# Bài 1 : Tổng quan về an toàn thông tin

## 1. Khái niệm

An toàn thông tin (Information Security - InfoSec) là một lĩnh vực tập trung vào việc bảo vệ thông tin khỏi các mối đe dọa, đảm bảo thông tin luôn được bảo mật, toàn vẹn và sẵn sàng sử dụng.

## 2. Nguyên tắc cốt lõi: CIA Triad

An toàn thông tin được xây dựng dựa trên ba nguyên tắc cốt lõi, thường được gọi là CIA Triad (Confidentiality, Integrity, Availability):

1. **Bảo mật ( Confidentiality ) :**

* Đảm bảo rằng chỉ những thực thể được ủy quyền (người dùng, hệ thống, hoặc quy trình) mới có thể truy cập thông tin.
* Ví dụ:
  + Một tài liệu nội bộ chỉ có thể được đọc bởi nhân viên cấp cao, được bảo vệ bằng mật khẩu hoặc mã hóa.
  + Dữ liệu khách hàng trong cơ sở dữ liệu chỉ có thể được truy cập bởi nhân viên có quyền.
* Phương pháp thực hiện:
  + Sử dụng mã hóa (encryption) như AES hoặc RSA để bảo vệ dữ liệu khi lưu trữ hoặc truyền tải.
  + Áp dụng kiểm soát truy cập (access control) như danh sách kiểm soát truy cập (ACL - Access Control List).
  + Sử dụng xác thực mạnh (strong authentication) để xác minh danh tính người dùng.

1. **Toàn vẹn ( Integrity )**

* Đảm bảo rằng thông tin không bị thay đổi trái phép, duy trì tính chính xác và đầy đủ của dữ liệu.
* Ví dụ:
  + Một giao dịch ngân hàng không bị sửa đổi để thay đổi số tiền hoặc người nhận.
  + Tệp hệ thống không bị virus thay đổi mã nguồn.
* Phương pháp thực hiện:
  + Sử dụng hàm băm (hash functions) như SHA-256 để kiểm tra xem dữ liệu có bị thay đổi hay không.
  + Áp dụng chữ ký số (digital signatures) để xác minh tính xác thực và toàn vẹn của thông điệp.
  + Sử dụng hệ thống phát hiện xâm nhập (IDS) để phát hiện các thay đổi bất thường.

1. **Khả dụng ( Availbility )**

* Đảm bảo rằng thông tin và hệ thống luôn sẵn sàng để người dùng hợp pháp truy cập khi cần thiết.
* Ví dụ:
  + Website của một ngân hàng phải hoạt động liên tục để khách hàng có thể giao dịch.
  + Dữ liệu trong cơ sở dữ liệu phải có thể truy xuất ngay lập tức khi cần.
* Phương pháp thực hiện:
  + Sử dụng hệ thống dự phòng (redundancy) như máy chủ sao lưu hoặc RAID để đảm bảo hoạt động liên tục.
  + Áp dụng các biện pháp chống tấn công từ chối dịch vụ (DDoS protection).
  + Thực hiện sao lưu (backup) định kỳ và có kế hoạch khôi phục sau thảm họa (disaster recovery).

## 3. Phạm vi

An toàn thông tin tập trung vào **bảo mật điện tử** (electronic security) và **bảo mật vật lý** (physical security):

* **Bảo mật điện tử**: Bảo vệ dữ liệu và hệ thống khỏi các cuộc tấn công mạng như hack, malware, hoặc phishing.
* **Bảo mật vật lý**: Ngăn chặn truy cập vật lý trái phép vào phần cứng, chẳng hạn như khóa cửa phòng máy chủ, sử dụng camera giám sát, hoặc bảo vệ thiết bị bằng mật khẩu BIOS.

Phạm vi bao gồm:

* **Dữ liệu**: Ở mọi trạng thái (lưu trữ, xử lý, truyền tải).
* **Hệ thống**: Máy chủ, máy trạm, thiết bị mạng, thiết bị IoT.
* **Mạng**: Các giao thức, kênh truyền thông, VPN.
* **Con người**: Nhân viên, khách hàng, đối tác cần được đào tạo để tránh các lỗi bảo mật do con người gây ra (như mở email lừa đảo).

## 4. Mục tiêu

* Bảo vệ dữ liệu và hệ thống: Ngăn chặn các mối đe dọa như hack, ransomware, hoặc đánh cắp dữ liệu.
* Đảm bảo tính liên tục của kinh doanh: Duy trì hoạt động ngay cả khi có sự cố bảo mật, thông qua các kế hoạch khôi phục và dự phòng.
* Tuân thủ pháp luật: Đáp ứng các yêu cầu quy định như GDPR, HIPAA, hoặc các tiêu chuẩn quốc tế như ISO 27001.

## 5. Biện pháp bảo mật

### 5.1. Đánh giá bảo mật (Security Assessment)

* **Mục đích**: Xác định các rủi ro tiềm ẩn và đánh giá mức độ an toàn của hệ thống.
* **Các bước**:
  + **Xác định khu vực rủi ro**:
    - Kiểm tra các điểm yếu trong hệ thống, chẳng hạn như phần mềm chưa được vá (unpatched software), cấu hình sai, hoặc thiết bị không được bảo mật.
    - Ví dụ: Một máy chủ chạy phiên bản cũ của Apache có thể dễ bị khai thác bởi lỗ hổng đã biết.
  + **Đánh giá khả năng vi phạm bảo mật hoặc sụp đổ hệ thống**:
    - Sử dụng các công cụ quét lỗ hổng (như Nessus, OpenVAS) để tìm kiếm các điểm yếu.
    - Thực hiện kiểm thử thâm nhập (penetration testing) để mô phỏng các cuộc tấn công thực tế.
  + **Đề xuất các bước giảm thiểu rủi ro**:
    - Cập nhật phần mềm, áp dụng tường lửa, hoặc tăng cường xác thực.
    - Ví dụ: Nếu phát hiện một cổng mở không cần thiết, khuyến nghị đóng cổng hoặc cấu hình tường lửa để chặn.

### 5.2. Áp dụng bảo mật

* **Sử dụng kiến thức chuyên môn**:
  + **Đào tạo nội bộ**: Đảm bảo đội ngũ CNTT được đào tạo về các kỹ thuật bảo mật mới nhất.
  + **Thuê chuyên gia**: Các tổ chức nhỏ có thể thuê tư vấn bảo mật hoặc sử dụng dịch vụ quản lý bảo mật (Managed Security Services).
* **Phương pháp nhiều lớp (Defense in Depth)**:
  + **Khái niệm**: Không dựa vào một giải pháp bảo mật duy nhất mà sử dụng nhiều lớp bảo vệ để tăng cường an toàn.
  + **Ví dụ về các lớp**:
    - **Lớp vật lý**: Khóa cửa phòng máy chủ, sử dụng camera giám sát.
    - **Lớp mạng**: Tường lửa, hệ thống phát hiện xâm nhập (IDS/IPS), mã hóa VPN.
    - **Lớp ứng dụng**: Cập nhật phần mềm, kiểm tra mã nguồn để phát hiện lỗi.
    - **Lớp dữ liệu**: Mã hóa, sao lưu định kỳ.
    - **Lớp con người**: Đào tạo nhận thức bảo mật, chính sách mật khẩu mạnh.
  + **Lợi ích**: Nếu một lớp bị phá vỡ, các lớp khác vẫn có thể bảo vệ hệ thống.
* **Chính sách và quy trình**:
  + Xây dựng các chính sách bảo mật rõ ràng, như chính sách mật khẩu, chính sách sử dụng thiết bị cá nhân (BYOD), hoặc chính sách phản ứng sự cố.
  + Quy trình phải được văn bản hóa và kiểm tra định kỳ để đảm bảo hiệu quả.
  + Ví dụ: Quy trình phản ứng sự cố có thể bao gồm các bước: phát hiện, cách ly, khắc phục, và báo cáo.

### 5.3. Nâng cao nhận thức bảo mật (Security Awareness)

* **Tầm quan trọng**:
  + Con người thường là mắt xích yếu nhất trong chuỗi bảo mật. Các lỗi như nhấp vào email lừa đảo hoặc sử dụng mật khẩu yếu có thể dẫn đến vi phạm lớn.
  + Nhận thức bảo mật không chỉ dành cho nhân viên kỹ thuật mà cần áp dụng cho **mọi cấp độ** trong tổ chức, từ nhân viên văn phòng đến ban lãnh đạo.
* **Các biện pháp**:
  + **Đào tạo liên tục**:
    - Tổ chức các buổi đào tạo định kỳ về các mối đe dọa phổ biến (phishing, ransomware, social engineering).
    - Sử dụng các bài kiểm tra giả lập, như gửi email phishing giả để kiểm tra phản ứng của nhân viên.
  + **Không phải hoạt động một lần**:
    - Nhận thức bảo mật phải được duy trì liên tục, vì các mối đe dọa thay đổi nhanh chóng.
    - Ví dụ: Một nhân viên được đào tạo năm 2023 có thể không nhận thức được các kỹ thuật phishing mới vào năm 2025.
  + **Tích hợp vào văn hóa tổ chức**:
    - Khuyến khích nhân viên báo cáo các hành vi đáng ngờ mà không sợ bị trừng phạt.
    - Tạo các chương trình khen thưởng cho nhân viên có ý thức bảo mật tốt.
    - Ví dụ: Một công ty có thể treo áp phích nhắc nhở về an toàn thông tin trong văn phòng hoặc gửi email định kỳ với các mẹo bảo mật.

## 6. Nguyên tắc Least Privilege

**Định nghĩa**:

Nguyên tắc Least Privilege (Nguyên tắc quyền hạn tối thiểu) yêu cầu mỗi chương trình, người dùng, hoặc quy trình chỉ được cấp quyền hạn tối thiểu cần thiết để hoàn thành công việc của mình.

**Mục đích**:

* Giảm thiểu rủi ro khi một tài khoản hoặc chương trình bị xâm phạm.
* Ví dụ: Nếu một nhân viên chỉ cần quyền đọc dữ liệu, họ không nên được cấp quyền sửa đổi hoặc xóa.

**Ứng dụng**:

* **Trong quản lý người dùng**:
  + Chỉ cấp quyền quản trị (admin) cho những người thực sự cần.
  + Ví dụ: Một nhân viên kế toán không cần quyền cài đặt phần mềm trên máy tính công ty.
* **Trong lập trình**:
  + Các ứng dụng chỉ nên có quyền truy cập vào các tài nguyên cần thiết.
  + Ví dụ: Một ứng dụng web chỉ nên có quyền đọc cơ sở dữ liệu, không nên có quyền sửa đổi hệ thống tệp.
* **Trong hệ thống**:
  + Áp dụng các chính sách kiểm soát truy cập dựa trên vai trò (Role-Based Access Control - RBAC).
  + Ví dụ: Một kỹ sư mạng chỉ có quyền truy cập vào cấu hình thiết bị mạng, không có quyền vào dữ liệu nhân sự.

**Lợi ích**:

* Giảm bề mặt tấn công (attack surface).
* Hạn chế thiệt hại nếu xảy ra vi phạm (ví dụ: một tài khoản bị hack chỉ có quyền hạn chế sẽ gây ít thiệt hại hơn).

**Thách thức**:

* Cần quản lý quyền truy cập một cách chi tiết, có thể tốn thời gian.
* Cân bằng giữa bảo mật và sự tiện lợi cho người dùng.

## 7. Các khái niệm bảo mật chính

Các khái niệm nền tảng trong an toàn thông tin, thường được gọi là “AAA” (Authentication, Authorization, Accounting) cùng với các khái niệm liên quan :

### 7.1 Xác thực (Authentication)

Là quá trình xác minh danh tính của một thực thể (người dùng, thiết bị, hoặc quy trình) để đảm bảo rằng họ là ai như họ tuyên bố.

**Ví dụ**:

* Nhập tên người dùng và mật khẩu để đăng nhập vào hệ thống.
* Sử dụng vân tay để mở khóa điện thoại.

**Phương pháp**:

* **Kiến thức (Something you know)**: Mật khẩu, PIN, câu trả lời cho câu hỏi bảo mật.
* **Sở hữu (Something you have)**: Thẻ thông minh, token, điện thoại nhận mã OTP.
* **Bản chất (Something you are)**: Sinh trắc học (vân tay, mống mắt, nhận diện khuôn mặt).
* **Xác thực đa yếu tố (MFA)**: Kết hợp nhiều phương pháp để tăng cường bảo mật (ví dụ: mật khẩu + mã OTP).

**Tầm quan trọng**:

* Là bước đầu tiên để kiểm soát truy cập, đảm bảo chỉ người dùng hợp pháp mới có thể vào hệ thống.

### 7.2 Ủy quyền (Authorization)

Quá trình quyết định xem một thực thể đã xác thực được phép thực hiện hành động nào hoặc truy cập tài nguyên nào.

**Ví dụ**:

* Một nhân viên đã đăng nhập vào hệ thống nhưng chỉ có quyền xem dữ liệu, không có quyền chỉnh sửa.
* Một ứng dụng chỉ được phép truy cập thư mục cụ thể trên máy chủ.

**Phương pháp**:

* Sử dụng danh sách kiểm soát truy cập (ACL).
* Áp dụng mô hình RBAC hoặc Attribute-Based Access Control (ABAC).

**Mối liên hệ với xác thực**:

* Xác thực trả lời câu hỏi “Bạn là ai?”, còn ủy quyền trả lời câu hỏi “Bạn được phép làm gì?”.
* Xác thực phải được thực hiện trước khi ủy quyền.

### 7.3 Kiểm toán (Accounting)

Quá trình ghi lại và theo dõi các hoạt động của người dùng hoặc hệ thống để phân tích, giám sát, và điều tra khi cần.

**Ví dụ**:

* Ghi lại thời gian đăng nhập, hành động thực hiện, và tài nguyên được truy cập của một người dùng.
* Nhật ký hệ thống (system logs) ghi lại các lần khởi động, lỗi, hoặc truy cập trái phép.

**Mục đích**:

* **Giám sát**: Phát hiện các hành vi bất thường (như đăng nhập từ địa điểm lạ).
* **Điều tra**: Xác định nguyên nhân của một sự cố bảo mật.
* **Tuân thủ**: Đáp ứng các yêu cầu pháp lý hoặc tiêu chuẩn (như ISO 27001 yêu cầu lưu nhật ký).

**Công cụ**:

* Hệ thống quản lý thông tin và sự kiện bảo mật (SIEM) như Splunk, ELK Stack.
* Nhật ký tích hợp trong hệ điều hành (như /var/log trên Linux).

### 7.4 Kiểm soát truy cập (Access Control)

Quá trình quản lý quyền truy cập vào tài nguyên dựa trên các chính sách bảo mật.

**Loại hình**:

* **Kiểm soát truy cập vật lý**: Hạn chế truy cập vào phòng máy chủ, tòa nhà.
* **Kiểm soát truy cập logic**: Hạn chế truy cập vào dữ liệu, ứng dụng, hoặc mạng.

**Mô hình**:

* **Discretionary Access Control (DAC)**: Chủ sở hữu tài nguyên quyết định quyền truy cập.
* **Mandatory Access Control (MAC)**: Quyền truy cập được áp dụng bởi hệ thống, thường dùng trong môi trường quân sự.
* **Role-Based Access Control (RBAC)**: Quyền truy cập dựa trên vai trò của người dùng.
* **Attribute-Based Access Control (ABAC)**: Quyền truy cập dựa trên thuộc tính (như vị trí, thời gian).

### 7.5 Không thể chối bỏ (Nonrepudiation)

Đảm bảo rằng một người hoặc thực thể không thể phủ nhận hành động của mình, chẳng hạn như gửi một thông điệp hoặc thực hiện một giao dịch.

**Ví dụ**:

* Một người ký số vào hợp đồng điện tử không thể phủ nhận việc ký.
* Một email được gửi với chữ ký số xác minh nguồn gốc và nội dung.

**Phương pháp**:

* Sử dụng chữ ký số (digital signatures) dựa trên mã hóa khóa công khai (public-key cryptography).
* Lưu trữ nhật ký hoạt động với dấu thời gian (timestamp) để làm bằng chứng.

**Tầm quan trọng**:

* Đảm bảo trách nhiệm pháp lý và tính minh bạch trong các giao dịch điện tử.
* Hỗ trợ điều tra khi xảy ra tranh chấp.

## 8. Các lệnh cơ bản

### 8.1 cd (Change Directory):

* **Chức năng**: Chuyển đổi thư mục làm việc hiện tại.
* **Cú pháp**: cd [đường dẫn]

**Ví dụ**:

* cd /home/user/documents: Chuyển đến thư mục documents.
* cd .. : Quay lại thư mục mẹ.
* cd ~ : Chuyển về thư mục home của người dùng.

**Ứng dụng trong bảo mật**: Dùng để di chuyển đến thư mục chứa các tệp nhật ký hoặc công cụ bảo mật.

### 8.2 ls (List):

* **Chức năng**: Liệt kê các tệp và thư mục trong thư mục hiện tại.
* **Cú pháp**: ls [tùy chọn]
* **Tùy chọn phổ biến**:
  + ls -l: Hiển thị chi tiết (quyền, chủ sở hữu, kích thước, ngày sửa đổi).
  + ls -a: Hiển thị cả tệp ẩn (bắt đầu bằng dấu chấm, như .bashrc).
* **Ví dụ**:
  + ls: Liệt kê file1.txt file2.txt folder1.
  + ls -la: Hiển thị chi tiết, bao gồm cả tệp ẩn.
* **Ứng dụng trong bảo mật**: Kiểm tra các tệp đáng ngờ trong thư mục hệ thống.
* **Lưu ý**: Trên Ubuntu, lệnh dir không phổ biến và thường được thay bằng ls. Tuy nhiên, dir có thể được dùng trong một số hệ thống hoặc kịch bản tương thích.

### 8.3 cp (Copy):

* **Chức năng**: Sao chép tệp hoặc thư mục.
* **Cú pháp**: cp [tùy chọn] [nguồn] [đích]
* **Tùy chọn phổ biến**:
  + cp -r: Sao chép thư mục và toàn bộ nội dung bên trong (đệ quy).
* **Ví dụ**:
  + cp file1.txt /home/user/backup/: Sao chép file1.txt vào thư mục backup.
  + cp -r folder1 /home/user/backup/: Sao chép thư mục folder1.
* **Ứng dụng trong bảo mật**: Sao lưu các tệp nhật ký hoặc cấu hình trước khi chỉnh sửa.

### 8.4 mkdir (Make Directory):

* **Chức năng**: Tạo thư mục mới.
* **Cú pháp**: mkdir [tên thư mục]
* **Ví dụ**:
  + mkdir backup: Tạo thư mục backup.
  + mkdir -p /home/user/backup/2025: Tạo thư mục lồng nhau, tự động tạo thư mục cha nếu chưa tồn tại.
* **Ứng dụng trong bảo mật**: Tạo thư mục để lưu trữ tệp sao lưu hoặc công cụ bảo mật.

### 8.5 chown (Change Owner):

* **Chức năng**: Thay đổi chủ sở hữu của tệp hoặc thư mục.
* **Cú pháp**: chown [tùy chọn] [người dùng][:nhóm] [tệp/thư mục]
* **Tùy chọn phổ biến**:
  + chown -R: Áp dụng đệ quy cho thư mục và nội dung bên trong.
* **Ví dụ**:
  + chown user1 file1.txt: Chuyển quyền sở hữu file1.txt cho user1.
  + chown -R user1:group1 folder1: Chuyển quyền sở hữu thư mục folder1 cho user1 và nhóm group1.
* **Ứng dụng trong bảo mật**: Đảm bảo chỉ người dùng hợp pháp sở hữu các tệp nhạy cảm.

### 8.6 chmod (Change Mode):

* **Chức năng**: Thay đổi quyền truy cập (read, write, execute) của tệp hoặc thư mục.
* **Cú pháp**: chmod [tùy chọn] [quyền] [tệp/thư mục]
* **Cách biểu diễn quyền**:
  + **Ký hiệu chữ**: u (user), g (group), o (others), r (read), w (write), x (execute).
  + **Số octal**: 4 (read), 2 (write), 1 (execute), cộng lại để biểu diễn quyền.
* **Ví dụ**:
  + chmod u+rwx file1.txt: Cấp quyền đọc, ghi, thực thi cho chủ sở hữu.
  + chmod 644 file1.txt: Cấp quyền đọc-ghi cho chủ sở hữu (6=4+2), đọc cho nhóm và khác (4).
  + chmod -R 755 folder1: Áp dụng quyền đọc-ghi-thực thi cho chủ sở hữu, đọc-thực thi cho nhóm và khác, trên toàn bộ thư mục.
* **Ứng dụng trong bảo mật**: Hạn chế quyền truy cập vào các tệp nhạy cảm, tuân thủ nguyên tắc Least Privilege.

### 8.7 Lệnh: gcc -o exploit exploit.c

**Giải thích**:

* gcc: Trình biên dịch GNU C.
* -o exploit: Đặt tên tệp thực thi đầu ra là exploit.
* exploit.c: Tệp mã nguồn C cần biên dịch.

# Bài 2: Bảo mật hệ điều hành