|  |  |
| --- | --- |
| **ỦY BAN NHÂN DÂN TỈNH THANH HÓA** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc** |
| Số: 13/CT-UBND | *Thanh Hóa, ngày 04 tháng 11 năm 2022* |

**CHỈ THỊ**

**Về việc đẩy mạnh bảo đảm an toàn thông tin mạng và triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh Thanh Hóa**

Trong thời gian qua, tỉnh Thanh Hóa đã triển khai đẩy mạnh ứng dụng công nghệ thông tin xây dựng chính quyền điện tử, đô thị thông minh tiến tới xây dựng chính quyền số, kinh tế số, xã hội số gắn với bảo đảm an toàn thông tin (ATTT) mạng. UBND tỉnh đã ban hành nhiều văn bản chỉ đạo; các cơ quan chuyên môn đã hướng dẫn, triển khai nhiều biện pháp, giải pháp kỹ thuật; các cấp, các ngành đã từng bước quan tâm triển khai thực hiện, bước đầu đã đem lại sự chuyển biến tích cực trong công tác bảo đảm ATTT mạng. Tuy nhiên, trong thực tế vẫn còn một số cơ quan, tổ chức, cá nhân chưa nhận thức đầy đủ về công tác bảo đảm ATTT mạng, ứng cứu sự cố ATTT mạng, còn coi nhẹ nhiệm vụ bảo đảm ATTT mạng trong công tác quản lý, điều hành dẫn đến một số hệ thống thông tin không đảm bảo an toàn, an ninh mạng và đã bị xâm nhập, mất an toàn hệ thống.

Để tăng cường công tác bảo đảm ATTT mạng, khả năng phòng, chống các nguy cơ tấn công mạng, bao gồm cả việc ứng cứu sự cố nhằm phục hồi, giảm thiểu thiệt hại, đưa các hệ thống thông tin trở lại hoạt động bình thường trong thời gian sớm nhất khi gặp sự cố tấn công mạng, Chủ tịch UBND tỉnh yêu cầu:

**1.** Giám đốc các Sở, Trưởng các ban, ngành cấp tỉnh, Chủ tịch UBND các huyện, thị xã, thành phố theo chức năng nhiệm vụ được giao, nghiêm túc triển khai và thực hiện tốt công tác bảo đảm ATTT mạng theo chỉ đạo tại Chỉ thị số 41-CT/TW ngày 24/3/2020 của Ban Bí thư Trung ương Đảng về tăng cường phối hợp và triển khai đồng bộ các biện pháp bảo đảm an toàn, an ninh mạng; Chỉ thị số 14/CT-TTg ngày 07/6/2019 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; Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ về đẩy mạnh triển khai các hoạt động ứng cứu sự cố ATTT mạng Việt Nam và các văn bản chỉ đạo, hướng dẫn của Bộ Thông tin và Truyền thông, của Chủ tịch UBND tỉnh liên quan đến công tác ATTT mạng và ứng cứu sự cố ATTT mạng trong cơ quan, tổ chức thuộc phạm vi quản lý. Trong đó, cần chú trọng một số nội dung sau:

a) Quán triệt tới tất cả các tổ chức, cá nhân thuộc phạm vi quản lý nguyên tắc “Ứng cứu sự cố ATTT mạng là hoạt động quan trọng nhằm phát hiện, ngăn chặn, xử lý và khắc phục kịp thời sự cố ATTT mạng” và “Hệ thống thông tin được kiểm tra, đánh giá ATTT mạng trước khi đưa vào sử dụng”. Thủ trưởng các cơ quan, đơn vị, địa phương trực tiếp chịu trách nhiệm trước Chủ tịch UBND tỉnh nếu để xảy ra sự cố mất ATTT mạng, để xảy ra hậu quả, thiệt hại nghiêm trọng tại cơ quan, đơn vị thuộc phạm vi quản lý.

b) Tổ chức triển khai bảo đảm ATTT mạng đầy đủ theo mô hình 4 lớp tại các cơ quan, đơn vị, địa phương trực thuộc. Xây dựng Hồ sơ đề xuất cấp độ và trình các cấp có thẩm quyền thẩm định và phê duyệt cấp độ an toàn hệ thống thông tin đối với 100% hệ thống thông tin thuộc thẩm quyền quản lý theo quy định; hoàn thành trước ngày 01/12/2022. Bảo đảm các hệ thống thông tin được triển khai đầy đủ phương án bảo đảm an toàn hệ thống thông tin theo cấp độ trước ngày 01/6/2023.

c) Hoạt động ứng cứu sự cố ATTT mạng phải chuyển từ bị động sang chủ động, bao gồm: Chủ động thực hiện săn lùng mối nguy hại và rà quét lỗ hổng trên các hệ thống thông tin trong phạm vi quản lý tối thiểu 01 lần/6 tháng; rà soát, ban hành phương án, kịch bản ứng cứu sự cố cho hệ thống thông tin trước ngày 31/12/2022 và cập nhật kịp thời khi có thay đổi; tổ chức diễn tập thực chiến tối thiểu 01 lần/năm đối với hệ thống thông tin cấp độ 3 trở lên nhằm đánh giá khả năng phòng ngừa xâm nhập và khả năng phát hiện kịp thời các điểm yếu về quy trình, công nghệ, con người. Trường hợp phát hiện điểm yếu, lỗ hổng bảo mật cho phép xâm nhập và kiểm soát hệ thống thì thực hiện đồng thời khắc phục điểm yếu, lỗ hổng và săn lùng mối nguy hại.

d) Tổ chức, kiện toàn lại các Tổ ứng cứu sự cố ATTT mạng của các cơ quan, đơn vị trước ngày 31/12/2022 theo hướng chuyên nghiệp, cơ động, khuyến khích có tối thiểu 01 chuyên gia ATTT mạng (bao gồm cả chuyên gia thuê ngoài) đáp ứng chuẩn kỹ năng về ATTT do Bộ Thông tin và Truyền thông quy định. Thường xuyên rà soát, cử cán bộ đầu mối (phụ trách/kiêm nhiệm) chịu trách nhiệm về ATTT mạng tại cơ quan, đơn vị, phối hợp chặt chẽ với Sở Thông tin và Truyền thông, Đội ứng cứu sự cố ATTT mạng của tỉnh trong công tác đảm bảo ATTT mạng cho các hệ thống thông tin trên địa bàn tỉnh.

đ) Không lưu trữ cơ sở dữ liệu, tài liệu có chứa thông tin thuộc phạm vi **bí mật nhà nước** trên máy tính có kết nối mạng Internet, mạng nội bộ. Kiểm tra an toàn, an ninh thông tin đối với các thiết bị điện tử, giải pháp công nghệ trước khi đưa vào sử dụng tại các bộ phận trọng yếu, cơ mật; loại bỏ triệt để thông tin, tài liệu khi chuyển đổi mục đích sử dụng các thiết bị đã lưu dữ liệu, tài liệu có chứa thông tin thuộc phạm vi bí mật nhà nước. Kiểm soát việc sửa chữa, thay thế trang thiết bị máy tính trong cơ quan, đơn vị nhằm hạn chế việc lộ, mất thông tin, dữ liệu.

e) Chỉ kết nối đến các hệ thống thông tin, ứng dụng dùng chung của tỉnh tại các cơ quan, đơn vị thông qua mạng Truyền số liệu chuyên dùng của tỉnh. Đối với các phần mềm dùng chung, phần mềm chuyên ngành cán bộ, công chức, viên chức, người lao động được cấp tài khoản riêng, yêu cầu thường xuyên thay đổi mật khẩu truy cập. Khi trao đổi thông tin phục vụ công việc nhà nước, yêu cầu sử dụng hệ thống thư điện tử công vụ dùng chung của tỉnh, của ngành, không sử dụng thư điện tử thương mại, thư điện tử công cộng.

g) Thường xuyên rà soát, thực hiện nâng cấp, chuẩn hóa hạ tầng kỹ thuật công nghệ thông tin, an toàn, an ninh mạng. Nghiêm túc thực hiện khắc phục kịp thời các lỗ hổng, điểm yếu theo cảnh báo của cơ quan chức năng; chủ động theo dõi, phát hiện sớm các nguy cơ mất ATTT mạng để kịp thời xử lý, khắc phục. Có biện pháp kiểm soát nguy cơ mất ATTT mạng gây ra bởi bên thứ ba và các chuỗi cung ứng công nghệ thông tin và truyền thông.

h) Nghiêm túc thực hiện các quy định về báo cáo sự cố ATTT mạng; đẩy mạnh tuyên truyền cho người dân về việc báo cáo, cung cấp thông tin sự cố. Khuyến khích triển khai các chiến dịch nâng cao ý thức cảnh giác của người dùng cuối đối với các cuộc tấn công mạng.

i) Công bố thông tin đầu mối Tổ ứng cứu sự cố ATTT mạng (số điện thoại, thư điện tử hoặc các kênh liên lạc khác) tiếp nhận thông báo sự cố trên trang thông tin điện tử của cơ quan, đơn vị, địa phương trước ngày 31/12/2022.

k) Xây dựng kế hoạch thực hiện các yêu cầu, nhiệm vụ tại Chỉ thị này, hoàn thành trước ngày 30/11/2022 gửi về Sở Thông tin và Truyền thông để tổng hợp, báo cáo UBND tỉnh; trước ngày 12/12 hàng năm (hoặc đột xuất) báo cáo UBND tỉnh (qua Sở Thông tin và Truyền thông) kết quả thực hiện Chỉ thị này.

**2.** Sở Thông tin và Truyền thông

a) Chủ trì, phối hợp với các cơ quan có liên quan xây dựng và tổ chức các hoạt động tuyên truyền, đào tạo, tập huấn nâng cao nhận thức cho cán bộ, công chức của các cơ quan nhà nước, các tổ chức, doanh nghiệp và người dân về ATTT mạng và ý thức cảnh giác đối với các cuộc tấn công mạng; tổ chức diễn tập thực chiến cấp tỉnh tối thiểu 01 cuộc/năm về bảo đảm ATTT mạng, ứng cứu sự cố trong hoạt động của cơ quan nhà nước.

b) Tham mưu, đề xuất Chủ tịch UBND tỉnh cử cán bộ, công chức, viên chức là thành viên trong Đội/Tổ ứng cứu sự cố của các cơ quan, đơn vị, địa phương tham gia các chương trình đào tạo, tập huấn và dự thi lấy chứng chỉ có uy tín về công nghệ thông tin, quản trị mạng và an toàn, an ninh mạng.

c) Tổ chức triển khai các giải pháp bảo đảm ATTT mạng cấp tỉnh và điều phối, tổ chức xử lý các nguy cơ, ứng cứu sự cố mất ATTT mạng trong hệ thống cơ quan nhà nước trên địa bàn tỉnh; thực hiện giám sát an toàn, an ninh mạng tập trung trên toàn tỉnh thông qua Trung tâm điều hành an toàn, an ninh mạng (SOC) tỉnh Thanh Hóa. Thiết lập kênh thông tin về ATTT mạng và ứng cứu sự cố trên địa bàn tỉnh Thanh Hóa.

d) Tham mưu tổ chức, kiện toàn lại Đội ứng cứu sự cố ATTT mạng của tỉnh trước ngày 31/12/2022 theo hướng chuyên nghiệp, cơ động, có tối thiểu 05 chuyên gia ATTT mạng (bao gồm cả chuyên gia thuê ngoài) đáp ứng chuẩn kỹ năng về ATTT do Bộ Thông tin và Truyền thông quy định. Công bố số điện thoại đường dây nóng 24/24 giờ để tiếp nhận thông tin báo cáo sự cố và hướng dẫn kịp thời cách phòng, ngừa, xử lý.

đ) Chủ trì, phối hợp với các cơ quan có liên quan tham mưu, đề xuất UBND tỉnh đầu tư trang bị các thiết bị, phần mềm bảo mật chuyên dùng làm phương tiện, công cụ nâng cao năng lực bảo đảm ATTT mạng trong hoạt động của các cơ quan nhà nước và Đội ứng cứu sự cố ATTT mạng của tỉnh.

e) Chủ trì tổ chức kiểm tra, đánh giá mức độ bảo đảm ATTT mạng và ứng cứu sự cố định kỳ hoặc đột xuất đối với các hệ thống thông tin của các cơ quan, đơn vị trên địa bàn tỉnh. Định kỳ hàng tháng đánh giá, xếp loại mức độ triển khai công tác bảo đảm ATTT mạng đối với các cơ quan, đơn vị trên địa bàn tỉnh.

g) Chủ trì tổ chức triển khai, hướng dẫn, theo dõi, đôn đốc, kiểm tra và đánh giá việc thực hiện Chỉ thị này; tổng hợp, báo cáo Chủ tịch UBND tỉnh kết quả thực hiện.

h) Chủ trì, phối hợp với Sở Tài chính và các đơn vị liên quan tham mưu, trình Chủ tịch UBND tỉnh bố trí nguồn kinh phí đảm bảo cho các hoạt động ATTT, ứng cứu sự cố tại các cơ quan nhà nước và Đội ứng cứu sự cố ATTT của tỉnh.

**3.** Công an tỉnh, Bộ Chỉ huy quân sự tỉnh

a) Triển khai các hoạt động bảo đảm an toàn, an ninh mạng và ứng cứu sự cố theo chức năng, nhiệm vụ được giao và chỉ đạo của Bộ Công an, Bộ Quốc phòng.

b) Phối hợp với Sở Thông tin và Truyền thông trong hoạt động bảo đảm an toàn ATTT mạng và ứng cứu sự cố ATTT mạng.

**4.** Sở Tài chính

Phối hợp với Sở Thông tin và Truyền thông đề xuất báo cáo Chủ tịch UBND tỉnh bố trí nguồn kinh phí triển khai các nhiệm vụ trong Chỉ thị; hướng dẫn các cơ quan, đơn vị và địa phương quản lý, sử dụng kinh phí được giao theo quy định.

**5.** Đài Phát thành và Truyền hình tỉnh, Báo Thanh Hóa chủ trì, phối hợp với Sở Thông tin và Truyền thông xây dựng các chương trình, kế hoạch để đẩy mạnh các hoạt động tuyên truyền, nâng cao nhận thức về công tác bảo đảm ATTT mạng và ứng cưu sự cố trên các phương tiện thông tin đại chúng.

**6.** Các doanh nghiệp cung cấp dịch vụ viễn thông, công nghệ thông tin

a) Có trách nhiệm chủ động phối hợp với Sở Thông tin và Truyền thông và các đơn vị liên quan trong công tác bảo đảm ATTT mạng, ứng cứu sự cố đối với hạ tầng viễn thông, Internet; công bố thông tin đầu mối (số điện thoại, thư điện tử hoặc các kênh liên lạc khác) tiếp nhận thông báo sự cố trên cổng/trang thông tin điện tử trước ngày 31/12/2022; tuyên truyền cho khách hàng về cách thức phản ánh sự cố mất ATTT mạng.

b) Nghiêm túc tuân thủ các yêu cầu điều phối từ Sở Thông tin và Truyền thông, Đội ứng cứu sự cố ATTT mạng của tỉnh trong các hoạt động ứng cứu, xử lý sự cố.

c) Cảnh báo cho khách hàng các nguy cơ, sự cố ATTT mạng trên diện rộng hoặc khi phát hiện nguy cơ, sự cố ATTT mạng liên quan tới khách hàng; hỗ trợ khách hàng ứng cứu, xử lý sự cố ATTT mạng liên quan tới dịch vụ do doanh nghiệp cung cấp.

Định kỳ hàng tháng, Sở Thông tin và Truyền thông tổng hợp, báo cáo Chủ tịch UBND tỉnh tình hình ATTT mạng trên địa bàn tỉnh (báo cáo trước ngày 05 của tháng tiếp theo).

Giám đốc các Sở, Trưởng các ban, ngành cấp tỉnh; Chủ tịch UBND các huyện, thị xã, thành phố và Thủ trưởng các cơ quan, đơn vị, các tổ chức, cá nhân liên quan có trách nhiệm thi hành nghiêm Chỉ thị này./.

|  |  |
| --- | --- |
|  | **KT. CHỦ TỊCH**  **PHÓ CHỦ TỊCH**  **Mai Xuân Liêm** |