ỦY BAN NHÂN DÂN **THÀNH PHỐ HƯNG YÊN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 1290/UBND-VHTT V/v hướng dẫn một số giải pháp tăng cường bảo đảm an toàn hệ thống thông tin	*TP. Hưng Yên, ngày 08 tháng 7 năm 2024*

Kính gửi:
- Các phòng, ban, đơn vị của thành phố;
- Ủy ban nhân dân các phường, xã.

Căn cứ Công văn số 886/STTTT-BCVTCNTT ngày 01/7/2024 của Sở Thông tin và Truyền thông tỉnh Hưng Yên về việc hướng dẫn một số giải pháp tăng cường bảo đảm an toàn hệ thống thông tin. Theo thông báo của Sở Thông tin và Truyền thông. Từ đầu năm 2024 đến nay đã xảy ra một số sự cố an toàn thông tin mạng, đặc biệt là sự cố tấn công mã độc mã hóa tống tiền (ransomware), gây thiệt hại và làm gián đoạn dịch vụ trực tuyến của các cơ quan, tổ chức, doanh nghiệp. Nguyên nhân chủ yếu là do chưa tuân thủ và triển khai đầy đủ các quy định bảo đảm an toàn thông tin mạng.

Để đảm bảo an toàn thông tin cho hệ thống thông tin dùng chung của tỉnh và của cơ quan, đơn vị trên địa bàn thành phố, góp phần bảo đảm cho không gian mạng Việt Nam. UBND thành phố, yêu cầu các phòng chuyên môn; UBND các phường xã thực hiện theo hướng dẫn triển khai 06 giải pháp trọng tâm như sau:

1. Định kỳ thực hiện sao lưu dữ liệu ngoại tuyến "offline". Với chiến lược sao lưu dữ liệu theo nguyên tắc 3-2-1: có ít nhất 03 bản sao dữ liệu, trữ bản sao trên 02 phương tiện lưu trữ khác nhau, với 01 bản sao lưu ngoại tuyến "offline" (sử dụng tape/USB/ổ cứng di động,...). Dữ liệu sao lưu offline phải được tách biệt hoàn toàn, không kết nối mạng, cô lập để phòng chống tấn công leo thang vào hệ thống lưu trữ.

2. Triển khai giải pháp để sẵn sàng phục hồi nhanh hoạt động của hệ thống thông tin khi gặp sự cố, đưa hoạt động của hệ thống thông tin trở lại bình thường trong vòng 24 tiếng hoặc theo yêu cầu nghiệp vụ.

3. Triển khai các giải pháp, đặc biệt là giải pháp giám sát an toàn thông tin, để ngăn ngừa, kịp thời phát hiện sớm nguy cơ tấn công mạng đối với cả 3 giai đoạn: (1) xâm nhập vào hệ thống; (2) nằm gián điệp trong hệ thống; (3) khởi tạo quá trình phá hoại hệ thống.

4. Phân tách, kiểm soát truy cập giữa các vùng mạng và chuyển đổi, nâng cấp các ứng dụng, giao thức, kết nối lạc hậu, không còn được hỗ trợ kỹ thuật

sang phương án sử dụng các nền tảng, ứng dụng để giảm nhiều nguy cơ tấn công mạng leo thang.

5. Tăng cường giám sát, quản lý các tài khoản quan trọng, tài khoản quản trị để phòng ngừa, giảm thiểu thiệt hại trong trường hợp kẻ tấn công có được tài khoản quản trị.

6. Rà soát, khắc phục và không để xảy ra các lỗi cơ bản dẫn đến mất an toàn hệ thống thông tin.

(Hướng dẫn chi tiết tại Phụ lục kèm theo Công văn số 2517/BTTTT-CATTT)

Trong trường hợp cần hướng dẫn, hỗ trợ và điều phối xử lý, ứng cứu sự cố an toàn thông tin mạng, đề nghị liên hệ với Cục An toàn thông tin, Bộ Thông tin và Truyền thông qua các đầu mối:

- Trung tâm Ứng cứu khẩn cấp không gian mạng Việt nam (VNCERT/CC), Cục An toàn thông tin, Bộ Thông tin và Truyền thông, 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 thông gian mạng quốc gia (NCSC), Cục an toàn thông tin, Bộ Thông tin và Truyền thông, điện thoại: 024.3209.1616 hoặc số điện thoại trực đường dây nóng hỗ trợ giám sát, cảnh báo sớm 038.9924.878 thư điện tử: ais@mic.gov.vn.

- Phòng An toàn hệ thống thông tin, Cục An toàn thông tin, Bộ thông tin và Truyền thông, số điện thoại 0869.100.319, thư điện tử athttt@mic.gov.vn để hướng dẫn tổng thể việc triển khai.

Vậy, UBND thành phố yêu cầu các đơn vị nghiêm túc triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Sở Thông tin và Truyền thông tỉnh;
- Chủ tịch, các PCT UBND TP;
- Phòng Văn hóa-Thông tin TP;
- Văn phòng HĐND-UBND TP;
- Lưu: VT.

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

ỦY BAN NHÂN DÂN THÀNH PHỐ HƯNG YÊN
Thời gian ký: 08/07/2024 16:09:53

Bùi Tuấn Anh