Chương 1: Tổng quan về An toàn thông tin

1.1) Khái niệm An toàn thông tin

- Các thuật ngữ tiếng Anh
  - Information Security:
  - Computer Security:
  - Cyber Security: an toàn thông tin trong môi trường mạng toàn cầu Internet

An toàn thông tin là gì ?

- An toàn thông tin là bảo vệ **tài nguyên thông tin** trước tác động của các hành vi *không hợp lệ* (trái phép) bao gồm
  - Làm lộ
  - Giả mạo
  - Thay đổi
  - Làm hư hỏng
  - Phá hủy

- **Tài nguyên thông tin** là tất cả các đối tượng mang thông tin cần được bảo vệ.

- **Người có thẩm quyền:**
  - Người chủ sở hữu tài nguyên
  - Người được ủy quyền quyền quản trị hay sử dụng tài nguyên

A) Tiếp cận An toàn thông tin

- Từ góc độ **sử dụng**: bảo vệ các tài nguyên thông tin thuộc sở hữu cá nhân
  - Máy tính
  - Thiết bị lưu trữ
  - Tài khoản và dữ liệu cá nhân
- Từ góc độ **chuyên môn**: bảo vệ **hệ thống thông tin** (thuộc về tổ chức và doanh nghiệp)

Bảo vệ hệ thống thông tin

- Cái gì trong hệ thống cần phải bảo vệ ?
  - Tài nguyên thông tin
- Bảo vệ khỏi cái gì ?
  - Các mối đe dọa, nguy cơ mất an toàn thông tin, gây ra thiệt hại về tài nguyên thông tin cho chủ thể sở hữu
- Bảo vệ bằng cách nào ?
  - **Xây dựng và triển khai giải pháp an toàn thông tin**, bao gồm các biện pháp bảo vệ tài nguyên khỏi các mối nguy cơ

- Tài nguyên bên trong hệ thống thông tin bao gồm:
  - Phần cứng: hạ tầng mạng, máy tính, thiết bị lưu trữ và các thiết bị hỗ trợ hoạt động
  - Phần mềm: hệ điều hành, hệ quản trị cơ sở dữ liệu, các phần mềm chuyên dụng và ứng dụng
  - Dữ liệu: hệ thống tệp tin, cơ sở dữ liệu tác nghiệp, tài liệu
  - Con người: các thành viên của hệ thống, là chủ thể sở hữu hoặc sử dụng

B) Nhận thức tầm quan trọng của ATTT

- An toàn thông tin đang ngày càng trở thành vấn đề nóng, được quan tâm hơn và diễn biến phức tạp hơn
  - Cấp độ quốc gia: thành lập cơ quan an ninh mạng, lực lược tác chiến mạng, đơn vị chống tội phạm công nghệ cao, trung tâm giám sát ứng cứu sự cố khẩn cấp máy tính
  - Cấp độ doanh nghiệp: thành lập bộ phận quản trị an toàn thông tin
  - Cấp độ cá nhân: phổ cập kiến thức an toàn thông tin trong việc sử dụng các ứng dụng số hóa.

Tại sao ATTT quan trọng ?

- Hiện nay, các hoạt động của chính phủ, tổ chức, doanh nghiệp và cá nhân đều dựa trên công nghệ thông tin và tài nguyên thông tin
- Tài nguyên thông tin là loại tài sản đặc biệt
  - Khó xác định giá trị thật sự
  - Chỉ ước lượng được giá trị thiệt hại khi mất an toàn thông tin xảy ra.
- Mất an toàn thông tin có thể dẫn đến những hậu quả nghiêm trọng và khó lường

Tình hình hiện nay

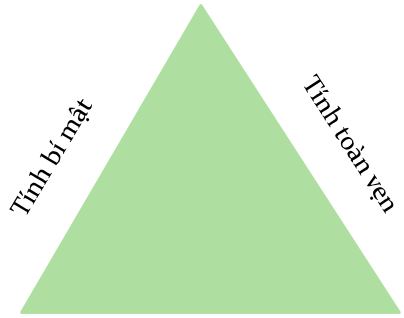
- Sự bùng nổ của Internet và các thiết bị kết nối: PC, laptop, tablet, smartphone, camera và nhiều thiết bị khác... tạo ra Internet của Vạn vật (Internet of Things)
- Sự gia tăng của các ứng dụng phân tán gồm thương mại điện tử, ngân hàng điện tử, mạng xã hội, Blockchain...
- Hầu hết các hệ thống thông tin của chính phủ, doanh nghiệp hay cá nhân đều kết nối Internet có thể bị tấn công từ bất cứ đâu.
- Tội phạm trên không gian mạng phát triển mạnh

1.2) Cơ sở an toàn thông tin

- Để xây dựng và triển khai giải pháp an toàn thông tin, người kỹ sư hệ thống cần nắm được các vấn đề sau

A) Các tính chất và mục tiêu của ATTT

An toàn thông tin có **3 tính chất cơ bản** cần đảm bảo



TAM GIÁC CIA

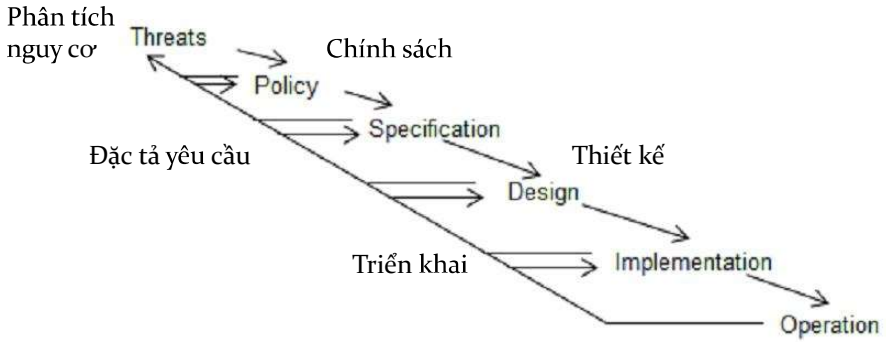
- Tính bí mật (confidentiality): bảo vệ thông tin không bị tiết lộ trái phép
  - Ví dụ: Trong hệ thống ngân hàng, một khách hàng được phép xem thông tin số dư tài khoản của mình nhưng không được phép xem thông tin của khách hàng khác.
- Tính toàn vẹn (integrity): bảo vệ thông tin không bị sửa đổi trái phép
  - Ví dụ: Trong hệ thống ngân hàng, không cho phép khách hàng tự thay đổi thông tin số dư của tài khoản của mình.

- Tính sẵn sàng (availability): bảo vệ thông tin không bị hư hỏng và gián đoạn
  - Ví dụ 1: Trong hệ thống ngân hàng, khi một khách hàng mở tài khoản thì tài khoản đó phải có mặt trong hệ thống cho đến khi nào còn hiệu lực.
  - Ví dụ 2: Khi cần, khách hàng có thể truy vấn thông tin số dư tài khoản bất kỳ lúc nào theo như quy định.

Mục tiêu ATTT

- **Ngăn chặn**: không để hành vi trái phép xảy ra
- **Phát hiện:** hành vi trái phép khi đang diễn ra
- **Phục hồi:** chấm dứt hành vi trái phép, khôi phục hoạt động bình thường hoặc đảm bảo hệ thống không bị gián đoạn ngay cả khi bị tấn công.

B) Giải pháp ATTT



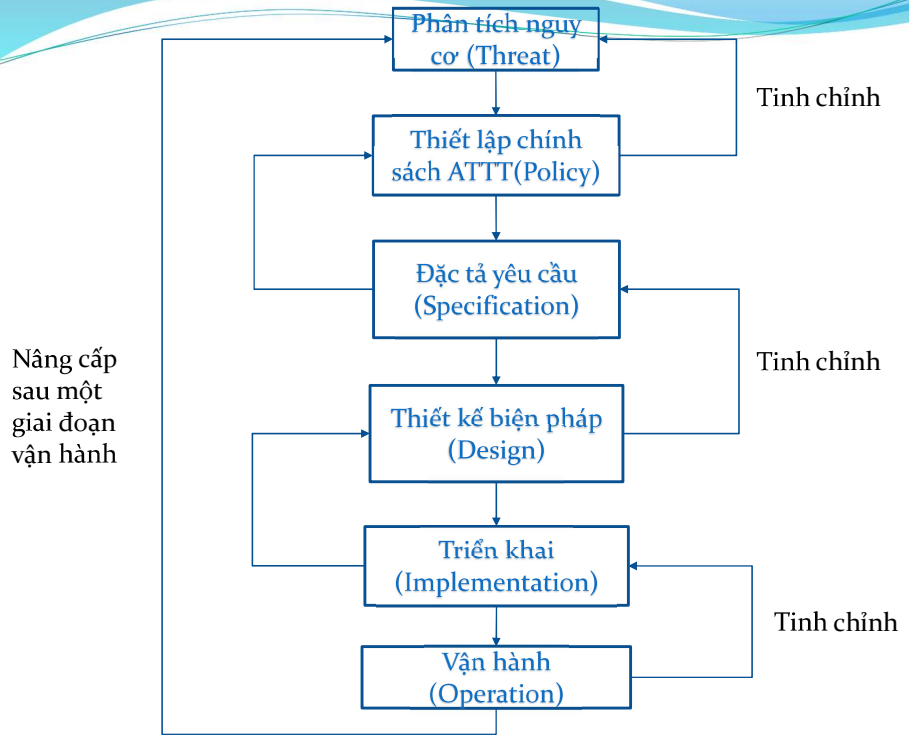
Hình vẽ 1. Vòng đời an toàn

Giải pháp an toàn thông tin là một tập hợp bao gồm

- 1) Chính sách về an toàn thông tin
  - Nguyên tắc cơ bản về an toàn thông tin bao gồm các yêu cầu và mục tiêu cần đạt được về an toàn thông tin…
  - Danh sách các tài sản là tài nguyên thông tin cần bảo vệ, nguy cơ và rủi ro với từng tài sản.
  - Quyền và nghĩa vụ của các chủ thể có liên quan như : người sở hữu, người quản trị, người sử dụng…
- 2) Các biện pháp bảo vệ an toàn thông tin gồm
  - Biện pháp kỹ thuật (áp dụng công nghệ)
  - Biện pháp về thủ tục (quy định trong quản lý)
- 3) Quản lý vận hành và cập nhật giải pháp
  - Hướng dẫn, đào tạo cho các thành viên thực hiện đúng các biện pháp
  - Giám sát việc thực hiện và lưu lại các dữ liệu
  - Phân tích dữ liệu để đánh giá kết quả vận hành
  - Điều chỉnh lại giải pháp để đảm bảo mục tiêu và đáp ứng các thay đổi.

Xây dựng giải pháp ATTT

- Là một quá trình liên tục và xuyên suốt sự tồn tại của hệ thống
- Đi theo vòng đời với nhiều bước tạo thành một quy trình thống nhất



C) Phân tích nguy cơ

- **Nguy cơ (threat):** là sự kiện **có khả năng (xác suất)** xảy ra gây mất an toàn thông tin
- Đặc điểm của nguy cơ:
  - Luôn tiềm ẩn và có thể xảy ra bất cứ lúc nào
  - Có thể dự đoán nhưng không lường hết được

Phân loại theo tác hại của nguy cơ

- Làm lộ: mất tính bí mật của thông tin
- Làm sai lệch: mất tính toàn vẹn, giả mạo thông tin
- Làm hỏng: phá hủy thông tin
- Làm gián đoạn hoặc ngừng: mất tính sẵn sàng của thông tin

Phân loại theo tác nhân gây ra

- Tác nhân không có chủ ý
  - Người dùng trong hệ thống sơ suất
  - Thảm họa: động đất, bão, lũ, cháy, tai nạn
- Tác nhân có chủ ý
  - Bên trong hệ thống: Nội gián
  - Bên ngoài hệ thống
    - Tội phạm công nghệ cao, hacker
    - Phần mềm mã độc
    - Các máy tính bị hacker kiểm soát

- (*) Hiện nay, **nguy cơ tấn công có chủ ý** đang gia tăng mạnh
- Cần hiểu về cách thức tấn công xảy để đưa ra các biện pháp khắc phục hiệu quả
- Ngoài ra, còn phải xác định điểm yếu (vulnerability) của hệ thống là nơi dễ bị nguy cơ khai thác

* Các dạng tấn công có chủ ý

- Nghe trộm và đánh cắp dữ liệu chuyển qua Internet
- Thăm dò và khai thác lỗi của phần mềm (lỗ hổng, điểm yếu)
- Xâm nhập hệ thống mạng, hệ thống máy tính, phát tán mã độc
- Chiếm quyền điều khiển máy tính để làm phương tiện để tấn công hệ thống khác
- Giả mạo tài khoản người dùng hợp lệ và email
- Lừa đảo trực tuyến (Phishing, Social Engineering)
- Tấn công từ chối dịch vụ DDoS làm cho hệ thống quá tải và ngừng phục vụ.
- .....

Kịch bản tấn công có chủ ý điển hình

- Giai đoạn 1: Thăm dò hệ thống để lấy thông tin, tìm điểm yếu và chuẩn bị công cụ tấn công
- Giai đoạn 2: Khai thác điểm yếu và xâm nhập vào hệ thống
- Giai đoạn 3: Cài đặt mã độc (virus, trojan, worm, backdoor)
- Giai đoạn 4: Nghe lén, thu thập và sửa đổi thông tin trái phép, điều khiển hệ thống từ xa, đánh cắp dữ liệu, tài khoản
- Giai đoạn 5: Xóa dấu vết

Sự phát triển của kỹ thuật tấn công