CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN CSDL

Nội dung

1.1. CSDL và các khái niệm liên quan

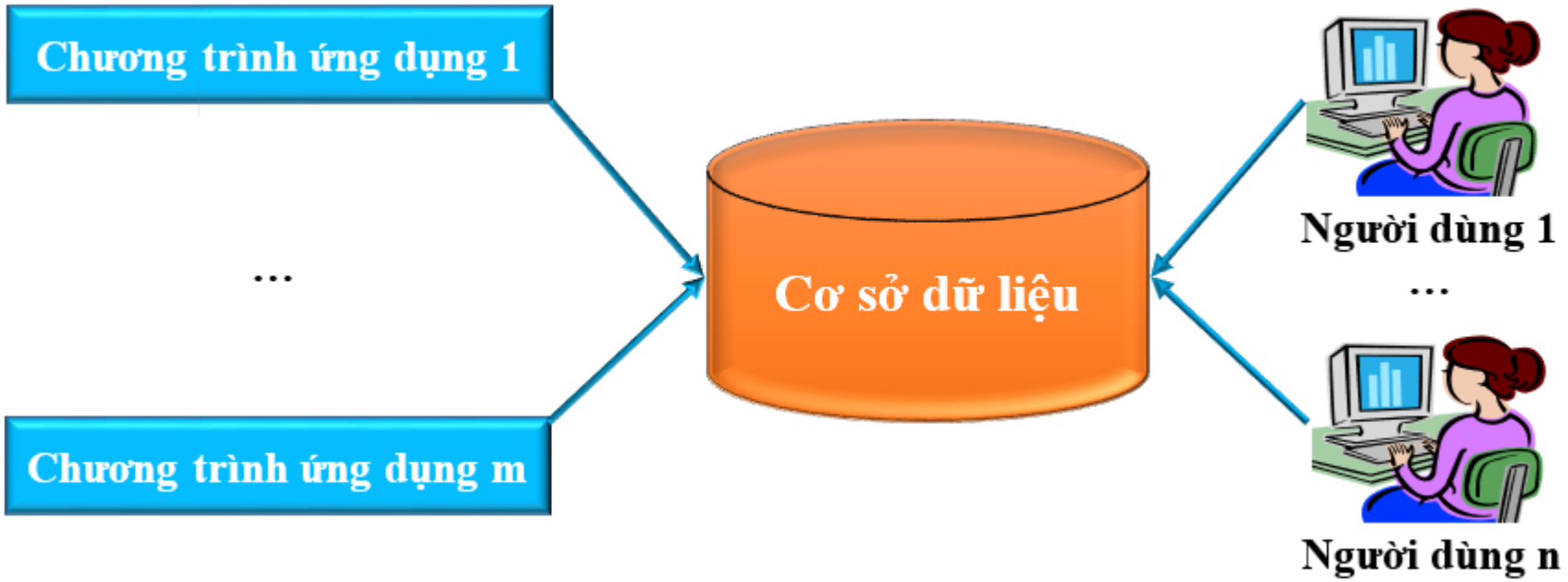
1.2. Tại sao phải bảo đảm an toàn CSDL

1.3. Các mối đe dọa an toàn CSDL

1.4. Các biện pháp bảo đảm an toàn CSDL

1.1. CSDL và các khái niệm liên quan

- **Cơ sở dữ liệu (CSDL):** *là một tập hợp các dữ liệu có liên quan với nhau chứa thông tin về một tổ chức nào đó (xí nghiệp, ngân hàng, bệnh viện, cơ quan,...) được lưu trữ trên các thiết bị nhớ thứ cấp (băng từ, đĩa từ,...) để đáp ứng nhu cầu khai thác thông tin của nhiều người sử dụng với nhiều mục đích khác nhau.*



1.1. CSDL và các khái niệm liên quan

- **Các đặc trưng của CSDL:**
  - Bền vững (Thường trú): Dữ liệu được lưu trên các thiết bị lưu trữ ổn định, cho phép sử dụng nhiều lần.
  - Liên kết (Tương tác): Dữ liệu được lưu trữ như những đơn vị riêng biệt, được liên kết với nhau (liên kết giữa các tập thực thể) tạo nên một tổng thể chung.
  - Chia sẻ: Cơ sở dữ liệu có thể có nhiều người dùng và có thể truy xuất đồng thời.

1.1. CSDL và các khái niệm liên quan

- **Ví dụ về CSDL:**
  - CSDL sinh viên trong một trường đại học
  - CSDL cán bộ viên chức trong một đơn vị hành chính sự nghiệp
  - CSDL hàng hóa trong siêu thị
  - CSDL của doanh nghiệp
  - CSDL quốc gia về dân cư
  - CSDL đất đai quốc gia
  - CSDL quốc gia về tài chính

1.1. CSDL và các khái niệm liên quan

- **Các đối tượng sử dụng CSDL:**
  - Người thiết kế CSDL
  - Người quản trị CSDL
  - Người lập trình ứng dụng
  - Người dùng cuối

1.1. CSDL và các khái niệm liên quan

- **Hệ quản trị CSDL (Database Management System - DBMS):** *Là một hệ thống phần mềm cho phép tạo lập CSDL, duy trì và điều khiển mọi truy nhập đối với CSDL đó*

  --> Hệ QTCSDL cung cấp môi trường thuận lợi, đơn giản và hiệu quả để người sử dụng có thể tạo lập, lưu trữ và thao tác trên CSDL mà không cần quan tâm nhiều đến thuật toán chi tiết và cách biểu diễn dữ liệu trong bộ nhớ máy tính

1.1. CSDL và các khái niệm liên quan

- **Các chức năng chính của một Hệ quản trị CSDL:**
  - Tổ chức dữ liệu
  - Thao tác dữ liệu
  - Lưu trữ và truy xuất dữ liệu một cách hiệu quả
  - Bảo đảm tính toàn vẹn và tính nhất quán của dữ liệu
  - Bảo đảm và thực thi các chính sách và thủ tục bảo mật dữ liệu
  - Sao lưu và phục hồi CSDL

  Các chức năng khác:
  - Cung cấp các dịch vụ hỗ trợ cho tính độc lập dữ liệu
  - Cung cấp một số dịch vụ tiện ích

1.1. CSDL và các khái niệm liên quan

- **Ngôn ngữ trong Hệ quản trị CSDL:**
  - Ngôn ngữ định nghĩa dữ liệu (*Data Definition Language - DDL*): cho phép mô tả, định nghĩa các đối tượng của CSDL (kết quả của việc dịch các câu hỏi của DDL là một tập các bảng được lưu trữ trong một tệp đặc biệt được gọi là từ điển dữ liệu)
  - Ngôn ngữ thao tác dữ liệu (*Data Manipulation Language - DML*): dùng để thao tác, xử lý trên các đối tượng của CSDL (thêm, xoá, sửa, tìm kiếm thông tin)
  - Ngôn ngữ điều khiển dữ liệu (*Data Control Language - DCL*): kiểm soát, điều khiển việc truy cập vào CSDL (Hệ thống an ninh, Hệ thống ràng buộc toàn vẹn dữ liệu, Hệ thống điều khiển tương tranh, Hệ thống khôi phục CSDL)

1.1. CSDL và các khái niệm liên quan

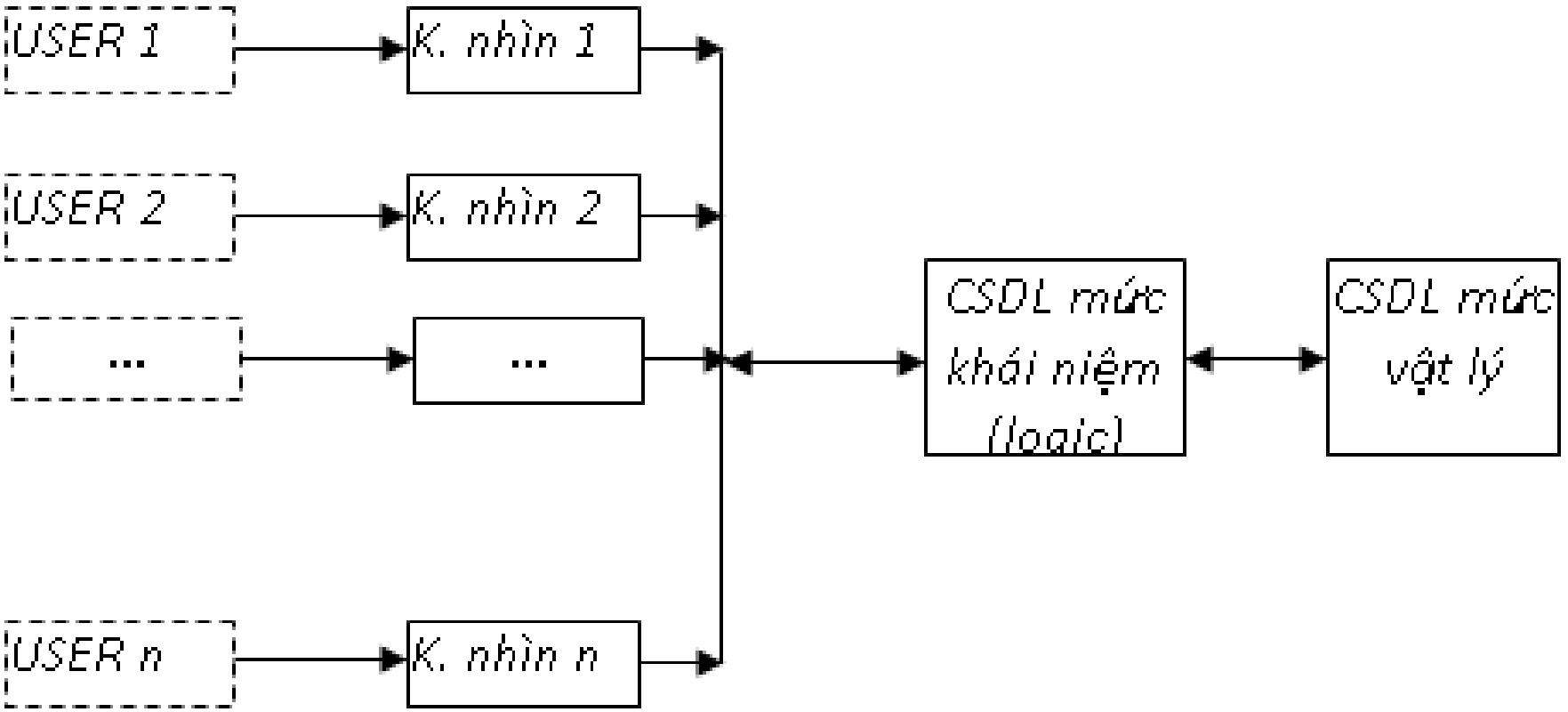
- **Một số hệ quản trị CSDL điển hình:**
  - Microsoft Access
  - DB2
  - FoxPro
  - Microsoft SQL Server
  - PostgreSQL
  - Oracle
  - MySQL
  - SQLite
  - …

1.1. CSDL và các khái niệm liên quan

- **Hệ CSDL:** hệ thống gồm 4 thành phần:
  - CSDL hợp nhất: có tính chất tối thiểu hóa và được chia sẻ
  - Những người sử dụng CSDL: những người có nhu cầu và có quyền truy nhập vào CSDL (Người thiết kế, Người quản trị CSDL, Người viết chương trình ứng dụng, Người dùng cuối)
  - Hệ quản trị CSDL
  - Phần cứng: gồm các thiết bị nhớ thứ cấp được sử dụng để lưu trữ CSDL

1.1. CSDL và các khái niệm liên quan

- **Kiến trúc Hệ CSDL:**
  - 3 mức: Mức vật lý, Mức khái niệm, Mức khung nhìn



1.1. CSDL và các khái niệm liên quan

- **Lợi ích của hệ CSDL:**
  - Giảm bớt dư thừa dữ liệu trong lưu trữ
  - Tránh được sự không nhất quán trong lưu trữ dữ liệu và bảo đảm được tính toàn vẹn của dữ liệu
  - Có thể triển khai đồng thời nhiều ứng dụng trên cùng một CSDL
  - Thống nhất các tiêu chuẩn, thủ tục và các chính sách bảo vệ, an toàn dữ liệu

1.1. CSDL và các khái niệm liên quan

- **Lược đồ CSDL (database schema):** là toàn bộ mô tả CSDL, gồm 3 loại:
  - Lược đồ ngoài (còn gọi là lược đồ con),
  - Lược đồ logic
  - Lược đồ vật lý
- **Thể hiện của CSDL (database instance):** toàn bộ dữ liệu lưu trữ trong CSDL tại một thời điểm nhất định
- **Tính độc lập dữ liệu:** 2 mức
  - Độc lập dữ liệu vật lý: là khả năng sửa đổi lược đồ vật lý mà không làm thay đổi lược đồ khái niệm
  - Độc lập dữ liệu mức logic: là khả năng sửa đổi lược đồ logic mà không làm thay đổi các khung nhìn → không phải viết lại các chương trình ứng dụng

1.1. CSDL và các khái niệm liên quan

- **Ràng buộc dữ liệu:** là các yêu cầu, quy định mà dữ liệu trong CSDL phải thoả mãn → nhằm bảo đảm tính độc lập và tính toàn vẹn dữ liệu, bảo đảm cho dữ liệu trong CSDL luôn phản ánh đúng các đối tượng
  - Ràng buộc kiểu: Mô tả tính chất của các thuộc tính khi tạo lập CSDL (tên thuộc tính, kiểu dữ liệu)
  - Ràng buộc giải tích: Là những ràng buộc giữa các thuộc tính được biểu diễn bằng các biểu thức toán học
  - Ràng buộc logic: Mối quan hệ giữa các thuộc tính với nhau không phải là các ràng buộc giải tích (được gọi là phụ thuộc hàm)

1.1. CSDL và các khái niệm liên quan

- **Mô hình dữ liệu:** *là một tập các khái niệm và kí pháp dùng để mô tả dữ liệu, mối quan hệ của dữ liệu, các ràng buộc trên quan hệ của một tổ chức (có thêm bao gồm tập hợp các phép toán cơ bản để đặc tả các thao tác trên CSDL như truy vấn và cập nhật dữ liệu)*

1.1. CSDL và các khái niệm liên quan

- **Các loại mô hình dữ liệu:**
  - Mô hình dữ liệu bậc cao (mô hình dữ liệu mức khái niệm): Mô hình thực thể - liên kết ER (Entity - Relationship Model)
  - Các mô hình dữ liệu bậc thấp (mô hình dữ liệu mức vật lý):
    + Mô hình hợp nhất (Unifying Model)
    + Mô hình bộ nhớ khung (Frame Memory Model)
  - Các mô hình dữ liệu thể hiện:
    + Mô hình quan hệ (Relational Model)
    + Mô hình phân cấp (Hierarchical Model)
    + Mô hình mạng (Network Model)

1.2. Tại sao phải bảo đảm an toàn CSDL

- **Tại sao phải bảo đảm an toàn CSDL:**
  - Hầu hết dữ liệu được tổ chức và lưu trữ dưới dạng CSDL: Theo thông tin từ Tạp chí An toàn thông tin - Ban cơ yếu chính phủ (2011), 90% dữ liệu trong máy tính được lưu trữ dưới dạng CSDL
  - CSDL là một trong các thành phần cốt lõi, trọng yếu nhất, cung cấp dữ liệu cho các ứng dụng và các dịch vụ hoạt động, là tài sản thông tin vô cùng giá trị của các tổ chức rất cần được bảo vệ, đồng thời cũng là một trong những mục tiêu tấn công hấp dẫn hàng đầu của các tin tặc.

1.2. Tại sao phải bảo đảm an toàn CSDL

- **Tại sao phải bảo đảm an toàn CSDL (tiếp):**
  - Mặc dù CSDL có thể được cấu hình để chỉ lưu trữ và truy xuất dữ liệu cục bộ - trong nội bộ tổ chức - song hiện nay, do sự phổ biến của Internet, sự phát triển mạnh mẽ của các ứng dụng web, do nhu cầu chia sẻ thông tin ngày càng tăng → hầu hết các CSDL của các tổ chức được thiết kế theo xu hướng mở - cung cấp rộng rãi quyền truy cập cho đông đảo người dùng qua một số mạng và trên phạm vi toàn cầu - rất nhiều giao dịch trực tuyến được thực hiện có liên quan đến các CSDL → các CSDL rất dễ bị xâm phạm
  - Tội phạm tin học ngày càng được huấn luyện chuyên nghiệp, có trình độ cao, sử dụng nhiều kỹ thuật và công nghệ hiện đại, tấn công có tổ chức

→ Bảo đảm an toàn CSDL là hết sức cần thiết, là vấn đề có tầm quan trọng toàn cầu

1.2. Tại sao phải bảo đảm an toàn CSDL

- **Môi trường dữ liệu an toàn**
  - Triển khai nhiều lớp bảo mật trong các môi trường CSDL quan trọng là cách tiếp cận hiệu quả nhất để giảm thiểu rủi ro vi phạm dữ liệu.
  - Ví dụ: Xét tình huống người quản trị muốn bảo vệ mạng của mình khỏi các tệp đính kèm e-mail độc hại:
    + Tầng 1: Người quản trị cần tổ chức một khóa đào tạo cho người dùng về sự nguy hiểm của e-mail, hướng dẫn họ cách xác định các dấu hiệu tệp đính kèm e-mail là độc hại
    + Tầng 2: Triển khai bộ lọc được đặt trên máy chủ trao đổi để chặn và cách ly một số tệp đính kèm e-mail độc hại phổ biến
    + Tầng 3: Cấu hình tường lửa (firewall) để từ chối một số loại lưu lượng truy cập vào mạng, làm giảm thiểu rủi ro

1.2. Tại sao phải bảo đảm an toàn CSDL

- **Môi trường dữ liệu an toàn (tiếp)**
  - Có 3 lớp bảo mật chính cần được giải quyết để đạt được môi trường lưu trữ dữ liệu an toàn nhiều lớp:

    +Bảo mật CSDL

    +Bảo mật máy tính

    +Bảo mật mạng

    Mỗi lớp trên cung cấp cho kẻ xâm nhập một cơ hội để xâm nhập hệ thống, vì vậy để bảo mật CSDL một cách hiệu quả, người ta cần phải bảo mật môi trường CSDL cũng như chính CSDL!

1.2. Tại sao phải bảo đảm an toàn CSDL

- **Môi trường dữ liệu an toàn (tiếp)**
  - ***Bảo mật CSDL*:**
    + Là một tập hợp các quy trình, tiêu chuẩn, chính sách và công cụ đã được thiết lập để bảo vệ dữ liệu khỏi bị đánh cắp, lạm dụng và các xâm nhập, các hoạt động và các tấn công không mong muốn.
    + Liên quan đến sự cho phép và truy cập vào cấu trúc dữ liệu và dữ liệu chứa trong nó.

1.2. Tại sao phải bảo đảm an toàn CSDL

- **Môi trường dữ liệu an toàn (tiếp)**
  - ***Bảo mật CSDL (tiếp)*:**
    + Các công cụ được sử dụng để bảo mật CSDL thường được bao gồm và định cấu hình trong các gói phần mềm CSDL, khả năng của các gói này là khác nhau tùy theo nhà cung cấp (Oracle, MySQL, Microsoft SQL Server, …)
    + Các tính năng bảo mật CSDL phổ biến được cung cấp bởi các nhà cung cấp:
      - Kiểm soát truy cập mức CSDL
      - Xác thực mức CSDL
      - Mã hóa lưu trữ dữ liệu

1.2. Tại sao phải bảo đảm an toàn CSDL

- **Môi trường dữ liệu an toàn (tiếp)**
  - ***Bảo mật máy tính*:**
    + Là một tập hợp các quy trình, tiêu chuẩn, chính sách và công cụ đã được thiết lập để bảo vệ máy tính khỏi bị đánh cắp, lạm dụng và các xâm nhập, các hoạt động và các tấn công không mong muốn.
    + Thường được xác định bởi hệ điều hành được sử dụng trên máy tính (khác nhau tùy theo nhà cung cấp và phiên bản hệ điều hành).

1.2. Tại sao phải bảo đảm an toàn CSDL

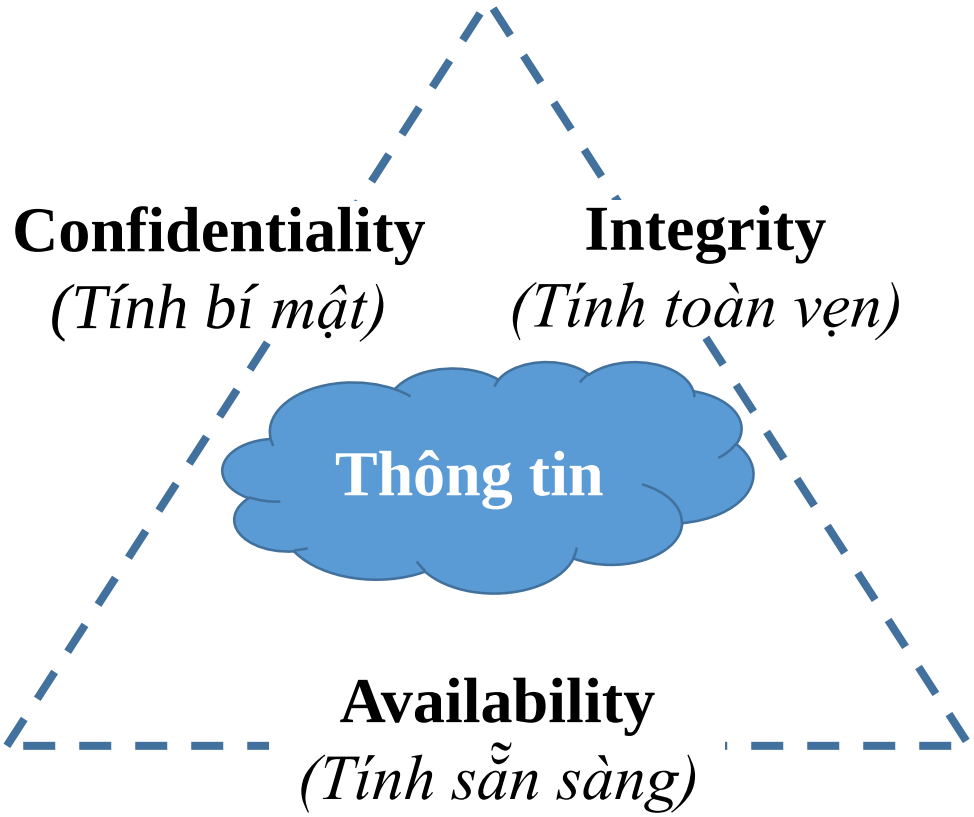
- **Môi trường dữ liệu an toàn (tiếp)**
  - ***Bảo mật máy tính (tiếp)*:**
    + Các tính năng bảo mật máy tính phổ biến:
      - Kiểm soát truy cập mức hệ điều hành
      - Xác thực mức hệ điều hành
      - Bảo mật ứng dụng
      - Giám sát, ghi nhật ký phần cứng và phần mềm

1.2. Tại sao phải bảo đảm an toàn CSDL

- **Môi trường dữ liệu an toàn (tiếp)**
  - ***Bảo mật mạng (An ninh mạng)*:**
    + Là tập hợp các quy trình, tiêu chuẩn, chính sách và công cụ đã được thiết lập để bảo vệ mạng khỏi bị đánh cắp, lạm dụng và các xâm nhập, các hoạt động và các tấn công không mong muốn.
    + Để bảo đảm an ninh mạng, cần có sự kết hợp giữa các thiết bị phần cứng và phần mềm, có thể bao gồm: tường lửa, các chương trình diệt vi-rút, giám sát mạng, các hệ thống phát hiện xâm nhập, các máy chủ proxy và các máy chủ xác thực, …

1.2. Tại sao phải bảo đảm an toàn CSDL

- **Mục tiêu bảo mật CSDL:**
  - Tam giác C.I.A



1.2. Tại sao phải bảo đảm an toàn CSDL

- **Mục tiêu bảo mật CSDL (tiếp):**
  - ***Tính bí mật (Confidentiality):***
    + Tính bí mật đề cập đến những nỗ lực được thực hiện thông qua chính sách, thủ tục và thiết kế để tạo và duy trì tính riêng tư của thông tin và các hệ thống. Để bảo đảm tính bí mật của hệ thống cần thực hiện:
      - Bảo đảm duy trì tính riêng tư của thông tin bằng cách giới hạn truy cập được ủy quyền vào các tài nguyên
      - Ngăn chặn quyền truy cập trái phép vào tài nguyên
    + Tính bí mật của các tài nguyên trong một hệ thống CSDL được bảo vệ thông qua biện pháp xác thực và điều khiển truy cập. Ví dụ: Người quản trị CSDL có thể sử dụng thông tin đăng nhập của một người dùng để hạn chế quyền truy cập của họ trong CSDL hoặc môi trường CSDL, từ đó duy trì tính bí mật.

1.2. Tại sao phải bảo đảm an toàn CSDL

- **Mục tiêu bảo mật CSDL (tiếp):**
  - ***Tính bí mật (tiếp):***
    + Tính bí mật không phải lúc nào cũng do người quản trị tùy ý quyết định. Nó còn bị chi phối bởi luật pháp hoặc các quy định của tổ chức. Các luật/quy định này yêu cầu người quản trị mạng duy trì một mức độ bảo mật nhất định để bảo đảm tính riêng tư của thông tin.
    + Tính bí mật là một mục tiêu quan trọng cần đạt trong các nỗ lực bảo mật. Các vi phạm tính bí mật có thể dẫn đến một số hậu quả vô cùng nghiêm trọng: danh tính bị đánh cắp, bí mật thương mại của doanh nghiệp bị lộ, chi phí khắc phục thảm họa lớn, danh tiếng bị ảnh hưởng, những tổn hại nghiêm trọng về cơ sở hạ tầng, ...

1.2. Tại sao phải bảo đảm an toàn CSDL

- **Mục tiêu bảo mật CSDL (tiếp):**
  - ***Tính toàn vẹn (Integrity):***
    + Tính toàn vẹn đề cập đến những nỗ lực được thực hiện thông qua các chính sách, thủ tục và thiết kế để tạo và duy trì thông tin và các hệ thống tin cậy, nhất quán và đầy đủ.
    + Tính toàn vẹn trong CSDL đề cập đến độ tin cậy, chính xác và tính nhất quán của dữ liệu được lưu trữ/truy xuất từ CSDL. Tính toàn vẹn của một CSDL được bảo vệ bằng cách ngăn chặn các sửa đổi dù là được phép hay trái phép, dù là vô tình hay cố ý mà có thể khiến việc lưu trữ hoặc truy xuất CSDL không đáng tin cậy và không nhất quán.

1.2. Tại sao phải bảo đảm an toàn CSDL

- **Mục tiêu bảo mật CSDL (tiếp):**
  - ***Tính toàn vẹn (tiếp):***
    + Một số hoạt động kiểm tra, đối chiếu là cần thiết nhằm phát hiện các thay đổi hoặc sai sót tồn tại trong toàn bộ CSDL. Quá trình này còn được gọi là kiểm toán.
    + Tính toàn vẹn là một đặc tính rất quan trọng của CSDL và nếu không được bảo đảm có thể dẫn đến các lỗi hệ thống, dữ liệu không đáng tin cậy, chương trình bị lỗi và hiệu suất kém.

1.2. Tại sao phải bảo đảm an toàn CSDL

- **Mục tiêu bảo mật CSDL (tiếp):**
  - ***Tính sẵn sàng (Availability):***
    + Tính sẵn sàng đề cập đến những nỗ lực được thực hiện thông qua các chính sách, quy trình và thiết kế để duy trì khả năng truy cập tài nguyên trên mạng hoặc trong CSDL (những tài nguyên này bao gồm: dữ liệu, ứng dụng, CSDL khác, máy tính, máy chủ, ứng dụng, tệp, ổ đĩa, chia sẻ và truy cập mạng, …)
    + Để bảo vệ các tài nguyên, cần xác định những mối đe dọa đối với tính sẵn sàng của CSDL, đánh giá mức độ đe dọa và lập kế hoạch can thiệp phù hợp.

1.2. Tại sao phải bảo đảm an toàn CSDL

- **Mục tiêu bảo mật CSDL (tiếp):**
  - ***Tính sẵn sàng (tiếp):***
    - + Các mối đe dọa tiềm ẩn phổ biến: các lỗi kỹ thuật (thiết bị bị lỗi hoặc bị hỏng, chương trình hoặc phần mềm bị lỗi, …), các thiên tai (lũ lụt, hỏa hoạn, …), các xâm nhập (vi rút, Trojan, sâu, ..) và người dùng (vô tình hoặc cố ý làm hại).
    - + Một doanh nghiệp không thể hoạt động được nếu CSDL không sẵn sàng. Mức độ không sẵn sàng càng lớn và kéo dài thì tổn thất sẽ càng lớn → cần xác định và lập kế hoạch duy trì, bảo đảm tính sẵn sàng

1.3. Các mối đe dọa an toàn CSDL

- **Hackers (Tin tặc):**
  - Hackers: Những người am hiểu, thành thạo về phần sụn, phần mềm của các hệ thống máy tính hiện đại và thích khám phá, phân tích bảo mật mạng mà không có ý định xâm nhập hoặc gây hại
  - Cracker: Những kẻ xâm nhập trái phép vào các hệ thống mạng nhằm phá hủy và/hoặc đánh cắp thông tin

→ 2 khái niệm trên thường được sử dụng nhầm lẫn, thay thế cho nhau

1.3. Các mối đe dọa an toàn CSDL

- **Hackers (tiếp):** Phân loại đối tượng xâm nhập trực tuyến

Loại	Định nghĩa	Ví dụ
Mũ trắng	Hacker có đạo đức: Sử dụng những kinh nghiệm và kiến thức rộng lớn của họ để kiểm tra và tư vấn bảo mật cho các hệ thống	Một nhà tư vấn bảo mật được một tổ chức thuê, sử dụng các phương pháp khác nhau để cố gắng xâm nhập vào hệ thống của họ nhằm kiểm tra tính bảo mật của hệ thống đó
Mũ xám	Cá nhân/nhóm cá nhân dao động giữa hacker và cracker; có lúc hành động theo hướng thiện chí và có lúc theo hướng ác ý	Một cá nhân đột nhập vào một trang báo điện tử, để lại lời cảnh báo trong CSDL cho người quản trị về các lỗ hổng đang tồn tại; một thời điểm khác, chính cá nhân này đã đột nhập vào hệ thống của một tổ chức, lấy cắp các thông tin nhạy cảm vì lợi ích cá nhân

1.3. Các mối đe dọa an toàn CSDL

- **Hackers (tiếp):** Phân loại đối tượng xâm nhập trực tuyến

Loại	Định nghĩa	Ví dụ
Mũ đen	Người đột nhập trái phép vào hệ thống với mục đích xấu (trộm cắp, phá hủy, …)	Một cá nhân đột nhập vào một hệ thống bán hàng, ăn cắp thông tin thẻ tín dụng của khách hàng nhằm mục đích xấu về tài chính
Hack tivist	Những hacker, cracker hoạt động vì mục đích chính trị	Một nhóm cực đoan chính trị chiếm quyền điều khiển một website có lượng truy cập lớn, hiển thị các nội dung, thông điệp chính trị nhằm chống phá nhà nước
Script kiddie	Một cracker nghiệp dư, thiếu kinh nghiệm thực hiện các tấn công mang tính thử nghiệm	Một cá nhân tìm kiếm, tải xuống một công cụ bẻ khóa trên mạng và sử dụng nó để xâm nhập vào hệ thống mạng của một tổ chức và đánh cắp thông tin

1.3. Các mối đe dọa an toàn CSDL

- **Social engineers:**
  - Kẻ tấn công sử dụng phương pháp Social engineering - một phương pháp phi kỹ thuật thông qua các tương tác xã hội để thao túng mọi người nhằm truy cập vào các hệ thống, các khu vực không được ủy quyền hoặc các thông tin bí mật.
  - Kẻ tấn công thường xây dựng niềm tin với những người dùng được ủy quyền, sau đó sử dụng các mánh khóe để đánh lừa, thuyết phục những người này phá vỡ các chính sách bảo mật thông thường (ví dụ: khéo léo hỏi mật khẩu của họ)

1.3. Các mối đe dọa an toàn CSDL

- **Users (Người dùng):** Hơn một nửa các vi phạm bảo mật xảy ra trên mạng liên quan đến người dùng mạng (do thiếu giáo dục, do sự coi thường chính sách, …). Các lỗi phổ biến của người dùng:
  - Thói quen bất lợi: rời khỏi máy tính mà không khóa/giám sát màn hình
  - Đặt mật khẩu dễ đoán hoặc làm lộ mật khẩu
  - Không tuân thủ chính sách của công ty, truy cập các trang web trái phép và tải xuống các phần mềm trái phép; gắn thiết bị trái phép vào máy tính (USB, ổ cứng ngoài); đăng nhập từ xa vào hệ thống thông qua một máy tính cá nhân không được chấp thuận
  - Mở e-mail lạ, xem hoặc tải các tệp tin độc hại đính kèm
  - Tiết lộ thông tin bí mật qua điện thoại, mạng xã hội, …
  - Không báo cáo kịp thời các sự cố máy tính hoặc sự cố mạng

  * Những người dùng am hiểu máy tính, những nhân viên bất mãn với tổ chức, … cũng là mối đe dọa với an toàn CSDL

1.3. Các mối đe dọa an toàn CSDL

- **Network and Database Administrators (Người quản trị mạng, quản trị CSDL):**
  - Những sai lầm ở cấp quản trị nếu có, hầu như chắc chắn sẽ gây hậu quả lớn cho tính toàn vẹn, tính bí mật và tính sẵn sàng
  - Vì CSDL có tính "động", tài khoản và quyền truy cập của người dùng cũng có thể thay đổi thường xuyên → dễ dẫn đến các lỗ hổng bảo mật → nếu người quản trị không kiểm tra và đánh giá lại CSDL và các vấn đề bảo mật một cách thường xuyên, toàn diện và đầy đủ sẽ có thể dẫn đến các lỗ hổng bảo mật lớn (ví dụ: Quên xóa tài khoản, quyền người dùng của các nhân viên bị sa thải)

1.3. Các mối đe dọa an toàn CSDL

- **Internet:** Cùng với sự phổ biến, và lợi ích to lớn mà Internet đem lại, đây cũng là môi trường lý tưởng thu hút một lượng lớn tội phạm thực hiện các cuộc tấn công, xâm nhập ngày càng tinh vi. Các công cụ người dùng sẵn có trên Internet cùng với các mối đe dọa tiềm ẩn của chúng:
  - Web Pages
  - Web Browsers
  - Misleading Applications
  - E-Mails
  - Instant Messages
  - Tweets

1.3. Các mối đe dọa an toàn CSDL

- **Internet:**
  - **Web Pages:**
    + Lướt/duyệt web có thể là một hoạt động nguy hiểm gây ra mối đe dọa lớn cho dữ liệu cá nhân/tổ chức. Một số trang web có thể bị tấn công (chiếm quyền điều khiển) và viết lại để phân phối phần mềm độc hại (malware) theo hoạt động của người dùng (VD: download) hoặc để chuyển hướng người dùng đến một trang web giả mạo được xây dựng bởi tin tặc (giả mạo URL, ví dụ: Gogle, Yaho, …)
    + Các trang web dễ bị tấn công
      - Các trang bất hợp pháp/có vấn đề về đạo đức
      - Các trang xã hội: MySpace, Facebook, Blogger, Twitter, ..
      - Các diễn đàn kỹ thuật, các nhóm tin tức: Usenet, BinSearch, …

1.3. Các mối đe dọa an toàn CSDL

- **Internet:**
  - **Web Browsers:**
    + Một công việc rất quan trọng của trình duyệt web là chuyển tiếp các yêu cầu của người dùng từ máy nguồn đến máy đích/máy chủ ứng dụng. Yêu cầu của người dùng xuất hiện khi người dùng nhập URL hoặc địa chỉ (ví dụ: http://www.yahoo.com) vào trường địa chỉ của trình duyệt hoặc khi một nút được kích hoạt trên biểu mẫu. Khi người dùng nhập địa chỉ, trình duyệt đọc địa chỉ này và gửi yêu cầu xem trang đến máy chủ Web. URL có thể bị thao túng và kẻ xâm nhập có thể sử dụng chúng để có quyền truy cập vào thông tin CSDL (SQL SQL injections).
    + Một số trình duyệt web phổ biến cùng là mục tiêu tấn công hàng đầu: Internet Explorer, Firefox, Netscape Navigator, Opera, …

1.3. Các mối đe dọa an toàn CSDL

- **Internet:**
  - **Misleading Applications:**
    + Các ứng dụng lừa đảo đánh lừa người dùng tin rằng bảo mật máy tính của họ đã bị vi phạm, do đó lừa người dùng tải xuống hoặc mua các công cụ chống vi-rút giả mạo để loại bỏ các vi phạm không có thật. Các ứng dụng này thường rất đáng tin cậy và có thể trông giống như các công cụ diệt phần mềm gián điệp và diệt virus thông thường.
    + Khi người dùng thực hiện một số hoạt động, ví dụ nhấp chuột vào liên kết hoặc cài đặt phần mềm và sau khi tải xuống, các ứng dụng này sẽ chiếm quyền điều khiển PC, lấy thông tin cá nhân, phá hủy tệp hoặc thu thập dữ liệu.
    + Các ứng dụng này được tìm thấy trên Internet, trong các trang web chia sẻ, các trang xã hội và các nhóm tin tức, hoặc ẩn trong các biểu ngữ, các quảng cáo, cũng như trong mã lập trình của các trang web hợp pháp.

1.3. Các mối đe dọa an toàn CSDL

- **Internet:**
  - **E-Mails:**
    + Thư điện tử đã trở thành một trong những hình thức giao tiếp phổ biến nhất trong xã hội ngày nay, được sử dụng để gửi các thông tin quan trọng, nhạy cảm, cá nhân và các thông tin kinh doanh hàng ngày. Đây cùng là một kênh tấn công hàng đầu của các cracker.
    + Cách tấn công phổ biến nhất là tấn công bằng mã độc nhằm chiếm quyền truy cập vào một doanh nghiệp. Cùng với các lỗ hổng cơ bản đi kèm với việc gửi và nhận e-mail, các tài khoản e-mail mang các lỗ hổng đi kèm với các trình duyệt. Các mối đe dọa phổ biến nhất đối với e-mail là các tấn công qua tệp tin đính kèm, lừa đảo và tấn công mã HTML.

1.3. Các mối đe dọa an toàn CSDL

- **Internet:**
  - **E-Mails (tiếp):**
    + *Tệp đính kèm (Attachments)*: Là mối đe dọa lớn nhất đối với hệ thống e-mail, các Cracker có thể gửi kèm vô số chương trình độc hại (sẽ phát huy tác hại khi người dùng tải xuống và mở/khởi chạy chúng) bằng cách:
      - Sử dụng các địa chỉ e-mail giả mạo (ví dụ: địa chỉ e-mail được đánh cắp từ các trường "From" và "Reply" của một tài khoản e-mail) nhằm đánh lừa người dùng tin rằng người gửi là bạn bè hoặc đồng nghiệp của họ
      - Sử dụng chiến lược đặt tên tệp (tên chính hoặc phần mở rộng) nhằm cố gắng khiến người nhận tin rằng các tệp có liên quan đến công việc của họ và mở chúng ra

1.3. Các mối đe dọa an toàn CSDL

- **Internet:**
  - **E-Mails (tiếp):**
    + *Tệp đính kèm (Attachments) (tiếp)*: Xét kịch bản: Một Cracker gửi e-mail chứa tệp đính kèm độc hại tới 1.000 người. Mỗi người trong số 1.000 người mở tệp đính kèm này, khởi chạy mã độc cho phép gửi một bản sao danh sách liên hệ của họ trở lại cho cracker và bắt đầu tấn công máy người dùng. Quan trọng nhất, virus đã giành được quyền truy cập vào mạng, lan truyền, gây hại đến mạng, môi trường CSDL và các máy (bao gồm cả máy chủ) trên đường đi. Với mỗi máy bị ảnh hưởng, kẻ xâm nhập sẽ nhận được một danh sách liên lạc các địa chỉ e-mail, để tiếp tục tấn công → Hậu quả khôn lường!

1.3. Các mối đe dọa an toàn CSDL

- **Internet:**
  - **E-Mails (tiếp):**

    + *Lừa đảo (Attachments)*:
      - Là nỗ lực để có được thông tin nhận dạng (định danh) cá nhân (PII) của người dùng thông qua việc sử dụng các địa chỉ e-mail và URL giả mạo. Ví dụ: E-mail giả mạo từ công ty thông báo cho nhân viên về việc mật khẩu tài khoản của họ sắp hết hạn, cần thay đổi ngay lập tức bằng cách sử dụng liên kết được cung cấp trong e-mail
      - Bao gồm hành động thuyết phục người dùng nhấp vào liên kết để chuyển hướng đến trang web thuộc sở hữu của cracker nơi cracker có thể thực hiện các cuộc tấn công. Ví dụ: Gửi liên kết để xem thiệp chúc mừng điện tử/nghe bài hát, … giả mạo qua e-mail

1.3. Các mối đe dọa an toàn CSDL

- **Internet:**
  - **E-Mails (tiếp):**
    + *Web-embedded HTML (mã HTML nhúng trong Web)*:
      - Hiện nay, không cần thiết phải sử dụng Webmail để gửi và nhận tin nhắn dựa trên HTML. Các E-mail Client, đã nâng cấp từ các tệp văn bản đơn giản đến các tài liệu được định dạng. HTML cho phép e-mail được định dạng phông chữ, màu sắc và kiểu, cũng như nhiều tính năng định dạng khác như trong một ứng dụng xử lý văn bản. Nó cũng có thể bao gồm các ngôn ngữ kịch bản như JavaScript hoặc các điều khiển ActiveX → có thể bị thao túng bởi vi rút
      - Các chương trình độc hại có thể được nhúng trực tiếp vào mã lập trình của e-mail, vì vậy không thể dễ dàng chặn chúng như đối với các tệp đính kèm. Chỉ cần người dùng đọc e-mail, chúng lập tức thực hiện các cuộc tấn công (lấy thông tin, phá hủy các tệp và chuyển tiếp địa chỉ e-mail cho cá nhân đã tạo ra vi rút)

1.3. Các mối đe dọa an toàn CSDL

- **Internet:**
  - **Instant Messages:**
    + Một công cụ kết nối, giao tiếp, chia sẻ tệp và tổ chức các phiên trò chuyện ngắn, được sử dụng phổ biến để cải thiện dịch vụ khách hàng và xây dựng mối quan hệ khách hàng trong kinh doanh.
    + Các tin nhắn tức thời thường không an toàn và dễ bị tấn công do không mã hóa dữ liệu khi truyền tải tệp tin hoặc đối thoại ngang hàng. Vì vậy, đây là một môi trường lý tưởng để thực hiện kỹ thuật lừa đảo thông qua việc giả mạo (ví dụ: giả mạo tên bạn bè) và các kỹ thuật chuyển hướng người dùng, dẫn người dùng vào bẫy của các mã độc được xây dựng bởi các cracker phân phối trên các trang web.

1.3. Các mối đe dọa an toàn CSDL

- **Internet:**
  - **Tweets:**
    + Trang Twitter.com cung cấp một dịch vụ giống như blog thu nhỏ, cho phép người dùng có thể đăng các tin nhắn nhỏ (<= 140 ký tự, về hoạt động/trạng thái của người dùng) để bạn bè và các thành viên gia đình xem, người dùng có thể đăng một tweet bằng điện thoại di động, máy tính hoặc bất kỳ thiết bị nào có kết nối Internet.
    + Giống như tin nhắn tức thời, tweet có thể bao gồm hình ảnh và liên kết - gây ra mối đe dọa lớn, là mục tiêu tấn công thông qua các các kỹ thuật lừa đảo, giả mạo và chuyển hướng của các cracker.

1.3. Các mối đe dọa an toàn CSDL

- **Malware (Phần mềm độc hại):**
  - ***Phần mềm độc hại*:** Có khả năng thực hiện các tác vụ có hại và phá hoại trên máy tính của các nạn nhân. Chúng có thể được viết bằng rất nhiều ngôn ngữ lập trình khác nhau và có nhiều loại:
    + Vi rút máy tính (Computer viruses)
    + Sâu (Worms)
    + Trojans
    + Phần mềm gián điệp (Spyware)
    + Phần mềm quảng cáo (Adware)
    + Bots

1.3. Các mối đe dọa an toàn CSDL

- **Malware (tiếp):**
  - ***Các đặc điểm thường thấy trong mã độc*** (được tích hợp vào mã của vi rút, sâu, Trojan, … và hoạt động như các chiến lược phòng thủ để tránh bị phát hiện và loại bỏ):
    + *Tự mã hóa*
    + *Tàng hình*
    + *Đa hình*
    + *Thường trú*

1.3. Các mối đe dọa an toàn CSDL

- **Malware (tiếp):**
  - + *Tự mã hóa (Self-encryption)*: Vi rút thường được nhận dạng bằng chữ ký của chúng - một mẫu các ký tự được xác định cho một họ virus cụ thể. Hầu hết các chương trình chống vi rút sử dụng các kỹ thuật quét nhận dạng chuỗi ký tự để xác định chữ ký của vi rút trên một mạng. Tuy nhiên, nếu vi rút có khả năng ngụy trang thì các chương trình chống vi rút thông thường sẽ rất khó nhận ra vi rút.

1.3. Các mối đe dọa an toàn CSDL

- **Malware (tiếp):**
  + *Tàng hình (Stealth)*:
    - Mỗi chương trình được cài đặt trên một hệ thống sẽ tạo ra các thay đổi nhất định trên hệ thống (sử dụng bộ nhớ, tăng kích thước tệp tin, …). Khi chương trình xâm nhập vào hệ thống, sự thay đổi là không thể tránh khỏi. Các chương trình chống vi rút thường xuyên theo dõi các thay đổi này bằng cách yêu cầu thông tin từ hệ điều hành (HĐH) nhằm tìm kiếm các tệp hệ thống bị thay đổi trái phép, các mục đăng ký đáng ngờ, ... Nếu tìm thấy thay đổi, các chương trình chống vi rút sẽ tìm cách tấn công.

1.3. Các mối đe dọa an toàn CSDL

- **Malware (tiếp):**
  + *Tàng hình (tiếp)*:
    - Vi rút tàng hình thường tìm cách che giấu mọi thay đổi mà chúng tạo ra: Chặn các yêu cầu từ các chương trình chống vi rút và trả lời chúng thay cho HĐH; cung cấp thông tin cho các chương trình chống vi rút, làm cho sự xuất hiện của chúng như thể không gây ra bất kỳ thay đổi nào đối với hệ thống, từ đó đánh lừa chương trình chống vi rút tin rằng hệ thống không có vi-rút.
    - Khi người dùng không biết về sự hiện diện của chúng, vi-rút tàng hình trên hệ thống sẽ phá hủy các tệp hoặc thu thập thông tin nhạy cảm trong một thời gian dài.

1.3. Các mối đe dọa an toàn CSDL

- **Malware (tiếp):**
  + *Đa hình (Polymorphism)*:
    - Đa hình liên quan đến khả năng thay đổi hình thức, hoặc tự sửa đổi. Các virus sử dụng tính đa hình như một biện pháp phòng vệ cho phép mã hóa lên một cấp độ khác bằng cách thay đổi hình thức sau mỗi lần lây nhiễm (mã đa hình thay đổi chữ ký của nó mỗi khi nó lây nhiễm một tệp và mỗi tệp bị lây nhiễm bởi một bản sao khác nhau của mã gốc) → chúng là mối đe dọa nghiêm trọng và khó phát hiện nhất!

1.3. Các mối đe dọa an toàn CSDL

- **Malware (tiếp):**

  + *Thường trú (Residence)*:

    - Vi rút không thường trú: Loại vi rút yêu cầu người dùng khởi chạy nó bằng cách tải xuống một chương trình hoặc mở một tệp đính kèm e-mail. Chúng không thể gây ảnh hưởng đến một hệ thống trừ khi được người dùng kích hoạt. Khi hoạt động, những vi rút này thường tấn công phần mềm nằm trên ổ cứng.
    - Vi rút thường trú (phổ biến hơn): Loại vi rút tự cài đặt hoặc cư trú trực tiếp trong bộ nhớ chính của hệ thống máy tính (RAM). Không cần người dùng kích hoạt, chúng có thể tấn công bất kỳ chương trình nào được kích hoạt trên hệ thống máy tính. Chúng thường tận dụng tính năng đa nhiệm của hệ thống máy tính, do đó có thể lây nhiễm các chương trình với tốc độ rất nhanh, dẫn đến yêu cầu cài đặt lại hầu hết các phần mềm trên máy tính.

1.3. Các mối đe dọa an toàn CSDL

- **Malware (tiếp):**

  + *Thường trú (Residence)*:

    - Vi rút không thường trú: Loại vi rút yêu cầu người dùng khởi chạy nó bằng cách tải xuống một chương trình hoặc mở một tệp đính kèm e-mail. Chúng không thể gây ảnh hưởng đến một hệ thống trừ khi được người dùng kích hoạt. Khi hoạt động, những vi rút này thường tấn công phần mềm nằm trên ổ cứng.
    - Vi rút thường trú (phổ biến hơn): Loại vi rút tự cài đặt hoặc cư trú trực tiếp trong bộ nhớ chính của hệ thống máy tính (RAM). Không cần người dùng kích hoạt, chúng có thể tấn công bất kỳ chương trình nào được kích hoạt trên hệ thống máy tính. Chúng thường tận dụng tính năng đa nhiệm của hệ thống máy tính, do đó có thể lây nhiễm các chương trình với tốc độ rất nhanh, dẫn đến yêu cầu cài đặt lại hầu hết các phần mềm trên máy tính.

1.3. Các mối đe dọa an toàn CSDL

- ***Virus máy tính***
  - ***Các lớp vi rút (Classes of Viruses)*:**
    + *Logic bomb và Time bomb*: Các loại virus không hoạt động cho đến khi các điều kiện cụ thể xác định trước được đáp ứng. Những vi rút này có thể nằm im và không bị phát hiện trong một thời gian dài trước khi chúng bắt đầu gây hại.
      - *Time boms* thường liên quan đến các điều kiện mà các biến là thời gian/ngày/các ngày cụ thể. Ví dụ: Một Time bomb được viết để phá hủy các hệ thống nhất định vào các khoảng thời gian đều đặn (VD: vào mỗi thứ 3) hoặc phá hủy một lần vào một ngày được chỉ định. Các biến và điều kiện được xác định trước và được viết trong mã của vi rút.
      - *Logic bombs* có thể có vô số biến, những điều kiện thường phụ thuộc vào môi trường cư trú. Ví dụ: một Logic bomb có thể được viết để phá hủy dữ liệu hoặc các hệ thống chỉ khi một người dùng cụ thể đăng nhập vào mạng hoặc chỉ khi một tên cụ thể xuất hiện trong truy vấn CSDL.

1.3. Các mối đe dọa an toàn CSDL

- ***Virus máy tính* (tiếp):**
  - ***Các lớp vi rút (tiếp)*:**
    + *Phần mềm gián điệp (Spyware)*:
      - Các phần mềm cố tình theo dõi và ghi lại các hoạt động trên một máy tính và/hoặc trên Internet của người dùng. Chúng thu thập các thông tin nhạy cảm về người dùng hoặc doanh nghiệp, biên dịch thông tin này thành một số loại tài liệu hoặc gói tin, sau đó chuyển thông tin này trở lại cho người khởi tạo/tạo chúng.
      - Phần mềm gián điệp thường được tải xuống và/hoặc cài đặt một cách tình cờ từ chính người dùng Internet, tuy nhiên chúng cũng có thể được cài đặt thủ công trên một máy tính cá nhân.

1.3. Các mối đe dọa an toàn CSDL

- ***Virus máy tính* (tiếp):**
  - ***Các lớp vi rút (tiếp)*:**

    + Phần mềm quảng cáo (Adware):

    - Sử dụng các kỹ thuật xâm nhập bằng phần mềm độc hại điển hình để lấy dữ liệu tiếp thị hoặc quảng cáo một sản phẩm hoặc dịch vụ.
    - Dạng điển hình: Thu thập thông tin cho mục đích nghiên cứu thị trường/quảng cáo và nghiên cứu thị trường thông qua việc sử dụng các phần mềm hấp dẫn - miễn phí hoặc chi phí thấp cho người dùng. Một số phần mềm quảng cáo, sau khi được cài đặt, sẽ tự động bật các chương trình quảng cáo dưới dạng cửa sổ pop-ups và chuyển hướng trang web. Ví dụ: một trang web có thể cung cấp một phần mềm lập lịch và tổ chức các cuộc họp miễn phí, sau khi được tải xuống, sẽ đồng thời thu thập thông tin về các hoạt động trên Internet của người dùng nhằm mục đích nghiên cứu thị trường hoặc quảng cáo cá nhân hóa cũng là một dạng phần mềm gián điệp.

1.3. Các mối đe dọa an toàn CSDL

- ***Virus máy tính* (tiếp):**
  - ***Các lớp vi rút (tiếp)*:**
    + *Phần mềm quảng cáo (tiếp)*:
      - Một dạng khác: Tự động bật quảng cáo trên một máy tính cá nhân của người dùng khi một phần mềm miễn phí được cài đặt và sử dụng. Các quảng cáo có thể được hiển thị bằng cách sử dụng cửa sổ pop-ups và chuyển hướng trang web. Hình thức phần mềm quảng cáo này có thể chiếm một lượng lớn tài nguyên trên mạng hoặc hệ thống máy tính, khiến máy tính và/hoặc Internet trở nên chậm, thậm chí không thể sử dụng được.
      - Nhìn chung, thường không được thiết kế với mục đích gây hại cho một máy tính cá nhân của người dùng, một mạng hoặc một môi trường CSDL.

1.3. Các mối đe dọa an toàn CSDL

- ***Virus máy tính* (tiếp):**
  - ***Các loại vi rút (Virus Types)*:** Có nhiều dạng và thường được viết để tấn công các lỗ hổng, các đối tượng và khu vực cụ thể.

    + *Vi rút khởi động (Boot Sector Viruses)*:
      - Vi rút tự tải vào khu vực khởi động (boot sector) của ổ đĩa cứng máy tính. Khu vực khởi động là một khu vực của ổ đĩa cứng chứa các bản ghi (records) cần thiết cho tiến trình khởi động máy tính. Nếu khu vực này bị xâm phạm, thì toàn bộ quá trình khởi động cũng bị xâm phạm.
      - Thường xâm nhập vào một hệ thống thông qua một đĩa mềm bị nhiễm vi rút trong ổ đĩa mềm. Do những tiến bộ trong công nghệ, hầu hết các hệ thống máy tính mới không bao gồm các ổ đĩa mềm như một thiết bị phần sụn mặc định, do đó, vi rút khởi động không phổ biến như trước đây.

1.3. Các mối đe dọa an toàn CSDL

- ***Virus máy tính* (tiếp):**
  - ***Các loại vi rút (tiếp)*:** Có nhiều dạng và thường được viết để tấn công các lỗ hổng, các đối tượng và khu vực cụ thể.

    + *Vi rút Macro (Macro Viruses)*:
      - Là một chương trình nhỏ cho phép người dùng tự động hóa một số lượng lớn các xử lý mang tính lặp lại trong một tài liệu. Thường được tìm thấy trong nhiều ứng dụng liên quan đến Office, chẳng hạn như chương trình xử lý văn bản, chương trình kết xuất bảng tính.
      - Có thể được gắn vào một macro hoặc thay thế một macro trong tài liệu, chúng tự động chạy khi tài liệu chứa macro bị nhiễm được mở hoặc đóng. Vì các tài liệu này rất phổ biến, người dùng hay mở và chia sẻ chúng nên vi-rút macro lan truyền khá nhanh và dễ dàng, thường là thông qua các tệp đính kèm e-mail.

1.3. Các mối đe dọa an toàn CSDL

- ***Virus máy tính* (tiếp):**
  - ***Các loại vi rút (tiếp)*:**
    + *Vi rút Macro (tiếp)*:
      - Khi vi rút macro được khởi tạo, nó sẽ ảnh hưởng đến tất cả các tài liệu cùng loại trên máy tính hoặc ổ đĩa mạng đó. Các tài liệu bị ảnh hưởng bao gồm những tài liệu đã được lưu và bất kỳ tài liệu nào sẽ được lưu trong tương lai. Những vi rút này rất dễ viết và có thể khá nguy hiểm. Chúng phá hủy dữ liệu, cài đặt phần mềm bên ngoài và trong một số trường hợp, như vi rút Melissa nổi tiếng năm 1999, chúng có thể phá hủy toàn bộ hệ thống mạng máy tính.

1.3. Các mối đe dọa an toàn CSDL

- ***Virus máy tính* (tiếp):**
  - ***Các loại vi rút (tiếp)*:**
    + *Vi rút tệp tin (File-infected viruses)*:
      - Hầu hết vi rút tệp tin đến từ những người dùng trên Internet (VD: khi người dùng tải xuống các tệp đính kèm e-mail, chuyển tệp qua tin nhắn tức thời và tải xuống các chương trình).
      - Không giống như vi rút macro tấn công dữ liệu trong một tệp, vi rút tệp tin sẽ tự gắn vào tệp thực thi, người dùng phải chạy nó trước khi nó có thể lây lan và phá hủy hệ thống. Vi rút tệp tin có thể bắt đầu dưới dạng vi rút không thường trú được tải xuống từ Internet và yêu cầu một hành động của người dùng để có thể hoạt động. Khi vi rút hoạt động, chúng trở thành vi rút thường trú bằng cách sao chép chính chúng vào bộ nhớ hệ thống và phá hoại hệ thống máy tính.

1.3. Các mối đe dọa an toàn CSDL

- ***Virus máy tính* (tiếp):**
  - ***Các loại vi rút (tiếp)*:**
    + *Multipartite viruses*:
      - Kết hợp các đặc điểm của vi rút khởi động và vi rút tệp tin. Có thể kích hoạt theo cách tương tự như một vi rút tệp tin. Tuy nhiên, sự khác biệt là nó cũng lây nhiễm vào bản ghi khởi động (boot record) của khu vực khởi động trên ổ đĩa cứng, do đó, ở lần khởi động tiếp theo, vi rút sẽ được phân phối trên toàn bộ hệ thống.

1.3. Các mối đe dọa an toàn CSDL

- **Sâu (Worms):**
  - ***Sâu máy tính*:** Là phần mềm độc hại có khả năng tự nhân bản và tự lây lan. Chúng có khả năng khai thác sức mạnh của các mạng và sử dụng sức mạnh này trong các cuộc tấn công của chúng chống lại các mạng. Chúng không cần đến người dùng để di chuyển từ máy tính này sang máy tính khác, chúng thường lây lan trên các mạng (Ví dụ: Internet).
  - Sâu chiếm quyền kiểm soát một máy tính, sử dụng điểm yếu và lỗ hổng đã học được trong khi duy trì quyền kiểm soát máy tính mục tiêu trước đó. Sâu sử dụng thông tin từ máy tính hiện đang là nạn nhân của nó để tìm kiếm các lỗ hổng trong các hệ thống gần đó. Khi các lỗ hổng này được xác định, sâu tấn công các lỗ hổng này và chiếm quyền kiểm soát máy tính mục tiêu tiếp theo. Sâu lặp lại mô hình này khi nó di chuyển qua các mạng và phá hủy các hệ thống trên đường đi.

1.3. Các mối đe dọa an toàn CSDL

- **Sâu (Worms):**
  - ***Quy trình di chuyển qua mạng của sâu*:**
    1. *Tìm kiếm các lỗ hổng*: Xác định và tận dụng các lỗ hổng (VD: e-mail, các trang chia sẻ tệp và mật khẩu không an toàn) để xâm nhập vào mạng và tiến gần hơn đến mục tiêu CSDL tiềm năng, sau đó sử dụng mã của nó để có được nạn nhân đầu tiên.
    2. *Kiểm soát máy tính*: Khi sâu đạt được quyền truy cập vào mục tiêu đã xác định, nó sẽ tự cài đặt vào hệ thống sau đó thực thi các hành động phá hoại theo các chỉ thị định trước: xóa các tệp khỏi máy, mở cửa sau vào hệ thống (back door: đường dẫn được tạo để cho phép truy cập trái phép, tránh tất cả các biện pháp an ninh môi trường và hệ thống) hoặc thực hiện các tấn công từ chối dịch vụ (DoS - tấn công giữ cho các tài nguyên hệ thống luôn bận rộn do đó tạm dừng các chức năng bình thường) trên toàn mạng.

1.3. Các mối đe dọa an toàn CSDL

- **Sâu (Worms):**
  - ***Quy trình di chuyển qua mạng của sâu (tiếp)*:**
    3. *Thẩm vấn máy*: Sau khi phá hủy mục tiêu đầu tiên, sâu bắt đầu tìm kiếm mục tiêu mới bằng cách thẩm vấn hệ thống mà nó đang cư trú. Địa chỉ e-mail và cấu hình mạng được tìm kiếm trong máy tính gần đó để khai thác. Các truy vấn DNS được thực hiện cho các máy chủ DNS gần nhất, tìm cách lấy địa chỉ IP của các máy gần đó. Nhiều thông tin được phát hiện trong quá trình này.
    4. *Thử nghiệm một mục tiêu mới*: Sau khi thu thập các thông tin về địa chỉ IP, địa chỉ e-mail và thông tin mạng lân cận, sâu sẽ gửi một loạt các gói đến các máy gần đó để thử nghiệm các lỗ hổng và các kỹ thuật mà sâu đã sử dụng để kiểm soát PC hiện tại. Dựa trên các thử nghiệm này, một mục tiêu mới được xác định và quá trình được lặp lại.

1.3. Các mối đe dọa an toàn CSDL

- **Sâu (Worms): - *Một số loại sâu*:**

Loại sâu	Mô tả
E-mail worm (Sâu e-mail)	Lan truyền từ e-mail sang e-mail bằng các thư có chứa tệp đính kèm bị nhiễm sâu hoặc liên kết chuyển hướng người dùng đến các trang web bị nhiễm sâu
Instant Messaging worm (Sâu tin nhắn tức thời)	Di chuyển từ messenger sang messenger bằng cách gửi các liên kết chuyển hướng người dùng đến các trang web bị nhiễm sâu (gửi cho toàn bộ danh sách bạn bè của mục tiêu)
Internet worm (Sâu Internet)	Di chuyển trên Internet bằng cách sử dụng các cuộc thăm dò Internet và các thông tin được tìm thấy trong một mục tiêu

1.3. Các mối đe dọa an toàn CSDL

- **Sâu (Worms): -** ***Một số loại sâu (tiếp)*****:**

Loại sâu	Mô tả
IRC (Internet Relay Chat) worm (Sâu IRC)	Di chuyển từ chat sang chat bằng cách gửi các tệp bị nhiễm sâu và chuyển hướng liên kết đến các trang web bị nhiễm sâu
File-sharing network worm (Sâu mạng chia sẻ tệp)	Di chuyển từ File-sharing network sang File-sharing network bằng cách tạo các bản sao của chính nó và đặt chúng vào một thư mục chia sẻ với một tên thích hợp

1.3. Các mối đe dọa an toàn CSDL

- **Trojan Viruses:**
  - Là các phần mềm độc hại hoàn chỉnh được cài đặt qua các lỗ hổng an ninh vào hệ thống do sơ suất của người dùng khi truy cập Internet
  - Có khả năng ngụy trang chính nó và mã độc của nó → khó bị phát hiện
  - Thường ẩn trong các chương trình hấp dẫn, có lợi cho người dùng (ví dụ một bản cập nhật phần mềm, một chương trình tiện ích, trò chơi, phim, … khiến người dùng tự download về và cài đặt)
  - Không có khả năng tự nhân bản
  - Mục đích chính của các Trojan là giành quyền truy cập vào hệ thống để có được các thông tin nhạy cảm, phá hủy các tệp quan trọng hoặc tạo cơ hội tải xuống và cài đặt các mối đe dọa lớn hơn (ví dụ: bot) vào hệ thống

1.3. Các mối đe dọa an toàn CSDL

- **Trojan Viruses (tiếp):**
  - Một số loại Trojan điển hình (phân loại theo mục đích):
    + Trojan truy cập và quản trị từ xa (RAT - Remote Access and administration Trojan): Cho phép cracker (người tạo ra Trojan đó) truy cập và điều khiển hoàn toàn máy tính nạn nhân từ xa, đồng thời cho phép cracker ghi lại nội dung (ví dụ: video, giọng nói từ webcam, micrô) → là loại Trojan nguy hiểm nhất.
    + Trojan gửi dữ liệu (Data-sending Trojan): Lấy dữ liệu nhạy cảm từ máy tính nạn nhân và gửi cho cracker. Phổ biến nhất là Key logger (ghi nhật ký nhấn phím và gửi cho cracker qua e-mail).

1.3. Các mối đe dọa an toàn CSDL

- **Trojan Viruses (tiếp):**
  - Một số loại Trojan điển hình (phân loại theo mục đích):
    + Trojan phá hủy (Destructive Trojan): Mục đích là phá hủy toàn bộ hệ thống. Chúng xóa ngẫu nhiên các tệp tin và các thư mục, làm hỏng registry. Nếu không bị phát hiện quá lâu, loại Trojan này sẽ khiến hệ điều hành bị lỗi và máy tính không hoạt động được.
    + Proxy Trojan: Cho phép cracker sử dụng máy tính của người khác để truy cập Internet và thực hiện các hành vi trộm cắp hoặc phạm tội khác qua mạng. Do địa chỉ IP được đăng ký với nhà cung cấp dịch vụ Internet và được sử dụng để nhận dạng người dùng trên Internet nên các hành vi trộm cắp, phạm tội này sẽ khiến nạn nhân bị vướng vào các cuộc điều tra pháp lý.

1.3. Các mối đe dọa an toàn CSDL

- **Bots:**
  - Còn được gọi là robot phần mềm do có khả năng thực hiện hàng loạt các tác vụ tự động cho kẻ đột nhập ở xa. Các tác vụ này có phạm vi rất lớn, từ spam hệ thống đến các cuộc tấn công DoS nhằm làm chậm thậm chí ngưng hoàn toàn hệ thống CSDL hoặc hệ thống mạng bằng cách làm ngập lụt/áp đảo với hàng loạt các yêu cầu.
  - Bot có thể ẩn trong các trò chơi và các chương trình hấp dẫn khác do người dùng vô tình tải xuống, hoặc ẩn trong các e-mail được gửi đi từ máy tính bị nhiễm sang các máy tính khác, hoặc được tải xuống từ các trang web bị nhiễm, hoặc có thể xâm nhập vào máy tính cá nhân thông qua các lỗ hổng được tìm thấy trong kiến trúc bảo mật.

1.3. Các mối đe dọa an toàn CSDL

- **Bots (tiếp):**
  - Việc loại bỏ và phát hiện bot thường yêu cầu sử dụng chương trình chống vi-rút đặc biệt được tạo riêng để tìm bot, tuy nhiên, thậm chí các chương trình dành riêng này cũng khó phát hiện ra bot vì:
    + Không phải tất cả các bot đều giống nhau
    + Bot biết cách tự cập nhật, các phiên bản mới của bot được tạo ra hàng ngày
    + Bot có khả năng ngụy trang để tránh bị phát hiện
    + Hoạt động thầm lặng
  - Do tính phức tạp của bot, việc phát hiện một bot thường yêu cầu cài đặt lại toàn bộ hệ thống (do người dùng không thể hoàn toàn chắc chắn rằng tất cả các bot đã bị xóa khỏi hệ thống)

1.3. Các mối đe dọa an toàn CSDL

- **Bots (tiếp):**
  - Bot chỉ là một thành phần trong sơ đồ lớn hơn để phá hủy các mạng: Khi một máy tính nằm dưới sự kiểm soát của bot, nó sẽ trở thành một phần của mạng bot, được gọi là botnet. Botnet này được kiểm soát bởi một cá nhân thường được gọi là botmaster. Botmaster tích lũy một số bot và sau đó cho những kẻ xâm nhập và tội phạm mạng thuê các botnet này với mục đích spam, lừa đảo và thực hiện các hành vi phạm tội nghiêm trọng khác qua mạng.

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Kiến trúc bảo mật:**
  - Có rất nhiều sự không chắc chắn trong lĩnh vực bảo mật. Việc tạo ra một kiến trúc bảo mật hiệu quả đảm bảo tính bí mật, tính toàn vẹn và tính sẵn sàng của môi trường CSDL không phải là một nhiệm vụ dễ dàng. Khi xem xét các bước để đạt được mục tiêu bảo mật, cần ghi nhớ: "*Bảo mật không bao giờ là 100% và các hệ thống không bao giờ có thể an toàn 100%!*"
  - Bảo mật là một chu trình không có hồi kết: Các kỹ thuật được sử dụng để tấn công CSDL và các hệ thống khác được phát triển sử dụng cùng một công nghệ bảo vệ các hệ thống này. Do đó, khi các hệ thống bảo mật trở nên tinh vi hơn thì virút, Trojan và sâu cũng trở nên tinh vi hơn; khi công nghệ trở nên tiên tiến hơn, những kẻ xâm nhập cũng vậy. Khi hệ thống bảo mật đạt đến mức "an toàn", một số cuộc xâm nhập mới sẽ được phát triển và quá trình bắt đầu lại từ đầu.

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Kiến trúc bảo mật:**
  - ***Quá trình tạo và duy trì kiến trúc bảo mật*:**
    + *Giai đoạn 1*: *Đánh giá, phân tích* (nhu cầu bảo mật dữ liệu)
      - Liên quan đến việc xác định các lỗ hổng, các mối đe dọa và các tài sản trong môi trường: các thiết bị, các tài nguyên và các mối quan hệ của các nhà cung cấp.
      - Kiểm toán bảo mật phải kỹ lưỡng và đầy đủ, cần tìm kiếm mọi loại mối đe dọa tiềm ẩn có thể tồn tại trong môi trường CSDL (từ các lỗ hổng kỹ thuật mang tính xã hội đến các lỗi tường lửa bên ngoài có trong bất kỳ lớp máy tính, mạng và CSDL nào)
      - Kiểm toán là một nhiệm vụ khó khăn, mất nhiều thời gian và nguồn lực để hoàn thành, có thể được thực hiện bởi một nhóm chuyên gia bảo mật trong nội bộ tổ chức hoặc bằng cách thuê một bên thứ ba (ví dụ một nhóm hacker mũ trắng).

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Kiến trúc bảo mật:**
  - ***Quá trình tạo và duy trì kiến trúc bảo mật*:**
    + *Giai đoạn 1 (tiếp)*:
      - Bằng cách xác định các rủi ro, xác định các mối đe dọa đối với tài sản và chi phí của tài sản bị vi phạm hoặc bị mất, cần ưu tiên lập kế hoạch cho các biện pháp hợp lý để chống lại các mối đe dọa này.
      - Các câu hỏi đặt ra trong giai đoạn 1:
        - Các thiết bị, tài nguyên trong môi trường CSDL là gì?
        - Loại đe dọa nào tồn tại trong môi trường CSDL?
        - Các tài sản nào cần được bảo vệ?
        - Giá trị của các tài sản?
        - Chi phí tổn thất gây ra bởi các mối đe dọa?
        - Khả năng xảy ra của mỗi mối đe dọa?
        - Mức bảo mật cần thiết để đối phó với mỗi mối đe dọa?

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Kiến trúc bảo mật:**
  - ***Quá trình tạo và duy trì kiến trúc bảo mật*:**
    + *Giai đoạn 1 (tiếp)*:
      - Các bước thực hiện trong giai đoạn 1:
        1. Lập danh sách tất cả các thiết bị và tài nguyên trong môi trường CSDL
        2. Xác định các lỗ hổng và các tài sản liên quan đến từng tài nguyên và thiết bị
        3. Xác định giá trị của các tài sản cũng như chi phí cho bất kỳ thiệt hại nào gây ra bởi các mối đe dọa
        4. Sự dụng thông tin từ Bước 2, cũng như hiểu biết về khả năng của từng mối đe dọa để tạo các biện pháp bảo mật chống lại các mối đe dọa này
        5. Ưu tiên các biện pháp bảo mật của bạn

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Kiến trúc bảo mật:**
  - ***Quá trình tạo và duy trì kiến trúc bảo mật*:**
    + *Giai đoạn 2*: *Thiết kế và mô hình hóa*
      - Bao gồm việc tạo ra các chính sách và kiến trúc bảo mật nguyên mẫu phù hợp với nhu cầu của một doanh nghiệp (dựa trên kết quả của giai đoạn 1): Tạo các chính sách và quy trình bảo mật, xác định các thay đổi phần sụn và phần mềm cần thiết, xác định các công cụ hoặc ứng dụng bảo mật cần sử dụng để giảm thiểu rủi ro.
      - Toàn bộ nhân viên trong tổ chức, từ nhân viên quản lý cấp cao, nhân viên quản lý nhân sự cho đến người dùng mạng cần tham gia vào giai đoạn này để biết được những nỗ lực bảo mật đang diễn ra, nhằm đảm bảo cho các chính sách tập trung chính xác và thực tế vào cả nhu cầu của người dùng và doanh nghiệp.

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Kiến trúc bảo mật:**
  - ***Quá trình tạo và duy trì kiến trúc bảo mật*:**
    + *Giai đoạn 2 (tiếp)*:
      - Các câu hỏi đặt ra trong giai đoạn 2:
        - Những chính sách nào cần được đưa ra để đáp ứng các mục tiêu bảo mật?
        - Để giảm thiểu các lỗ hổng và hỗ trợ cho các chính sách và các thủ tục bảo mật, cần thực hiện các thay đổi phần sụn và bổ sung các phần mềm nào?
        - Phần sụn và phần mềm sẽ được kiểm tra như thế nào?
        - Các bước để thực hiện kế hoạch là gì?
        - Cần đào tạo thêm những gì cho nhân viên?
        - Cách xác định thành công và thất bại?
        - Kế hoạch truyền thông là gì?
        - Truyền thông và đào tạo sẽ được triển khai như thế nào?

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Kiến trúc bảo mật:**
  - ***Quá trình tạo và duy trì kiến trúc bảo mật*:**
    + *Giai đoạn 2 (tiếp)*:
      - Các bước cần thực hiện trong giai đoạn 2:

      1. Xác định các chính sách, thủ tục cần được đưa ra
      2. Xác định các thay đổi phần sụn và phần mềm nhằm hỗ trợ các chính sách được xác định trong Bước 1
      3. Xác định kế hoạch thực hiện
      4. Tạo đường cơ sở để xác định thành công, thất bại
      5. Xác định kế hoạch đào tạo và nâng cao nhận thức của người dùng

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Kiến trúc bảo mật:**
  - ***Quá trình tạo và duy trì kiến trúc bảo mật*:**
    + *Giai đoạn 3*: *Triển khai*
      - Các chính sách bảo mật, phần sụn và các công cụ được xác định trong các giai đoạn trước được triển khai
      - Việc triển khai thường được thực hiện theo hình thức thử nghiệm ban đầu: Một môi trường thử nghiệm được tạo ra để mô phỏng môi trường triển khai. Phần sụn và phần mềm được mua và cũng được thử nghiệm để đảm bảo rằng các thay đổi không lường trước không làm ảnh hưởng đến toàn bộ việc triển khai và các mục tiêu bảo mật. Những thay đổi về đào tạo và nhận thức của người dùng cũng được đưa vào giai đoạn này.

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Kiến trúc bảo mật:**
  - ***Quá trình tạo và duy trì kiến trúc bảo mật*:**
    + *Giai đoạn 3 (tiếp)*:
      - Các câu hỏi đặt ra trong giai đoạn 3:
        - Điều chỉnh việc đào tạo người dùng đã được chấp nhận?
        - Tất cả thử nghiệm phần sụn và phần mềm có thành công không?
        - Các biện pháp bảo mật đã sẵn sàng để thực hiện triển khai toàn bộ trong môi trường hoạt động chưa?

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Kiến trúc bảo mật:**
  - ***Quá trình tạo và duy trì kiến trúc bảo mật*:**
    + *Giai đoạn 3 (tiếp)*:
      - Các bước được thực hiện trong giai đoạn 3:
        - Điều chỉnh đào tạo và nhận thức của người dùng dựa trên sự chấp nhận của người dùng
        - Thử nghiệm thay đổi phần sụn và phần mềm trong môi trường mô phỏng được kiểm soát
        - Triển khai các thay đổi được xác định theo kế hoạch triển khai

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Kiến trúc bảo mật:**
  - ***Quá trình tạo và duy trì kiến trúc bảo mật*:**
    + *Giai đoạn 4*: *Quản lý và hỗ trợ*
      - Bao gồm hỗ trợ, bảo trì và đánh giá liên tục kiến trúc bảo mật đã được triển khai trong giai đoạn 3.
      - Hiệu suất của hệ thống bảo mật được giám sát và bất kỳ lỗi hoặc vi phạm nào cũng sẽ dẫn đến việc đánh giá lại kiến trúc bảo mật.
      - Các chính sách bảo mật có thể có các thay đổi nhỏ, nhưng nếu có quá nhiều thay đổi nhỏ hoặc lỗi trong hệ thống thì cần yêu cầu lặp lại toàn bộ quy trình ngay từ đầu.

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Kiến trúc bảo mật:**
  - ***Quá trình tạo và duy trì kiến trúc bảo mật*:**

    + *Giai đoạn 4 (tiếp)*:

      - Các câu hỏi đặt ra trong giai đoạn 4:
        - Kế hoạch bảo mật có bảo vệ các tài sản định trước không?
        - Đã đầu tư đủ thời gian và tài nguyên vào các mối đe dọa và tài sản được ưu tiên cao chưa?
        - Các biện pháp bảo mật có tác động gì đến khả năng hoàn thành nhiệm vụ của người dùng?
        - Các biện pháp bảo mật có tác động gì đến khả năng hoàn thành một chức năng một cách bình thường của mạng?
        - Có cần thực hiện các sửa đổi nhỏ không?
        - Các biện pháp bảo mật đã hết hạn chưa?
        - Các vi phạm có tăng lên không?
        - Đã đến lúc đánh giá lại môi trường chưa?

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Kiến trúc bảo mật:**
  - ***Quá trình tạo và duy trì kiến trúc bảo mật*:**
    + *Giai đoạn 4 (tiếp)*:
      - Các bước thực hiện trong giai đoạn 4:
        - Giám sát hiệu suất của kiến trúc bảo mật cũng như nhận thức và việc đào tạo bảo mật cho người dùng
        - Thực hiện các sửa đổi chính sách nhỏ khi cần thiết
        - Xác định sự cần thiết phải đánh giá lại và bắt đầu lại chu trình bảo mật.

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Các chính sách chung cho môi trường CSDL:**
  - Việc bảo mật thông tin hoạt động đảm bảo an ninh hoạt động của một tổ chức thông qua sự phát triển và mức độ tin cậy của các chính sách và thủ tục của môi trường
  - Tập trung vào 4 thành phần:
    + Các chính sách bảo mật
    + Quản lý thay đổi, nâng cấp
    + Kế hoạch ứng phó với thảm họa

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Chính sách bảo mật:**
  - Xác định mục tiêu chung của bảo mật, xác định phạm vi những gì cần bảo mật, xác định vai trò và trách nhiệm của các cá nhân trong tổ chức, xác định các thủ tục truyền thông cụ thể và thảo luận về việc thực thi các chính sách.
  - Các chính sách bảo mật rất quan trọng đối với sự thành công của một kiến trúc bảo mật. Nếu không có các chính sách bảo mật, các nhân viên buộc phải tạo ra các quy tắc riêng cho các quyết định liên quan đến bảo mật, dẫn đến hậu quả khôn lường trong một môi trường CSDL. Một chính sách bảo mật hiệu quả có thể giúp một công ty phục hồi nhanh chóng sau khi bị tấn công bởi các mối đe dọa và giảm thiểu chi phí tổn thất.
  - Tất cả các bên liên quan cần tham gia vào việc tạo các chính sách bảo mật.

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Chính sách bảo mật (tiếp):**
  - ***Chính sách bảo mật cần bao gồm các thông tin*:**
    + *Các mục tiêu chung của chính sách* (phản ánh mối quan hệ trực tiếp với các mục tiêu kinh doanh chung)
    + *Quy mô của chính sách*. Cần xác định dữ liệu, con người, phòng ban, cơ sở và công nghệ, tài sản được bao gồm và bảo vệ bởi chính sách
    + V*ai trò và trách nhiệm của tất cả nhân viên*. Bao gồm việc xác định nhóm bảo mật, người ra quyết định, người thực thi chính sách và trách nhiệm của người dùng trong việc giữ an toàn bả mật mạng.
    + *Các quy trình*. Bao gồm các quy trình phòng ngừa, phát hiện và phản ứng với các mối đe dọa bảo mật (bảo mật, cập nhật, duy trì, quản lý và giám sát mạng) cho cả các cuộc tấn công ngẫu nhiên và có chủ ý.

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Chính sách bảo mật (tiếp):**
  - ***Chính sách bảo mật cần bao gồm các thông tin (tiếp)*:**
    + *Xử lý sự không tuân thủ*. Bao gồm các hậu quả của việc không tuân thủ chính sách bảo mật: những biện pháp kỷ luật được thực hiện. Các biện pháp kỷ luật nên dựa trên mức độ nghiêm trọng của vi phạm (không nên dựa trên vai trò của nhân viên), và cần phải đủ linh hoạt để được áp dụng nhất quán cho mọi người trong tổ chức.
  - ***Chú ý*:**
    + Khi hoàn tất việc xác định các chính sách bảo mật, cần tạo kế hoạch truyền thông chính sách (đào tạo thường xuyên hoặc chuyển giao cho từng nhân viên).
    + Do các mục tiêu kinh doanh có thể thay đổi, kế hoạch bảo mật cần cũng được đánh giá và sửa đổi thường xuyên.

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Quản lý cập nhật và nâng cấp:**
  - Việc xác định các thủ tục để cập nhật môi trường CSDL, phần mềm và phần sụn cũng rất quan trọng đối với kiến trúc bảo mật hệ thống
  - Chính sách quản lý cập nhật bao gồm các quy trình cập nhật bản vá lỗi, nâng cấp phần mềm, nâng cấp hệ điều hành và thay đổi phần sụn.
  - ***Để đảm bảo an toàn cho môi trường CSDL***, mọi hành động cập nhật, thay đổi hệ thống cần được lên kế hoạch và cân nhắc kỹ lưỡng. Trước khi cập nhật, cần trả lời một số câu hỏi:
  - ***Câu hỏi thứ nhất: Việc cập nhật có thực sự cần thiết không?***

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Quản lý cập nhật và nâng cấp (tiếp):**
  - Cập nhật (Update): Thay đổi đối với hệ thống được thêm vào phần mềm hoặc chương trình cơ sở đã được cài đặt trên mạng (có thể bao gồm ứng dụng CSDL, máy chủ CSDL, ứng dụng khách và máy khách). Các bản cập nhật thường là những thay đổi nhỏ được thực hiện đối với phần mềm hoặc phần sụn để cải thiện một chút chức năng của hệ thống hoặc để giúp đảm bảo rằng phần mềm hoặc phần sụn hiện tại duy trì khả năng tương thích trong môi trường CSDL. Những thay đổi nhỏ này thường dễ áp dụng hoặc hủy bỏ, và được phân phối miễn phí từ nhà cung cấp. Ví dụ cập nhật: Từ bản 1.0 sang 1.1.

  → Các bản cập nhật là cần thiết nếu chúng cung cấp các bản sửa lỗi (nếu có) cho phiên bản phần mềm hoặc phần sụn hiện có trong CSDL hoặc nếu cần thiết để duy trì khả năng tương thích trong toàn bộ môi trường.

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Quản lý cập nhật và nâng cấp (tiếp):**
  - Bản nâng cấp: Các thay đổi lớn hơn, xâm nhập sâu hơn, thường là sự thay thế cho các phiên bản phần mềm hoặc phần sụn cũ hơn. Chúng khó áp dụng hơn và thậm chí khó hủy bỏ hơn và thường phải trả phí. Ví dụ về nâng cấp: Từ phiên bản 1.0 lên phiên bản 2.0.

→Nâng cấp là cần thiết khi các phiên bản cũ không còn được nhà cung cấp hỗ trợ nữa, hoặc nếu chúng cung cấp các cải tiến đáng kể cho hệ thống hoặc nếu phiên bản cũ không còn phù hợp với nhu cầu của tổ chức.

→Trừ khi thực sự cần thiết, không nên áp dụng nâng cấp cho CSDL hoặc môi trường của nó ngay sau khi phát hành, vì các bản nâng cấp thường không ổn định và cần sửa chữa trong một thời gian dài sau khi phát hành.

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Quản lý cập nhật và nâng cấp (tiếp):**
  - ***Câu hỏi thứ 2*** *(nhằm xác định nên cập nhật hay nâng cấp):* ***Những hậu quả có thể có của việc cài đặt là gì?***

→ Các vấn đề tương thích hoặc hậu quả tiêu cực có thể xảy ra do sự thay đổi đối với môi trường có thể rất quan trọng để duy trì tính toàn vẹn và tính sẵn sàng của tài nguyên. Các nhà cung cấp phần mềm thường không sẵn sàng chia sẻ về các vấn đề này, vì vậy có thể tham khảo một vài gợi ý sau:

+ Kiểm tra các trang trợ giúp, xử lý sự cố của nhà cung cấp
+ Tìm kiếm các diễn đàn hỗ trợ kỹ thuật, các nhóm tin tức và các blog
+ Hỏi đồng nghiệp những người có thể đã cài đặt sản phẩm gần đây
+ Kiểm tra hướng dẫn sử dụng CSDL về các thông số của phần mềm và phần sụn nhằm đảm bảo tính tương thích.

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Quản lý cập nhật và nâng cấp (tiếp):**

→Cần không ngừng tìm kiếm thông tin để đảm việc cập nhật/nâng cấp không gây nguy hiểm cho môi CSDL và các tài nguyên. Nếu có thể, nên tạo một môi trường CSDL thử nghiệm để cài đặt bản nâng cấp.

→Trước khi thực hiện bất kỳ thay đổi nào cần lên kế hoạch sao lưu, phục hồi, hủy bỏ các thay đổi (nên kiểm tra để chắc chắn rằng bản cập nhật cho phép hủy bỏ các thay đổi đã thực hiện)

→Sau khi cập nhật, nên ghi lại những thay đổi đã được thực hiện, xác định các vấn đề và khôi phục hệ thống nếu cần

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Quản lý cập nhật và nâng cấp (tiếp):**
  - ***Các loại cập nhật và nâng cấp*:**
    + *Bản vá lỗi (patch)*: Là một chương trình nhỏ được sử dụng để sửa chữa hoặc cập nhật các chương trình phần mềm hoặc thiết bị phần sụn, thường được tạo ra để giải quyết các lỗ hổng mới được phát hiện trong chương trình.
    + *Bản nâng cấp phần mềm (software upgrade):* Kết hợp một số bản vá lỗi để tạo ra phiên bản mới của phần mềm. Các bản nâng cấp xâm nhập sâu hơn các bản cập nhật do chúng liên quan đến các thay đổi của hệ thống; vì vậy cần có kế hoạch cẩn thận để tránh các vấn đề về tính sẵn sang và độ tin cậy.

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Quản lý cập nhật và nâng cấp (tiếp):**
  - ***Các loại cập nhật và nâng cấp (tiếp)*:**
    + *Bản nâng cấp hệ điều hành (OS upgrade)*: Được thực hiện bằng cách cài đặt phiên bản mới vào máy chủ (host hoặc server), là những nâng cấp quan trọng và rủi ro. Nâng cấp máy chủ CSDL đồng thời ảnh hưởng đến mọi máy khách trong môi trường và nếu máy khách là ứng dụng Web hoặc biểu mẫu Web trực tuyến, chúng có thể ảnh hưởng đến khả năng của người dùng trong việc truy cập CSDL

    → Cần lập kế hoạch, nghiên cứu và thực hiện các thử nghiệm thích hợp trước khi nâng cấp hệ điều hành

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Quản lý cập nhật và nâng cấp (tiếp):**
  - ***Kế hoạch quản lý các bản sao lưu:***
    - + *Bản sao lưu (backup):* Là một bản sao có chủ ý của dữ liệu, tệp chương trình và cấu hình hệ thống được sử dụng với mục đích lưu trữ thông tin nhằm thay thế hoặc khôi phục các tệp và hệ thống sau khi bị lỗi mạng hoặc bị tấn công bởi các phần mềm độc hại.
    - + *Kế hoạch quản lý sao lưu* nhằm đảm bảo an toàn cho dữ liệu trên mạng

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Quản lý cập nhật và nâng cấp (tiếp):**
  - ***Giải pháp sao lưu*:** Để lựa chọn giải pháp phù hợp nhất cần trả lời một số câu hỏi:
    + Nên sử dụng loại phương tiện nào để lưu trữ bản sao lưu?
    + Bản sao lưu dự phòng sẽ được đặt ở đâu? (nên lưu lại các bản sao lưu trên mạng - không cùng vị trí dữ liệu gốc để tránh trường hợp cả bản gốc và bản sao bị hủy cùng một lúc)
    + Cần sao lưu những gì? (ưu tiên các dữ liệu quan trọng)
    + Mức độ thường xuyên của việc sao lưu? (dữ liệu càng có giá trị và quan trọng, thì càng cần sao lưu thường xuyên hơn)
    + Nên sao lưu vào thời điểm nào? (không nên sao lưu trong khi thông tin đang được lưu và cập nhật)
    + Nên sử dụng hình thức sao lưu nào (full backup, incremental backup, differential backup)?

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Kế hoạch ứng phó với thảm họa:**
  - Kế hoạch được lập để ứng phó với các thảm họa trong tự nhiên hoặc do con người gây ra (Ví dụ: động đất, hỏa hoạn, lũ lụt, tuyết, băng, bão, lốc xoáy, vụ nổ, cháy hóa chất, … và lỗi của con người)
  - Mục tiêu: Đảm bảo phục hồi nhanh chóng các khía cạnh quan trọng nhất của doanh nghiệp

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Kế hoạch ứng phó với thảm họa:**
  - ***Nội dung lập kế hoạch*:**
    - + Cần xác định thông tin liên lạc của nhân viên ứng phó khẩn cấp, vai trò và trách nhiệm của họ trong việc thực hiện khắc phục thảm họa.
    - + Bao gồm các bản sao lưu (với các thông tin về dữ liệu và máy chủ được sao lưu, tần suất sao lưu, nơi lưu trữ bản sao lưu và thông tin về cách phục hồi) để đảm bảo có thể khôi phục chính xác dữ liệu tại thời điểm gần nhất, nhanh nhất.
    - + Xác định các chiến lược truyền thông để liên lạc với nhân viên và khách hàng trước, trong và sau thảm họa.
    - + Thông tin liên quan đến bất kỳ hợp đồng hiện có nào với các tổ chức chuyên về dịch vụ khắc phục thảm họa và trợ giúp bên ngoài cũng nên được đưa vào.

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Kế hoạch ứng phó với thảm họa:**
  - ***Nội dung lập kế hoạch (tiếp)*:**
    + Các tổ chức khắc phục thảm họa của bên thứ ba cung cấp các giải pháp khắc phục thảm họa:
      - "Cold sites" là một cơ sở cung cấp các nhu cầu cơ bản để xây dựng lại mạng
      - "Warm sites" là một thỏa thuận hứa hẹn sự tồn tại của một cơ sở chứa các mối quan tâm cơ bản về môi trường, cũng như máy tính, phần sụn kết nối và các thiết bị phần mềm cần thiết để xây dựng lại hệ thống mạng
      - "Hot sites" là một bản sao chính xác trang web của tổ chức, nói cách khác, là một trang web phản chiếu. Nhà cung cấp sẽ chịu mọi trách nhiệm trong việc đảm bảo rằng hệ thống luôn sẵn sàng trong trường hợp xảy ra thảm họa, chi phí thường rất cao.

1.4. Các biện pháp bảo đảm an toàn CSDL

- **Kế hoạch ứng phó với thảm họa:**
  - ***Nội dung lập kế hoạch (tiếp)*:**
    + Cân nhắc về các thỏa thuận trang web chia sẻ (Shared site agreements): Thỏa thuận giữa các tổ chức với các trung tâm dữ liệu tương tự - có sự tương thích về phần cứng và phần mềm - cho phép các công ty đồng ý với một trang web được chia sẻ để sao lưu dữ liệu của nhau. Nếu thảm họa xảy ra và có thỏa thuận chia sẻ trang web, tổ chức bị ảnh hưởng sẽ chuyển đến tổ chức không bị ảnh hưởng để xây dựng và tiếp tục kinh doanh tại đó.