UBND TỈNH LAI CHÂU
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số:18 /STTTT-BCVTCNTT
V/v Tăng cường công tác bảo đảm an toàn thông tin mạng trong dịp Tết Nguyên đán Giáp Thìn 2024.

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

Lai Châu, ngày 03 tháng 01 năm 2023

Kính gửi:
- Các Sở, ban, ngành tỉnh;
- UBND các huyện, thành phố;
- Cac doanh nghiệp Bưu chính, Viễn thông.

Sự cố mất an toàn thông tin mạng nghiêm trọng tại Việt Nam thường được ghi nhận tại thời điểm diễn ra dịp nghỉ lễ của đất nước. Qua công tác theo dõi, giám sát, Sở Thông tin và Truyền thông thấy rằng các đối tượng thường tăng cường tấn công mạng vào các hệ thống thông tin quan trọng hoặc lợi dụng không gian mạng để phát tán thông tin xấu độc, lừa đảo trong các dịp này.

Nhằm nâng cao cảnh giác và trách nhiệm bảo đảm an toàn thông tin mạng theo quy định của pháp luật trong thời gian diễn ra dịp nghỉ lễ Tết Nguyên đán Giáp Thìn, Sở Thông tin và Truyền thông kính đề nghị các cơ quan, tổ chức, doanh nghiệp triển khai một số biện pháp đảm bảo an toàn thông tin, như sau:

1. Đối với các Sở, ban, ngành, UBND các huyện, thành phố:

a) Rà soát các hệ thống thông tin, bảo đảm các hệ thống thông tin được triển khai đầy đủ các biện pháp bảo vệ theo cấp độ an toàn.

b) Phân công lực lượng tại chỗ triển khai trực giám sát 24/7; Chủ động theo dõi thường xuyên, liên tục các hệ thống giám sát an toàn thông tin tập trung, hệ thống phòng, chống mã độc tập trung đảm bảo xử lý, khắc phục kịp thời tấn công mạng, cảnh báo mã độc được xác minh.

c) Rà soát, kiểm tra và bóc gỡ các phần mềm độc hại cho toàn bộ máy chủ, máy trạm trong hệ thống mạng. Trong đó, cần ưu tiên các hệ thông tin có địa chỉ IP nằm trong Danh sách IP mạng Botnet được Cục An toàn thông tin cảnh báo hàng tháng hoặc đột xuất.

d) Chủ động rà soát các lỗ hổng, điểm yếu trên các hệ thống thông tin thuộc phạm vi quản lý và triển khai các giải pháp phòng ngừa và khắc phục triệt để các lỗ hổng, điểm yếu đã được Cục An toàn thông tin cảnh báo, đặc biệt như: lỗ hổng ảnh hưởng nghiêm trọng trong F5 BIG-IP (văn bản số 1943/CATTT-NCSC ngày

01/11/2023 của Cục An toàn thông tin) và các lỗ hổng bảo mật ảnh hưởng mức cao và nghiêm trọng trong các sản phẩm Microsoft từ tháng 8 đến tháng 12 năm 2023 *(văn bản gửi kèm theo)*.

đ) Sử dụng và khai thác hiệu quả Nền tảng Điều phối xử lý sự cố an toàn thông tin mạng quốc gia (IRLab) và Nền tảng Hỗ trợ điều tra số (DFLab) trong công tác điều phối và xử lý sự cố tấn công mạng.

e) Bảo đảm duy trì kết nối liên tục tới hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia để được hỗ trợ giám sát, phát hiện và cảnh bảo sớm, xử lý; kịp thời chia sẻ thông tin với Cục An toàn thông tin, Sở Thông tin và Truyền thông khi phát hiện dấu hiệu tấn công mạng vào hệ thống thông tin.

g) Tổ chức tuyên truyền, nâng cao nhận thức cơ bản kỹ năng về an toàn thông tin mạng, cảnh giác về thông tin xấu độc, tin giả và thông tin lừa đảo trên không gian mạng cho cán bộ thuộc cơ quan.

2. Đối với các doanh nghiệp Bưu chính, viễn thông:

a) Các doanh nghiệp cung ứng dịch vụ bưu chính thực hiện đồng bộ giải pháp nhằm tăng cường công tác bảo đảm an toàn, an ninh trong quá trình cung ứng dịch vụ; tăng cường kiểm soát, ngăn chặn vận chuyển hàng lậu, hàng cấm qua đường bưu chính, kịp thời phối hợp với các cơ quan chức năng để xử lý theo quy định. Tổ chức rà soát, sắp xếp các bộ phận khoa học, hợp lý nhằm bảm đảm kịp thời lưu thoát thư, gói, kiện hàng hóa, không để xảy ra tình trạng thất lạc, ứ đọng, mất mát gây phát sinh khiếu nại của khách hàng, phục vụ tốt nhất nhu cầu của người dân trước, trong và sau Tết Nguyên đán.

b) Các doanh nghiệp viễn thông trên địa bàn tỉnh bảo đảm tuyệt đối an toàn mạng lưới, thông tin liên lạc thông suốt đáp ứng nhu cầu thông tin liên lạc của các cơ quan nhà nước, tổ chức, doanh nghiệp và người dân trong dịp Tết. Bảo đảm hoạt động ổn định, liên tục, an toàn hạ tầng kết nối Internet, các hệ thống đường truyền dữ liệu, thông tin của tỉnh kết nối với Trung ương. Tăng cường triển khai hoạt động bảo đảm an toàn thông tin mạng đối với các hệ thống thông tin quan trọng; theo dõi, giám sát, phát hiện xử lý sớm các nguy cơ mất an toàn thông tin mạng, dấu hiệu tấn công mạng, kịp thời xử lý các vấn đề phát sinh. Cử cán bộ kỹ thuật trực theo dõi, giám sát an toàn thông tin liên tục trong suốt kỳ nghỉ Tết.

c) Bảo đảm bố trí đầy đủ nguồn nhân lực để trực giám sát, hỗ trợ và khắc phục sự cố bảo đảm hạ tầng viễn thông, internet an toàn, thông suốt.

d) Triển khai đầy đủ các biện pháp bảo vệ, bảo đảm phát hiện và ngăn chặn kịp thời hoạt động tấn công mạng, phát tán thông tin xấu độc, thông tin vi phạm pháp luật trên hệ thống thông tin, hạ tầng mạng lưới thuộc phạm vi quản lý.

đ) Thực hiện nghiêm và kịp thời các biện pháp xử lý theo yêu cầu của Bộ Thông tin và Truyền thông (Cục An toàn thông tin), Sở Thông tin và Truyền thông và cơ quan chức năng có thẩm quyền.

3. Trong trường hợp cần hỗ trợ giám sát, xử lý, ứng cứu sự cố đề nghị liên hệ với Cục An toàn thông tin, Bộ Thông tin và Truyền thông thông qua các đầu mối:

- Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC), điện thoại 024.3640.4421 hoặc số điện thoại trực đường dây nóng ứng cứu sự cố 086.9100.317, thư điện tử: ir@vncert.vn.

- Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), điện thoại: 02432091616 hoặc số điện thoại trực đường dây nóng hỗ trợ giám sát, cảnh báo sớm 0389942878, thư điện tử: ais@mic.gov.vn.

- Sở Thông tin và Truyền thông, điện thoại: 02133798798, thư điện tử: sotttt@laichau.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Lưu: VT, BCVTCNTT.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH LAI CHÂU

Nguyễn Minh Hiệu