**THAM LUẬN**

**Công tác đảm bảo an toàn thông tin, an ninh mạng
phục vụ Chuyển đổi số và triển khai Đề án 06/CP trên địa bàn tỉnh**

Kính thưa Quý lãnh đạo

Kính thưa Quý Đại biểu tham dự hội nghị

Được sự phân công của lãnh đạo Hội nghị, tôi tham gia trình bày tham luận Tổng kết Đề án 06/CP và công tác an toàn thông tin, an ninh mạng năm 2024;

Trước tiên, tôi xin tóm tắt tình hình an toàn thông tin, an ninh mạng trong năm qua

***Về công tác an toàn thông tin, an ninh mạng phục vụ Chuyển đổi số***

Theo số liệu Cục An toàn thông tin công bố, tình hình chung ghi nhận trên cả nước, đáng mừng là số sự cố an toàn thông tin nghiêm trọng đã giảm so với năm 2023. Nổi bật là sự kiện Ransomware ảnh hưởng nghiêm trọng nhiều Công ty, Doanh nghiệp, tổ chức lớn trong 03 tháng đầu năm: VNDirect, [PVOIL](https://antoanthongtin.gov.vn/hacker-malware/he-thong-cong-nghe-thong-tin-cua-pvoil-bi-tan-cong-ransomware-109941), Vietnam Post và các cơ sở y tế, giáo dục …

Theo báo cáo của [Hiệp hội An ninh mạng quốc gia](https://antoanthongtin.gov.vn/an-toan-thong-tin/hiep-hoi-an-ninh-mang-quoc-gia-ra-mat-chuong-trinh-dao-tao-chuyen-gia-bao-ve-du-lieu-ca-nhan-vndpo-110804) 1, có tới 46,15% cơ quan, doanh nghiệp cho biết đã từng bị tấn công mạng ít nhất 1 lần trong năm qua, trong đó 6,77% thường xuyên bị tấn công. Tổng số vụ tấn công mạng trong năm ước tính lên tới hơn 659.000 vụ. Theo báo cáo của Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05), Bộ Công an, chỉ tính riêng các đơn vị trọng yếu đã có tới hơn 74.000 cảnh báo tấn công mạng, trong đó có 83 chiến dịch tấn công có chủ đích APT.

**Theo đó, Tấn công có chủ đích APT là hình thức tấn công phổ biến nhất năm 2024.** 26,14% các vụ tấn công trong năm là tấn công APT sử dụng mã độc gián điệp nằm vùng. Có 04 loại lỗ hổng thường bị tin tặc khai thác để tấn công có chủ đích gồm: *Lỗ hổng trong các phần mềm đang sử dụng; Lỗ hổng trong quy trình quản lý, cấu hình, phân quyền; Lỗ hổng từ các chuỗi cung ứng (Supply Chain) không đảm bảo an toàn, an ninh; Lỗ hổng do con người trong hệ thống.*

Ngoài nguy cơ bị đánh cắp thông tin, dữ liệu, các cơ quan, doanh nghiệp còn phải đối mặt với mối đe dọa bị mã hoá dữ liệu tống tiền. Theo khảo sát, có tới 14,59% cơ quan, doanh nghiệp cho biết đã bị tấn công bằng mã độc tống tiền trong năm qua. Đây là tỷ lệ đáng báo động bởi hình thức tấn công này rất nguy hiểm, mang tính “sát thương” cao. Khi đã bị mã hoá dữ liệu, không có cách nào để giải mã, hoạt động của cơ quan, doanh nghiệp bị gián đoạn, đặc biệt uy tín bị ảnh hưởng.

Trên địa tỉnh ta năm qua đáng mừng là ghi nhận chưa xảy ra sự cố nghiêm trọng nào.

Tuy nhiên, tình hình lây nhiễm mã độc, virut máy tính, botnet, lọt lộ thông tin cá nhân, tài khoản người dùng trên địa bàn tỉnh An Giang qua công tác theo dõi, báo cáo định kỳ, thường xuyên và đột xuất theo vụ việc của Thường trực Đội ứng cứu sự cố an toàn thông tin tỉnh cho thấy đây là vấn đề khó khăn, tồn tại, hạn chế dai dẳng, có dấu hiệu ngày càng nghiêm trọng hơn với nhiều vụ lọt lộ tài khoản dịch vụ công, thư điện tử tỉnh, botnet tại một số đơn vị tái nhiễm, tái diễn chưa xử lý được.

Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh với Thường trực là Sở Thông tin và Truyền thông đã thực hiện tốt một số nhiệm hỗ trợ, cảnh báo, hướng dẫn khắc phục lỗ hổng, sự cố an toàn thông tin, an ninh mạng đến các cơ quan, đơn vị trên địa bàn tỉnh.

Một số hoạt động nổi bật của Đội ứng cứu năm qua:

* Định kỳ, thường xuyên, đột xuất gửi thông tin cảnh báo lỗ hổng bảo mật, an toàn thông tin
* Thực hiện rà soát, phát hiện và khắc phục các lỗ hổng, điểm yếu theo nhiệm vụ, kế hoạch Kiểm tra, rà quét lỗ hổng các hệ thống thông tin tại Trung tâm tích hợp dữ liệu tỉnh và một số hệ thống quan trọng của tỉnh (dichvucong, quản lý cán bộ cbccvc)
* Tổ chức Diễn tập ứng cứu sự cố an toàn thông tin cho các hệ thống thông tin cấp độ 3 trên địa bàn tỉnh
* Cử thành viên Tham dự các khóa tập huấn, đào tạo về an toàn thông tin do Cục An toàn thông tin tổ chức: [Khóa đào tạo chuyên gia ứng cứu sự cố theo chương trình Certified Incident Handler.](https://vpdt.angiang.gov.vn/van-ban-di/xem-van-ban-di-chi-tiet?id=3415023&t=tra_cuu_van_ban&xld=0) [Khóa đào tạo về kỹ thuật phân tích bảo mật theo chương trình CySA+](https://vpdt.angiang.gov.vn/van-ban-di/xem-van-ban-di-chi-tiet?id=3363472&t=tra_cuu_van_ban&xld=0), [Khóa đào tạo về phòng thủ mạng nâng cao theo chương trình Advanced Network Defense - CAST614 (ECCouncil)](https://vpdt.angiang.gov.vn/van-ban-di/xem-van-ban-di-chi-tiet?id=3327711&t=tra_cuu_van_ban&xld=0)
* Tham gia các hoạt động Diễn tập thực chiến Cụm 9 các tỉnh ĐBSCL, Diễn tập an toàn thông tin trực tuyến do Cục An toàn thông tin tổ chức: Diễn tập quốc tế ACID năm 2024, [Diễn tập APCERT năm 2024](https://vpdt.angiang.gov.vn/van-ban-den/xem-van-ban-den-chi-tiet?id=13220681&t=tra_cuu_van_ban&xld=82564157)

***Về công tác triển khai Đề án 06/CP***

Năm 2024, An Giang đã triển khai đầy đủ các nội dung, yêu cầu, nhiệm vụ của Đề án 06 trên địa bàn tỉnh, cụ thể:

1. Hệ thống thông tin giải quyết thủ tục hành chính tỉnh An Giang đã được phê duyệt Hồ sơ cấp độ an toàn thông tin theo quy định; chính thức kết nối với Cơ sở dữ liệu quốc gia về dân cư từ ngày tháng 12/2022, giúp kiểm tra danh tính công dân, tự động điền thông tin công dân vào biểu mẫu thông tin người nộp hồ sơ. Theo đó, tháng 11 năm 2024, Tổ công tác của Bộ Công an và Bộ Thông tin và Truyền thông đã phối hợp các đơn vị liên quan kiểm tra, đánh giá an ninh mạng, an toàn thông tin Hệ thống thông tin giải quyết thủ tục hành chính của đơn vị triển khai cung cấp dịch vụ cho các tỉnh/thành phố (trong đó có tỉnh An Giang), qua kiểm tra Hệ thống thông tin giải quyết thủ tục hành chính của tỉnh đã hoàn thành việc khắc phục các lỗ hổng bảo mật; Đồng thời Hệ thống đã nâng cấp, bổ sung tính năng thống kê số lượng, mục đích, thời gian, địa chỉ IP máy tính, thiết bị truy cập, thông tin tra cứu dữ liệu thông tin công dân trong Cơ sở dữ liệu quốc gia về dân cư để phục vụ công tác theo dõi, giám sát, truy vết khi có xảy ra sự cố.

2. Thành lập Tổ quản trị và vận hành kỹ thuật Hệ thống thông tin giải quyết thủ tục hành chính tỉnh An Giang.

3. Tỉnh đã thành lập Bộ phận đảm bảo an toàn, an ninh thông tin mạng thuộc Đề án 06/CP trên địa bàn tỉnh An Giang.

4. Tỉnh có Kế hoạch và chỉ đạo thành lập Đoàn kiểm tra công tác chuyển đổi số và bảo đảm an toàn thông tin mạng trong cơ quan Nhà nước trên địa bàn tỉnh năm 2024, nhằm khắc phục các hạn chế về an toàn thông tin khi truy cập cơ sở dữ liệu Quốc gia về dân cư.

5. Tỉnh đã Kết nối 02 nhóm thủ tục hành chính: Đăng ký khai sinh, đăng ký thường trú, cấp thẻ bảo hiểm y tế cho trẻ em dưới 6 tuổi; thực hiện cấp phiếu lý lịch tư pháp qua ứng dụng VNeID theo đúng lộ trình.

6. An Giang đã ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động của các cơ quan Nhà nước; Quy chế quản lý truy cập mạng truyền số liệu chuyên dùng các cơ quan Đảng và Nhà nước. Ngoài ra, tỉnh còn có nhiều văn bản chỉ đạo các cơ quan, đơn vị thực hiện đảm bảo an toàn thông tin trong truy cập cơ sở dữ liệu Quốc gia về dân cư và tăng tỷ lệ cung cấp và thực hiện dịch vụ công trực tuyến toàn trình.

7. Về nhận thức, kỹ năng, nhân lực chuyển đổi số, tỉnh Kế hoạch số 1197/KH-UBND về đào tạo nâng cao nhận thức về chuyển đổi số, chính phủ số, kinh tế số, công dân số, đảm bảo cơ bản về an toàn thông tin, khai thác, sử dụng dịch vụ công trực tuyến cho cán bộ, công chức, viên chức. Tổng số hơn 1.256 học viên được đào tạo;

*Kính thưa Quý đại biểu*

 An Giang xác định an toàn thông tin là vấn đề quan trọng, cốt lõi trong Chuyển đổi số trên địa bàn tỉnh. Do vậy, trong thời gian tới Sở sẽ tiếp tục tham mưu Tỉnh chỉ đạo các Bộ phận chuyên môn khẩn trương tham mưu thực hiện một số nhiệm vụ sau:

 1. Khẩn trương thực hiện các thủ tục triển khai giải pháp Trung tâm giám sát an toàn thông tin (SOC) trong 6 tháng đầu năm 2025;

 2. Trong năm 2025, tham mưu UBND tỉnh triển khai Trung tâm dữ liệu tỉnh phù hợp theo lộ trình 175/NQ-CP của Chính phủ, bảo đảm các phương án an toàn thông tin, an ninh mạng theo hướng dẫn tại Công văn số 1552/BTTTT-CATTT và Công văn số 708/BTTTT-CATTT của Bộ Thông tin và Truyền thông.

3. Tiếp tục triển khai công tác đảm bảo an toàn thông tin theo mô hình 4 lớp, đáp ứng theo yêu cầu, hướng dẫn của Bộ Thông tin và truyền thông.

4. Duy trì, nâng cấp, bổ sung Cổng dịch vụ công tỉnh đảm bảo an ninh, an toàn khi kết nối cơ sở dữ liệu Quốc gia về dân cư;

5. Đào tạo cập nhật kiến thức về Chuyển đổi số, an toàn thông tin mạng cho công chức, viên chức; đặc biệt công chức có khai thác dữ liệu dân cư.

6. Duy trì diễn tập thực chiến an toàn thông tin ít nhất 01 lần trong năm;

7. Kiểm tra hướng dẫn về công tác chuyển đổi số và an toàn thông tin trên địa bàn tỉnh;

 \* Đối với triển khai Đề án 06/CP

 1. Các địa phương cần quán triệt bộ phận một cửa cấp huyện, cấp xã trong công tác đảm bảo an toàn thông tin như: không lưu mật khẩu trên trình duyệt, cài đặt phần mềm chống mã độc, tách lớp mạng LAN của cán bộ công chức và hệ thống phục vụ truy cập internet công cộng của người dân.

 2. Cán bộ tại bộ phận một cửa tuyệt đối không được phần mềm tự động khai thác trái phép cơ sở dữ liệu dân cư

Trên đây là báo cáo kết quả triển khai Đề án 06, cũng như lộ trình triển khai an toàn thông tin Đề án 06 trên địa bàn tỉnh.

Nhân dịp đầu xuân, kính chúc Quý lãnh đạo, Quý đại biểu mạnh khỏe, hạnh phúc và thành công !