UBND TỈNH ĐỒNG NAI
SỞ CÔNG THƯƠNG

Số: 7462 /SCT-VP
V/v thực hiện phòng, chống mã độc mã hóa dữ liệu Ramsomware.

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

Đồng Nai, ngày 14 tháng 12 năm 2023

Kính gửi: Các phòng, đơn vị thuộc Sở.

Sở Công Thương nhận được Công văn số 3702/STTTT-CĐS ngày 12/12/2023 của Sở Thông tin và Truyền thông về việc thực hiện phòng, chống mã độc mã hóa dữ liệu Ramsomware.

Căn cứ các Văn bản ngày 11/12/2023 của Sở Thông tin và Truyền thông gồm: số 3690/STTTT-CĐS về triển khai giải pháp đảm bảo an toàn thông tin thiết bị đầu cuối; số 3701/STTTT-CĐS về việc các lỗ hổng bảo mật của Microsoft công bố tháng 11/2023 và F5 BIG-IP.

Tiếp theo Văn bản số 7096/SCT-VP ngày 28/11/2023 của Sở Công Thương về việc cài phần mềm phòng chóng mã độc, Virus, Malware (Bitdefender).

Thời gian gần đây, một số hệ thống thông tin của các cơ quan tại TP. HCM bị nhiễm mã độc Ransomware (loại virus mã hóa, bắt cóc dữ liệu đòi tiền chuộc) có tên là Blackcat ransomeware RaaS, tấn công vào các hệ thống có sử dụng phần mềm VMware từ lỗ hổng vCenter, đây là sự cố được đánh giá nghiêm trọng, gây ảnh hưởng đến hoạt động của đơn vị, làm gián đoạn hệ thống cung cấp dịch vụ, mất một số dữ liệu gần nhất (do chưa backup kịp thời). Hacker đã thực hiện xâm nhập và chiếm quyền điều khiển máy tính cá nhân của người dùng có quyền truy cập từ xa qua VPN. Sau khi kết nối VPN, hacker thâm nhập và đánh cắp tài khoản quản trị người dùng. Sau đó, tiếp tục xâm nhập vào một máy chủ đặt trên mạng IT, làm bàn đạp để tấn công vào máy chủ AD, hệ thống máy chủ ảo hóa vCenter, máy chủ quản lý sao lưu đặt tại Trung tâm dữ liệu; hacker chiếm quyền điều khiển máy chủ vCenter, mã hóa 250 máy chủ ảo.

Nhằm đảm bảo an toàn thông tin, bảo vệ dữ liệu, phòng chống mã độc Ransomware tấn cống hệ thống thông tin của các cơ quan, đơn vị trên địa bàn tỉn, và góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Công Thương đề nghị các phòng, đơn vị thực hiện một số nội dung sau:

1. Cảnh giác với các email lừa đảo và tệp tin đính kèm trong email

- Email lừa đảo là một trong những phương thức phổ biến nhất để phát tán ransomware. Tin tặc thường gửi email giả mạo là từ các tổ chức uy tín như ngân hàng, công ty bảo hiểm,... Nội dung email thường thông báo rằng người dùng có vấn đề về tài khoản hoặc cần cập nhật thông tin. Khi người dùng mở email và nhấp vào liên kết hoặc đính kèm trong email, ransomware sẽ được tải xuống và cài đặt trên máy tính của họ. Tăng cường sử dụng email công vụ tỉnh Đồng Nai (@dongnai.gov.vn).

- Không mở các tệp tin đính kèm trong email từ các nguồn không đáng tin cậy: Trong trường hợp không biết rõ về nguồn gốc của tệp tin đính kèm trong email, đề nghị cán bộ công chức, viên chức không nên mở tệp tin này. Tệp tin đính kèm trong

email có nhiều khả năng chứa ransomware hoặc các loại phần mềm độc hại khác.

2. Sao lưu dữ liệu thường xuyên

Đối với cá nhân, thực hiện sao lưu dữ liệu thường xuyên như Ổ cứng cắm ngoài, Ổ cứng di động, USB, Cloud để lưu trữ các dữ liệu quan trọng. Sử dụng công cụ, giải pháp chuyên dùng để sao lưu dữ liệu như: các máy chủ quản lý tập tin, máy chủ sao lưu từ xa, các công cụ lưu trữ đám mây cho phép khôi phục lịch sử thay đổi tập tin.

3. Trường hợp bị nhiễm ransomware

- Khi phát hiện máy tính bị nhiễm mã độc, tắt máy tính ngay lập tức bằng cách ngắt nguồn điện, nhằm ngăn chặn mã độc tiếp tục lây lan và phá hủy dữ liệu trên máy tính. Khởi động máy tính từ môi trường an toàn như ổ đĩa CD, USB và thực khôi phục dữ liệu từ bản sao lưu trước đó (nếu có).

- Không được trả tiền chuộc cho tin tặc, việc này có thể khiến tin tặc tiếp tục phát tán mã độc và không đảm bảo rằng dữ liệu sẽ được giải mã.

- Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616, thư điện tử: ais@mic.gov.vn hoặc Sở Thông tin và Truyền thông, điện thoại 0251.3810.269, thư điện tử: attt@dongnai.gov.vn

4. Giao Văn phòng Sở chủ trì thực hiện:

- Cập nhật bản vá lỗ hổng bảo mật thường xuyên:

+ Thường xuyên theo dõi, cập nhật bản vá lỗ hổng bảo mật của các nhà sản xuất phần mềm (Vmware, Microsoft, Google, ...) thông báo, phát hành để khắc phục các lỗ hổng bảo mật có thể bị tin tặc tấn công, khai thác để phát tán ransomware.

+ Kiểm tra, rà soát, thực hiện cập nhật bản vá kịp thời đã được Sở Thông tin và Truyền thông thông báo, hướng dẫn như lỗ hổng bảo mật trong các sản phẩm Microsoft, F5 BIG-IP, Chrome, Fortinet và một số hãng, sản phẩm khác.

- Cài đặt, sử dụng phần mềm phòng, chống mã độc có kết nối chia sẻ thông tin với NCSC:

Thực hiện cài đặt hệ thống phòng, chống mã độc và chia sẻ thông tin với Trung tâm Giám sát an toàn không gian mạng quốc gia theo hướng dẫn của Sở Thông tin và Truyền thông. Thời gian hoàn thành việc cài đặt trước 31/12/2023 (*theo chỉ đạo của Chủ tịch UBND tỉnh tại văn bản số 12839/UBND-KGVX ngày 28/11/2023*).

Đề nghị các phòng, đơn vị nghiêm túc thực hiện các chỉ đạo trên./.

Nơi nhận:
- Như trên;
- Sở TTTTT(b/c);
- BLĐ Sở;
- Lưu:VT, VP.

(Thủy - mtt)

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ CÔNG THƯƠNG
TỈNH ĐỒNG NAI

Phạm Văn Cường