BAN CHẤP HÀNH TRUNG ƯƠNG
BAN CÁN SỰ ĐẢNG BHXH VIỆT NAM
*

ĐẢNG CỘNG SẢN VIỆT NAM

Số 398 -NQ/BCSĐ

Hà Nội, ngày 15 tháng 3 năm 2024

NGHỊ QUYẾT
CỦA BAN CÁN SỰ ĐẢNG BẢO HIỂM XÃ HỘI VIỆT NAM
Tăng cường công tác bảo đảm an toàn thông tin mạng ngành Bảo hiểm xã hội Việt Nam

I. TÌNH HÌNH THỰC HIỆN

1. Kết quả đạt được

An toàn thông tin mạng là nhiệm vụ quan trọng và đột phá để tạo lập niềm tin số, xây dựng môi trường mạng trung thực, văn minh, lành mạnh và phòng, chống vi phạm pháp luật trên không gian mạng, bảo vệ sự phát triển của ngành Bảo hiểm xã hội (BHXH) Việt Nam nhằm thực hiện thành công chuyển đổi số quốc gia. Một số kết quả đạt được cụ thể như sau:

a) Công tác lãnh đạo, chỉ đạo, quán triệt và tổ chức triển khai thực hiện bảo đảm an toàn thông tin mạng

Nhận thức được tầm quan trọng và ý nghĩa của an toàn thông tin mạng, Ban Cán sự đảng BHXH Việt Nam đã lãnh đạo tổ chức nghiên cứu, quán triệt và tổ chức triển khai các nội dung của Nghị quyết số 30-NQ/TW ngày 25/7/2018 của Bộ Chính trị về Chiến lược an ninh mạng quốc gia, qua đó tạo sự chuyển biến rõ rệt, hiệu quả về nhận thức, hành động trong bảo đảm an toàn, an ninh mạng trong toàn Ngành của đảng viên, công chức, viên chức và người lao động (CCVC) trong toàn Ngành về vị trí, tầm quan trọng của an ninh mạng trong sự nghiệp xây dựng và bảo vệ Tổ quốc. Bảo đảm sự lãnh đạo tuyệt đối của Ban Cán sự đảng, sự chỉ đạo thống nhất của Tổng Giám đốc BHXH Việt Nam trong bảo đảm an ninh mạng, xây dựng hệ thống thông tin của Ngành luôn đáp ứng các yêu cầu về công tác an toàn thông tin mạng.

Ban Cán sự đảng BHXH Việt Nam đã chỉ đạo quán triệt và tổ chức triển khai nội dung các Nghị quyết của Chính phủ, Chỉ thị của Thủ tướng Chính phủ về công tác bảo đảm an toàn, an ninh mạng, bảo vệ bí mật nhà nước trên không gian mạng, trọng tâm là các văn bản chỉ đạo: Nghị quyết số 22/NQ-CP ngày 18/10/2019 của Chính phủ ban hành Chương trình hành động của Chính phủ thực hiện Nghị quyết số 30-NQ/TW ngày 25/7/2018 của Bộ Chính trị về Chiến lược An ninh mạng quốc gia, Chỉ thị số 02/CT-TTg ngày 04/7/2018 về công tác bảo vệ bí mật nhà nước trên không gian mạng; Chỉ thị số 02/CT-TTg ngày 15/11/2019 về tăng cường công tác bảo vệ bí mật nhà nước trong tình hình hiện nay, Chỉ thị số 14/CT-TTg ngày 25/5/2018 về việc nâng cao năng lực phòng, chống phần mềm độc hại, Chỉ thị số 14/CT-TTg ngày 07/6/2019 về việc tăng cường bảo đảm an toàn, an

ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam, Chỉ thị số 01/CT-TTg ngày 18/02/2021 về việc tăng cường công tác bảo vệ an ninh mạng trong tình hình hiện nay, Quyết định số 964/QĐ-TTg ngày 10/08/2022 về chiến lược an toàn, an ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn năm 2030, Chỉ thị số 18/CT-TTg ngày 13/10/2022 về đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam.

Ban Cán sự đảng BHXH Việt Nam đã xác định rõ những vấn đề trọng tâm, trọng điểm trong công tác chuyển đổi số nói chung và bảo đảm an ninh, an toàn thông tin mạng nói riêng để ban hành, chỉ đạo ban hành các văn bản, cụ thể như: Nghị quyết số 362-NQ/BCSĐ ngày 12/05/2023 của Ban Cán sự đảng BHXH Việt Nam về tăng cường thực hiện" Đề án phát triển ứng dụng dữ liệu dân cư, định danh và xác thực điện tử phục vụ chuyển đổi số quốc gia giai đoạn 2022-2025, tầm nhìn đến năm 2030 (Đề án 06); Quyết định số 1167/QĐ-BHXH ban hành Chương trình hành động của BHXH Việt Nam thực hiện Nghị quyết số 362-NQ/BCSĐ; Quyết định số 967/QĐ-BHXH ngày 20/6/2017 quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin (CNTT) của ngành BHXH; Quyết định số 1114/QĐ-BHXH ngày 04/7/2017 quy chế quản lý và sử dụng thư điện tử ngành BHXH; Quyết định số 2366/QĐ-BHXH ngày 28/11/2018 quy chế quản lý, khai thác và sử dụng thông tin từ cơ sở dữ liệu tập trung ngành BHXH; Quyết định số 283/QĐ-BHXH ngày 25/02/2020 quy chế quản trị, vận hành hệ thống thu nộp, chi trả BHXH điện tử; Quyết định số 352/QĐ-BHXH ngày 06/3/2020 quy chế hoạt động cổng dịch vụ công và hệ thống thông tin điện tử ngành BHXH; Quyết định số 515/QĐ-BHXH ngày 27/3/2020 quy chế quản lý cơ sở dữ liệu hộ gia đình và mã số bảo BHXH của người tham gia BHXH, BHYT; Quyết định số 893/QĐ-BHXH ngày 10/7/2020 quy chế quản trị, vận hành, khai thác, sử dụng hệ thống tổng hợp và phân tích dữ liệu tập trung ngành BHXH; Quyết định số 1166/QĐ-BHXH ngày 22/9/2020 quy chế cung cấp, quản lý và sử dụng chứng thư số, dịch vụ chứng thực chữ ký số trong ngành BHXH; Quyết định số 3735/QĐ-BHXH ngày 29/12/2022 quy chế quản lý, triển khai, vận hành và khai thác hệ thống hạ tầng thông tin trong ngành BHXH Việt Nam; Quyết định số 1668/QĐ-BHXH ngày 20/11/2023 quy chế bảo đảm an toàn hệ thống thông tin theo cấp độ ngành BHXH Việt Nam; Kế hoạch số 3280/KH-BHXH ngày 29/08/2018 ứng cứu sự cố và bảo đảm an toàn thông tin mạng trong ngành BHXH Việt Nam. Qua đó chỉ đạo các đơn vị trong toàn Ngành bám sát, triển khai, thực hiện hiệu quả công tác bảo đảm an toàn, an ninh mạng theo các quy định của nhà nước, khuyến nghị của các cơ quan quản lý nhà nước và gắn trách nhiệm của thủ trưởng các đơn vị về công tác an toàn thông tin mạng.

Ban Cán sự đảng BHXH Việt Nam đã chỉ đạo tuyên truyền trên Cổng thông tin điện tử BHXH Việt Nam, xây dựng chuyên mục "Hoạt động ứng cứu sự cố, bảo đảm an toàn thông tin mạng" để đăng tải các chủ đề, thông tin, phóng sự, video clip về an toàn thông tin mạng; cẩm nang nhận diện và phòng chống lừa đảo trực tuyến; chiến dịch làm sạch mã độc trên không gian mạng... được Bộ Thông tin và Truyền thông cung cấp và cập nhật thông tin liên quan đến hoạt động ứng cứu sự cố, các hoạt động bảo đảm an toàn thông tin mạng của ngành BHXH

Việt Nam đang triển khai nhằm nâng cao nhận thức, trách nhiệm, tăng cường năng lực, kỹ năng ứng cứu sự cố, bảo đảm an toàn thông tin mạng trong toàn Ngành. Chỉ đạo tổ chức hội nghị toàn Ngành về an toàn thông tin mạng hàng năm (2018, 2019, 2020, 2021, 2022) và tổ chức tập huấn kỹ năng an toàn thông tin mạng, hướng dẫn bảo đảm an toàn thông tin mạng khi sử dụng và khai thác các ứng dụng CNTT của Ngành, các kỹ năng nhận diện dấu hiệu mã độc mới và kỹ năng rà quét, bóc gỡ mã độc cho CCVC chuyên trách về an toàn thông tin mạng tham gia qua hệ thống hội nghị trực tuyến. Chỉ đạo tổ chức các khóa đào tạo trong các năm 2018, 2019, 2020 và đã cấp chứng chỉ, chứng nhận nội dung nâng cao nhận thức về an toàn thông tin mạng cho CCVC trong toàn Ngành với 03 khóa học và 09 lớp, bảo đảm 100% CCVC được tiếp cận hoạt động nâng cao nhận thức, kỹ năng và công cụ bảo đảm an toàn thông tin mạng.

b) Công tác phân loại, xác định, phê duyệt đề xuất cấp độ hệ thống thông tin ngành BHXH Việt Nam

BHXH Việt Nam đã phê duyệt đề xuất cấp độ theo Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ cho 17 hệ thống thông tin thuộc ngành BHXH Việt Nam, trong đó 07 hệ thống thông tin cấp độ 3 phê duyệt tại Quyết định số 1954/QĐ-BHXH ngày 08/11/2019 kèm theo phương án bảo đảm an toàn thông tin mạng với tiêu chuẩn quốc gia TCVN 11930:2017 tương ứng, phù hợp cấp độ 3; 10 hệ thống thông tin cấp độ 2 phê duyệt tại Quyết định số 1137/QĐ-BHXH ngày 08/11/2019 kèm theo phương án bảo đảm an toàn thông tin mạng với tiêu chuẩn quốc gia TCVN 11930:2017 tương ứng, phù hợp cấp độ 2.

c) Công tác triển khai các hệ thống kỹ thuật bảo đảm an toàn thông tin mạng cho hệ thống thông tin ngành BHXH Việt Nam

Hệ thống kỹ thuật của ngành BHXH Việt Nam được phân chia thành các nhóm để tổ chức triển khai đầy đủ các giải pháp kỹ thuật an toàn thông tin mạng theo quy định của cơ quan quản lý nhà nước, đáp ứng yêu cầu bảo vệ cho hệ thống cấp độ 3 trở lên của ngành BHXH Việt Nam: Quản lý truy cập, quản trị hệ thống từ xa an toàn, phòng chống xâm nhập (IDS/IPS), phòng, chống tấn công mạng cho ứng dụng web (WAF), tường lửa cho máy chủ cơ sở dữ liệu (DBF), chặn lọc phần mềm độc hại trên môi trường mạng, phòng chống tấn công từ chối dịch vụ (DDoS), giám sát an toàn hệ thống thông tin tập trung (SIEM), phòng chống mã độc (AVR), phòng, chống thất thoát dữ liệu (DLP), quản lý tài khoản đặc quyền (PAM). Các máy tính người dùng được triển khai các biện pháp kỹ thuật bảo vệ, nâng cao năng lực phòng, chống phần mềm độc hại theo Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ gồm: hệ điều hành Windows bản quyền; kết nối dịch vụ quản lý tập trung máy tính người dùng (AD), cài đặt đặt phần mềm diệt vi rút, phần mềm phát hiện và phản ứng với các cuộc tấn công chưa biết (EDR), phần mềm quản lý cập nhật bản vá (Patch Manager), phần mềm chống thất thoát dữ liệu (DLP), phần mềm kiểm soát truy cập mạng (NAC).

BHXH Việt Nam tổ chức triển khai bảo đảm an toàn thông tin mạng cho hệ thống thông tin ngành BHXH theo mô hình "4 lớp" tại Chỉ thị số 14/CT-TTg

ngày 07/6/2019: "Lớp 1" - Lực lượng tại chỗ là Ban Chỉ đạo chuyển đổi số ngành BHXH Việt Nam, đầu mối chuyên trách về an toàn thông tin mạng tại Trung tâm CNTT, Văn phòng BHXH Việt Nam, BHXH các tỉnh, thành phố trực thuộc Trung ương (gọi chung là BHXH các tỉnh) và Đội ứng cứu sự cố, bảo đảm an toàn thông tin mạng ngành BHXH Việt Nam (Đội ứng cứu sự cố) được thành lập tại Quyết định số 345/QĐ-BHXH ngày 09/04/2021, đơn vị thuê dịch vụ hỗ trợ, vận hành kỹ thuật các hệ thống thông tin ngành BHXH Việt Nam; "Lớp 2" - Thuê đơn vị giám sát, bảo vệ chuyên nghiệp tổ chức thu thập, phân tích, xử lý, giám sát tập trung và cảnh báo sớm các hoạt động, nguy cơ về an toàn đối với hệ thống thông tin tại Trung tâm dữ liệu Ngành và BHXH các tỉnh; "Lớp 3" - Thuê đơn vị độc lập kiểm tra, đánh giá an toàn thông tin mạng đối với hệ thống thông tin cấp độ 3 trở lên định kỳ theo quy định Nghị định số 85/2016/NĐ-CP, bảo đảm mức độ sẵn sàng của hệ thống thông tin ngành BHXH Việt Nam; "Lớp 4" - Kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia được duy trì thường xuyên với với Trung tâm Giám sát an toàn không gian mạng quốc gia trực thuộc Cục An toàn thông tin, Bộ Thông tin và Truyền thông.

d) Công tác bảo đảm nguồn nhân lực đáp ứng yêu cầu an toàn thông tin mạng

Nguồn nhân lực bảo đảm an toàn thông tin mạng ngành BHXH Việt Nam gồm: Ban Chỉ đạo chuyển đổi số ngành BHXH Việt Nam (Quyết định số 861/QĐ-BHXH ngày 01/09/2021) lãnh đạo, chỉ đạo công tác bảo đảm an toàn, an ninh mạng trong toàn Ngành; Lãnh đạo phụ trách về an toàn thông tin mạng tại các đơn vị (Trung tâm CNTT, Văn phòng BHXH Việt Nam và BHXH các tỉnh); CCVC quản lý về an toàn thông tin mạng, CCVC chuyên trách về an toàn thông tin mạng tại Trung tâm CNTT, Văn phòng BHXH Việt Nam và BHXH các tỉnh); CCVC kiêm nhiệm về CNTT tại BHXH cấp huyện và Đội ứng cứu sự cố (Quyết định số 345/QĐ-BHXH ngày 09/04/2021).

Trong các năm 2018, 2019, 2020 BHXH Việt Nam đã tổ chức các khóa đào tạo, cấp chứng chỉ, chứng nhận về an toàn thông tin mạng cho CCVC chuyên trách về CNTT tại BHXH Việt Nam và BHXH cấp tỉnh nhằm nâng cao trình độ cho đội ngũ CCVC làm công tác bảo đảm an toàn thông tin mạng, sẵn sàng ứng phó khi có sự cố xảy ra với 06 khóa học và 11 lớp. Năm 2022, tổ chức khóa bồi dưỡng về an toàn thông tin mạng cho CCVC Trung tâm CNTT, BHXH các tỉnh và Đội ứng cứu sự cố với 03 chuyên đề về tấn công mã độc, tấn công tống tiền, tấn công giả mạo được chọn lọc phù hợp với tình hình, xu hướng an toàn thông tin mạng trên thế giới cũng như tại Việt Nam, các CCVC đã được tham khảo các trường hợp tấn công thực tế và rút ra kinh nghiệm xử lý sự cố đối với BHXH Việt Nam.

Năm 2020 và 2022, BHXH Việt Nam tổ chức triển khai 06 đợt diễn tập ứng cứu sự cố an toàn thông tin mạng có sự tham gia của lãnh đạo, CCVC phụ trách an toàn thông tin mạng của các đơn vị trực thuộc BHXH Việt Nam và BHXH các tỉnh với đầy đủ cơ sở vật chất, hệ thống kỹ thuật và kịch bản diễn tập phù hợp, sát thực tế, trong đó năm 2022 có nội dung diễn tập thực chiến. Qua đó, nâng cao năng lực, kiến thức và kỹ năng kỹ thuật của CCVC chuyên trách và bán chuyên trách về an toàn thông tin mạng cũng như nâng cao nhận thức và trách nhiệm của

các cấp lãnh đạo quản lý, các đơn vị, bộ phận tham mưu công tác bảo đảm an toàn thông tin mạng; Tăng cường năng lực ứng cứu sự cố, bảo đảm an toàn thông tin mạng cho CCVC ngành BHXH Việt Nam.

Năm 2023, các thành viên Đội ứng cứu sự cố được cử tham gia khoá đào tạo bảo mật điện toán đám mây theo chương trình Certified Cloud Security Engineer, đào tạo kỹ năng bảo đảm an toàn thông tin cho hạ tầng mạng theo chương trình Certified Network Defender, đào tạo Hacker mũ trắng theo chương trình Certified Ethical Hacker và khóa đào tạo về an toàn thông tin cho lãnh đạo quản lý theo chương trình Certified Chief Information Security Officer trong khuôn khổ Đề án "Đào tạo và phát triển nguồn nhân lực an toàn thông tin mạng giai đoạn 2021 – 2025" (Quyết định số 21/QĐ-TTg ngày 06/01/2021 của Thủ tướng Chính phủ) và lớp bồi dưỡng, tập huấn về bảo đảm an toàn thông tin theo cấp độ và triển khai bảo đảm an toàn thông tin theo mô hình 04 lớp.

đ) Công tác tăng cường, mở rộng quan hệ và nâng cao hiệu quả phối hợp về an toàn thông tin mạng

BHXH Việt Nam giao đơn vị quản lý, chuyên trách về an toàn thông tin mạng trong toàn Ngành là đầu mối của BHXH Việt Nam tham gia Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia tuân thủ Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ, Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông và các văn bản chỉ đạo khác của cơ quan quản lý nhà nước trong lĩnh vực an toàn thông tin và hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam. Đơn vị chuyên trách về an toàn thông tin mạng ngành BHXH có trách nhiệm phối hợp cùng với đơn vị chức năng về an toàn, an ninh mạng của Bộ Công an, Bộ Thông tin – Truyền thông, Ban Cơ yếu Chính phủ triển khai các biện pháp bảo đảm an toàn thông tin mạng cho hệ thống thông tin ngành BHXH Việt Nam; tổ chức đánh giá mức độ sẵn sàng của hệ thống thông tin và bảo đảm an toàn thông tin mạng cho hệ thống thông tin quan trọng, hệ thống thông tin theo cấp độ.

Đội ứng cứu sự cố tham gia các đợt diễn tập ứng cứu sự cố được Bộ Thông tin – Truyền thông: Năm 2021 tham gia diễn tập ACID "Ứng phó tấn công chuỗi cung ứng nhắm vào các tổ chức doanh nghiệp"; Năm 2022 tham gia diễn tập ASEAN – Nhật Bản "Phối hợp xử lý tấn công mạng qua VPN vào các hệ thống cơ quan thuộc Chính phủ và tấn công mã hóa tống tiền vào cơ quan Y tế", diễn tập APCERT "Data Breach through Security Malpractice - Lộ lọt dữ liệu do thực hành bảo mật", diễn tập ACID "Dealing with Disruptive Cyber-Attacks Arising from Exploitation of Vulnerabilities - Ứng phó tấn công gián đoạn mạng từ việc khai thác lỗ hổng bảo mật"; Năm 2023 tham gia diễn tập APCERT "Digital Supply Chain Redemption – Mua ứng dụng qua chuỗi cung ứng số"; diễn tập ACID "Responding to Multi-Pronged Attacks Arising from Hacktivism - Ứng phó với tấn công đa hướng gia tăng từ tin tặc cực đoan".

Những kết quả đạt được nêu trên của BHXH Việt Nam đã khẳng định việc thực hiện đúng các quy định của nhà nước, Chính phủ, Thủ tướng Chính phủ và các cơ quan quản lý nhà nước chuyên ngành về bảo đảm an toàn, an ninh mạng.

Cùng với việc triển khai áp dụng đầy đủ các tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng trong các hoạt động ứng dụng CNTT đáp ứng tiêu chuẩn quốc gia TCVN 11930:2017, tiêu chuẩn quản lý an toàn thông tin ISO/IEC 27001, hệ thống kỹ thuật của ngành BHXH Việt Nam đã bảo vệ được an ninh, an toàn dữ liệu trước các tấn công mạng trong thời gian qua đến nay.

2. Tồn tại, hạn chế và nguyên nhân

a) Tồn tại, hạn chế

- CCVC chuyên trách an ninh, an toàn thông tin mạng còn thiếu cả về số lượng và chất lượng.

- Tại một số thời điểm, đội ngũ CCVC chuyên trách an ninh, an toàn thông tin còn chưa được cập nhật kịp thời các kiến thức, kỹ năng xử lý các vụ tấn công mạng với kỹ thuật mới, tinh vi, chưa đáp ứng yêu cầu triển khai, vận hành các giải pháp, công nghệ hiện đại.

- Việc duy trì chế độ bảo hành cho các hệ thống hạ tầng kỹ thuật an toàn thông tin còn chưa kịp thời dẫn đến rủi ro khi xảy ra sự cố (Trường hợp thiết bị hỏng làm suy giảm hiệu năng xử lý rà quét, nhận diện và ngăn chặn tấn công mạng).

- Tồn tại nguy cơ rủi ro đối với các sản phẩm CNTT, hệ thống hạ tầng kỹ thuật an toàn thông tin cũ, lạc hậu.

- Còn tình trạng CCVC thiếu cảnh giác trước các thủ đoạn tấn công mạng, chưa tuân thủ quy trình nghiệp vụ, cho mượn tài khoản công vụ.

- Việc lập hồ sơ đề xuất phê duyệt cấp độ an toàn thông tin cho các hệ thống thông tin của Ngành còn chậm.

b) Nguyên nhân

- Chế độ đãi ngộ cho CCVC CNTT, chuyển đổi số nói chung và CCVC chuyên trách an ninh, an toàn thông tin mạng còn hạn chế, chưa đủ hấp dẫn để thu hút, tuyển dụng được nhân sự chất lượng cao vào làm việc tại các cơ quan nhà nước nói chung và BHXH Việt Nam nói riêng.

- Các kỹ thuật tấn công mạng ngày càng tinh vi, thay đổi thường xuyên, khó phát hiện; thông tin cảnh báo từ các đơn vị chức năng đôi khi còn chưa kịp thời, dẫn tới việc nắm bắt thông tin và cập nhật kiến thức cho đội ngũ CCVC chuyên trách an toàn thông tin Ngành còn gặp nhiều khó khăn. Các giải pháp kỹ thuật, công nghệ để bảo đảm an ninh, an toàn thông tin mạng mới hiện nay đòi hỏi CCVC chuyên trách an toàn thông tin mạng phải am hiểu, có thời gian nghiên cứu và được đào tạo chuyển giao mới có thể triển khai, vận hành được.

- Việc duy trì chế độ bảo hành, nâng cấp cho các hệ thống phần mềm, hạ tầng kỹ thuật an toàn thông tin mạng còn chưa kịp thời dẫn đến rủi ro khi xảy ra sự cố.

- Một số CCVC trong ngành BHXH chưa nhận thức được vai trò, ý nghĩa của công tác an toàn thông tin mạng.

- Các tiêu chuẩn, quy chuẩn kỹ thuật trong việc lập hồ sơ đề xuất cấp độ bảo đảm an toàn thông tin mạng cho các hệ thống thông tin; công tác kiểm tra, đánh giá an toàn thông tin mạng và giám sát, bảo vệ an toàn thông tin mạng; giải pháp hạ tầng kỹ thuật công nghệ bảo đảm an toàn thông tin mạng cho các hệ thống thông tin thiếu các văn bản hướng dẫn của Nhà nước.

3. Bài học kinh nghiệm

Từ những kết quả đã đạt được và những tồn tại hạn chế BHXH Việt Nam rút ra được những bài học kinh nghiệm sau:

Một là, cần tiếp tục đẩy mạnh công tác chỉ đạo, lãnh đạo, kiểm tra, hướng dẫn các đơn vị trong công tác bảo đảm an toàn thông tin mạng.

Hai là, thường xuyên bồi dưỡng, tập huấn nâng cao nhận thức, trách nhiệm, năng lực về bảo đảm an toàn thông tin mạng cho lãnh đạo quản lý, CCVC tại các đơn vị trực thuộc, tham gia vào quá trình quản lý, vận hành, khai thác các hệ thống thông tin. Có chính sách trong tuyển chọn CCVC, ưu đãi trong quá trình công tác đối với CCVC làm công tác CNTT, chuyển đổi số, an toàn thông tin mạng trong toàn Ngành.

Ba là, tăng cường công tác phối hợp với các đơn vị chức năng của Bộ Thông tin và Truyền thông, các đơn vị nghiệp vụ của Bộ Công an và các tổ chức hoạt động trong lĩnh vực an toàn, an ninh mạng để trao đổi kinh nghiệm, chuyển giao công nghệ; phối hợp xây dựng cơ chế, nội dung hợp tác quốc tế trong lĩnh vực an toàn thông tin mạng. Cần đặc biệt tăng cường mối quan hệ với các nước có trình độ công nghệ phát triển, quan hệ hợp tác hữu nghị truyền thống với Việt Nam.

Bốn là, công tác bảo đảm an toàn thông tin mạng là công việc khó, phức tạp, hoạt động liên tục, xuyên suốt. Nếu có sự quan tâm, thông suốt về nhận thức của lãnh đạo, cùng với những giải pháp, phương án bảo đảm an toàn thông tin mạng phù hợp và sự tuân thủ, trách nhiệm của CCVC quản lý, vận hành, khai thác sẽ tạo ra môi trường mạng an toàn, đáp ứng yêu cầu ứng dụng CNTT, thực hiện thành công công tác bảo đảm an ninh mạng quốc gia.

II. QUAN ĐIỂM, MỤC TIÊU

1. Quan điểm

- An toàn thông tin mạng ngành BHXH Việt Nam là nhiệm vụ chính trị quan trọng, bảo đảm an toàn thông tin mạng là hoạt động thường xuyên, liên tục với cơ chế, chính sách phù hợp. Việc triển khai công tác an toàn thông tin mạng cần xác định rõ những vấn đề trọng tâm, trọng điểm để chỉ đạo thực hiện hiệu quả nhằm nâng cao ý thức trách nhiệm và các kỹ năng về an toàn thông tin mạng cho CCVC trong toàn Ngành.

- Quán triệt tinh thần quyết tâm, quyết liệt trong việc chỉ đạo triển khai thực hiện công tác bảo đảm an toàn thông tin mạng. Nhận thức rõ ý nghĩa, tầm quan trọng, tính cấp bách của công tác an toàn thông tin mạng trong giai đoạn hiện nay, là yếu tố quyết định, bảo đảm sự thành công công tác chuyển đổi số của Ngành BHXH Việt Nam. Huy động sự vào cuộc của tất cả CCVC trong toàn Ngành.

2. Mục tiêu

a) Mục tiêu tổng quát

Khắc phục được những tồn tại, hạn chế; phát huy vai trò tích cực, chủ động, tập trung trí tuệ và sức mạnh tổng hợp của toàn Ngành để tiếp tục tổ chức nghiên cứu, quán triệt, thực hiện nghiêm túc các Chỉ thị, Nghị quyết của Đảng, chính sách pháp luật của Nhà nước về công tác bảo đảm an toàn, an ninh mạng, bảo vệ bí mật nhà nước trên không gian mạng; chú trọng xây dựng đào tạo nguồn nhân lực chất lượng cao về an ninh mạng; rà soát, xây dựng và ban hành các văn bản chỉ đạo, văn bản quản lý và các quy định về an ninh mạng để triển khai thực hiện thống nhất trong toàn ngành BHXH Việt Nam; Xây dựng ngành BHXH Việt Nam hiện đại, chuyên nghiệp, hiệu quả, đáp ứng yêu cầu xây dựng Chính phủ điện tử, hướng tới Chính phủ số.

b) Mục tiêu cụ thể

- 100% CCVC trong toàn Ngành được phổ biến, quán triệt quan điểm, mục tiêu, nhiệm vụ, giải pháp trong thực hiện công tác bảo đảm an toàn thông tin mạng được nêu tại Nghị quyết này, kịp thời phổ biến chủ trương, chỉ đạo để thống nhất trong triển khai thực hiện.

- 100% CCVC trong toàn Ngành được đào tạo, bồi dưỡng nâng cao nhận thức, trách nhiệm trong công tác bảo đảm an toàn thông tin mạng; tập huấn về kỹ năng số, kỹ năng bảo mật thông tin trên môi trường mạng.

- Kiện toàn Đội ứng cứu sự cố, bảo đảm 100% BHXH cấp tỉnh có CCVC chuyên trách về an toàn thông tin mạng tham gia Đội ứng cứu sự cố; duy trì giao ban Đội ứng cứu sự cố tối thiểu 01 lần/quý để kịp thời chia sẻ thông tin và tháo gỡ vướng mắc trong quá trình thực hiện công tác bảo đảm an toàn thông tin mạng.

- Hoàn thiện các quy định, hướng dẫn của Ngành về an toàn thông tin mạng của ngành BHXH Việt Nam và các quy trình nghiệp vụ gắn với việc phân cấp, phân quyền trên phần mềm nghiệp vụ bảo đảm rõ người, rõ việc, rõ trách nhiệm.

- Tiếp tục duy trì và đầu tư, phát triển hạ tầng thông tin, bảo đảm hệ thống hạ tầng kỹ thuật an toàn thông tin mạng có đầy đủ chế độ bảo hành, hỗ trợ kỹ thuật và bản quyền tính năng.

- Tiếp tục nghiên cứu, triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin mạng theo quy định của nhà nước.

- Hằng năm tổ chức triển khai công tác đào tạo, tập huấn, phát triển nguồn nhân lực chuyên trách công tác an toàn thông tin mạng; tổ chức hội nghị an toàn thông tin mạng trong toàn Ngành; tổ chức diễn tập ứng cứu sự cố an toàn thông tin mạng trong toàn Ngành.

- Hằng năm, tổ chức các Đoàn kiểm tra, hướng dẫn công tác bảo đảm an toàn thông tin mạng tại các đơn vị trong toàn Ngành.

- Hằng năm tiến hành đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin đã được phê duyệt để điều chỉnh, phê duyệt hồ sơ đề xuất cấp độ và

phương án bảo đảm an toàn thông tin đối với các hệ thống đang triển khai hoặc triển khai mới.

III. NHIỆM VỤ, GIẢI PHÁP

1. Đào tạo, tập huấn

- Tiếp tục thực hiện đào tạo, huấn luyện nâng cao kiến thức chuyên sâu nghiệp vụ về an toàn thông tin mạng cho CCVC quản lý, kỹ thuật.

- Chú trọng công tác tập huấn, bồi dưỡng nâng cao nhận thức và kỹ năng số, kỹ năng an toàn thông tin mạng cho CCVC trong toàn Ngành. Các khóa tập huấn có sự tham gia trình bày của các chuyên gia, báo cáo viên của các đơn vị thuộc Bộ Công an, Bộ Thông tin – Truyền thông, Ban Cơ yếu Chính phủ.

- Triển khai các hình thức tuyên truyền, phổ biến chuyên đề về an toàn, an ninh thông tin số trước tình hình an toàn, an ninh mạng có nhiều diễn biến phức tạp như hiện nay để đảng viên, CCVC tích cực tham gia, hưởng ứng học tập.

- Triển khai công tác bảo đảm an toàn thông tin mạng đa dạng dưới nhiều hình thức như hội nghị giao ban, hội nghị chuyên đề, hội nghị diễn tập…

2. Quán triệt bằng quy trình, quy chế, khen thưởng, kỷ luật, kỷ cương

- Tăng cường công tác lãnh đạo, chỉ đạo của các Cấp ủy đảng, Thủ trưởng các đơn vị trực thuộc BHXH Việt Nam và BHXH các tỉnh. Tổ chức xây dựng, bổ sung vào nghị quyết, kế hoạch thực hiện công tác bảo đảm an toàn thông tin mạng của đơn vị. Người đứng đầu đơn vị sẽ chịu trách nhiệm chính khi có sự cố gây mất an toàn thông tin trong đơn vị của mình quản lý.

- Tăng cường kỷ luật, kỷ cương hành chính, đổi mới phương thức, lề lối làm việc, kiên quyết xử lý theo quy định những tổ chức đảng, đảng viên, CCVC có hành vi vi phạm quy chế, quy định của Ngành về an toàn thông tin mạng, làm lộ lọt, mất tài khoản, dữ liệu…; Biểu dương, khen thưởng các tập thể, cá nhân có thành tích xuất sắc trong thực hiện công tác bảo đảm an toàn thông tin mạng.

- Tăng cường công tác quán triệt kịp thời, liên tục, nâng cao nhận thức, ý thức trách nhiệm của mỗi đảng viên, CCVC để nhận thức đầy đủ vị trí, vai trò và tầm quan trọng của công tác bảo đảm an toàn thông tin mạng, đặc biệt là ý thức trách nhiệm bảo vệ tài khoản nghiệp vụ của CCVC trong toàn Ngành.

3. Quy hoạch, xây dựng các "hàng rào kỹ thuật" theo lộ trình phù hợp, song song với việc hoàn thiện phần mềm nghiệp vụ

- Thường xuyên rà soát, điều chỉnh, bổ sung, hoàn thiện các quy định, quy chế về an toàn thông tin mạng của ngành BHXH Việt Nam; các quy trình nghiệp vụ gắn với việc phân cấp, phân quyền trên phần mềm nghiệp vụ bảo đảm rõ người, rõ việc, rõ trách nhiệm.

- Xây dựng các tiêu chuẩn, quy chuẩn kỹ thuật, quy hoạch chính sách an toàn thông tin mạng trong hoạt động ứng dụng CNTT phù hợp với tình hình an toàn thông tin mạng trong từng giai đoạn.

- Tăng cường công tác đôn đốc, kiểm tra, hướng dẫn các đơn vị trực thuộc trong công tác triển khai các giải pháp kỹ thuật an toàn thông tin mạng bảo đảm hạn chế tối đa các hành vi vi phạm; giám sát và ngăn chặn kịp thời các hành vi vi phạm chính sách an toàn thông tin mạng; khoanh vùng, cô lập, khống chế các vi phạm an toàn thông tin mạng trong phạm vi hẹp để giảm thiểu thiệt hại về tài sản thông tin, dữ liệu; đánh giá, tháo gỡ khó khăn, vướng mắc trong việc thực hiện công tác bảo đảm an toàn thông tin mạng.

- Tiếp tục rà soát, đánh giá và phê duyệt hồ sơ đề xuất cấp độ và phương án bảo đảm an toàn thông tin cho các hệ thống thông tin của BHXH Việt Nam.

4. Xây dựng nguồn nhân lực

- Nghiên cứu, đánh giá kiện toàn về mô hình, bộ máy tổ chức, nhân sự phù hợp với yêu cầu chuyển đổi số nói chung và thực hiện công tác bảo đảm an toàn thông tin mạng trong ngành BHXH Việt Nam nói riêng. Rà soát việc thực hiện cơ cấu lại Phòng CNTT về Văn phòng BHXH cấp tỉnh của 56 đơn vị BHXH cấp tỉnh, bảo đảm nguồn nhân lực làm CNTT, an toàn thông tin mạng theo đúng hướng dẫn của BHXH Việt Nam về bàn giao nhiệm vụ của Phòng CNTT và Văn phòng BHXH cấp tỉnh.

- Kiện toàn và đẩy mạnh hoạt động của Đội ứng cứu sự cố, CCVC chuyên trách an toàn thông tin mạng của BHXH các tỉnh là lực lượng nòng cốt trong việc triển khai thực hiện nhiệm vụ bảo đảm an toàn thông tin mạng tại các đơn vị.

5. Trang bị hạ tầng kỹ thuật

- Trang bị hạ tầng kỹ thuật mới, hiện đại, có khả năng ngăn chặn tấn công bảo đảm an toàn dữ liệu, an toàn thông tin mạng.

- Duy trì chế độ bảo hành cho các hệ thống hạ tầng kỹ thuật an toàn thông tin mạng bảo đảm luôn hoạt động ổn định và có sự hỗ trợ kỹ thuật từ các đơn vị cung cấp sản phẩm nhằm tối ưu hóa các tính năng của thiết bị. Đẩy nhanh triển khai các nhiệm vụ/dự án đã được xây dựng.

6. Phối hợp với các cơ quan liên quan

- Tăng cường công tác phối hợp với các đơn vị chức năng về an ninh mạng của Bộ Công an, Bộ Quốc phòng, Bộ Thông tin – Truyền thông, Ban Cơ yếu Chính phủ nhằm thực hiện giám sát các hệ thống thông tin của Ngành; kịp thời phát hiện và xử lý sự cố, lỗ hổng, ngăn chặn, bóc gỡ mã độc tấn công vào hệ thống mạng; áp dụng các giải pháp quản lý và kỹ thuật bảo đảm an toàn thông tin mạng phù hợp.

- Tăng cường hợp tác quốc tế trong đào tạo, nghiên cứu và ứng dụng khoa học, kỹ thuật, công nghệ về an toàn thông tin mạng.

V. TỔ CHỨC THỰC HIỆN

1. Ban Cán sự đảng BHXH Việt Nam phối hợp với Ban Thường vụ Đảng ủy cơ quan BHXH Việt Nam lãnh đạo, chỉ đạo toàn Ngành thực hiện Nghị quyết này.

2. Ban Chỉ đạo chuyển đổi số ngành BHXH Việt Nam chỉ đạo, đôn đốc, kiểm tra, giám sát, đánh giá kết quả công tác bảo đảm an toàn, an ninh mạng trong toàn Ngành, thường xuyên hoặc đột xuất báo cáo Ban Thường vụ Đảng ủy cơ quan và Ban Cán sự đảng BHXH Việt Nam.

3. Cấp ủy đảng Trung tâm Truyền thông phối hợp với các đơn vị chức năng tăng cường công tác tuyên truyền, phổ biến ý nghĩa, vai trò của Nghị quyết này.

4. Cấp ủy đảng Vụ Thanh tra - Kiểm tra, Vụ Tổ chức cán bộ tăng cường kiểm tra thực thi công vụ, xử lý nghiêm các tổ chức, cá nhân vi phạm quy định bảo đảm an toàn thông tin mạng.

5. Cấp ủy đảng các đơn vị trực thuộc BHXH Việt Nam phối hợp cấp ủy đảng Vụ Pháp chế tổ chức rà soát, điều chỉnh, bổ sung, hoàn thiện các quy định, quy chế về an toàn thông tin mạng của ngành BHXH Việt Nam; các quy trình nghiệp vụ gắn với việc phân cấp, phân quyền trên phần mềm nghiệp vụ.

6. Cấp ủy đảng Trung tâm CNTT lãnh đạo, chỉ đạo đơn vị cụ thể nội dung Nghị quyết thành các kế hoạch chi tiết để tham mưu, đề xuất và tổ chức thực hiện.

7. Cấp ủy đảng, Thủ trưởng các đơn vị trực thuộc BHXH Việt Nam và BHXH các tỉnh tổ chức học tập, quán triệt, chủ động xây dựng kế hoạch, chương trình hành động để thực hiện có hiệu quả Nghị quyết./.

TM. BAN CÁN SỰ ĐẢNG
BÍ THƯ

ĐẢNG CỘNG SẢN VIỆT NAM
BAN CÁN SỰ ĐẢNG BẢO HIỂM XÃ HỘI VIỆT NAM
BAN CHẤP HÀNH TRUNG ƯƠNG

Nguyễn Thế Mạnh

Nơi nhận:
- Ban Bí thư Trung ương Đảng (để b/c),
- Ban Cán sự Đảng Chính phủ (để b/c),
- Ban Cán sự Đảng Văn phòng Chính phủ,
- Ban Cán sự Đảng Bộ Công an,
- Bộ Thông tin và Truyền thông,
- Đ/c PBT và các đ/c Ủy viên BCSĐ,
- BTV Đảng ủy CQ BHXH Việt Nam (để p/h),
- Cấp ủy đảng và Thủ trưởng các đơn vị trực thuộc BHXH Việt Nam (để t/h),
- Cấp ủy đảng và Giám đốc BHXH các tỉnh, TP trực thuộc TW (để t/h),
- Cấp ủy đảng và Giám đốc BHXH Bộ Quốc phòng, Công an nhân dân (để phối hợp t/h),
- Lưu: VPBCSĐ, CNTT.