

UBND TỈNH ĐẮK NÔNG  
TIỂU BAN AN TOÀN,  
AN NINH MẠNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM  
Độc lập - Tự do - Hạnh phúc

Số: ~~5597~~ /UBND-TBATANM

Đắk Nông, ngày ~~17~~ tháng 9 năm 2024

V/v tăng cường công tác bảo đảm an ninh mạng và phòng, chống tấn công mạng

Kính gửi:

- Các Sở, Ban, ngành, đoàn thể;
- UBND các huyện, thành phố.

Thời gian qua, tình hình an ninh mạng và tấn công mạng trong nước diễn ra hết sức phức tạp, nguy hiểm trong khi hệ thống thông tin của các ban, bộ ngành, địa phương, doanh nghiệp còn bộc lộ nhiều điểm yếu có nguy cơ gây mất an ninh mạng, chỉ một cuộc tấn công nhỏ lẻ có thể lan rộng, xâm nhập toàn bộ hệ thống thông tin trọng yếu quốc gia. Trong 6 tháng đầu năm 2024, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao đã phát hiện, xử lý **211.000** cảnh báo tấn công mạng và **20** sự cố an ninh mạng, đặc biệt trong bối cảnh các bộ ngành, địa phương, doanh nghiệp đẩy mạnh quá trình chuyển đổi số, xây dựng nhiều hệ thống thông tin quan trọng, mang tính liên kết sâu rộng càng làm cho hoạt động tấn công mạng, gián điệp mạng phức tạp, nguy hiểm hơn. Nổi lên thời gian qua là hoạt động tấn công mã hoá dữ liệu, đòi tiền chuộc nhằm vào các tập đoàn, doanh nghiệp tài chính, năng lượng, viễn thông “mũi nhọn” gây ngưng trệ hoạt động quản lý, điều hành, thiệt hại lớn về kinh tế, uy tín của doanh nghiệp; hệ thống thông tin của một số cơ quan Trung ương, bộ, ngành, địa phương còn bị các nhóm tin tặc tấn công chiếm quyền quản trị, thay đổi giao diện, lây nhiễm mã độc gián điệp; hoạt động trao đổi, mua bán trái phép thông tin, dữ liệu cá nhân diễn ra công khai trên một số diễn đàn, hội nhóm, các đối tượng tổ chức thành đường dây quy mô lớn, hoạt động chuyên nghiệp, với hàng nghìn thành viên tham gia.

Nguyên nhân của tình trạng trên xuất phát từ nhận thức về vai trò, tầm quan trọng của công tác bảo đảm an toàn, an ninh mạng, bảo vệ dữ liệu cá nhân còn tồn tại hạn chế; khả năng ứng cứu, xử lý, khắc phục sự cố trước các cuộc tấn công mạng còn thấp, nhiều hệ thống công nghệ thông tin quan trọng đầu tư không đồng bộ, không được giám sát, kiểm tra, đánh giá định kỳ, thường xuyên, tồn tại điểm yếu kỹ thuật, lỗ hổng bảo mật; việc chấp hành quy trình, quy định về bảo đảm an ninh mạng, bảo vệ dữ liệu cá nhân chưa nghiêm, không đầy đủ; việc quan tâm đầu tư về nguồn lực phục vụ công tác bảo đảm an ninh hệ thống mạng còn hạn chế, chưa đáp ứng yêu cầu...



Để khắc phục khó khăn, hạn chế, tăng cường công tác phòng, chống tấn công mạng, bảo vệ dữ liệu cá nhân, Tiểu ban An toàn, An ninh mạng tỉnh Đắk Nông đề nghị các Sở, Ban, ngành, địa phương; các tổ chức chính trị, xã hội; các tổ chức, doanh nghiệp trên địa bàn tỉnh khẩn trương triển khai thực hiện một số nội dung sau đây:

1. Tiếp tục quán triệt, thực hiện nghiêm Luật An ninh mạng năm 2018, Nghị định số 53/2020/NĐ-CP ngày 15/8/2022 của Chính phủ quy định chi tiết một số điều Luật An ninh mạng, Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về bảo vệ dữ liệu cá nhân, Hướng dẫn các biện pháp tăng cường bảo đảm an ninh mạng cho hệ thống thông tin quan trọng về an ninh quốc gia... Cụ thể hoá trách nhiệm của đơn vị, tổ chức, cá nhân trong công tác bảo vệ an ninh mạng hệ thống thông tin trọng yếu, bảo vệ dữ liệu cá nhân; định kỳ, đột xuất kiểm tra, giám sát thực hiện các quy định về bảo vệ an ninh mạng, bảo vệ hệ thống thông tin trọng yếu, bảo vệ dữ liệu cá nhân, xử lý nghiêm theo quy định các vụ việc gây mất an ninh mạng, lộ mất bí mật nhà nước, vi phạm dữ liệu cá nhân trên không gian mạng.

2. Tổ chức tuyên truyền, phổ biến trong toàn hệ thống chính trị, các cơ quan, đơn vị nâng cao nhận thức, trách nhiệm đối với công tác bảo đảm an ninh mạng, an toàn hệ thống mạng, bảo vệ bí mật nhà nước, thông tin dữ liệu cá nhân trên không gian mạng; thường xuyên cập nhật, thực hiện nghiêm các thông báo, cảnh báo của cơ quan chuyên trách về các loại hình tấn công mạng, tội phạm mạng, tội phạm sử dụng công nghệ cao, nguy cơ mất an ninh mạng, xâm phạm dữ liệu cá nhân.

3. Tiến hành rà soát, xây dựng, hoàn thiện các quy định, quy trình, quy chế, hướng dẫn bảo vệ an ninh mạng, đồng thời thường xuyên kiểm tra, giám sát, đảm bảo việc chấp hành, thực hiện nghiêm túc trong toàn đơn vị. Chủ quản các hệ thống thông tin chủ động xây dựng, triển khai phương án, tổ chức diễn tập phòng, chống tấn công mạng và ứng phó, khắc phục sự cố an ninh mạng theo quy định; thiết lập các kênh thông tin trao đổi, chia sẻ thông tin, thông báo ngay sự cố an ninh mạng với các lực lượng chuyên trách bảo vệ an ninh mạng.

4. Tăng cường đầu tư về công nghệ, hệ thống kỹ thuật đảm bảo các quy chuẩn, tiêu chuẩn theo quy định, tránh tình trạng tập trung chuyển đổi số mà thiếu sự quan tâm đến công tác bảo đảm an toàn, an ninh mạng; ưu tiên sử dụng sản phẩm, thiết bị mạng được kiểm tra, đánh giá đảm bảo an ninh mạng. Chủ quản hệ thống thông tin trọng yếu khẩn trương kết nối với các hệ thống giám sát của Trung tâm An ninh mạng quốc gia đặt tại Bộ Công an để kịp thời phát hiện, cảnh báo, giám sát, khắc phục các sự cố, tình huống nguy cấp mất an ninh mạng.

5. Tập trung đầu tư, phân bổ kinh phí, bố trí nhân lực bảo vệ an ninh mạng; thường xuyên tổ chức tập huấn, bồi dưỡng, nâng cao kiến thức, kỹ năng

cho cán bộ, đảng viên, đội ngũ chuyên trách công nghệ thông tin, an ninh mạng tại các cơ quan, đơn vị đáp ứng năng lực, yêu cầu bảo vệ an ninh mạng và bí mật nhà nước trên không gian mạng.

6. Bộ phận An toàn, An ninh mạng chủ trì, phối hợp với Công an các huyện, thành phố tăng cường công tác tuyên truyền, quản lý, nâng cao năng lực ứng phó tấn công mạng, bảo vệ dữ liệu cá nhân của các tổ chức, doanh nghiệp trên địa bàn.

Quá trình tổ chức thực hiện, nếu có khó khăn, vướng mắc, các Sở, Ban, ngành, UBND các huyện, thành phố gửi về Công an tỉnh (qua Phòng PA05) để tổng hợp. Tiểu ban An toàn, An ninh mạng tỉnh Đắk Nông thông báo để các Sở, Ban, ngành, đơn vị, địa phương biết, tổ chức thực hiện./.

**Nơi nhận:**

- Như trên;
- Văn phòng Ban Chỉ đạo ATANMQG;
- CT, các PCT UBND tỉnh;
- Công an tỉnh;
- CVP, các PCVP UBND tỉnh;
- Lưu: VT, NC (Ln).

02

**TRƯỞNG TIỂU BAN**



**CHỦ TỊCH UBND TỈNH**  
**Hồ Văn Mười**

