**PHỤ LỤC**

**Các tình huống có thể phát sinh và phương án xử lý ban đầu trong công tác bảo đảm an toàn thông tin, an ninh mạng phục vụ Đại hội Đại biểu toàn quốc lần thứ XIV của Đảng**

*(Kèm theo Công văn số 193/CAT-ANM ngày 12/01/2025 của Công an tỉnh)*

**1. Trang thông tin điện tử Đại hội bị tấn công từ chối dịch vụ (DdoS)**

*Cách nhận biết:* Trang thông tin điện tử https://daihoidangtoanquoc.vn chậm bất thường hoặc không thể truy cập, thời gian tải trang tăng đột ngột, trình duyệt báo lỗi Gateway timeout, Service Unavailable (503)..; có một số dịch vụ trên web hoạt động, có dịch vụ thì không...

*Hướng xử lý:* Kịp thời trao đổi Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Công an tỉnh để phối hợp tiếp nhận, tổ chức xử lý. Đồng thời, triển khai các biện pháp kỹ thuật bảo đảm an ninh mạng, an toàn thông tin theo các quy định, hướng dẫn đã được ban hành, bảo đảm duy trì hoạt động ổn định, an toàn của Cổng thông tin điện tử phục vụ Đại hội *(theo Công văn số 2705/CAT-TM(ANM) ngày 09/10/2025 của Công an tỉnh).*

**2. Cổng/Trang thông tin điện tử của các cơ quan Đảng, Nhà nước trên địa bàn tỉnh bị tấn công từ chối dịch vụ (DdoS)**

*Cách nhận biết:* Cổng/Trang thông tin điện tử chậm bất thường hoặc không thể truy cập, thời gian tải trang tăng đột ngột, trình duyệt báo lỗi Gateway timeout, Service Unavailable (503)..; lưu lượng truy cập tăng đột biến, số lượng request tới server tăng bất thường; tài nguyên máy chủ bị sử dụng quá mức; sự cố không theo quy luật bình thường, có một sô dịch vụ trên web hoạt động, có dịch vụ thì không...

*Hướng xử lý:* Đội ứng cứu nội bộ xử lý sự cố phối hợp với đơn vị vận hành, lập tức cô lập hệ thống bằng Firewall hoặc sử dụng dịch vụ chống DDoS để lọc traffic; giới hạn truy cập, ưu tiên các dịch vụ quan trọng; xác định IP nguồn và loại hình tấn công là SYN flood hay UDP flood..; liên hệ nhà cung cấp dịch vụ ISP bổ sung băng thông nếu thấy cần thiết.

**3. Máy tính bị nhiễm virus, mã độc, phần mềm độc hại**

*Cách nhận biết:* Máy tính chạy chậm bất thường; thời gian khởi động máy tính kéo dài hơn bình thường; các ứng dụng bị treo, đơ hoặc tự động tắt mà không rõ lý do; Pop-up quảng cáo xuất hiện liên tục, kể cả không truy cập trình duyệt; trình duyệt bị chuyển hướng đến các trang web lạ; biểu tượng (icon) phần mềm, file, thư mục bị thay đổi, mất hoặc xuất hiện file lạ...

*Hướng xử lý:* Ngắt kết nối mạng để ngăn lan truyền qua máy tính khác; khởi động máy vào chế độ SafeMode; quét virus bằng phần mềm antivirus bản quyền; gỡ phần mềm lạ, đáng ngờ; cân nhắc cài đặt lại hệ điều hành (chú ý sao lưu dữ liệu quan trọng) nếu các công cụ Antivirus không loại bỏ được hết malware, ransomeware..

**4. Bị tấn công Phishing**

*Cách nhận biết:* Tin tặc thường gửi Email, SMS, tin nhắn messenger, zalo, facebook có đường link lạ giống như thật nhưng có sai khác nhỏ (ví dụ như daihoidangtq.ai, daihoidangxiv.com thay vì daihoidangtoanquoc.vn), chúng yêu cầu người dùng đăng nhập thông tin cá nhân, yêu cầu thông tin tài khoản/mật khẩu, mã OTP bất thường.

*Hướng xử lý:* Hướng dẫn, tuyên truyền người dùng, đại biểu không nhấp vào đường link hoặc tải tệp đính kèm, không trả lời tin nhắn, email đáng nghi; nếu đã lỡ nhấp vào đường link hoặc tải tệp tin đính kèm thì lập tức ngắt kết nối internet, xóa lịch sử, cookie, cache trong trình duyệt, chạy chương trình antivirus, gỡ bỏ ứng dụng lạ, khởi động lại máy (nếu dùng iphone); nếu đã nhập thông tin vào đường link lạ thì ngay lập tức đổi mật khẩu của tài khoản bị xâm nhập và tài khoản khác dùng chung mật khẩu đó, kích hoạt xác thực hai yếu tố để tăng cường bảo mật; trường hợp đã lỡ nhập thông tin ngân hàng vào đường dẫn lạ thì phải gọi ngay cho tổng đài ngân hàng yêu cầu khóa tài khoản, thẻ, tắt Internet banking tạm thời, đổi mật khẩu, kiểm tra biến động số dư.

**5. Hệ thống thông tin bị tấn công qua lỗ hổng ứng dụng, website**

*Cách nhận biết:* Hệ thống bị tấn công mạng lưu lượng truy cập tăng đột biến bất thường, website phản hồi chậm, xuất hiện dữ liệu lạ trong cơ sở dữ liệu, các hành vi bất thường trong log SQL Injection, xss pay loads, brute-force login...

*Hướng xử lý:* Chặn IP tấn công qua firewall hoặc WAF, cập nhật các rule WAF để chặn payload tấn công, rollback hệ thống về bản backup an toàn nếu có thể, cập nhật code và thư viện lên phiên bản cao nhất và an toàn, cập nhật framework/CMS, kiểm tra định kỳ và backup dữ liệu thường xuyên.

**6. Cổng/Trang thông tin điện tử bị tấn công thay đổi giao diện**

*Cách nhận biết:* Trên giao diện website bị chèn ký tự, thông điệp của tin tặc (deface), xuất hiện hình ảnh lạ, nội dung phản cảm...

*Hướng xử lý:* Để hạn chế thiệt hại, rủi ro khi bị tấn công deface, quản trị hệ thống phải ngắt kết nối internet hoặc chuyển hướng website sang chế độ bảo trì để ngăn chặn tin tặc tiếp tục khai thác, cần thiết chuyển server về chế độ bảo trì; sau đó ghi nhận logfile của web server, hệ điều hành, firewall; phân tích nguyên nhân, kiểm tra lỗ hổng bảo mật (SQL injection, XSS, uploadfile, plugin cũ..), xem xét đến khả năng tài khoản quản trị bị lộ, phần mềm hệ thống hoặc CMS có lỗ hổng, có shell/backdoor bị cài...; sau đó khôi phục hệ thống, tăng cường bảo mật bằng các cách như: đổi toàn bộ mật khẩu (FTP, SSH, CMS, DB..), cài đặt và cấu hình lại WAF, hạn chế quyền truy cập, cập nhật các bản vá bảo mật mới nhất, tắt hoặc giới hạn các chức năng upload, thực thi mã.

**7. Khi màn hình LED, LCD, pano số, áp phích điện tử bị tấn công chèn nội dung, hình ảnh trái phép**

*Cách nhận biết:* Nội dung hiển thị bị thay đổi mà không có ai điều khiển, tự động hiện ra video, hình ảnh lạ, nội dung phản cảm, quảng cáo trá hình, cờ bạc, thông điệp chính trị, màn hình nhấp nháy, bị bật tắt hoặc reset bất thường...

*Hướng xử lý:* Lập tức ngắt nguồn điện, hoặc ngắt kết nối mạng, tắt bộ điều khiển (controller) để dừng nội dung hình ảnh bị chèn; lập biên bản sự cố trình bày đầy đủ thông tin, ghi nhận hình ảnh lại làm bằng chứng, ghi nhận thông tin, thời gian xảy ra sự cố; kiểm tra và ngắt các kết nối không cần thiết (wifi, NFC, Bluetooth); kiểm tra các Port điều khiển từ xa qua internet có bị mở hay không (3389, 8080); kiểm tra thiết bị xem có bị kết nối từ xa qua VNC, AnyDesk, Teamviewer, Ultraview, RemoteDesktop, Seecreen..; gỡ toàn bộ phần mềm điều khiển cũ, cài lại phiên bản mới và sạch; thay đổi mật khẩu truy cập thiết bị mặc định do nhà sản xuất thiết lập (88888888, 11111111,...) hoặc các mật khẩu dễ đoán (12341234, 12345678,...); tắt quyền truy cập từ xa nếu thấy không cần thiết.