình tổ chức "4 lớp" bảo đảm an toàn thông tin, BHXH Việt Nam hoàn thành việc triển khai, được Cục An toàn thông tin công nhận qua công văn số 355/CATTT-ATHTTT ngày 26/04/2021 về việc xác nhận hoàn thành triển khai công tác bảo đảm an toàn thông tin theo mô hình 4 lớp.

- Các biện pháp quản lý an toàn thông tin: Về cơ bản các biện pháp quản lý về Chính sách an toàn thông tin, Tổ chức bảo đảm an toàn thông tin, Quản lý thiết kế, xây dựng hệ thống, Quản lý vận hành an toàn hệ thống thông tin về cơ bản đã được ban hành và thực hiện trong toàn Ngành. Các biện pháp quản lý sẽ được bổ sung và ban hành để hoàn thiện hồ sơ đề xuất cấp độ cho các hệ thống thông tin.

- Các biện pháp kỹ thuật bảo đảm an toàn thông tin: Các biện pháp kỹ thuật gồm 4 nhóm An toàn hạ tầng mạng, An toàn máy chủ, An toàn ứng dụng, An toàn dữ liệu đều đã được trang bị với các trang bị, giải pháp hàng đầu. Có thể nói BHXH Việt Nam đã trang bị đầy đủ về các biện pháp kỹ thuật đảm bảo an toàn thông tin.

3.2. Đánh giá hiện trạng thực thi bảo đảm an toàn thông tin cho hệ thống thông tin

Căn cứ Công văn số 235/CATTT-ATHTTT ngày 08/04/2020 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông, các hoạt động thực thi bảo đảm an toàn thông tin gồm có: (1) Xây dựng Hồ sơ đề xuất cấp độ và triển khai phương án bảo đảm an toàn thông tin theo cấp độ, (2) Triển khai Trung tâm điều hành an toàn, an ninh mạng, (3) Kiểm tra, đánh giá an toàn thông tin, (4) Xây dựng phương án ứng cứu sự cố an toàn thông tin mạng, (5) Phòng, chống phần mềm độc hại.

- Xây dựng Hồ sơ đề xuất cấp độ và triển khai phương án bảo đảm an toàn thông tin theo cấp độ: BHXH Việt Nam đã phê duyệt cấp độ với 17 hệ thống thông tin (10 cấp độ 2 và 7 cấp độ 3), trong quá trình vận hành và phát triển, mở rộng, Trung tâm CNTT đang tiến hành rà soát và lập hồ sơ đề xuất cấp độ mới với 16 hệ thống cấp độ 3, 8 hệ thống cấp độ 4. Đây là hoạt động hết sức quan trọng, được thực hiện nhằm đánh giá tổng quát về tình hình triển khai các chính sách và giải pháp bảo đảm an toàn thông tin mạng của BHXH Việt Nam do đó nội dung này cần được thực hiện nhanh chóng trong thời gian tới.

- Triển khai Trung tâm điều hành an toàn, an ninh mạng: Việc triển khai hệ thống giám sát, điều hành an toàn, an ninh mạng tập trung (SOC) cho một bộ, ngành, địa phương là hết sức cần thiết. Với việc triển khai các thiết bị, giải pháp một cách đồng bộ, đầy đủ BHXH Việt Nam đã đáp ứng đủ các thành phần của hạng mục Công nghệ tuy nhiên việc triển khai một hệ thống SOC hiệu quả còn nằm ở đội ngũ nhân sự, chuyên gia phân tích, vận khai, khai thác theo quy trình chuyên nghiệp. Vì vậy, việc triển khai hệ thống SOC cần được cân nhắc trên quan điểm tổng thể, tránh việc chỉ đơn giản đầu tư, mua sắm giải pháp, trang thiết bị mà không khai thác, vận hành hiệu quả.

- Kiểm tra, đánh giá an toàn thông tin: Đi đôi với việc xác định cấp độ an toàn hệ thống thông tin, việc kiểm tra, đánh giá an toàn thông tin cho các hệ thống thông tin là việc quan trọng và cần được thực hiện thường xuyên. Thực tế cho thấy có dấu hiệu xuất hiện dần nhiều các cuộc tấn công nguy hiểm nhắm vào các hệ thống thông tin BHXH, bước đầu có thể khẳng định rằng hệ thống thông tin BHXH đã bị các đối tượng thăm dò, có thể là đích nhắm của các cuộc tấn công nguy hiểm trong giai đoạn tới. Trong khi đó các hệ thống, dịch vụ có sự thay đổi, nâng cấp thường xuyên do đó cần có phân tích chuyên sâu liên quan tới sự cố an toàn thông tin, các cuộc tấn công từ bên ngoài vào hệ thống một cách thường xuyên để có phương án phòng ngừa, ngăn chặn, xử lý sớm. Do đó BHXH Việt Nam cần thực hiện đánh giá định kỳ đối với từng hệ thống thông tin theo cấp độ theo quy định tại Nghị định 85/NĐ-CP.

- Xây dựng phương án ứng cứu sự cố an toàn thông tin mạng: Hiện BHXH Việt Nam chưa có phương án ứng cứu sự cố an toàn thông tin mạng theo Quyết định 05/2017/QĐ-TTg và Thông tư 20/2017/TT-BTTTT. Hoạt động ứng cứu sự cố an toàn thông tin mạng phải tiếp cận theo hướng chủ động: Chủ động xây dựng

các phương án phát hiện, xử lý đối với các tình huống tấn công mạng; chủ động thực hiện săn tìm các mối đe dọa trong hạ tầng công nghệ thông tin; chủ động rà quét để phát hiện và khắc phục kịp thời lỗ hổng bảo mật. Việc xây dựng phương án ứng cứu sự cố an toàn thông tin mạng là hoạt động vô cùng quan trọng để đảm bảo sự chủ động, giúp các lực lượng tham gia ứng cứu xác định đúng vai trò nhiệm vụ và cách thức thực hiện các bước cụ thể cho từng loại sự cố.

- Phòng, chống phần mềm độc hại: BHXH Việt Nam đã trang bị các biện pháp tăng cường năng lực phòng chống phần mềm độc hại theo chỉ đạo của Thủ tướng Chính phủ tại Chỉ thị số 14/CT-TTg ngày 25/5/2018 đảm bảo 100% máy chủ, máy trạm, thiết bị đầu cuối được cài đặt. Hàng tháng, Trung tâm CNTT đã có báo cáo Tổng giám đốc về tình hình tấn công, lây nhiễm mã độc tại Trung tâm dữ liệu cũng như báo cáo các máy trạm có hành vi thực thi mã độc, tồn tại điểm yếu và hướng dẫn khắc phục đến các đơn vị trong hệ thống BHXH Việt Nam. Tuy nhiên, sau khi phát hiện và ngăn chặn các loại mã độc, phần mềm độc hại, cần có hoạt động phân tích để phát hiện nguồn lây nhiễm cũng như cách thức hoạt động, lây nhiễm từ đó có biện pháp ngăn chặn.

3.3. Sự cần thiết xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng

Đẩy mạnh chuyển đổi số quốc gia là một trong những nhiệm vụ trọng tâm và đột phá chiến lược của Nghị quyết Đại hội đại biểu toàn quốc lần thứ XIII của Đảng, trong đó an toàn thông tin mạng là yếu tố then chốt đảm bảo sự thành công của chuyển đổi số. Trong giai đoạn vừa qua, các cuộc tấn công mạng ngày càng tinh vi, khó dự báo và mang tính toàn cầu, kéo theo tình hình đảm bảo an toàn thông tin trên không gian mạng ở Việt Nam tiềm ẩn nhiều rủi ro, thách thức. Các cuộc tấn công mạng có thể đe dọa tới mọi hoạt động của mọi tổ chức, nếu công tác ứng phó không được thực hiện nghiêm túc sẽ gây ra hậu quả khó lường đối việc phát triển và ổn định kinh tế, chính trị, xã hội.

Tình hình an toàn thông tin ngày càng phức tạp, việc ứng dụng CNTT nhiều kéo theo rủi ro mất an toàn thông tin càng lớn. Ngày càng nhiều các cuộc tấn công có chủ đích nhằm vào các hệ thống quan trọng, các hệ thống của Nhà nước, của Chính phủ. Sự đầu tư hệ thống thiết bị về an toàn thông tin là hạn chế và khó có thể liên tục, thường xuyên, không những thế không có hệ thống nào là tuyệt đối an toàn. Thực tế cho thấy có dấu hiệu xuất hiện dần nhiều các cuộc tấn công nguy hiểm nhắm vào các hệ thống thông tin BHXH, bước đầu có thể khẳng định rằng hệ thống thông tin BHXH đã bị các đối tượng thăm dò, có thể là đích nhắm của các cuộc tấn công nguy hiểm trong giai đoạn tới.

Hiện nay, Chính phủ đã yêu cầu các cơ quan Nhà nước, đặc biệt là các Bộ, Ngành, các cơ quan có các hệ thống thông tin quan trọng phải tăng cường đầu tư, chú trọng về công tác đảm bảo an toàn thông tin, không để xảy ra các sự cố mất an toàn thông tin đối với các hệ thống thông tin quan trọng, các cơ sở dữ liệu quốc gia. Ứng cứu sự cố an toàn thông tin mạng từ lâu được xem như tuyến phòng thủ

cuối cùng sau khi các biện pháp đảm bảo an toàn thông tin thất bại, việc ứng cứu sự cố nếu được thực hiện tốt sẽ giúp các cơ quan, tổ chức giảm thiểu tối đa thiệt hại khi sự cố xảy ra. BHXH là một cơ quan có rất nhiều hệ thống thông tin quan trọng cần được giám sát, bảo vệ cũng như có quy trình rõ ràng cho việc ứng cứu sự cố khi xảy ra qua đó sẽ xử lý và khắc phục các lỗ hổng, điểm yếu còn tồn tại trên hệ thống.

Mặc dù các quy định pháp luật về hoạt động ứng cứu sự cố bảo đảm an toàn thông tin mạng đã có, tuy nhiên tình trạng bị tấn công mạng không có dấu hiệu thuyên giảm và hoạt động ứng cứu sự cố chưa đạt hiệu quả mong muốn. Hiện nay nhận thức và hành động về ứng cứu sự cố an toàn thông tin mạng tại BHXH Việt Nam vẫn chưa được tốt, nguồn lực đầu tư cho hoạt động của Đội Ứng cứu sự cố còn hạn chế; năng lực Đội Ứng cứu sự cố vẫn còn yếu kém, hoạt động ứng cứu sự cố tại các đơn vị còn bị động. Do đó để khắc phục các tồn tại, hạn chế nêu trên, góp phần đảm bảo an toàn thông tin trên không gian mạng, tiếp tục nâng xếp hạng an toàn thông tin của BHXH Việt Nam, cần triển khai công tác chủ động ứng cứu sự cố thông qua các hoạt động:

- Xây dựng, triển khai, cập nhật kịp thời các phương án, kịch bản ứng cứu sự cố và diễn tập thường xuyên.

- Thường xuyên thực hiện truy tìm các mối đe dọa an toàn thông tin mạng tồn tại bên trong hệ thống và dò quét lỗ hổng bảo mật, kiểm thử xâm nhập.

- Thường xuyên diễn tập thực chiến để đánh giá khả năng phòng ngừa xâm nhập, phát hiện kịp thời các điểm yếu về quy trình, công nghệ, con người trong các hệ thống thông tin.

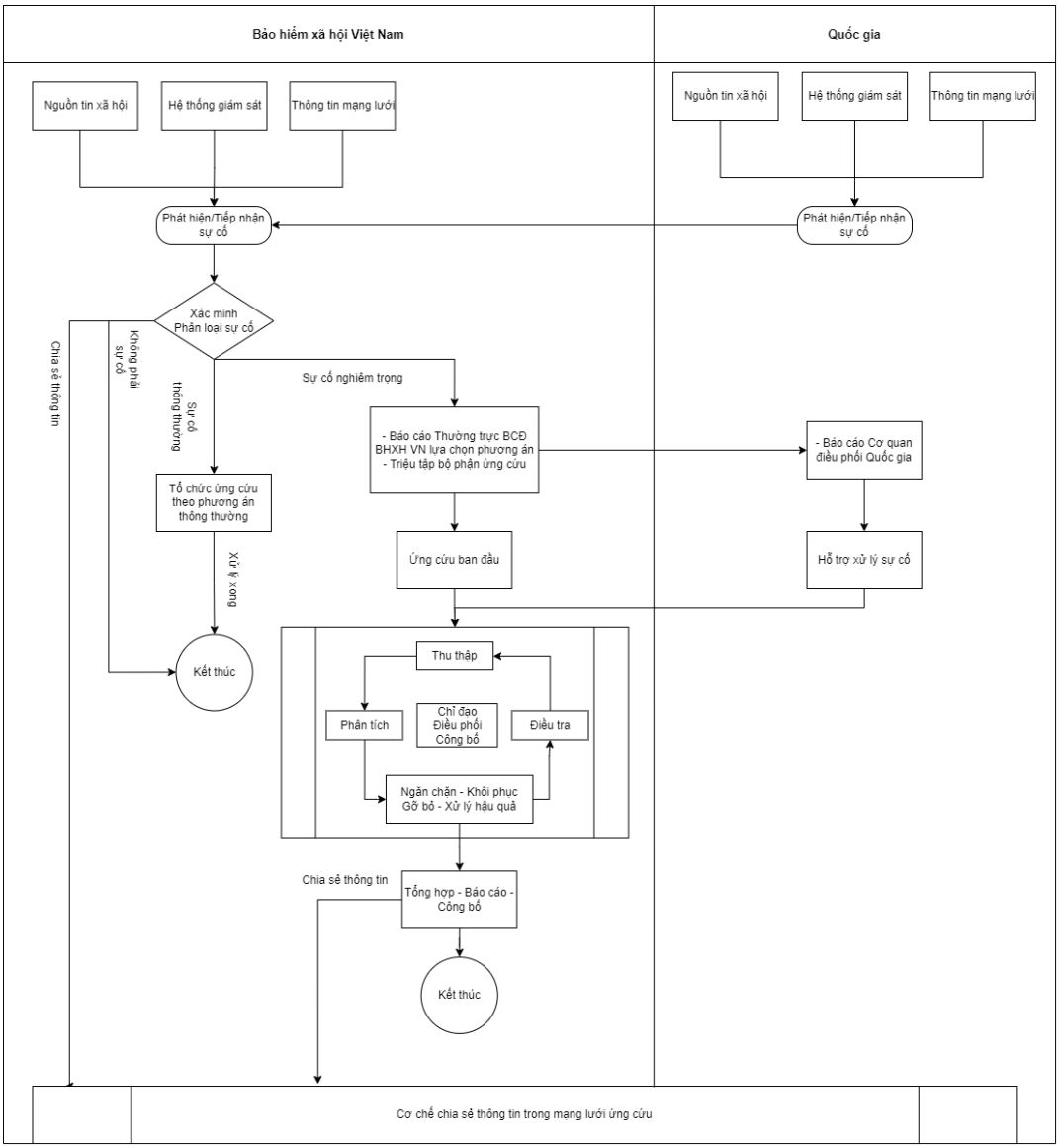
- Chủ động theo dõi, phát hiện sớm các nguy cơ tấn công, thông tin về các lỗ hổng, điểm yếu đã được cảnh báo đối với hệ thống đang được sử dụng và thực hiện khắc phục kịp thời.

Trong đó việc xây dựng và thực hiện quy trình ứng cứu sự cố an toàn thông tin có vai trò tiên quyết để thực hiện chủ động các hoạt động ứng cứu thông qua việc xác định cụ thể các sự cố từ đó phân công nhiệm vụ, trách nhiệm của từng thành phần tham gia để việc ứng cứu hoạt động hiệu quả, tối ưu.

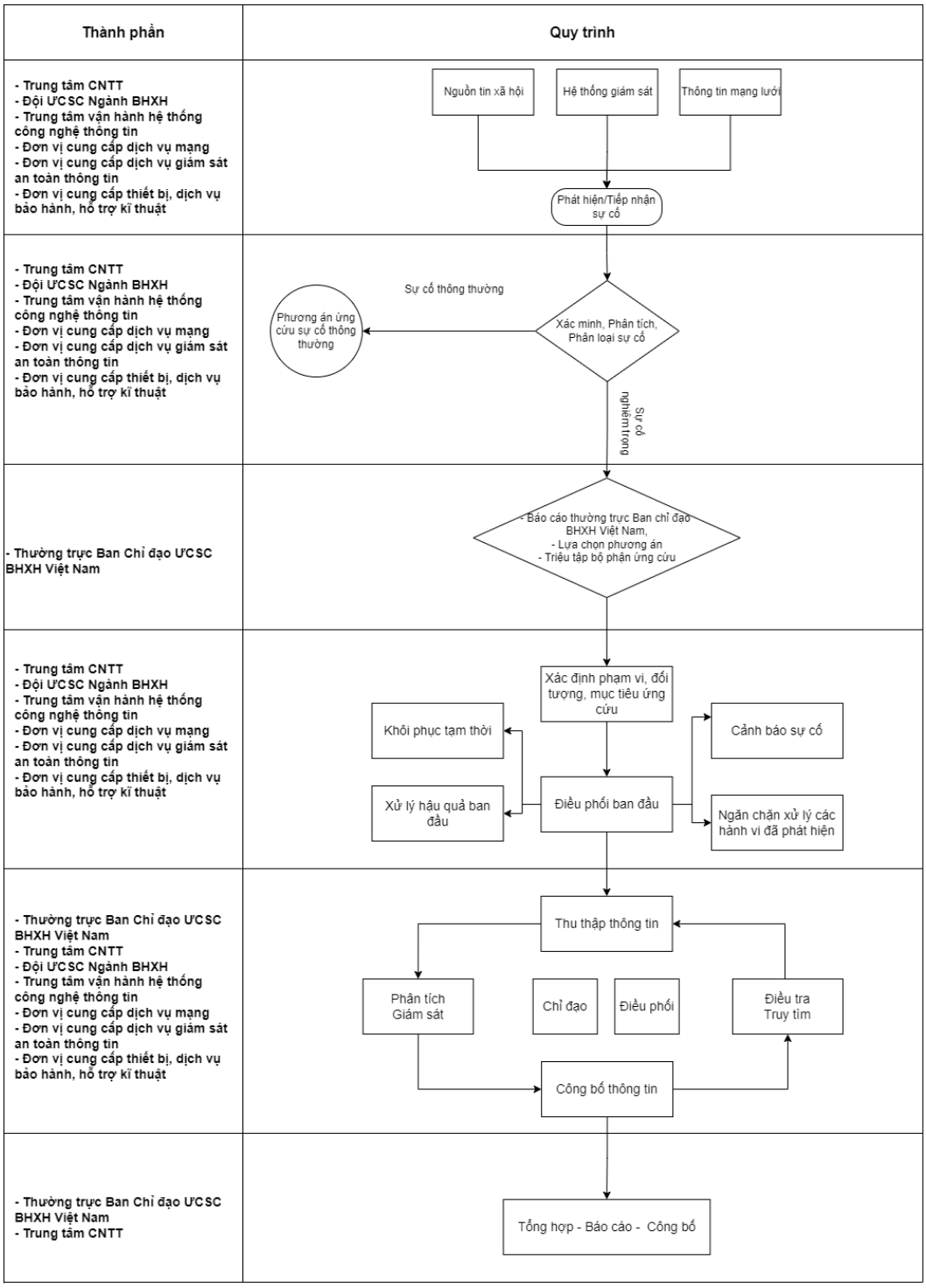
CHƯƠNG 4. XÂY DỰNG QUY TRÌNH ỨNG CỨU KHẨN CẤP SỰ CỐ AN TOÀN THÔNG TIN NGÀNH BHXH VIỆT NAM

I. Quy trình ứng cứu sự cố an toàn thông tin nghiêm trọng tại Trung tâm dữ liệu Ngành BHXH Việt Nam

1.1. Quy trình tổng thể ứng cứu sự cố nghiêm trọng tại Trung tâm dữ liệu



Hình 4. Quy trình tổng thể hệ thống phương án ứng cứu sự cố an toàn thông tin mạng



Hình 5. Quy trình tổng thể ứng cứu sự cố nghiêm trọng tại Trung tâm dữ liệu

Các bước thực hiện quy trình ứng cứu sự cố phải thực hiện đúng các quy định:

1.1.1. Phát hiện hoặc tiếp nhận sự cố

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ mạng; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

1.1.2. Xác minh, phân tích, đánh giá và phân loại sự cố

- Đơn vị chủ trì: Trung tâm CNTT

- Đơn vị phối hợp: Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ mạng; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

1.1.3. Lựa chọn phương án và triệu tập các thành viên của bộ phận tác nghiệp ứng cứu khẩn cấp

- Đơn vị chủ trì: TTBCĐ BHXH VN.

1.1.4. Triển khai phương án ứng cứu ban đầu

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ mạng; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

1.1.5. Triển khai phương án ứng cứu khẩn cấp

a. Chỉ đạo xử lý sự cố

- Đơn vị chủ trì: TTBCĐ BHXH VN.

b. Điều phối công tác ứng cứu

- Đơn vị chủ trì: TTBCĐ BHXH VN.

c. Phát ngôn và công bố thông tin

- TTBCĐ BHXH VN chịu trách nhiệm chỉ định người phát ngôn, cung cấp thông tin; quyết định địa điểm, nội dung, thời điểm phát ngôn, cung cấp thông tin cho các cơ quan thông tin đại chúng, các cá nhân và tổ chức có liên quan đến sự cố.

d. Thu thập thông tin:

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ mạng; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

e. Phân tích, giám sát tình hình liên quan sự cố

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ mạng; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

f. Khắc phục sự cố

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ mạng; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

g. Ngăn chặn, xử lý hậu quả:

- Trung tâm CNTT và các đơn vị liên quan có trách nhiệm xử lý các hậu quả do sự cố hệ thống thông tin của mình gây ra ảnh hưởng đến người dân, cơ quan, tổ chức khác.

h. Xác minh nguyên nhân và truy tìm nguồn gốc:

1.1.6. Đánh giá kết quả triển khai phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia

- Đơn vị chủ trỉ: Trung tâm CNTT

1.1.7. Kết thúc

- Đơn vị chủ trì: TTBCĐ BHXH VN

1.2. Quy trình ứng cứu sự cố nghiêm trọng hệ thống mạng

1.2.1. Phát hiện hoặc tiếp nhận sự cố

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ứng cứu sự cố Ngành BHXH; Đội vận hành hệ thống mạng; Đơn vị cung cấp dịch vụ mạng.

1.2.2. Xác minh, phân tích, đánh giá và phân loại sự cố

- Đơn vị chủ trì: Trung tâm CNTT

- Đơn vị phối hợp: Đội ứng cứu sự cố Ngành BHXH; Đội vận hành hệ thống mạng; Đơn vị cung cấp dịch vụ mạng.

1.2.3. Lựa chọn phương án và triệu tập các thành viên của bộ phận tác nghiệp ứng cứu khẩn cấp

1.2.4. Triển khai phương án ứng cứu ban đầu

1.2.5. Triển khai phương án ứng cứu khẩn cấp

a. Chỉ đạo xử lý sự cố

b. Điều phối công tác ứng cứu

c. Phát ngôn và công bố thông tin

d. Thu thập thông tin:

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ mạng; Đơn vị cung cấp dịch vụ giám sát ATTT.

e. Phân tích, giám sát tình hình liên quan sự cố

f. Khắc phục sự cố

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ mạng; Đơn vị cung cấp dịch vụ giám sát ATTT.

g. Ngăn chặn, xử lý hậu quả:

- Trung tâm CNTT và các đơn vị liên quan có trách nhiệm xử lý các hậu quả do sự cố hệ thống thông tin của mình gây ra ảnh hưởng đến người dân, cơ quan, tổ chức khác.

h. Xác minh nguyên nhân và truy tìm nguồn gốc

1.2.6. Đánh giá kết quả triển khai phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng

1.2.7. Kết thúc

1.3. Quy trình ứng cứu sự cố nghiêm trọng hệ thống máy chủ, lưu trữ

1.3.1. Phát hiện hoặc tiếp nhận sự cố

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội vận hành hệ thống máy chủ, lưu trữ; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

1.3.2. Xác minh, phân tích, đánh giá và phân loại sự cố

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội vận hành hệ thống máy chủ, lưu trữ; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

a. Xác minh sự cố:

b. Sau khi xác minh được sự cố, Trung tâm CNTT có trách nhiệm phân loại sự cố và triển khai tiếp

1.3.3. Lựa chọn phương án và triệu tập các thành viên của bộ phận tác nghiệp ứng cứu khẩn cấp

1.3.4. Triển khai phương án ứng cứu ban đầu

1.3.5. Triển khai phương án ứng cứu khẩn cấp

a. Chỉ đạo xử lý sự cố

b. Điều phối công tác ứng cứu

c. Phát ngôn và công bố thông tin

d. Thu thập thông tin:

- Đơn vị chủ trì: vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ƯCSC Ngành BHXH.

e. Phân tích, giám sát tình hình liên quan sự cố

f. Khắc phục sự cố

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ƯCSC Ngành BHXH và các đơn vị liên quan khác.

g. Ngăn chặn, xử lý hậu quả:

- Trung tâm CNTT và các đơn vị liên quan có trách nhiệm xử lý các hậu quả do sự cố hệ thống thông tin của mình gây ra ảnh hưởng đến người dân, cơ quan, tổ chức khác.

- Các cá nhân thuộc thành phần tác nghiệp ứng cứu khẩn cấp của ngành BHXH tham gia điều tra, phân tích, xử lý sự cố và đưa ra biện pháp ngăn chặn chống tải diễn cách tấn công lừa đảo trong ngành và đơn vị mình.

h. Xác minh nguyên nhân và truy tìm nguồn gốc

1.3.6. Đánh giá kết quả triển khai phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng

1.3.7. Kết thúc

1.4. Quy trình ứng cứu sự cố an toàn thông tin nghiêm trọng

1.4.1. Quy trình xử lý sự cố nghiêm trọng tấn công mã độc (Malware)

1.4.1.1. Phát hiện hoặc tiếp nhận sự cố

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ứng cứu sự cố Ngành BHXH; Đội vận hành hệ thống ATTT; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp giải pháp phòng chống mã độc.

1.4.1.2. Xác minh, phân tích, đánh giá và phân loại sự cố

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ứng cứu sự cố Ngành BHXH; Đội vận hành hệ thống ATTT; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp giải pháp phòng chống mã độc.

a. Xác minh sự cố:

b. Sau khi xác minh được sự cố, Trung tâm CNTT có trách nhiệm phân loại sự cố và triển khai tiếp.

1.4.1.3. Lựa chọn phương án và triệu tập các thành viên của bộ phận tác nghiệp ứng cứu khẩn cấp

1.4.1.4. Triển khai phương án ứng cứu ban đầu

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ứng cứu sự cố Ngành BHXH; Đội vận hành hệ thống ATTT; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp giải pháp phòng chống mã độc.

- Nội dung thực hiện:

a. Xác định phạm vi, đối tượng, mục tiêu cần ứng cứu:

b. Điều phối các hoạt động ứng cứu ban đầu.

c. Báo cáo sự cố trên mạng lưới ứng cứu quốc gia.

d. Tiến hành các biện pháp khôi phục tạm thời.

e. Xử lý hậu quả ban đầu

1.4.1.5. Triển khai phương án ứng cứu khẩn cấp

a. Chỉ đạo xử lý sự cố

b. Điều phối công tác ứng cứu

c. Phát ngôn và công bố thông tin

d. Thu thập thông tin:

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp giải pháp phòng chống mã độc.

e. Phân tích, giám sát tình hình liên quan sự cố

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp giải pháp phòng chống mã độc.

f. Khắc phục sự cố

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp giải pháp phòng chống mã độc.

g. Ngăn chặn, xử lý hậu quả:

- Trung tâm CNTT và các đơn vị liên quan có trách nhiệm xử lý các hậu quả do sự cố hệ thống thông tin của mình gây ra ảnh hưởng đến người dân, cơ quan, tổ chức khác.

h. Xác minh nguyên nhân và truy tìm nguồn gốc.

1.4.1.6. Đánh giá kết quả triển khai phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia

1.4.1.7. Kết thúc

- Đơn vị chủ trì: TTBCĐ BHXH VN

1.4.2. Quy trình xử lý sự cố nghiêm trọng thay đổi giao diện (Deface)

1.4.2.1. Phát hiện hoặc tiếp nhận sự cố

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ứng cứu sự cố Ngành BHXH; Đội vận hành hệ thống ATTT; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp giải pháp hệ thống.

1.4.2.2. Xác minh, phân tích, đánh giá và phân loại sự cố

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ứng cứu sự cố Ngành BHXH; Đội vận hành hệ thống ATTT; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp giải pháp hệ thống.

a. Xác minh sự cố:

b. Sau khi xác minh được sự cố, Trung tâm CNTT có trách nhiệm phân loại sự cố và triển khai tiếp.

1.4.2.3. Lựa chọn phương án và triệu tập các thành viên của bộ phận tác nghiệp ứng cứu khẩn cấp

1.4.2.4. Triển khai phương án ứng cứu ban đầu

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ứng cứu sự cố Ngành BHXH; Đội vận hành hệ thống ATTT; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp giải pháp hệ thống.

- Nội dung thực hiện:

a. Xác định phạm vi, đối tượng, mục tiêu cần ứng cứu.

b. Điều phối các hoạt động ứng cứu ban đầu.

c. Báo cáo sự cố trên mạng lưới ứng cứu quốc gia.

d. Tiến hành các biện pháp khôi phục tạm thời.

e. Xử lý hậu quả ban đầu.

1.4.2.5. Triển khai phương án ứng cứu khẩn cấp

a. Chỉ đạo xử lý sự cố

b. Điều phối công tác ứng cứu

c. Phát ngôn và công bố thông tin

d. Thu thập thông tin:

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp giải pháp hệ thống.

e. Phân tích, giám sát tình hình liên quan sự cố

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp giải pháp hệ thống.

f. Khắc phục sự cố

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp giải pháp hệ thống.

g. Ngăn chặn, xử lý hậu quả:

h. Xác minh nguyên nhân và truy tìm nguồn gốc.

1.4.2.6. Đánh giá kết quả triển khai phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia

1.4.2.7. Kết thúc

- Đơn Đơn vị chủ trì: TTBCĐ BHXH VN

1.4.3. Quy trình xử lý sự cố nghiêm trọng tấn công chối dịch vụ (DoS/DDoS)

1.4.3.1. Phát hiện hoặc tiếp nhận sự cố

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ứng cứu sự cố Ngành BHXH; Đội vận hành hệ thống ATTT; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp dịch vụ mạng.

1.4.3.2. Xác minh, phân tích, đánh giá và phân loại sự cố

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ứng cứu sự cố Ngành BHXH; Đội vận hành hệ thống ATTT; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp dịch vụ mạng.

a. Xác minh sự cố.

b. Sau khi xác minh được sự cố, Trung tâm CNTT có trách nhiệm phân loại sự cố và triển khai tiếp.

1.4.3.3. Lựa chọn phương án và triệu tập các thành viên của bộ phận tác nghiệp ứng cứu khẩn cấp

1.4.3.4. Triển khai phương án ứng cứu ban đầu

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ứng cứu sự cố Ngành BHXH; Đội vận hành hệ thống ATTT; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp dịch vụ mạng.

- Nội dung thực hiện:

a. Xác định phạm vi, đối tượng, mục tiêu cần ứng cứu:

b. Điều phối các hoạt động ứng cứu ban đầu.

c. Báo cáo sự cố trên mạng lưới ứng cứu quốc gia.

d. Tiến hành các biện pháp khôi phục tạm thời.

e. Xử lý hậu quả ban đầu.

1.4.3.5. Triển khai phương án ứng cứu khẩn cấp

a. Chỉ đạo xử lý sự cố.

b. Điều phối công tác ứng cứu

c. Phát ngôn và công bố thông tin

d. Thu thập thông tin:

- Đơn vị chủ trì Trung tâm CNTT.

- Đơn vị phối hợp: Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp dịch vụ mạng.

e. Phân tích, giám sát tình hình liên quan sự cố

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp dịch vụ mạng.

f. Khắc phục sự cố

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

g. Ngăn chặn, xử lý hậu quả:

- Trung tâm CNTT và các đơn vị liên quan có trách nhiệm xử lý các hậu quả do sự cố hệ thống thông tin của mình gây ra ảnh hưởng đến người dân, cơ quan, tổ chức khác.

h. Xác minh nguyên nhân và truy tìm nguồn gốc.

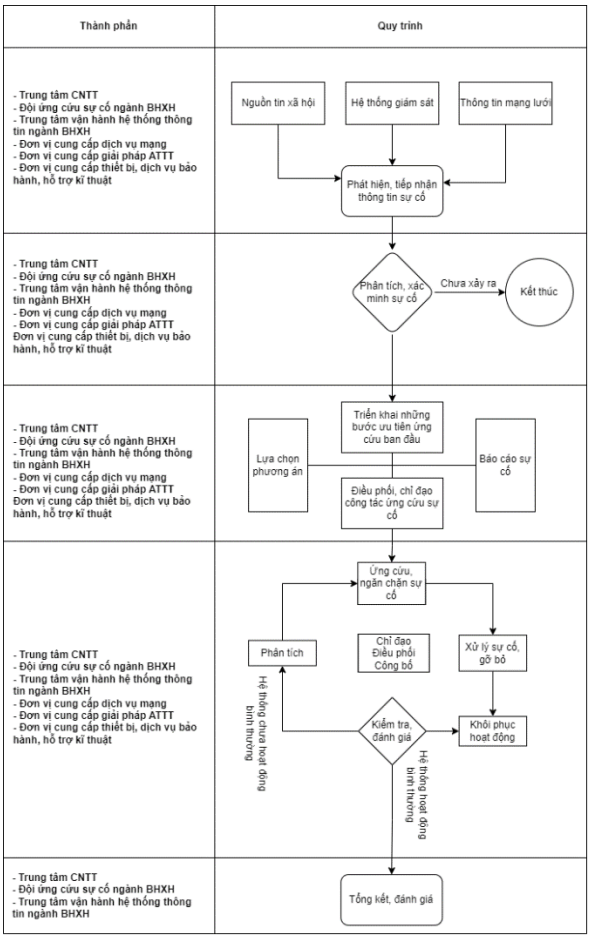
1.4.3.6. Đánh giá kết quả triển khai phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia

1.4.3.7. Kết thúc

- Đơn vị chủ trì: TTBCĐ BHXH VN.

II. Quy trình ứng cứu sự cố an toàn thông tin thông thường tại Trung tâm dữ liệu Ngành BHXH Việt Nam

2.1. Quy trình tổng thể ứng cứu sự cố thông thường tại Trung tâm dữ liệu



Hình 6. Quy trình tổng thể ứng cứu sự cố thông thường tại Trung tâm dữ liệu

Quy trình tổng thể ứng cứu sự cố an toàn thông tin thông thường gồm có:

a. Phát hiện/Tiếp nhận sự cố:

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ mạng; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

b. Triển khai các bước ưu tiên ứng cứu ban đầu:

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ mạng; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

c. Triển khai lựa chọn phương án ứng cứu

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ mạng; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

d. Chỉ đạo xử lý sự cố (nếu cần)

- Đơn vị chủ trì: TTBCĐ BHXH VN

e. Báo cáo sự cố

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ mạng; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

f. Điều phối công tác ứng cứu

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ mạng; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

g. Triển khai ứng cứu, ngăn chặn và xử lý sự cố

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ mạng; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

h. Xử lý sự cố, gỡ bỏ và khôi phục

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ mạng; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

i. Khôi phục hoạt động hệ thống

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ mạng; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

j. Kiểm tra, đánh giá hệ thống thông tin

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ mạng; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

k. Tổng kết, đánh giá

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ƯCSC Ngành BHXH, Trung tâm vận hành HTTT.

2.2. Quy trình ứng cứu sự cố hệ thống mạng

a. Phát hiện/Tiếp nhận sự cố:

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ƯCSC Ngành BHXH; Đội vận hành hệ thống mạng; Đơn vị cung cấp dịch vụ mạng.

b. Triển khai các bước ưu tiên ứng cứu ban đầu:

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ƯCSC Ngành BHXH; Đội vận hành hệ thống mạng; Đơn vị cung cấp dịch vụ mạng.

c. Triển khai lựa chọn phương án ứng cứu

d. Chỉ đạo xử lý sự cố (nếu cần)

e. Báo cáo sự cố

f. Điều phối công tác ứng cứu

g. Triển khai ứng cứu, ngăn chặn và xử lý sự cố

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ƯCSC Ngành BHXH; Đội vận hành hệ thống mạng; Đơn vị cung cấp dịch vụ mạng.

h. Xử lý sự cố, gỡ bỏ và khôi phục

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ƯCSC Ngành BHXH; Đội vận hành hệ thống máy chủ, lưu trữ; Đơn vị cung cấp dịch vụ mạng.

i. Khôi phục hoạt động hệ thống

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ƯCSC Ngành BHXH; Đội vận hành hệ thống máy chủ, lưu trữ; Đơn vị cung cấp dịch vụ mạng.

j. Kiểm tra, đánh giá hệ thống thông tin

k. Tổng kết, đánh giá

2.3. Quy trình ứng cứu sự cố hệ thống máy chủ, lưu trữ

a. Phát hiện/Tiếp nhận sự cố:

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ƯCSC Ngành BHXH; Đội vận hành hệ thống máy chủ, lưu trữ; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

b. Triển khai các bước ưu tiên ứng cứu ban đầu:

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ƯCSC Ngành BHXH; Đội vận hành hệ thống máy chủ, lưu trữ; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

c. Triển khai lựa chọn phương án ứng cứu

d. Chỉ đạo xử lý sự cố (nếu cần)

e. Báo cáo sự cố

f. Điều phối công tác ứng cứu

g. Triển khai ứng cứu, ngăn chặn và xử lý sự cố

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ƯCSC Ngành BHXH; Đội vận hành hệ thống máy chủ, lưu trữ; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

h. Xử lý sự cố, gỡ bỏ và khôi phục

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ƯCSC Ngành BHXH; Đội vận hành hệ thống máy chủ, lưu trữ; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

i. Khôi phục hoạt động hệ thống

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ƯCSC Ngành BHXH; Đội vận hành hệ thống máy chủ, lưu trữ; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

j. Kiểm tra, đánh giá hệ thống thông tin

k. Tổng kết, đánh giá

2.4. Quy trình ứng cứu sự cố an toàn thông tin

2.4.1. Quy trình ứng cứu sự cố tấn công lừa đảo (Phishing)

a. Phát hiện/Tiếp nhận sự cố:

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ƯCSC Ngành BHXH; Đội vận hành hệ thống ATTT; Đơn vị cung cấp dịch vụ giám sát ATTT.

b. Triển khai các bước ưu tiên ứng cứu ban đầu:

c. Triển khai lựa chọn phương án ứng cứu

d. Chỉ đạo xử lý sự cố (nếu cần)

e. Báo cáo sự cố

f. Điều phối công tác ứng cứu

g. Triển khai ứng cứu, ngăn chặn và xử lý sự cố

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ƯCSC Ngành BHXH; Đội vận hành hệ thống ATTT; Đơn vị cung cấp dịch vụ giám sát ATTT.

h. Xử lý sự cố, gỡ bỏ và khôi phục

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ƯCSC Ngành BHXH; Đội vận hành hệ thống ATTT; Đơn vị cung cấp dịch vụ giám sát ATTT.

i. Khôi phục hoạt động hệ thống

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ƯCSC Ngành BHXH; Đội vận hành hệ thống ATTT; Đơn vị cung cấp dịch vụ giám sát ATTT.

j. Kiểm tra, đánh giá hệ thống thông tin

k. Tổng kết, đánh giá

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ƯCSC Ngành BHXH; Đội vận hành hệ thống ATTT.

2.4.2. Quy trình ứng cứu sự cố tấn công khai thác lỗ hổng bảo mật (Vulnerability Exploitation)

a. Phát hiện/Tiếp nhận sự cố:

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ƯCSC Ngành BHXH; Đội vận hành hệ thống ATTT; Đơn vị cung cấp dịch vụ giám sát ATTT.

b. Triển khai các bước ưu tiên ứng cứu ban đầu:

c. Triển khai lựa chọn phương án ứng cứu

d. Chỉ đạo xử lý sự cố (nếu cần)

e. Báo cáo sự cố

f. Điều phối công tác ứng cứu

g. Triển khai ứng cứu, ngăn chặn và xử lý sự cố

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ƯCSC Ngành BHXH; Đội vận hành hệ thống ATTT; Đơn vị cung cấp dịch vụ giám sát ATTT.

h. Xử lý sự cố, gỡ bỏ và khôi phục

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ƯCSC Ngành BHXH; Đội vận hành hệ thống ATTT; Đơn vị cung cấp dịch vụ mạng; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

i. Khôi phục hoạt động hệ thống

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ƯCSC Ngành BHXH; Đội vận hành hệ thống ATTT; Đơn vị cung cấp dịch vụ mạng; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

j. Kiểm tra, đánh giá hệ thống thông tin

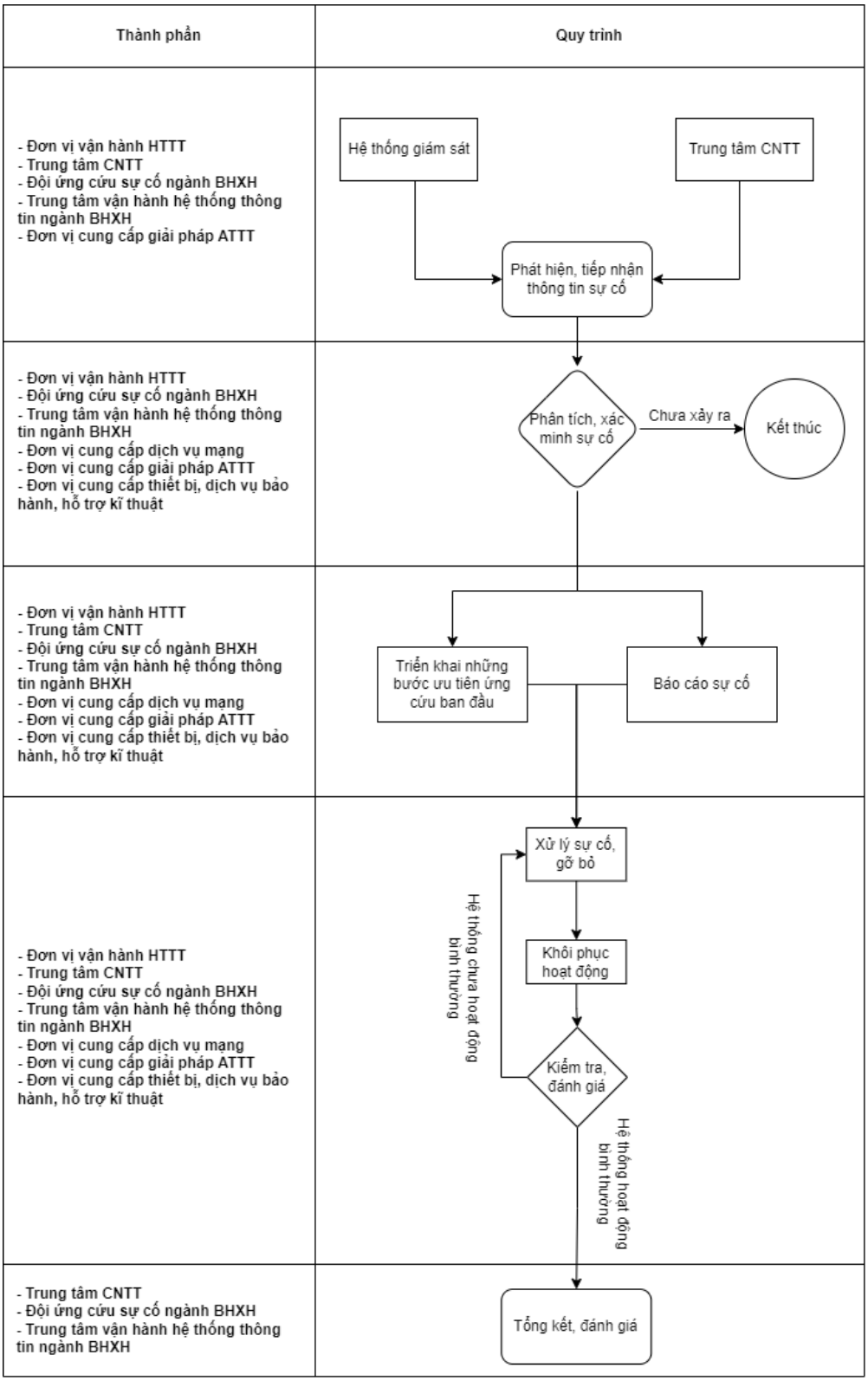
k. Tổng kết, đánh giá

- Đơn vị chủ trì: Trung tâm CNTT.

- Đơn vị phối hợp: Đội ƯCSC Ngành BHXH; Đội vận hành hệ thống ATTT.

III. Quy trình ứng cứu sự cố an toàn thông tin thông thường các đơn vị trong hệ thống BHXH Việt Nam

3.1. Quy trình tổng thể ứng cứu sự cố thông thường tại các đơn vị trong hệ thống BHXH Việt Nam



Hình 7. Quy trình tổng thể ứng cứu sự cố thông thường tại các đơn vị trong hệ thống BHXH Việt Nam

a. Phát hiện/Tiếp nhận sự cố:

- Đơn vị chủ trì: Đơn vị vận hành HTTT.

- Đơn vị phối hợp: Trung tâm CNTT, Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ giám sát ATTT.

b. Triển khai các bước ưu tiên ứng cứu ban đầu:

- Đơn vị chủ trì: Đơn vị vận hành HTTT.

- Đơn vị phối hợp: Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ mạng; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

c. Báo cáo sự cố

- Đơn vị chủ trì: Đơn vị vận hành HTTT.

- Đơn vị phối hợp: Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ mạng; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

d. Triển khai ứng cứu, ngăn chặn và xử lý sự cố

- Đơn vị chủ trì: Đơn vị vận hành HTTT.

- Đơn vị phối hợp: Trung tâm CNTT, Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ mạng; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

e. Xử lý sự cố, gỡ bỏ và khôi phục

- Đơn vị chủ trì: Đơn vị vận hành HTTT.

- Đơn vị phối hợp: Trung tâm CNTT, Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ mạng; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

f. Khôi phục hoạt động hệ thống

- Đơn vị chủ trì: Đơn vị vận hành HTTT.

- Đơn vị phối hợp: Trung tâm CNTT, Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ mạng; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

g. Kiểm tra, đánh giá hệ thống thông tin

- Đơn vị chủ trì: Đơn vị vận hành HTTT.

- Đơn vị phối hợp: Trung tâm CNTT, Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ mạng; Đơn vị cung cấp dịch vụ giám sát ATTT; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

h. Tổng kết, đánh giá

- Đơn vị chủ trì: Đơn vị vận hành HTTT.

- Đơn vị phối hợp: Trung tâm CNTT, Trung tâm vận hành HTTT; Đội ƯCSC Ngành BHXH.

3.2. Quy trình ứng cứu sự cố hệ thống mạng

a. Phát hiện/Tiếp nhận sự cố:

- Đơn vị chủ trì: Đơn vị vận hành HTTT.

- Đơn vị phối hợp: Trung tâm CNTT; Đội vận hành hệ thống mạng; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ mạng.

b. Triển khai các bước ưu tiên ứng cứu ban đầu:

- Đơn vị chủ trì: Đơn vị vận hành HTTT.

- Đơn vị phối hợp: Đội vận hành hệ thống mạng; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ mạng.

c. Báo cáo sự cố

d. Triển khai ứng cứu, ngăn chặn và xử lý sự cố

- Đơn vị chủ trì: Đơn vị vận hành HTTT.

- Đơn vị phối hợp: Trung tâm CNTT; Đội vận hành hệ thống mạng; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ mạng.

e. Xử lý sự cố, gỡ bỏ và khôi phục

- Đơn vị chủ trì: Đơn vị vận hành HTTT.

- Đơn vị phối hợp: Trung tâm CNTT; Đội vận hành hệ thống mạng; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ mạng; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

f. Khôi phục hoạt động hệ thống

- Đơn vị chủ trì: Đơn vị vận hành HTTT.

- Đơn vị phối hợp: Trung tâm CNTT; Đội vận hành hệ thống mạng; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ mạng; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

g. Kiểm tra, đánh giá hệ thống thông tin

h. Tổng kết, đánh giá

3.3. Quy trình ứng cứu sự cố hệ thống máy chủ, lưu trữ

a. Phát hiện/Tiếp nhận sự cố:

- Đơn vị chủ trì: Đơn vị vận hành HTTT.

- Đơn vị phối hợp: Trung tâm CNTT; Đội vận hành hệ thống máy chủ, lưu trữ; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

b. Triển khai các bước ưu tiên ứng cứu ban đầu:

- Đơn vị chủ trì: Đơn vị vận hành HTTT.

- Đơn vị phối hợp: Đội vận hành hệ thống máy chủ, lưu trữ; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

c. Báo cáo sự cố

d. Triển khai ứng cứu, ngăn chặn và xử lý sự cố

- Đơn vị chủ trì: Đơn vị vận hành HTTT.

- Đơn vị phối hợp: Trung tâm CNTT; Đội vận hành hệ thống máy chủ, lưu trữ; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

e. Xử lý sự cố, gỡ bỏ và khôi phục

- Đơn vị chủ trì: Đơn vị vận hành HTTT.

- Đơn vị phối hợp: Trung tâm CNTT; Đội vận hành hệ thống máy chủ, lưu trữ; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

f. Khôi phục hoạt động hệ thống

- Đơn vị chủ trì: Đơn vị vận hành HTTT.

- Đơn vị phối hợp: Trung tâm CNTT; Đội vận hành hệ thống máy chủ, lưu trữ; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

g. Kiểm tra, đánh giá hệ thống thông tin

h. Tổng kết, đánh giá

3.4. Quy trình ứng cứu sự cố an toàn thông tin

3.4.1. Quy trình ứng cứu sự cố mã độc (Malware)

a. Phát hiện/Tiếp nhận sự cố:

- Đơn vị chủ trì: Đơn vị vận hành HTTT.

- Đơn vị phối hợp: Trung tâm CNTT; Đội vận hành hệ thống ATTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ ATTT; Đơn vị cung cấp giải pháp phòng chống mã độc.

b. Triển khai các bước ưu tiên ứng cứu ban đầu:

- Đơn vị chủ trì: Đơn vị vận hành HTTT.

- Đơn vị phối hợp: Đội vận hành hệ thống ATTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ ATTT; Đơn vị cung cấp cung cấp giải pháp phòng chống mã độc.

c. Báo cáo sự cố

d. Triển khai ứng cứu, ngăn chặn và xử lý sự cố

- Đơn vị chủ trì: Đơn vị vận hành HTTT, Trung tâm CNTT.

- Đơn vị phối hợp: Đội ƯCSC Ngành BHXH.

e. Xử lý sự cố, gỡ bỏ và khôi phục

- Đơn vị chủ trì: Đơn vị vận hành HTTT.

- Đơn vị phối hợp: Trung tâm CNTT, Đội ƯCSC Ngành BHXH.

f. Khôi phục hoạt động hệ thống

- Đơn vị chủ trì: Đơn vị vận hành HTTT.

- Đơn vị phối hợp: Trung tâm CNTT, Đội ƯCSC Ngành BHXH.

g. Kiểm tra, đánh giá hệ thống thông tin

h. Tổng kết, đánh giá

3.4.2. Quy trình cứu sự cố tấn công lừa đảo (Phishing)

a. Phát hiện/Tiếp nhận sự cố:

- Đơn vị chủ trì: Đơn vị vận hành HTTT.

- Đơn vị phối hợp: Trung tâm CNTT; Đội vận hành hệ thống ATTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ ATTT.

b. Triển khai các bước ưu tiên ứng cứu ban đầu:

- Đơn vị chủ trì: Đơn vị vận hành HTTT.

- Đơn vị phối hợp: Đội vận hành hệ thống ATTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ ATTT.

c. Báo cáo sự cố

d. Triển khai ứng cứu, ngăn chặn và xử lý sự cố

- Đơn vị chủ trì: Đơn vị vận hành HTTT.

- Đơn vị phối hợp: Trung tâm CNTT; Đội vận hành hệ thống ATTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ ATTT; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

e. Xử lý sự cố, gỡ bỏ và khôi phục

- Đơn vị chủ trì: Đơn vị vận hành HTTT.

- Đơn vị phối hợp: Trung tâm CNTT; Đội vận hành hệ thống ATTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ ATTT; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

f. Khôi phục hoạt động hệ thống

- Đơn vị chủ trì: Đơn vị vận hành HTTT.

- Đơn vị phối hợp: Trung tâm CNTT; Đội vận hành hệ thống ATTT; Đội ƯCSC Ngành BHXH; Đơn vị cung cấp dịch vụ ATTT; Đơn vị cung cấp thiết bị, dịch vụ bảo hành, hỗ trợ kĩ thuật.

g. Kiểm tra, đánh giá hệ thống thông tin

h. Tổng kết, đánh giá

CHƯƠNG 5. KẾT LUẬN VÀ CÁC KIẾN NGHỊ, ĐỀ XUẤT

I. Hướng phát triển tiếp theo của đề án

1.1. Bổ sung các quy trình ứng cứu sự cố

Đối với mỗi hệ thống thông tin, chương trình, ứng dụng, cần xây dựng tình huống, kịch bản sự cố cụ thể và đưa ra phương án đối phó, ứng cứu sự cố tương ứng. Trong phương án đối phó, ứng cứu phải đặt ra được các tiêu chí để có thể nhanh chóng xác định được tính chất, mức độ nghiêm trọng của sự cố khi sự cố xảy ra. Trong đề án này, nhóm nghiên cứu đã đưa ra một số quy trình ứng cứu sự cố an toàn thông tin cụ thể, tuy nhiên vẫn còn nhiều sự cố có thể xảy ra cần có quy trình, ví dụ như:

- Quy trình ứng cứu sự cố do bị tấn công mạng:

- Tấn công truy cập trái phép, chiếm quyền điều khiển
- Tấn công mã hóa phần mềm, dữ liệu, thiết bị
- Tấn công phá hoại thông tin, dữ liệu, phần mềm
- Tấn công nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu
- Tấn công tổng hợp sử dụng kết hợp nhiều hình thức

- Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật:

- Sự cố nguồn điện
- Sự cố đường kết nối Internet
- Sự cố do lỗi phần mềm, phần cứng, ứng dụng của hệ thống thông tin
- Sự cố liên quan đến quá tải hệ thống
- Sự cố khác do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật

- Sự cố do lỗi của người quản trị, vận hành hệ thống:

- Lỗi trong cập nhật, thay đổi, cấu hình phần cứng;
- Lỗi trong cập nhật, thay đổi, cấu hình phần mềm;
- Lỗi liên quan đến chính sách và thủ tục an toàn thông tin;
- Lỗi liên quan đến việc dừng dịch vụ vì lý do bắt buộc;
- Lỗi khác liên quan đến người quản trị, vận hành hệ thống.
- Tình huống sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn

1.2. Đánh giá rủi ro các hệ thống thông tin

Việc đảm bảo an toàn thông tin (ATTT) cho các hệ thống trong Chính phủ điện tử (CPĐT) là một trong những bài toán lớn, luôn được Chính phủ, các

bộ/ngành quan tâm. Từ đó, đặt ra vấn đề cần phải có công tác đánh giá, quản lý rủi ro và xử lý sự cố ATTT trong CPĐT. Việc đánh giá rủi ro cũng là một phần quan trọng trong việc xác định mức độ quan trọng của từng hệ thống, thành phần hệ thống từ đó xác định được mức độ của sự cố khi xảy ra.

Theo quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ, hệ thống thông tin phải đáp ứng các yêu cầu an toàn cơ bản, tối thiểu. Tuy nhiên, mỗi hệ thống thông tin khác nhau sẽ có sẽ có đặc thù riêng và yêu cầu mức độ an toàn khác nhau phù hợp với yêu cầu thực tế của mỗi cơ quan, tổ chức. Do đó, trên cơ sở đánh giá và quản lý rủi ro, cơ quan, tổ chức cần rà soát, bổ sung các yêu cầu an toàn cho phù hợp với yêu cầu thực tế. Khi triển khai các biện pháp kiểm soát rủi ro, trước hết cần xem xét các biện pháp cần thiết đã có trong yêu cầu cơ bản hay chưa. Trường hợp, biện pháp kiểm soát đã nằm trong yêu cầu cơ bản thì cần thực hiện theo quy định. Trường hợp cần bổ sung các yêu cầu an toàn mới để đáp ứng yêu cầu thực tế thì cần đưa ra phương án cụ thể để thực hiện.

Các biện pháp kiểm soát cơ bản đối với hệ thống thông tin được quy định tại Điều 19 Nghị định 85/2016/NĐ-CP ngày 10/7/2016, Điều 8, 9 Thông tư 03/2017/TT-BTTTT ngày 24/4/2017 và hướng dẫn chi tiết tại tiêu chuẩn quốc gia TCVN 11930:2017. Các yêu cầu an toàn được chia làm nhóm các yêu cầu về quản lý và các yêu cầu về kỹ thuật. Trong đó, các yêu cầu về kỹ thuật đưa ra các yêu cầu liên quan đến thiết kế, thiết lập, các biện pháp, giải pháp công nghệ đối với hệ thống trong quá trình xây dựng và thiết lập. Các yêu cầu về quản lý đưa ra chính sách, quy chế, quy trình, tổ chức bộ máy bảo đảm an toàn thông tin nhằm bảo đảm an toàn thông tin cho hệ thống thông tin trong quá trình vận hành, khai thác.

Khi thực hiện đánh giá và quản lý rủi ro an toàn thông tin, cần xây dựng một bức tranh đầy đủ về các rủi ro an toàn thông tin mà tổ chức có khả năng gặp phải, đánh giá sắp xếp mức độ ưu tiên và xây dựng hệ thống các biện pháp kiểm soát tổng thể, thống nhất và đầy đủ để giảm thiểu rủi ro.

Trong phạm vi của đề án, nhóm nghiên cứu tập trung vào việc xây dựng quy trình tổng thể xử lý các sự cố cho các hệ thống thông tin tuy nhiên chưa chi tiết cụ thể từng thành phần của từng hệ thống thông tin để có phân loại chi tiết các sự cố với từng mức độ nguy hiểm. Do đó, trong thời gian tới nhóm nghiên cứu cùng với Trung tâm CNTT, Đội ứng cứu sự cố ngành BHXH sẽ tiếp tục xây dựng các tài liệu đánh giá rủi ro của từng hệ thống thông tin.

II. Một số kiến nghị, đề xuất

2.1. Với Bảo hiểm xã hội Việt Nam

- Chỉ đạo các đơn vị trực thuộc BHXH Việt Nam, các tỉnh, thành phố tăng cường chỉ đạo công tác tổ chức thực hiện các chính sách đảm bảo ATTT trong đơn vị; đẩy mạnh công tác truyền thông nâng cao nhận thức của công chức viên

chức và người lao động, công tác kiểm tra việc thực hiện các chính sách ATTT trong toàn Ngành.

- Ban hành quy định về quy trình ứng cứu khẩn cấp sự cố ATTT để các đơn vị tổ chức thực hiện.

- Sớm có chính sách hỗ trợ về điều kiện, phương tiện làm việc và phụ cấp đặc thù cho Đội ƯCSC Ngành BHXH.

- Hàng năm, tổ chức sơ kết, tổng kết, đánh giá, rút kinh nghiệm, nhân rộng mô hình hiệu quả; biểu dương, khen thưởng các đơn vị, cá nhân có thành tích xuất sắc trong công tác đảm bảo ATTT.

2.2. Với BHXH các tỉnh, thành phố

- Bố trí nguồn lực, kết hợp với sự hỗ trợ từ BHXH Việt Nam để thực hiện công tác đảm bảo ATTT tại đơn vị: Thực hiện giám sát các hệ thống thông tin thuộc phạm vi quản lý, sớm phát hiện cảnh báo các sự cố hệ thống, các nguy cơ về ATTT để kịp thời áp dụng quy trình ứng cứu sự cố và kịp thời thông tin, báo cáo BHXH Việt Nam.

- Tăng cường công tác phổ biến các chính sách về đảm bảo ATTT để công chức, viên chức hiểu rõ sự cần thiết, vai trò, lợi ích, ý nghĩa của công tác đảm bảo ATTT trong đơn vị, tạo sự đồng thuận, thống nhất trong tổ chức thực hiện đảm bảo các hệ thống thông tin, CSDL chuyên ngành hoạt động ổn định, thông suốt.

2.3. Với các cơ quan quản lý Nhà nước về ATTT

- Đề nghị Cục ATTT (Bộ Thông tin – truyền thông) hướng dẫn các bước thực hiện chính sách về đảm bảo ATTT theo cấp độ. Kết nối, chia sẻ các thông tin về mã độc, sự cố ATTT và các bước phân tích, xử lý, ứng cứu sự cố ATTT.

- Đề nghị Cục Chứng thực số và bảo mật thông tin cung cấp, chia sẻ các thông tin về ATTT; cung cấp các thiết bị lưu trữ, mã hóa chuyên dùng cho Ngành BHXH Việt Nam.

2.4. Với các cung cấp dịch vụ mạng, dịch vụ ATTT

- Tham gia, hỗ trợ cho các đơn vị trực thuộc BHXH Việt Nam có liên quan trong việc giám sát, phát hiện, đánh giá và ứng cứu sự cố ATTT cho các hệ thống thông tin của Ngành BHXH Việt Nam.

- Hoàn thiện các hệ thống kết nối, cung cấp dịch vụ chất lượng cao về ATTT cho BHXH Việt Nam, đảm bảo nhân lực trực tiếp, gián tiếp quản trị, vận hành, giám sát, đánh giá ATTT cho các hệ thống thông tin của cơ quan BHXH kịp thời hỗ trợ ứng cứu sự cố khi phát hiện hoặc được thông báo.

- Phối hợp với các tổ chức ATTT chuyên ngành triển khai giải pháp, sản phẩm ATTT sử dụng công nghệ hiện đại, tiến tiến hỗ trợ cho BHXH Việt Nam giảm thiểu tối đa các thiệt hại khi có sự cố ATTT xảy ra.

III. Kết luận

Quy trình ứng cứu sự cố ATTT cho các hệ thống thông tin của BHXH Việt Nam là một nội dung rất quan trọng trong mô hình tam giác ATTT (Con người, công nghệ và Quy trình). Trong chiến lược đảm bảo ATTT của một tổ chức, một ngành, hay một quốc gia, được đặt trong bối cảnh nhiều thách thức của thời đại Công nghiệp 4.0, Quy trình đảm bảo ATTT là nhiệm vụ được lãnh đạo các cấp đưa lên hàng đầu.

Trong giai đoạn tiếp theo, ngành BHXH Việt Nam sẽ tiếp tục nhiều các hệ thống thông tin, hệ thống dịch vụ công trực tuyến về BHXH, BHYT, BHTN cung cấp cho người dân và doanh nghiệp. Để đảm bảo ATTT cho các hệ thống thông tin của Ngành là rõ ràng là công việc rất nhiều khó khăn, thách thức mà Ngành cần đối diện và vượt qua.

Để chủ động, sẵn sàng trong thực hiện nhiệm vụ cũng như phát triển hệ thống thông tin của ngành BHXH Việt Nam chuyên nghiệp, hiệu quả, hiện đại; đảm bảo ATTT cho các hệ thống hoạt động ổn định, thông suốt thì việc xây dựng quy trình đảm bảo ATTT là cần thiết và cấp bách.

Đề án này được xây dựng trên cơ sở tổng hợp các vấn đề lý luận và thực tiễn xây dựng, tổ chức thực hiện chính sách đảm bảo ATTT ngành BHXH Việt Nam, kết hợp với nghiên cứu, học tập các kinh nghiệm trong nước và quốc tế. Với sự nỗ lực, nghiêm túc, thận trọng và khoa học, nhóm nghiên cứu đã hoàn thành dự thảo Quy trình ứng cứu sự cố ATTT ngành BHXH để trình Tổng Giám đốc phê duyệt.

Mặc dù vậy, trong quá trình nghiên cứu, phân tích, nhất là khi xây dựng các dự thảo sẽ không tránh khỏi những thiếu sót, nhóm tác giả rất mong nhận được những phản hồi từ các nhà nghiên cứu, các nhà quản lý để tiếp tục hoàn thiện, đáp ứng mục tiêu nghiên cứu đề ra./.

DANH MỤC TÀI LIỆU THAM KHẢO

1. Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ.

2. Thông tư 03/2017/TT-BTTTT ngày ngày 24/04/2017 về việc quy định chi tiết và hướng dẫn một số điều của nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

3. Quyết định 05/2017/QĐ-TTg ngày 16/03/2017 ban hành Quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm An toàn thông tin mạng Quốc gia.

4. Thông tư số 20/2017/TT-BTTTT ngày 12/09/2017 về việc quy định điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc.

5. Thông tư số 24/2020/TT-BTTTT ngày 09/09/2020 quy định công tác triển khai, giám sát công tác triển khai và nghiệm thu dự án đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách Nhà nước.

6. Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 cuả Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ.

7. Kế hoạch số 3280/KH-BHXH ngày 29/08/2018 về việc ứng phó sự cố bảo đảm an toàn thông tin mạng trong ngành BHXH Việt Nam.

8. Tiêu chuẩn quốc gia TCVN 11930:2017 về Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ.

9. Tiêu chuẩn quốc gia TCVN ISO/IEC 27001:2019 và ISO/IEC 27001:2013 "Công nghệ thông tin - Các kỹ thuật an toàn - Hệ thống quản lý an toàn thông tin - Các yêu cầu".

10. TCVN ISO/IEC 27002:2020 về Công nghệ thông tin - Các kỹ thuật an toàn - Quy tắc thực hành Quản lý an toàn thông tin.

11. Tiêu chuẩn ISO/IEC 27005:2018 “Công nghệ thông tin – Kỹ thuật bảo mật – Quản lý rủi ro an toàn thông tin”.

12. TCVN 9801-3:2014 Công nghệ thông tin - Kỹ thuật an toàn - An toàn mạng - Phần 3: Các kịch bản kết nối mạng tham chiếu - Nguy cơ, kỹ thuật thiết kế và các vấn đề kiểm soát (ISO/IEC 27033-3:2010).

13. TCVN 9801-2:2015 Công nghệ thông tin - Các kỹ thuật an toàn - An toàn mạng - Phần 2: Hướng dẫn thiết kế và triển khai an toàn mạng (ISO/IEC 27033-2:2012).

14. TCVN 11239:2015 về Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý sự cố an toàn thông tin.

15. Lê Nguyên Bồng (2021) “Giải pháp hoàn thiện việc xây dựng và vận hành cơ sở dữ liệu điện tử về quản lý bảo hiểm xã hội trong phạm vi cả nước”.

16. Hoàng Đăng Trị và nhóm nghiên cứu tại Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (2017) Nghiên cứu xây dựng tiêu chuẩn “Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn đảm bảo sự phù hợp và đầy đủ theo phương pháp điều tra sự cố”.

17. Nghiên cứu “Denial of Service (DoS) guidance” của Trung tâm ninh mạng quốc gia Anh Quốc – NCSC UK ngày 16/03/2016.

18. Cyber Incident Respone: Phishing Playbook v2.3 của Chính phủ Scotland ngày 20/01/2020.

19. ISO/IEC 15408:2017 Information technology — Security techniques — Evaluation criteria for IT security.

20. ISO/IEC 27001:2005, Information technology - Security techniques - lnformation security management systems – Requirements.

21. ISO/IEC 27005:2011, Informatinon technology-Security techniques-Informatinon Security Risk management system.

22. NIST SP 800-30r1, Guide for Conducting Risk Assessments.

23. NIST SP 800-53R4, Security and Privacy Controls for Federal Information Systems and Organizations.