BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM CHỨNG THỰC ĐIỆN TỬ QUỐC GIA

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

Số: 183 /NEAC-NCKT

Hà Nội, ngày 01 tháng 4 năm 2024

V/v tăng cường đảm bảo an toàn cho hệ thống thực hiện công bố thông tin, công cụ cài đặt của các Tổ chức chứng thực chữ ký số

Kính gửi:
- Các Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng;
- Các Tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng của cơ quan, tổ chức được cấp giấy chứng nhận đủ điều kiện đảm bảo an toàn cho chữ ký số chuyên dùng.

Căn cứ tình hình thực tế vào ngày 24/03/2024, Công ty Chứng khoán VNDirect tại Việt Nam đã trở thành điểm nóng mới nhất trên bản đồ của các cuộc tấn công ransomware quốc tế, dẫn đến bị đe doạ xoá dữ liệu hoặc dữ liệu bị mã hoá không thể phục hồi nếu không nhận được tiền chuộc. Nhằm tăng cường đảm bảo an toàn cho việc thực hiện công bố thông tin và công cụ cài đặt của các tổ chức chứng thực chữ ký số không trở thành kênh lan truyền ransomware, Trung tâm Chứng thực điện tử quốc gia **khuyến nghị** các Tổ chức cung cấp dịch vụ chứng thực chữ ký số (CA) công cộng, CA chuyên dùng một số biện pháp sau:

1. Các thông tin được công bố của CA

- Tài liệu Quy chế chứng thực.

- Các tài liệu hướng dẫn của CA cho thuê bao.

- Các tài liệu của CA công bố để phục vụ tích hợp cho các bên phát triển ứng dụng hoặc cung cấp giải pháp.

- Danh sách thu hồi chứng thư số (CRL)

- Chứng thư số được công bố (Cert)

Cần phải được công bố kèm theo mã băm của tài liệu/file hoặc các tài liệu/file phải được ký số khi công bố để đảm bảo tính toàn vẹn của tài liệu.

2. Các công cụ của CA cung cấp cho thuê bao

- Bộ cài đặt kèm theo phương tiện lưu khoá bí mật.

- Bộ cài đặt ứng dụng kèm theo để cho thuê bao thực hiện ký số, kiểm tra chữ ký số (nếu có).

- Bộ công cụ phát triển phục vụ cho tích hợp cung cấp cho các bên phát triển ứng dụng hoặc cung cấp giải pháp.

Cần phải được công bố kèm theo mã băm của bộ cài đặt /công cụ hoặc phải được ký code signing khi công bố để đảm bảo tính toàn vẹn.

3. Hướng dẫn kiểm tra tính toàn vẹn để không bị nhiễm ransomware

Các CA cần có thông báo/ công cụ công bố hướng dẫn việc kiểm tra mã băm, chữ ký số, code signing cho thuê bao, các bên phát triển ứng dụng hoặc cung cấp giải pháp để đảm bảo tài liệu/file không bị nhiễm ransomware và trở thành kênh lan truyền ransomware. Lưu ý cần hướng dẫn cho người sử dụng kiểm ta tính toàn vẹn, chữ ký hợp lệ (nếu có) cần được thực hiện trước khi mở tài liệu hoặc file.

4. Hệ thống thực hiện công bố thông tin

- Đối với thành phần của hệ thống thông tin thực hiện việc cung cấp dịch vụ công bố thông tin của CA, cho phép truy xuất trực tuyến kiểm tra trạng thái chứng thư số, truy xuất chứng thư số…, gọi chung là thành phần cung cấp các dịch vụ trực tuyến của hệ thống CA.

- Thành phần cung cấp các dịch vụ trực tuyến của hệ thống CA cần được rà soát quét toàn bộ về an toàn thông tin, về mã độc, đặc biệt là ransomware thông việc cập nhật các bản vá bảo mật của hệ điều hành, cập nhật các bản cập nhật đối với thiết bị phòng chống tấn công xâm nhập, phần mềm rà quét virut…Thiết bị có kết nối đến vùng mạng cung cấp các dịch vụ trực tuyến của hệ thống CA để phục công tác quản trị vận hành thì cần được đảm bảo là thiết bị chỉ sử dụng duy nhất cho một mục đích quản trị vận hành không sử dụng cho các mục đích khác, các thiết bị này đã được đảm bảo rà quét "sạch" trước khi được sử dụng cho việc quản trị vận hành.

- Về sao lưu dữ liệu cho thành phần cung cấp các dịch vụ trực tuyến của hệ thống CA cần được đảm bảo rà quét mã độc, ransomware sau khi tiến trình

sao lưu dữ liệu kết thúc và trước khi đưa vào lưu trữ, việc này để bảo khôi phục được dữ liệu "sạch" khi có rủi ro xảy ra đối với hệ thống.

- Các biện pháp **khuyến nghị** này nhằm tăng cường độ an toàn đối với việc cung cấp dịch vụ chứng thực chữ ký số, ứng dụng chữ ký số, giúp thị trường chữ ký số tạo được sự tin tưởng ngày một rộng rãi hơn. Rất mong sự hợp tác của quý CA.

Thông tin liên hệ: Phòng Nghiên cứu, kiểm thử, Trung tâm Chứng thực điện tử quốc gia, tầng 7, tòa nhà Cục Tần số vô tuyến điện, số 115 đường Trần Duy Hưng, Thành phố Hà Nội, email: lqtu@mic.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thứ trưởng Phạm Đức Long (để b/c);
- Giám đốc (để b/c);
- Lưu: VT, NCKT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM CHỨNG THỰC ĐIỆN TỬ QUỐC GIA

Phạm Quốc Hoàn