**A. LÝ THUYẾT:**

**1) Hãy nêu các chiến lược của an toàn và bảo mật hệ thống thông tin?**

* **Giới hạn quyền hạn tối thiểu (Last Privilege**)**:** theo nguyên tắc này bất kỳ một đối tượng nào cũng chỉ có những quyền hạn nhất định đối với tài nguyên mạng
* **Bảo vệ theo chiều sâu (Defence In Depth):** Không nên dựa vào một chế độ an toàn dù cho chúng rất mạnh, mà nên tạo nhiều cơ chế an toàn để tương hỗ cho nhau
* **Nút thắt (Choke Point):** Tạo ra một “cửa khẩu” hẹp, và chỉ cho phép thông tin đi vào hệ thống của mình bằng con đường duy nhất chính là “cửa khẩu” này.
* **Điểm nối yếu nhất (Weakest Link):** Chiến lược này dựa trên nguyên tắc: “Một dây xích chỉ chắc tại mắt duy nhất, một bức tường chỉ cứng tại điểm yếu nhất”
* **Tính toàn cục:** Các hệ thống an toàn đòi hỏi phải có tính toàn cục của các hệ thống cục bộ.
* **Tính đa dạng bảo vệ:** Cần phải sử dụng nhiều biện pháp bảo vệ khác nhau cho hệ thống khác nhau. Nếu không, chỉ cần có kẻ tấn công vào được một hệ thống thì chúng cũng dễ dàng tấn công vào các hệ thống khác.

**2) Trình bày ngắn gọn các xu hướng tấn công hiện nay?**

* **Tấn công bằng phần mềm độc hại (Malware):** Bao gồm Spyware (phần mềm gián điệp), Ransomware (mã độc tống tiền), Virus, Worm (phần mềm độc hại lây lan với tốc độ nhanh).
* **Tấn công giả mạo (Phishing):** Hacker giả mạo là ngân hàng, ví điện tử, trang giao dịch trực tuyến hoặc các công ty thẻ tín dụng để lừa người dùng chia sẻ các thông tin cá nhân.
* **Tấn công vào hệ thống thông tin của các cơ quan quan trọng:** truyền thông, hàng không, năng lượng, các cơ sở y tế nhằm phá hoại, đánh cắp dữ liệu.
* **Tấn công từ chối dịch vụ (DoS và DdoS):** là “đánh sập tạm thời” một hệ thống, máy chủ hoặc mạng nội bộ

**3) Mục tiêu của an toàn và bảo mật hệ thống thông tin trong doanh nghiệp là gì? Vì sao luôn cần xác định mục tiêu trước khi ứng dụng các biện pháp đảm bảo an toàn cho HTTT doanh nghiệp?**

- Mục tiêu của an toàn và bảo mật hệ thống thông tin trong doanh nghiệp gồm:

* **Tính bí mật:** Đảm bảo rằng thông tin không bị truy cập bất hợp pháp.
* **Tính toàn vẹn:** Đảm bảo rằng thông tin không bị sửa đổi bất hợp pháp
* **Tính sẵn dùng:** Tài sản luôn sẵn sàng được sử dụng bởi những người có thẩm quyền.
* **Tính xác thực:** Đảm bảo rằng dữ liệu nhận được chắc chắn dữ liệu gốc ban đầu.
* **Tính không thể chối bỏ:** Đảm bảo rằng người gửi hay người nhận dữ liệu không thể chối bỏ trách nhiệm sau khi đã gửi và nhận thông tin.

- Việc xác định mục tiêu trước khi ứng dụng các biện pháp đảm bảo an toàn cho hệ thống thông tin doanh nghiệp là rất quan trọng vì:

* Mục tiêu giúp chúng ta có một phương hướng rõ ràng và tập trung nỗ lực của mình vào những điều quan trọng, cần thiết nhất.
* Mục tiêu cung cấp một kết quả mong muốn mà một người hay một tổ chức cố gắng đạt được thông qua hoạt động và nỗ lực của mình.
* Việc đạt được mục tiêu mang lại cho chúng ta cảm giác hài lòng và tự tin hơn trong cuộc sống.
* Mục tiêu giúp chúng ta quản lý thời gian một cách hiệu quả nhất.
* Mục tiêu giúp chúng ta xác định được những trở ngại, khó khăn mà chúng ta có thể gặp phải trong quá trình thực hiện mục tiêu, từ đó tìm ra giải pháp để vượt qua.

**4) Bảo mật kênh truyền là gì? Vì sao cần bảo mật kênh truyền tin? Có những cơ chế bảo mật kênh truyền nào?**

- [**Bảo mật kênh truyền** là việc bảo mật các dữ liệu khi chúng được truyền trên kênh truyền thông](https://123docz.net/trich-doan/3667959-bao-mat-kenh-truye-n.htm).

- [Việc bảo mật kênh truyền tin là cần thiết vì](https://viblo.asia/p/tai-sao-phai-thuc-hien-cac-giai-phap-bao-mat-thong-tin-PdbknLnDGyA):

* Bảo vệ thông tin dữ liệu cá nhân, tổ chức nhằm tránh khỏi sự “đánh cắp, ăn cắp” bởi những kẻ xấu hoặc tin tặc.
* Bảo mật tốt những dữ liệu & thông tin sẽ tránh những nguy cơ không đáng có cho chính cá nhân & doanh nghiệp của bạn.
* Thông tin mật nếu bị rò rỉ ra ngoài sẽ gây ra tổn thất nghiêm trọng về niềm tin và sức cạnh trạnh giữa các tổ chức, công ty.

- [Có một số cơ chế bảo mật kênh truyền như](https://ictvietnam.vn/co-che-bao-mat-va-nhung-thach-thuc-an-ninh-trong-iot-27641.html):

* **Mã hóa**: Giữ bí mật thông tin và chỉ có người có khóa bí mật mới giải mã được.
* **Tạo chữ ký số**: Cho phép kiểm tra một văn bản có phải đã được tạo với một khóa bí mật nào đó hay không.
* **Thỏa thuận khóa**: Cho phép thiết lập khóa dùng để trao đổi thông tin mật giữa 2 bên.
* **IPSec, PKI, cơ chế trao đổi khóa Diffie-Hellman**: Các phương pháp bảo mật truyền thống đòi hỏi khối lượng tính toán lớn.
* **Mã hóa AES**: Một giải pháp tốt để bảo vệ việc truyền dữ liệu từ ở khoảng cách xa.

**5) An toàn và bảo mật thông tin là gì? Vì sao an toàn và bảo mật thông tin lại đóng vai trò rất quan trọng trong doanh nghiệp hiện nay?**

**- An toàn và bảo mật thông tin** là việc bảo vệ thông tin khỏi sự truy cập, sử dụng, tiết lộ, sửa đổi, hoặc phá hủy trái phép. Nó bao gồm việc bảo vệ thông tin cá nhân và thông tin doanh nghiệp

- An toàn và bảo mật thông tin đóng vai trò rất quan trọng trong doanh nghiệp hiện nay vì:

* Thông tin mật nếu bị rò rỉ ra ngoài sẽ gây ra tổn thất nghiêm trọng về niềm tin và sức cạnh tranh giữa các tổ chức, công ty.
* Một môi trường thông tin an toàn, sạch sẽ có tác động không nhỏ đến giảm thiểu chi phí quản lý và hoạt động của doanh nghiệp, nâng cao uy tín của doanh nghiệp, tạo điều kiện thuận lợi cho sự hội nhập một môi trường thông tin lành mạnh.
* Bảo vệ thông tin dữ liệu cá nhân, tổ chức nhằm tránh khỏi sự “đánh cắp, ăn cắp” bởi những kẻ xấu hoặc tin tặc.
* Ngăn chặn tin tặc đánh cắp danh tính, cài các phần mềm độc hại vào hệ thống doanh nghiệp.
* Đảm bảo những trao đổi thông tin dữ liệu, giao dịch, kinh doanh online ở trạng thái an toàn nhất

**6) Tấn công từ chối dịch vụ là gì? Trình bày đặc trưng của các kiểu tấn công từ chối dịch vụ phổ biến hiện nay? Vì sao tấn công từ chối dịch vụ rất khó phòng tránh?**

[Tấn công từ chối dịch vụ (DoS) là một nỗ lực độc hại nhằm làm cho những người dùng không thể sử dụng tài nguyên của một máy tính](https://vi.wikipedia.org/wiki/T%E1%BA%A5n_c%C3%B4ng_t%E1%BB%AB_ch%E1%BB%91i_d%E1%BB%8Bch_v%E1%BB%A5). [Mục tiêu của tấn công từ chối dịch vụ có thể khác nhau, nhưng nói chung nó gồm có sự phối hợp, sự cố gắng ác ý của một người hay nhiều người để một trang, hay hệ thống mạng không thể sử dụng, làm gián đoạn, hoặc làm cho hệ thống đó chậm đi một cách đáng kể với người dùng bình thường, bằng cách làm quá tải tài nguyên của hệ thống1](https://vi.wikipedia.org/wiki/T%E1%BA%A5n_c%C3%B4ng_t%E1%BB%AB_ch%E1%BB%91i_d%E1%BB%8Bch_v%E1%BB%A5).

[Có một số kiểu tấn công từ chối dịch vụ phổ biến hiện nay](https://vi.wikipedia.org/wiki/T%E1%BA%A5n_c%C3%B4ng_t%E1%BB%AB_ch%E1%BB%91i_d%E1%BB%8Bch_v%E1%BB%A5)

* [**SYN Flood:** Gửi hàng loạt kết nối TCP tới máy chủ nhưng không hoàn thành chúng](https://vi.wikipedia.org/wiki/T%E1%BA%A5n_c%C3%B4ng_t%E1%BB%AB_ch%E1%BB%91i_d%E1%BB%8Bch_v%E1%BB%A5)
* [**UDP Flood:** Gửi một lượng lớn các gói tin UDP tới cổng ngẫu nhiên trong một kết nối từ xa](https://vi.wikipedia.org/wiki/T%E1%BA%A5n_c%C3%B4ng_t%E1%BB%AB_ch%E1%BB%91i_d%E1%BB%8Bch_v%E1%BB%A5).
* [**HTTP Flood:** Sử dụng các yêu cầu URL tiêu chuẩn thay vì các tập lệnh bị hỏng hoặc khối lượng lớn](https://vi.wikipedia.org/wiki/T%E1%BA%A5n_c%C3%B4ng_t%E1%BB%AB_ch%E1%BB%91i_d%E1%BB%8Bch_v%E1%BB%A5)
* [**Ping of Death:** Gửi nhiều đoạn mã độc đến một hệ thống để giành quyền điều khiển các giao thức IP](https://vi.wikipedia.org/wiki/T%E1%BA%A5n_c%C3%B4ng_t%E1%BB%AB_ch%E1%BB%91i_d%E1%BB%8Bch_v%E1%BB%A5)
* [**Smurf Attack:** Sử dụng một phần mềm độc hại có tên là smurf để khai thác các giao thức Internet (IP) và ICMP (Internet Control Message Protocol) bằng cách giả mạo 1 địa chỉ IP và sử dụng ICMP](https://bizflycloud.vn/tin-tuc/cac-kieu-tan-cong-tu-choi-dich-vu-pho-bien-tu-truoc-den-nay-20210510120321232.htm).

[Tấn công từ chối dịch vụ rất khó phòng tránh vì](https://niics.gov.vn/meo-hay-cong-nghe/tan-cong-tu-choi-dich-vu-dos-va-ddos-cach-phong-chong):

* [Mỗi bot là một thiết bị Internet hợp pháp, việc tách lưu lượng tấn công khỏi lưu lượng truy cập thông thường sẽ rất khó khăn](https://b1.edu.vn/tan-cong-tu-choi-dich-vu-dos-va-ddos-tac-hai-va-phong-chong/).
* [Rất khó có thể tìm ra máy tính của hacker từ những request gửi tới máy chủ dịch vụ](https://niics.gov.vn/meo-hay-cong-nghe/tan-cong-tu-choi-dich-vu-dos-va-ddos-cach-phong-chong).
* [Khó phân biệt và loại bỏ được các truy cập gây tổn hại tới hoạt động của máy chủ dịch vụ](https://niics.gov.vn/meo-hay-cong-nghe/tan-cong-tu-choi-dich-vu-dos-va-ddos-cach-phong-chong).
* [Tấn công DDoS nhiều khi được sử dụng để che dấu cuộc tấn công mạng phía sau](https://antoanthongtin.vn/gp-atm/tan-cong-tu-choi-dich-vu-tai-viet-nam-va-giai-phap-phong-chong-109197).

**7) Thế nào là truyền tin an toàn? Trình bày mô hình truyền tin an toàn?**

**8) Trình bày các ứng dụng của mã hóa khóa công khai hiện nay? Cho ví dụ? Hãy phân tích những lợi điểm của mã hóa khóa công khai trong bảo mật dữ liệu?**

**9) Chữ ký số là gì? Trình bày các ứng dụng của chữ ký số? Nêu các đặc điểm của chữ ký số? Cho ví dụ minh họa.**

**10) Tường lửa là phần mềm gì? Tại sao cần cài đặt phần mềm tường lửa cho máy tính cá nhân của bạn?**

**11) Trình bày sơ đồ mã hóa khóa đối xứng? Nêu các ứng dụng của mã hóa khóa đối xứng hiện nay? Cho ví dụ minh họa.**

**12) Mã hóa dữ liệu là gì? Khi nào cần mã hóa dữ liệu? Trình bày các ứng dụng của mã hóa dữ liệu?**

**13) Trình bày các nguy cơ mất an toàn trong HTTT thương mại điện tử? Vì sao các HTTT thương mại điện tử lại dễ bị tấn công hơn các HTTT khác?**

**14) Các yêu cầu an toàn bảo mật đối với một HTTT trong doanh nghiệp là gì? Cho ví dụ minh họa.**

**15) Phân quyền người dùng là gì? Vì sao trong HTTT doanh nghiệp cần phân quyền người dùng?**