# RỦI RO ATTT TRÊN CÁC HỆ THỐNG CNTT NHÀ NƯỚC

Từ thực tế đến cách thức phát hiện & xử lý rủi ro trên không gian mạng

Người Trình Bày: Nguyễn Thành Nam

Công ty Cổ phần Dịch vụ Công nghệ tin học HPT

# Giới thiệu về diễn giả

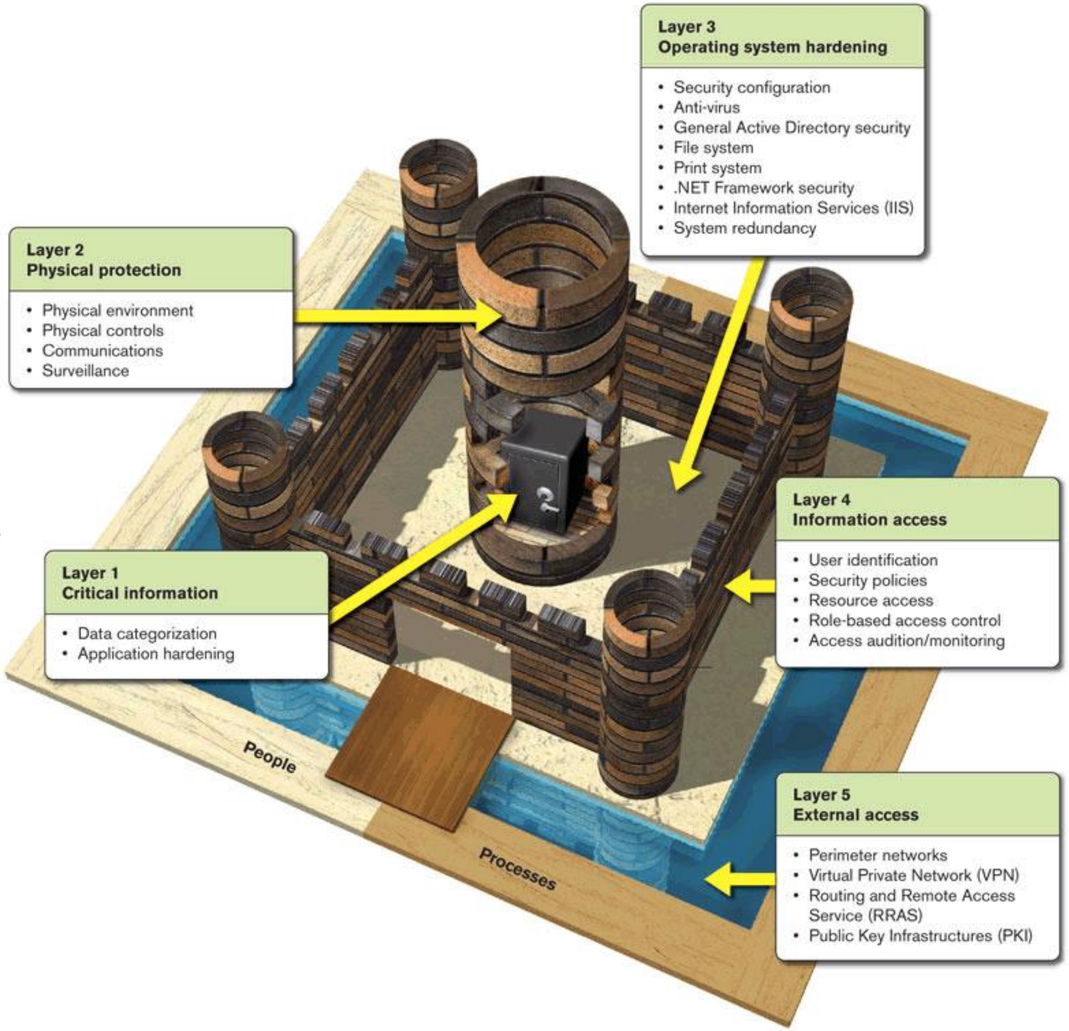
- Giám đốc chiến lược An toàn thông tin Mạng công ty cổ phần dịch vụ Công nghệ tin học HPT
- 10 Năm nghiên cứu lĩnh vực ATTT
- Đánh giá & Tư vấn  ATTT cho nhiều dự án trong các lĩnh vực trọng yếu: Cơ quan Nhà nước, Ngân Hàng, Tài chính,…
- Chứng chỉ Certified Ethical Hacker
- Tham gia nhiều công tác hỗ trợ sự cố an toàn thông tin cho các tổ chức, cơ quan nhà nước

# Nội dung trình bày

- Tổng quan về An toàn hệ thống CNTT cơ quan Nhà nước
- Các khó khăn trong việc đảm bảo ATTT cho hệ thống
- Cách thức phát hiện và xử lý rủi ro ATTT trên không gian mạng
- Một số khuyến nghị

# Tổng quan về An toàn hệ thống CTTT cơ quan Nhà nước

- Các hệ thống đều được triển khai theo các kiến trúc ATTT tiên tiến: Self Defense Network, Defense In Depth, Castle Defense…
- Các giải pháp công nghệ ATTT được trang bị tương đối đầy đủ: Firewall, IPS, Web Protection, Database Protection,…
- Đội ngũ được định kỳ đào tạo về An toàn thông tin: đào tạo, diễn tập
- Hệ thống CNTT quan trọng (vd ứng dụng, email,…) thường được đặt tập trung tại các trung tâm dữ liệu chính với nhiều trang bị và giám sát bởi đội ngũ 24/7



# Các khó khăn trong việc đảm bảo ATTT cho hệ thống



1/ Hệ thống hiện tại có đang đối mặt với các tấn công hàng ngày?

2/ Các tấn công đã thành công, chiếm quyền hệ thống, đánh cắp dữ liệu tổ chức?

3/ Các đầu tư giải pháp ATTT đã trang bị có đang bảo vệ tốt cho tổ chức?

4/ Ngân sách đầu tư ATTT có giới hạn, làm sao để nâng cao năng lực giám sát ATTT cho quản trị viên?

# Các điểm yếu trong thực tế triển khai

- Các giải pháp công nghệ chưa thực sự ứng phó tốt với các tấn công có chủ đích và có chiến thuật phức tạp
- Việc kết hợp nhiều giải pháp công nghệ lại thành 1 bức tranh hoàn chỉnh yêu cầu thiết lập nhiều về các chính sách nâng cao
- Đội ngũ thường trực được định kỳ đào tạo về An toàn thông tin nhưng không chuyên trách về xử lý các sự cố ATTT
- Các tấn công vào hệ thống CNTT quan trọng ngày càng khó theo dõi và giám sát, yêu cầu hệ thống phải không ngừng được tối ưu nâng cao thiết lập an toàn bảo mật

# Cách thức phát hiện và xử lý rủi ro ATTT trên không gian mạng

ĐỊNH KỲ

- Thực hiện các kiểm tra an ninh vào hệ thống và triển khai & tối ưu các chính sách thiết bị phòng thủ chuyên dụng: WAF, FW, DBFW, MailGW,…
  - Kiểm tra khả năng phòng vệ của hệ thống
  - Triển khai & Nâng cao thiết lập an toàn cho công nghệ
  - Đào tạo đội ngũ con người khả năng vận hành, xử lý sự cố
- Thiết lập các hệ thống giám sát mã độc (Sandbox/ APT/ EDR ) & Rà soát, phát hiện các tấn công định kỳ
  - Triển khai & Nâng cao thiết lập an toàn cho công nghệ
  - Rà soát các hành vi bất thường trên Log file
  - Rà soát mã độc và các hành vi bất thường trên hệ thống thông tin quan trọng
- Đánh giá tổng thể, nâng cao thiết lập an ninh hệ thống
  - Tăng cường khả năng phòng vệ của công nghệ
  - Tăng cường kỹ năng giám sát hệ thống
  - Đầu tư theo lộ trình, kiến trúc đầy đủ, chú trọng việc tích hợp các giải pháp công nghệ - quy trình – con người tạo thành 1 hệ thống phòng thủ chặt chẽ

# Một số khuyến nghị

## ĐÁNH GIÁ KHẢ NĂNG PHÒNG VỆ

1/ Hệ thống hiện tại có đang đối mặt với các tấn công hàng ngày?

3/ Các đầu tư giải pháp ATTT đã trang bị có đang bảo vệ tốt cho tổ chức?

## THEO DÕI & RÀ SOÁT HỆ THỐNG ĐỊNH KỲ

1/ Hệ thống hiện tại có đang đối mặt với các tấn công hàng ngày?

2/ Các tấn công đã thành công, chiếm quyền hệ thống, đánh cắp dữ liệu tổ chức?

## XÂY DỰNG HỆ THỐNG THEO CÁC KIẾN TRÚC CHUẨN, KẾT HỢP CÔNG NGHỆ - QUY TRÌNH – ĐỘI NGŨ

3/ Các đầu tư giải pháp ATTT đã trang bị có đang bảo vệ tốt cho tổ chức?

4/ Ngân sách đầu tư ATTT có giới hạn, làm sao để nâng cao năng lực giám sát ATTT cho quản trị viên?


THANK
YOU