

Số: /BGTVT-TTCNTT

Hà Nội, ngày tháng năm 2024

V/v tăng cường bảo đảm an toàn thông tin, an ninh mạng cho các hệ thống thông tin

Kính gửi:

- Các cơ quan, đơn vị, doanh nghiệp trực thuộc Bộ;
- Công ty cổ phần Giao thông số Việt Nam;
- Công ty TNHH Thu phí tự động VETC.

Bộ Giao thông vận tải (GTVT) nhận được thông tin cảnh báo từ các cơ quan chức năng của Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và Truyền thông về chiến dịch tấn công mạng, đặc biệt là mã hóa tấn công tống tiền (ransomware) tại Việt Nam. Đối tượng chính mà tin tặc nhắm đến là các hệ thống thông tin trọng yếu của các cơ quan Đảng, Nhà nước và các tổ chức, doanh nghiệp lớn có giá trị dữ liệu cao, gây gián đoạn hoạt động và thiệt hại về vật chất, hình ảnh của các cơ quan, tổ chức, doanh nghiệp, cũng như hoạt động bảo đảm an toàn không gian mạng quốc gia. Theo dự báo của các chuyên gia an ninh mạng, trong thời gian tới, tình hình an toàn thông tin tiếp tục có diễn biến phức tạp, tin tặc tiếp tục tấn công vào hệ thống thông tin của các cơ quan, tổ chức, doanh nghiệp của Việt Nam, trong đó có ngành GTVT. Nguy cơ mất an toàn thông tin luôn hiện hữu.

Từ tình hình trên, để bảo đảm an toàn thông tin, an ninh mạng cho các hệ thống thông tin của ngành, Bộ GTVT yêu cầu Thủ trưởng các cơ quan, đơn vị trực tiếp chỉ đạo công tác bảo đảm an toàn thông tin mạng và chịu trách nhiệm trước Bộ trưởng nếu để xảy ra sự cố mất an toàn thông tin mạng tại đơn vị mình, trong đó tập trung thực hiện các nội dung sau:

- Tiếp tục quán triệt, tổ chức tuyên truyền nâng cao nhận thức và trách nhiệm bảo đảm an toàn thông tin, an ninh mạng đến tất cả cán bộ, công chức, viên chức và người lao động thuộc phạm vi quản lý của đơn vị.
- Tăng cường triển khai các biện pháp quản lý, kỹ thuật nhằm bảo đảm an toàn, an ninh mạng cho hệ thống thông tin; kịp thời cập nhật các bản vá, cấu hình tăng cường bảo mật cho hệ thống và triển khai các giải pháp phòng ngừa để tránh bị lợi dụng, khai thác để tấn công.
- Chủ động thực hiện rà soát các điểm yếu, lỗ hổng bảo mật trên hệ thống thông tin thuộc phạm vi quản lý, trong trường hợp phát hiện các nguy cơ, lỗ hổng, điểm yếu, cần lập tức triển khai các biện pháp khắc phục, đặc biệt là các hệ thống thông tin lưu trữ, xử lý thông tin, dữ liệu cá nhân.
- Thường xuyên tổ chức sao lưu hệ thống và dữ liệu quan trọng trên thiết bị lưu trữ dữ liệu, hệ thống máy chủ và máy tính cá nhân (đối với người dùng) để

kịp thời khôi phục khi bị tấn công mã hóa dữ liệu.

5. Tăng cường theo dõi, giám sát, chủ động phát hiện sớm các nguy cơ, dấu hiệu tấn công mạng, kịp thời xử lý các vấn đề phát sinh. Cử cán bộ kỹ thuật trực hệ thống và yêu cầu các đơn vị cung cấp dịch vụ an toàn thông tin mạng (nếu có) cam kết bố trí nguồn lực, nhân lực cho nhiệm vụ giám sát và bảo vệ các hệ thống thông tin.

Khi xảy ra sự cố hoặc cần hỗ trợ, liên hệ: ông Phùng Văn Trọng, Phó Giám đốc Trung tâm CNTT; điện thoại: 0983227688; e-mail: trongpv@mt.gov.vn.

Bộ GTVT yêu cầu các đơn vị khẩn trương, nghiêm túc triển khai thực hiện./.

Nơi nhận:

- Như trên;
- Các đồng chí Thứ trưởng;
- Lưu: VT, TTCNTT.

BỘ TRƯỞNG

Nguyễn Văn Thắng