Chương 1: Tổng quan về An toàn thông tin

Phần 2

D) Lựa chọn biện pháp bảo vệ an toàn thông tin

- Sau khi chỉ ra các mối nguy cơ và thiết lập được chính sách ATTT,
- Trên mỗi tài nguyên thông tin, xác định các biện pháp bảo vệ khác nhau để

Biện pháp kỹ thuật

- Sử dụng giải pháp
- Ví dụ để phòng chống nguy cơ xâm nhập hệ thống Server trái phép, đưa ra:
  - Chính sách: chặn truy nhập vào máy chủ Server từ bên ngoài Internet
  - Biện pháp kỹ thuật: áp dụng giải pháp tường lửa Firewall nâng cao

Biện pháp thủ tục

- Sử dụng
- Ví dụ: phòng chống nguy cơ xâm nhập hệ thống Server
  - Chính sách: máy tính không thuộc công ty không được kết nối với hệ thống mạng
  - Biện pháp thủ tục: quy định nhân viên không được mang máy tính cá nhân và kết nối vào mạng công ty

E) Đặc tả, thiết kế, triển khai ATTT

- **Đặc tả kỹ thuật**:
  - VD1: Các chức năng của giải pháp tường lửa Firewall
  - VD2: Các yêu cầu kỹ thuật đối với biện pháp xác thực người dùng đăng nhập hệ thống.
- **Thiết kế**:
  - VD1: Sơ đồ tường lửa Firewall 2 lớp
  - VD2: Cơ chế hoạt động và quy trình vận hành của giải pháp xác thực 2 yếu tố với mật khẩu OTP
- **Triển khai**:
  - Triển khai biện pháp thủ tục: ban hành quy định, tổ chức tập huấn cho các thành viên, thiết lập cơ chế giám sát việc tuân thủ
  - Triển khai biện pháp kỹ thuật: lắp đặt thiết bị, cấu hình và thử nghiệm

F) Vận hành và cập nhật

- Vận hành:
- Cập nhật:
  - Các sự cố, các vấn đề phát sinh
  - Các hạn chế và lỗi gặp phải
  - Các nguy cơ mới về ATTT
  - Tình hình tài nguyên thông tin
  - Các giải pháp cần phải cải tiến hoặc triển khai mới

- Từ đó, giải pháp ATTT sẽ được

- Vòng đời của giải pháp ATTT gắn liền với vòng đời của hệ thống thông tin.

G) Chi phí và hiệu quả của giải pháp ATTT

- Một giải pháp ATTT tốt cần

  - Chức năng nghiệp vụ của hệ thống (functionality)
  - Tính khả dụng (usability)

An toàn thông tin

Chức năng nghiệp vụ

Khả dụng

1.3) Kỹ thuật An toàn thông tin

- Vai trò của người kỹ sư An toàn thông tin là

- Kỹ sư ATTT cần nắm vững các yếu tố kỹ thuật căn bản

Các yếu tố kỹ thuật căn bản trong ATTT

- Điểm yếu (vulnerability):
- Nguy cơ (threat):
- Tấn công (attack) :
- Cơ chế biện pháp bảo vệ (control):

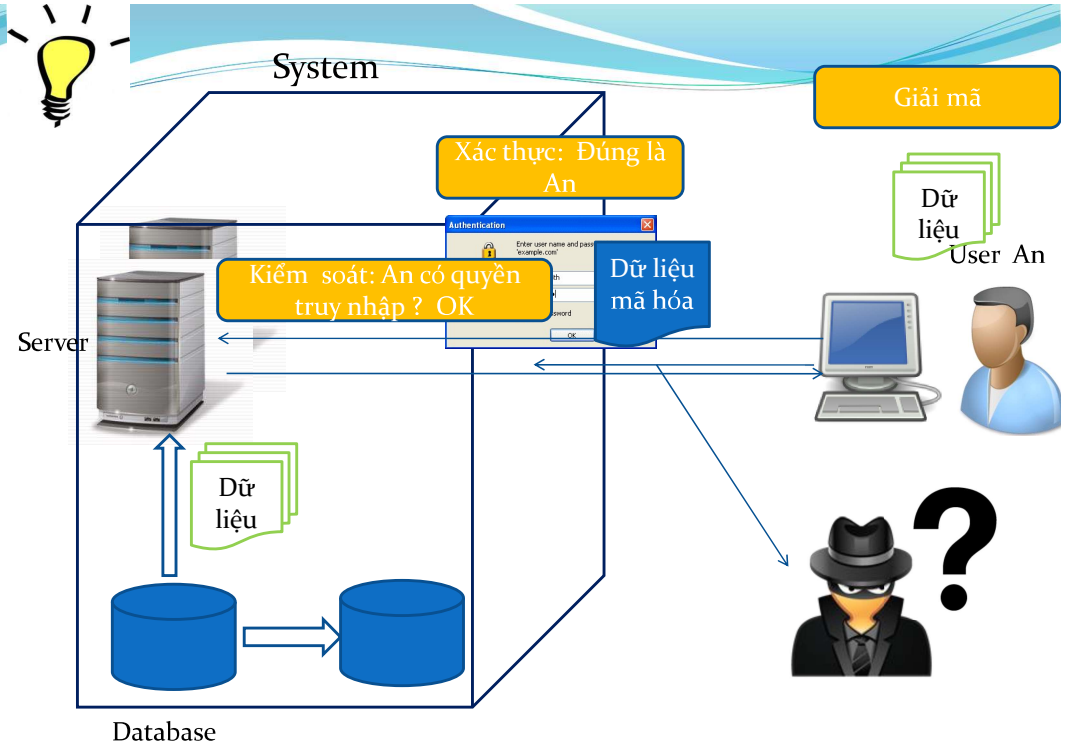
A) Cơ chế bảo vệ (control)

Sắp xếp theo mục đích và trình tự áp dụng của cơ chế:

- Ngăn chặn (**Prevent**) :
- Dò tìm và phát hiện (**Detect**)
- Phục hồi (**Recover**)

Các cơ chế ngăn chặn

- **Mật mã:**
  làm cho việc lưu trữ, xử lý và trao đổi thông tin được bảo mật.
- **Xác thực**: của
  các bên tham gia vào hệ thống
  của thông tin
- **Điều khiển truy nhập**:
  đúng theo quyền hạn được cấp.



B. Các lĩnh vực bảo mật (đọc thêm)

- **Nền tảng kỹ thuật an toàn thông tin** gồm: **mật mã** và các kỹ thuật như **xác thực**, **điều khiển truy nhập...**
- Ngoài ra, người kỹ sư ATTT cần có kiến thức và kỹ năng trong nhiều lĩnh vực
  - Hệ thống mạng máy tính
  - Hệ quản trị cơ sở dữ liệu
  - Hệ điều hành và phần mềm
  - Web và các dịch vụ Internet
  - Phát triển phần mềm an toàn

An ninh mạng chuyên về

- Các lỗ hổng hệ thống và giao thức mạng
- Các dạng tấn công hệ thống mạng
- Các giao thức bảo mật
- Các công cụ, kỹ thuật bảo mật mạng:
  - Tường lửa, security gateway,
  - Hệ thống phát hiện/ngăn chặn xâm nhập mạng
  - Công cụ quét lỗ hổng trên các dịch vụ mạng
  - Công cụ cập nhật các bản vá lỗi hệ thống

Bảo mật ứng dụng Web

- Các vấn đề về phần mềm mã độc: virus, worm, trojan, ransomware, spyware...
- Các lỗ hổng phần mềm
- Các dạng tấn công vào ứng dụng Web
- Công cụ bảo mật Web:
  - Quy trình phát triển ứng dụng Web an toàn
  - Công cụ phân tích mã để phát hiện lỗ hổng bảo mật
  - Công cụ kiểm tra và cập nhật các bản vá dành cho hệ điều hành và nền tảng mà ứng dụng đang chạy trên đó.

Tóm lại, các ý chính cần nắm được

- 3 tính chất của ATTT: bảo mật, toàn vẹn và sẵn sàng
- 3 mục tiêu bảo vệ ATTT: ngăn chặn, phát hiện và phục hồi
- 6 bước xây dựng giải pháp ATTT: phân tích nguy cơ, chính sách, đặc tả, thiết kế, triển khai và vận hành.
- 4 yếu tố: điểm yếu (vulnerable), nguy cơ (threat), tấn công (attack) và cơ chế biện pháp bảo vệ (control)
- 2 nhánh của ATTT: An ninh mạng và bảo mật ứng dụng Web