Giới thiệu các khái niệm an toàn thông tin

WWW.UIT.EDU.VN

TS. Nguyễn Tấn Cầm

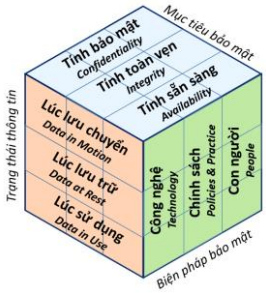
Nội dung

WWW.UIT.EDU.VN

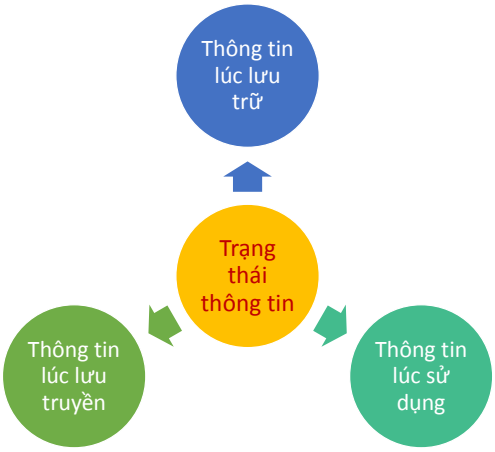
- Khái niệm an toàn thông tin
- Trạng thái thông tin
- Mục tiêu an toàn thông tin
- Phương pháp đảm bảo an toàn thông tin
- Kiến trúc bảo mật
- Câu hỏi ôn tập

Khái niệm an toàn thông tin

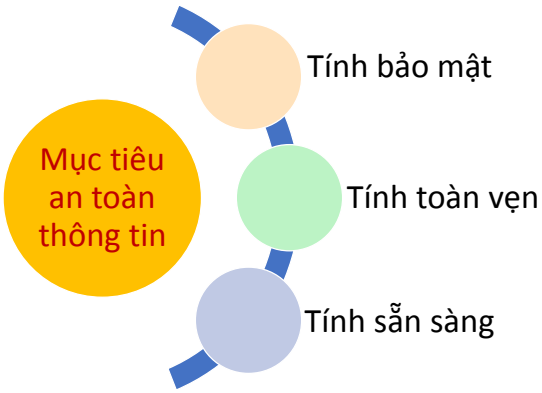
- Đảm bảo an ninh thông tin là sự bảo vệ các hệ thống thông tin tự động để đảm bảo tính toàn vẹn, tính sẵn sàng và tính bí mật của các tài nguyên hệ thống thông tin như phần cứng, phần mềm, hệ điều hành, dữ liệu và các kênh giao tiếp [1].



Trạng thái thông tin



Mục tiêu an toàn thông tin



Phương pháp đảm bảo an toàn thông tin

Phương pháp đảm bảo an toàn thông tin

- Nhóm công nghệ
  - Chúng ta có thể sử dụng các giải pháp phần mềm hoặc phần cứng để đảm bảo các mục tiêu bảo mật (theo bộ ba CIA) của dữ liệu ở cả các trạng thái khác nhau.
  - Phần mềm duyệt virus, tường lửa, hệ thống phát hiện và phòng chống xâm nhập, giải pháp sao lưu dự phòng,… là các ví dụ cho hướng tiếp cận công nghệ trong việc đảm bảo an toàn thông tin.

Phương pháp đảm bảo an toàn thông tin

- Nhóm chính sách
  - Việc trang bị các giải pháp công nghệ là cần thiết.
  - Tuy nhiên, để vận hành chúng một cách hiệu quả thì việc ban hành các chính sách và hướng dẫn sử dụng cũng cần thiết không kém.
  - Trong nỗ lực bảo vệ tính an toàn cho dữ liệu, các tổ chức cần ban hành các chính sách, nội quy một cách chi tiết và hiệu quả.
  - Thông thường, tính dễ sử dụng hay tỉ lệ nghịch với độ an toàn của hệ thống.
  - Do đó, các hệ thống có tính an toàn cao cần phải được viết các tài liệu hướng dẫn sử dụng chi tiết.
  - Điều này giúp người dùng không những thao tác nhanh mà còn hạn chế lỗi trong quá trình sử dụng hệ thống.

Phương pháp đảm bảo an toàn thông tin

- Nhóm con người
  - Con người đóng vai trò quan trọng trong bất kỳ hệ thống công nghệ thông tin nào.
  - Con người là móc xích liên quan trực tiếp đến việc bảo đảm tính an toàn cho dữ liệu.
  - Nâng cao kiến thức về an toàn thông tin, nâng cao nhận thức về việc sử dụng hệ thống an toàn là việc làm cần thiết trong việc đảm bảo an toàn thông tin.
  - Giải pháp kỹ thuật có hiện đại đến đâu, chính sách và tài liệu hướng dẫn có chi tiết đến đâu thì hệ thống bảo mật của tổ chức vẫn có thể bị vượt qua bởi yếu tố con người.
  - Các tổ chức thường triển khai các lớp đào tạo nâng cao nghiệp vụ và nhận thức cho nhân viên, tuyển dụng nhân viên có kiến thức, kỹ năng và nhận thức tốt cũng là một trong những giải pháp để gia tăng tính bảo mật cho hệ thống theo hướng tiếp cận thứ ba này.

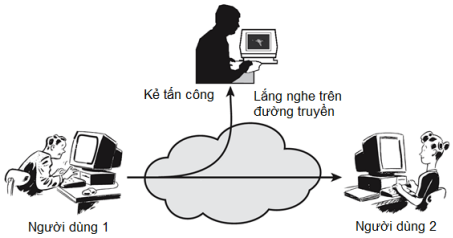
Kiến trúc bảo mật

- Cuộc tấn công
  - là bất kỳ hành động nào làm tổn hại đến tính bảo mật của thông tin thuộc sở hữu của một tổ chức.
  - Có hai loại cuộc tấn công: tấn công chủ động (active attack) và tấn công thụ động (passive attack).
  - Công thức sau trình bày điều kiện để xuất hiện một cuộc tấn công.
  - Để hạn chế các cuộc tấn công lên hệ thống công nghệ thông tin, chúng ta cần giảm các lỗ hổng bảo mật, hạn chế khả năng khai thác các lỗ hổng bảo mật, đồng thời giảm động cơ thực hiện tấn công của kẻ tấn công.

$$\text{Cuộc tấn công} = \text{Lỗ hổng bảo mật} + \text{phương pháp khai thác} + \text{động cơ}$$

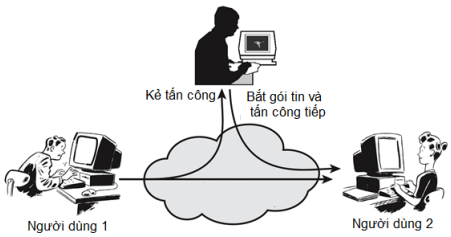
Kiến trúc bảo mật

- Cuộc tấn công
  - Tấn công thụ động
    - Là dạng tấn công mà kẻ tấn công không cần tương tác với máy tính hoặc hệ thống của nạn nhân.
    - Kẻ tấn công chỉ lắng nghe thông tin trao đổi trên đường truyền.
    - Trong dạng tấn công này, kẻ tấn công không chỉnh sửa hoặc làm thay đổi tài nguyên hệ thống



Kiến trúc bảo mật

- Cuộc tấn công
  - Tấn công chủ động
    - Là dạng tấn công mà kẻ tấn công không những thu thập mà còn chỉnh sửa thông tin trên đường truyền.
    - Trong dạng tấn công này, kẻ tấn công tương tác với máy tính hoặc hệ thống của nạn nhân.
    - Sau cuộc tấn công chủ động, dấu vết của kẻ tấn công thường nhiều hơn so với tấn công thụ động



Kiến trúc bảo mật

- Cơ chế bảo mật
  - Là một quy trình (hoặc một thiết bị kết hợp một quy trình) được thiết kế để phát hiện, ngăn chặn hoặc phục hồi sau một cuộc tấn công bảo mật.
- Dịch vụ bảo mật
  - Là một dịch vụ xử lý hoặc truyền thông nhằm nâng cao tính bảo mật của hệ thống xử lý dữ liệu và việc truyền thông tin của một tổ chức.
  - Các dịch vụ nhằm chống lại các cuộc tấn công bảo mật và chúng sử dụng một hoặc nhiều cơ chế bảo mật khác nhau để cung cấp dịch vụ.

Câu hỏi ôn tập

Câu hỏi ôn tập

- **Câu 1:** Trình bày sự khác biệt giữa tấn công chủ động và tấn công thụ động.
- **Câu 2:** Trình bày công thức để dẫn đến một cuộc tấn công.
- **Câu 3:** Cho một ví dụ của việc mất an toàn dữ liệu trong quá trình truyền.
- **Câu 4:** Cho một ví dụ của việc mất an toàn dữ liệu trong quá trình lưu trữ.
- **Câu 5:** Trình bày ba phương pháp chính để đảm bảo an toàn thông tin.
- **Câu 6:** Trình bày ba trạng thái chính của thông tin.
- **Câu 7:** Trình bày ba mục tiêu chính của bảo mật thông tin.

Câu hỏi trắc nghiệm

Câu hỏi trắc nghiệm

- Câu 1.1:
  - Có bao nhiêu trạng thái thông tin?
    - A. 2
    - B. 3
    - C. 4
    - D. 5

Câu hỏi trắc nghiệm

- Câu 1.2:
  - Việc trang bị kính chống nhìn trộm giúp đảm bảo an ninh thông tin ở trạng thái nào?
    - A. Data at Rest
    - B. Data in Motion
    - C. Data in Use
    - D. Data in Line

Câu hỏi trắc nghiệm

- Câu 1.3:
  - Phát biểu nào sau đây đúng:
    - Phát biểu A: Việc mã hóa mật khẩu khi lưu trữ là nhằm đảm bảo tính bảo mật (Confidentiality).
    - Phát biểu B: Việc cấu hình RAID 10 là nhằm đảm bảo tính sẵn sàng (Availability).
    - A. Phát biểu A và B đúng
    - B. Phát biểu A và B sai
    - C. Phát biểu A đúng, Phát biểu B sai
    - D. Phát biểu A sai, Phát biểu B đúng

Câu hỏi trắc nghiệm

- Câu 1.4:
  - Phát biểu nào sau đây đúng:
    - Phát biểu A: Ba nhóm phương pháp đảm bảo an toàn thông tin bao gồm: công nghệ, chính sách và con người.
    - Phát biểu B: Ba nhóm phương pháp đảm bảo an toàn thông tin bao gồm: công nghệ, chính sách và thiết bị.
    - A. Phát biểu A và B đúng
    - B. Phát biểu A và B sai
    - C. Phát biểu A đúng, Phát biểu B sai
    - D. Phát biểu A sai, Phát biểu B đúng

Câu hỏi trắc nghiệm

- Câu 1.5:
  - Phát biểu nào sau đây đúng:
    - Phát biểu A: Công thức biểu diễn điều kiện xảy ra đợt tấn công là: Cuộc tấn công = Lỗ hổng bảo mật + phương pháp khai thác + công cụ khai thác.
    - Phát biểu B: Công thức biểu diễn điều kiện xảy ra đợt tấn công là: Cuộc tấn công = Lỗ hổng bảo mật + phương pháp khai thác + động cơ.
    - A. Phát biểu A và B đúng
    - B. Phát biểu A và B sai
    - C. Phát biểu A đúng, Phát biểu B sai
    - D. Phát biểu A sai, Phát biểu B đúng

Cảm ơn!