



NGUY CƠ CHIẾN TRANH MẠNG VÀ SỰ CẦN THIẾT CỦA VIỆC PHỐI HỢP GIỮA CÁC CƠ QUAN CHUYÊN TRÁCH TRONG LĨNH VỰC BẢO MẬT VÀ AN TOÀN THÔNG TIN

Người trình bày:

TS. Đặng Vũ Sơn

Phó trưởng ban Ban Cơ yếu Chính phủ

Nguy cơ chiến tranh không gian mạng

- **Chiến tranh không gian mạng** được biết đến như việc sử dụng Internet để tổ chức các cuộc tấn công từ một nước có chủ quyền vào một nước khác trong không gian mạng

Nguy cơ chiến tranh không gian mạng

- Các quốc gia đều phải đối mặt với những nguy cơ của những cuộc chiến tranh trên không gian mạng và đều phải chuẩn bị sẵn sàng cho hình thức chiến tranh này bằng cách xây dựng khả năng tác chiến trên không gian mạng.

Nguy cơ chiến tranh không gian mạng

- Một khi chiến tranh mạng xảy ra chúng ta sẽ phải đối đầu với các nguy cơ
 - Bị lộ lọt thông tin,
 - Thay đổi, phá hủy thông tin,
 - Tê liệt hệ thống thông tin

Các yếu tố cơ bản cho hệ thống phòng thủ

- Để chống lại các nguy cơ đó, chúng ta cần xây dựng một hệ thống phòng thủ vững chắc trong không gian mạng. Điều đó phải đảm bảo các yếu tố:
 - Hành lang pháp lý và hệ thống tổ chức của các cơ quan chuyên trách trong lĩnh vực bảo mật, an toàn thông tin,
 - Nâng cao nhận thức của tổ chức, cá nhân trong lĩnh vực bảo mật, an toàn thông tin,

Các yếu tố cơ bản cho hệ thống phòng thủ

- Nghiên cứu xây dựng và ứng dụng các giải pháp kỹ thuật trong phòng chống nguy cơ chiến tranh không gian mạng,
- Đào tạo đội ngũ chuyên gia có trình độ cao trong lĩnh vực bảo mật và an toàn thông tin,
- Sự phối hợp chặt chẽ giữa các cơ quan chuyên trách trong lĩnh vực bảo mật và an toàn thông tin.

Các giải pháp kỹ thuật

- Bảo vệ các thông tin, dữ liệu quan trọng được lưu trữ và truyền tải trên các mạng công nghệ thông tin và Internet bằng biện pháp ứng dụng kỹ thuật mật mã

Các giải pháp kỹ thuật

- Các chức năng của mật mã có thể kể đến như:
 - Bảo vệ tính bí mật của thông tin
 - Đảm bảo tính toàn vẹn của thông tin
 - Đảm bảo tính xác thực của thông tin
- Vai trò rất quan trọng của mật mã trong hệ thống chứng thực điện tử

Các giải pháp kỹ thuật

- Áp dụng các giải pháp an toàn hệ thống và giám sát an toàn mạng để kịp thời phát hiện, ngăn chặn và xử lý các tấn công qua không gian mạng
- Cần có sự phối hợp đồng bộ giữa các giải pháp mật mã và các giải pháp an toàn hệ thống, giám sát an toàn mạng

Vai trò của Ban Cơ yếu Chính phủ

- Một trong những lực lượng chuyên trách bảo vệ bí mật nhà nước được giao các nhiệm vụ:
 - *Sử dụng kỹ thuật mật mã và các giải pháp có liên quan để bảo vệ thông tin bí mật nhà nước (Luật Cơ yếu năm 2011)*
 - *Thành lập và duy trì tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng phục vụ các cơ quan thuộc hệ thống Chính trị” (Nghị định số 26/2007/NĐ-CP ngày 15/02/2007)*
 - *Triển khai hệ thống giám sát an toàn thông tin trên mạng công nghệ thông tin trọng yếu của các cơ quan Đảng, Chính phủ”, trong đó ưu tiên các mạng CNTT có triển khai các sản phẩm mật mã của ngành Cơ yếu (Chỉ thị số 897/CT-TTg ngày 10/06/2011)*

Vai trò của Ban Cơ yếu Chính phủ

- Ban Cơ yếu Chính phủ đã và đang triển khai các biện pháp kỹ thuật như:
 - Nghiên cứu, chế tạo các sản phẩm mật mã chuyên dụng,
 - Xây dựng và quản lý **Trung tâm chứng thực điện tử chuyên dùng Chính phủ**,
 - Xây dựng và vận hành **Trung tâm Giám sát an ninh mạng** có chức năng giám sát an toàn mạng cho các mạng CNTT trọng yếu của các cơ quan Đảng, Chính phủ.

Vai trò của Ban Cơ yếu Chính phủ

- Quản lý nhà nước về mật mã dân sự (nghị định số 73/2007/NĐ-CP ngày 08/5/2007):
 - Chủ trì, phối hợp với các Bộ, ngành có liên quan dự thảo tiêu chuẩn, quy chuẩn kỹ thuật đối với các sản phẩm mật mã dân sự
 - Chủ trì, phối hợp với các Bộ, ngành có liên quan xây dựng chính sách mật mã quốc gia, chiến lược phát triển tiềm lực khoa học và công nghệ mật mã dân sự.
 - Tổ chức bộ máy quản lý, đăng ký, thẩm định, đánh giá, chứng nhận hợp chuẩn, chứng nhận hợp quy sản phẩm mật mã dân sự.

Sự cần thiết của việc phối hợp chặt chẽ giữa các cơ quan chuyên trách

- Công tác bảo đảm chủ quyền quốc gia trên không gian mạng cần có sự phối hợp chặt chẽ ở quy mô quốc gia giữa các cơ quan chuyên trách
- Cần tiếp tục thể chế hóa chức năng nhiệm vụ của mỗi cơ quan chuyên trách như Bộ Thông tin và Truyền thông, Bộ Công An, Bộ Quốc phòng, Ban Cơ yếu Chính phủ,... và các tổ chức xã hội như Hiệp hội an toàn thông tin

Sự cần thiết của việc phối hợp chặt chẽ giữa các cơ quan chuyên trách

- Việc xây dựng cơ chế phối hợp giữa các cơ quan chuyên trách đóng vai trò hết sức quan trọng trong việc xây dựng và triển khai giải pháp tổng thể trong việc đảm bảo chủ quyền quốc gia trên không gian mạng

KẾT LUẬN

- Đảm bảo chủ quyền quốc gia trên không gian mạng có vai trò hết sức quan trọng đối với sự phát triển của đất nước trong thời đại hiện nay, trong đó việc phối hợp giữa các cơ quan chuyên trách là yêu cầu khách quan và cần được đặc biệt quan tâm.

KẾT LUẬN

- Đồng thời, chúng ta cần tiếp tục giải quyết một số nội dung sau:
 - Tiếp tục hoàn thiện hành lang pháp lý trong lĩnh vực bảo mật và an toàn thông tin.
 - Tăng cường nâng cao nội lực, đầu tư nghiên cứu, chế tạo, ưu tiên sử dụng các sản phẩm bảo mật và an toàn thông tin được sản xuất trong nước.
 - Áp dụng các giải pháp kỹ thuật tiên tiến. Đặc biệt là các giải pháp ứng dụng mật mã và các giải pháp an toàn hệ thống, giám sát an toàn mạng



Xin chân thành cảm ơn!