Nội dung trình bày

- Các đe dọa đến từ nhân tố con người
- Các đe dọa đến từ tấn công hệ thống máy tính
- Các đe dọa mang tính vật lý khác

Chương 2. Đe doạ đên bảo mật thông tin

- Nguy cơ đến từ con người 80%
- Nguy cơ tấn công từ mạng, hệ thống máy tính 8%
- Nguy cơ liên quan hệ thống vật lý 8%

Đe dọa liên quan đến con người

- Lỗi và bỏ quên
  - Không lây lan nhưng đe dọa lớn đến hệ thống
  - Phát sinh do những người có quyền với thông tin đó
  - Tấn công vào toàn vẹn và cẩn mật dữ liệu
  - Giải pháp: cấp quyền bé nhất, backup thường xuyên

Đe dọa liên quan đến con người

- Gian lận và trộm cắp
  - Làm lỗi hệ thống có chủ tâm
  - Nhân viên phải biết được giới hạn cho phép
  - Cần có chính sách tốt để phát hiện hành động sai
  - Lưu trữ thông tin, và đảm bảo thông tin tốt nhất để xem xét
  - Lưu trữ thông tin đề phòng

Đe dọa liên quan đến con người

- Tấn công xã hội (social engireering)
  - Tiếp cận, lôi kéo để lấy được thông tin cần thiết
  - Đặc tính có thể bị lợi dụng:
    - Mong muốn trở thành người hữu ích
    - Xu hướng tin tưởng người khác
    - Lo sợ sẽ gặp phải rắc rối
    - Hài lòng góc làm việc
    - Tò mò và ham muốn của người dùng
  - Tấn công thói quen, kiến thức
- Người dùng là mắt xích yếu nhất trong các hệ thống

Đe dọa liên quan đến con người

- Một số mô hình tấn công
  - Lừa qua mạng máy tính: phishing
  - Tin tưởng vào các ứng dụng cung cấp mạng
  - Tin tưởng vào các người dùng khác trong hệ thống
  - Sử dụng các hệ thống không đúng chỉ dẫn, tuân thủ quy đinh

Đe dọa liên quan đến con người

- Phương thức: đóng vai trò người khác, là người dùng quan trọng, qua hệ thống rác thải, …
- Một số vấn đề
  - Mật khẩu: mật khẩu quá ngắn, hoặc quá dài
  - Modems: không sử dụng hết, tạo sơ hở
  - Nhân viên hỗ trợ: không xác định được đối tác
  - Website: cung cấp quá nhiều thông tin

Đe dọa liên quan đến con người

- Một số giải pháp
  - Yêu cầu dịch vụ để thể hiện xác định bản thân (phân biệt khách hàng và nhân viên)
  - Đưa ra tiêu chuẩn, mật khẩu không được đọc thông qua điện thoại
  - Đưa ra tiêu chuẩn để cho mật không được ghi lộ ra
  - Đăng ký dịch vụ xác định người gọi để cho người hỗ trợ khách hàng và dịch vụ hỗ trợ khác
  - Đầu tư máy xén giấy trên mỗi tầng.

Đe dọa liên quan đến con người

- Yêu cầu về chính sách
  - Không được có những tiêu chuẩn, chỉ định không thể thực hiện được
  - Chỉ rõ điều được phép, không được phép
  - Ngắn gọn súc tích
  - Phải được xem lại thường xuyên đảm bảo cập nhật
  - Dễ thực hiện và có thể tra cứu được dễ dàng

Đe dọa liên quan đến con người

- Cung cấp thường xuyên thông tin về tấn công xã hội
  - Từ chối cung cấp thông tin hợp đồng
  - Thực hiện nhanh các xử lý
  - Lộ tên
  - Hăm dọa
  - Các lỗi nhỏ
  - Yêu cầu truy xuất hoặc những thông tin bị cấm

Tấn công kỹ thuật

- Nhóm người dùng tấn công qua mạng
- Phân loại
  - Craker: tấn công phá hủy dữ liệu, hệ thống
  - Hacker: Xâm nhập hệ thống, thông báo quản trị lỗi hệ thống
  - Phreak: lợi dụng, sử dụng mạng viễn thông của người khác

Tấn công kỹ thuật

- Các giai đoạn tấn công của hacker
  - Do thám: Tìm hiểu thông tin về công ty: ip, …
  - Duyệt: Tìm kiếm các điểm yếu có khả năng tấn công
  - Thay đổi quyền truy xuất: Tăng quyền sử dụng hệ thống
  - Duy trì quyền truy xuất: Tạo cửa hậu có khả năng tiếp tục tấn công
  - Xóa bỏ dấu vết: Xóa bỏ nhật ký sự kiện

Tấn công kỹ thuật

- Là đoạn mã thực hiện ngoài ý muốn để thực hiện mục đích người thiết kế
  - Virus
  - Worm
  - Trojan
  - Logic bomb

Tấn công kỹ thuật

- Làm cho người sử dụng không tiếp cận được dịch vụ
  - Denial of service (DoS) ví dụ như Syn flood, Fin flood, Smurfs, Fraggle
  - DoS là distributed denial of service (DDoS)

Tấn công kỹ thuật

- Giải pháp
  - Đưa ra giải pháp kỹ thuật tương ứng với các hình thức tấn công
  - Đưa ra các quy định tuân thủ quy trình kỹ thuật
  - Đội phản ứng với các vấn đề kỹ thuật
  - Cập nhât các phương thức tấn công và cách thức phòng ngừa

Kết hợp tân công con người và kỹ thuật

- Có sự kết hợp nhất định giữa các loại hình tấn công
  - Tấn công xã hội có thông tin nhất định
  - Tấn công kỹ thuật dựa trên thông tin từ tấn công xã hội
  - Tấn công xã hội dựa trên nền khởi nguồn từ tấn công kỹ thuật

Đe dọa từ hệ thống vật lý

- Tấn công vào hệ thống vật lý
  - Trộm, cướp
  - Tấn công phá hoại hệ thống vật lý
- Hỏng hóc vật lý
  - Xác suất lỗi các hệ thống lưu trữ xử lý
  - Tính ổn định các hệ thống xử lý
- Đe dọa của các thảm họa
  - Cháy, nổ
  - Lũ lụt, thiên tai

Nội dung trình bày

- Các đe dọa đến từ nhân tố con người
- Các đe dọa đến từ tấn công hệ thống máy tính
- Các đe dọa mang tính vật lý khác
- Chi tiết tấn công mạng được trình bày trong slides tiếp theo