**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?**

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

**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?**

**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?**

**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?**