

Số: /CHHVN-KHCNMT
V/v tăng cường công tác bảo đảm an toàn
thông tin, an ninh mạng.

Hà Nội, ngày tháng 8 năm 2024

Kính gửi:

- Văn phòng;
- Các đơn vị trực thuộc.

Trong thời gian qua, Cục Hàng hải Việt Nam nhận được nhiều thông tin cảnh báo về nguy cơ tấn công mạng liên quan tới các lỗ hổng bảo mật trong các sản phẩm của Microsoft, Foxit PDF Reader, Check Point, CrowdStrike (*các lỗ hổng bảo mật này cho phép đối tượng tấn công thực thi mã từ xa*); các cảnh báo về nhiều nhóm tấn công có chủ đích (APT) đang thực hiện tấn công vào Hệ thống thông tin của nhiều quốc gia trên thế giới, trong đó có Việt Nam; thông tin về việc nhiều máy tính bị mã nguồn độc tấn công; đặc biệt là báo cáo của Cảng vụ Hàng hải Hải Phòng về việc tên miền cấp 2 của Cảng vụ Hàng hải Hải Phòng bị tấn công (*tại công văn số 1757/CVHHHP-TCHC ngày 08/8/2024 gửi kèm theo*); ...

Để bảo đảm an toàn thông tin, an ninh mạng cho Hệ thống công nghệ thông tin của Cục Hàng hải Việt Nam và các đơn vị trực thuộc, Cục Hàng hải Việt Nam yêu cầu các đơn vị thực hiện các nội dung sau:

1. Chủ động tuyên truyền nâng cao nhận thức về bảo đảm an toàn thông tin, an ninh mạng cho công chức, viên chức và người lao động 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 phục vụ hoạt động nội bộ của đơn vị và các hệ thống cung cấp dịch vụ công trực tuyến. Tăng cường giám sát, quản lý các tài khoản quan trọng, tài khoản quản trị hệ thống nhằm phòng ngừa, giảm thiểu thiệt hại trong trường hợp kẻ tấn công chiếm được mật khẩu của tài khoản quản trị. Hạn chế truy cập vào các đường dẫn (*link*) lạ, các email không rõ địa chỉ mà không phục vụ mục đích giải quyết công việc của cơ quan, đơn vị; ...

Thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức về an toàn thông tin, an ninh mạng để phát hiện kịp thời các nguy cơ tấn công mạng; và thường xuyên truy cập Trang thông tin điện tử của Cục Hàng hải Việt Nam (*chuyên mục Chuyển đổi số tại website có địa chỉ <https://vinamarine.gov.vn/vi/chuyen-doi-so>*) để cập nhật các cảnh báo, hướng dẫn về an toàn thông tin, an ninh mạng.

2. Cài đặt, sử dụng các phần mềm (*trong đó có phần mềm diệt virus*) có bản quyền cho các thiết bị máy tính, máy chủ của đơn vị mình để phục vụ nhu cầu công việc.

Khi xảy ra sự cố hoặc cần hỗ trợ, đề nghị liên hệ với Trung tâm Công nghệ thông tin - Bộ Giao thông vận tải (*đồng chí Dương Đình Trung - số điện thoại 0985366388, email: trungdd@mt.gov.vn*) để được hỗ trợ xử lý.

3. Tổ chức thực hiện bảo trì các sản phẩm của dự án công nghệ thông tin theo quy định tại khoản 26, Điều 1 của Nghị định số 82/2024/NĐ-CP ngày 10/7/2024 của Chính phủ sửa đổi, bổ sung một số điều của Nghị định số 73/2019/NĐ-CP ngày 05 tháng 9 năm 2019 của Chính phủ quy định quản lý đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước.

Cục Hàng hải Việt Nam yêu cầu các đơn vị nghiêm túc triển khai thực hiện. Thủ trưởng các đơn vị chịu trách nhiệm trước Cục trưởng Cục Hàng hải Việt Nam nếu để xảy ra sự cố mất an toàn thông tin, an ninh mạng tại đơn vị mình./.

Nơi nhận:

- Như trên;
- Cục trưởng (*để b/c*);
- Công ty Vishipel;
- Lưu: VT, KHCNMT.

**KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG**

Nguyễn Hoàng